ámbito

1º TRIMESTRE DE 2006 • Nº 20

LA REVISTA DE LOS USUARIOS DE LAS TELECOMUNICACIONES Y LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

Seguridad y Negocio

Experiencias y Claves para Directivos

autelsi
ASOCIACIÓN ESPAÑOLA DE USUARIOS DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Lo primero es llegar tan lejos
como podamos imaginar.
Que cualquier
rincón del mundo esté a la
vuelta de la esquina.
Facilitar la comunicación.
Mejorar nuestra forma de vivir.
Estar al lado de las personas.
Verlas. Sentirlas.
Lo primero para Telefónica
es lo mismo que para ti.
Por eso estamos presentes
en 40 países, especialmente
en los de América Latina,
desarrollando la comunicación.

Alicia · Chema · Walter · Felipe · Clara · Nadia · Miriam · Inés · Rafael

Lo primero es acortar distancias

www.telefonica.es

Telefónica

Lo primero eres tú

sumario

Seguridad y

Juan José Martínez Pagán, Vicepresidente del Sur de EMEA (ENTERASYS NET WORK), *presidente del GT de Seguridad de AUTELSI, durante la Apertura del Seminario celebrado el pasado marzo en el salón de actos del Museo Thyssen-Bornemisza.*

Desde hace algún tiempo vengo observando tanto en reuniones con directores de Sistemas de Información y profesionales de las TIC, como en los foros profesionales del sector —españoles y extranjeros— cómo todas las problemáticas relacionadas con la Seguridad de la Información —su integridad, su protección, el acceso controlado, la continuidad de los procesos de negocio, el cumplimiento con las normativas vigentes en materia de protección de datos, etc.— van tomando cada vez más protagonismo en las agendas de los directivos como temas prioritarios.

Creo que esto es una señal positiva de que está surgiendo una nueva cultura, que hace que no sean sólo los profesionales de la Seguridad de la Información y de las TIC los que tomen conciencia de las responsabilidades que implica esta materia, sino que esta toma de conciencia alcance también a los altos directivos: presidentes, consejeros delegados y directores generales.

Estas responsabilidades están recogidas en leyes y reglamentos, y no se limita la obligación de disponer de un departamento de Seguridad en el que delegar esta problemática, sino que exigen de los directivos una mayor comprensión, involucración y patrocinio activo de cara a toda la organización.

Tradicionalmente, y con independencia del reciente desarrollo normativo en esta área, en la Seguridad de la Información no se requería una especial atención por parte de los máximos ejecutivos ni de los directores TIC, al menos desde el punto de vista técnico. La arquitectura de los sistemas de información y comunicaciones tradicionales, basada en *mainframes* propietarios con terminales no inteligentes, y las comunicaciones punto a punto configuraban sistemas que, aun cuando pudieran llegar a tener miles de terminales conectados remotamente, no dejaban de ser sistemas aislados, puesto que no tenían conectividad con el exterior. El acceso a los terminales estaba circunscrito a un conjunto determinado de personas, y se limitaba a la capacidad de ejecutar las aplicaciones corporativas. Este modelo restringía el acceso a la información y a los propios recursos del sistema, de tal manera que los propios mecanismos de seguridad de acceso incluidos en los *mainframes* bastaban para dar un nivel de protección adecuado.

Como contraste a este modelo tradicional, hoy en día tenemos una multitud de servidores que soportan una gran variedad de aplicaciones y procesos de negocio,

Negocio

acceden a bases de datos que a menudo se encuentran en otros sistemas, no necesariamente en el mismo data center. Al mismo tiempo, el acceso a estos servidores se realiza a través de diversos tipos de dispositivos: PCs fijos, PCs portátiles y PDAs conectados a la red local, a redes inalámbricas o remotamente a través de Internet; los PCs pueden ejecutar no solamente las aplicaciones corporativas, sino una gran infinidad de aplicaciones disponibles de manera ubicua. Las redes que dan conectividad a todo esto, ya ni siquiera son "redes de datos" para conectar PCs y servidores, sino que son redes multiservicio que dan conectividad igualmente a otros dispositivos como teléfonos IP, cámaras de videovigilancia, tornos de acceso, etc., y que están conectadas de manera permanente a la red Internet global.

De todos los cambios ocurridos en los últimos años, quizás sea la red, con su ubicuidad, su estandarización, apertura y universalidad el elemento que más ha contribuido a posibilitar la amenaza. Pero también los son los PCs por los mismos motivos de estandarización y apertura. Las ganancias de productividad que todos estos avances han aportado son enormes, sin embargo, han creado también una vulnerabilidad que hay que conocer, valorar y gestionar de manera preventiva.

Es esta necesidad, junto con la alarma que provocan los casos divulgados en prensa y la existencia de una normativa más exigente y con responsabilidades más claramente definidas, la que está llamando la atención de los profesionales de la Seguridad, de las TIC y de los directivos en general hacia el mundo de la Seguridad Informática.

A este mundo es al que dedica su esfuerzo el Grupo de Trabajo de Seguridad de AUTELSI, creado hace dos años y en el que participan profesionales tanto de las empresas usuarias de las TIC, como de las empresas fabricantes de soluciones y de las Administraciones Públicas. Esto nos permite tener una visión más amplia de los temas en que trabajamos, y contribuir a promover el desarrollo de las buenas prácticas de seguridad en las empresas y organismos de nuestro país.

En este tiempo hemos realizado un catálogo de recomendaciones o buenas prácticas en materia de seguridad tanto para usuarios como para departamentos de TI, que se encuentra accesible en nuestra web.

En este momento estamos trabajando en dos comités, uno de ellos dedicado a la certificación electrónica y firma digital, y a su aplicación práctica a los procesos de negocio, y el otro dedicado a la gestión de la Seguridad.

Recientemente hemos organizado un seminario bajo el nombre de "Seguridad y Negocio: claves y experiencias para directivos". Se trata de un evento de carácter divulgativo, que ha reunido en una jornada a profesionales de la Seguridad junto con directivos de otras áreas, para compartir conocimientos y experiencias en esta materia.

Se han tratado temas de interés general como la protección de datos en las redes locales a través de políticas, la protección de los accesos remotos a través de redes públicas, Internet, la protección de las aplicaciones, la consolidación de dispositivos y plataformas de seguridad y la protección de los puestos de trabajo, tanto fijos como portátiles. En la sesión de preguntas se han discutido temas de carácter organizativo, como cuál es el papel del responsable de seguridad en una organización, su ubicación (a quién debe reportar), la comunicación entre el área de seguridad y la alta dirección y los problemas y oportunidades que plantea el outsourcing de la gestión de la seguridad.

Algunos de estos temas los desarrollamos también en este monográfico dedicado a la Seguridad Informática, que esperamos sea de tu interés.

Juan José Martínez Pagán [Vicepresidente del Sur de EMEA (ENTERASYS NET WORK), Presidente del GT de Seguridad de AUTELSI]

La seguridad es un valor inherente a los Sistemas de Información

Carlos Jiménez, Presidente de Secuware

Para hablar del futuro y la evolución de esta sociedad, es preciso entender que partimos hoy de una plataforma tecnológica ni siquiera imaginable hace unos años.

Como Presidente de Secuware, ¿cuál es su visión global sobre la Seguridad Informática en estos momentos?

Afortunadamente la idea de Seguridad Informática ha evolucionado en los últimos años para dejar de verlo como un valor añadido o una propiedad adicional de la Infraestructura Informática. Hoy la seguridad es una funcionalidad básica, sin la cual no resulta serio hablar de Infraestructura Informática o de Sistemas de Información.

En resumen, la Seguridad Informática hoy es una propiedad inherente a cualquier componente de una Arquitectura Informática, al menos para la utilización pública y con un sentido industrial o empresarial. Cualquier infraestructura que no contenga la seguridad como un aspecto inherente a su funcionalidad puede ser un juguete, o un divertimento, pero jamás una plataforma de utilización empresarial, pública, o para relacionarse seria y correctamente con un mundo conectado y globalizado como el actual.

Entonces, ¿cómo ve usted en general la evolución de la Sociedad de la Información?

La Sociedad de la Información es una denominación relativamente antigua. Creo que se utilizó por primera vez en 1957, cuando el número de trabajadores relacionados con la información en EEUU superó el número de trabajadores relacionados con la fabricación y la agricultura.

Desde entonces hasta ahora, la Sociedad de la Información ha ido construyendo valor económico sobre la importancia de información de los contenidos y sus cambios. Otras denominaciones como Sociedad y Economía Digital, Sociedad en Red, Organizaciones en Red, incluso Sociedad del

Conocimiento, etc., han ido matizando los diferentes caminos que ha recorrido la Sociedad de la Información.

Si lo pensamos detenidamente, el año que viene se cumplirá medio siglo de la existencia de este término. Dada la velocidad a la que se han sucedido los acontecimientos durante este tiempo, su evolución ha sido impresionante. En ese transcurso los catalizadores más importantes han sido la convergencia de las Tecnologías de la Información y las telecomunicaciones y el desarrollo de las redes públicas, muy especialmente Internet.

Por lo tanto, para hablar del futuro y la evolución de esta sociedad, es preciso entender que partimos hoy de una plataforma tecnológica ni siquiera imaginable hace unos años. Ahora nos resulta habitual movernos en un entorno de movilidad, virtualidad de los sistemas, masiva capacidad de transmisión y almacenamiento de información como un valor establecido.

Sería absurdo que en esta situación nos planteáramos si la seguridad juega o no un papel importante. Desde Secuware pensamos que la seguridad es la propiedad que permite a un sistema, a una plataforma de trabajo, a un PC o a cualquier otro dispositivo estar dentro de ese

> **"Cualquier infraestructura que no contenga la seguridad como un aspecto inherente a su funcionalidad puede ser un juguete, o un divertimento, pero jamás una plataforma de utilización empresarial, pública, o para relacionarse seria y correctamente con un mundo conectado y globalizado como el actual."**

contexto. Repito, cualquier sistema no seguro en este contexto, no solamente es detestable, sino que no tiene sentido.

En su opinión, ¿cómo se construye la confianza de los participantes en este contexto?

Le voy a contestar poniendo un ejemplo. Cuando alguien se sube a un coche, cree que lo domina y que lo conoce únicamente porque sabe manejar el volante, los frenos, y ha pasado un examen. Cuando conducimos, nos sentimos confiados. Sin embargo, mucha gente tiene miedo a volar. Es decir, desconfía de volar. Y sin embargo, si esta persona mirara las estadísticas, los controles de calidad, el número de accidentes que hay, tendría claro el hecho objetivo de que es mucho más seguro volar en un avión que conducir un coche. Hay muchos menos accidentes aéreos que en las carreteras. Es decir, percibir que algo es seguro no siempre significa que lo sea. Sin embargo, el mercado y los usuarios individuales, en general, suben constantemente el nivel de su demanda en materia de seguridad y adquieren confianza cuando ven que están protegidos ante los fraudes, desastres o incursiones que han sufrido previamente.
En la industria estamos haciendo grandes esfuerzos para que esta confianza sea constatable. En Secuware trabajamos desde hace más de diecisiete años en esta materia, y hemos podido comprobar que nuestros clientes han dado un salto cualitativo de confianza cuando han incluido en sus plataformas de trabajo los elementos de seguridad de Secuware. Cada uno en función de sus propios intereses ha cubierto aquellas áreas de riesgo que le eran más importantes. Podríamos citar a Telefónica Móviles, Iberdrola, importantes entidades financieras, incluido Banco de España, Ministerio de Interior y un largo etcétera, donde han adoptado la seguridad como una función indispensable de su plataforma de trabajo. Esa adopción es la que crea el nivel de confianza requerido.

Por ejemplo: ¿Los pagos con tarjeta de crédito en Internet son seguros?

Las entidades financieras han puesto los medios para que este tipo de transacciones sean seguras. Sin embargo hoy, gracias al chip criptográfico que se utiliza por ejemplo en el DNI electrónico, este tipo de pagos aún podría ser más seguro.

¿Y cómo sería esto posible?

Déjeme explicarle el caso del DNI para después generalizarlo. El DNI electrónico es, sin duda, la aportación más brillante y avanzada que se ha hecho en nuestro país para hacer confiable nuestra infraestructura de Sociedad Digital o si quiere Sociedad de la Información. La identificación del usuario final desde su plataforma de trabajo individual, es decir, desde su PC con el lector adecuado y seguro para el DNI electrónico erradica el anonimato en la utilización de los servicios en red. Por lo tanto, asegura el acceso y la correspondencia entre el usuario y los recursos accesibles.

¿Es decir, antes no había seguridad porque el usuario estaba enmascarado?

Exactamente. Sin esa capacidad de identificación que proporciona el DNI electrónico cualquiera podría usurpar datos de su plataforma de usuario o de los sistemas a los que tenía acceso esa plataforma. Como ve, el DNI electrónico es precisamente un elemento que hace de la seguridad una propiedad inherente a su funcionalidad y, por lo tanto, está en línea con las características que hemos hablado al principio, y que desde Secuware venimos promoviendo y apoyando intensamente desde hace muchos años.

¿Qué inversión dedican ustedes a I+D en este campo?

Durante mucho tiempo, más del 50% de nuestra cifra de negocio ha sido dedicado exclusivamente a I+D. Y ahora estamos realizando un importante esfuerzo

El DNI electrónico es, sin duda, la aportación más brillante y avanzada que se ha hecho en nuestro país para hacer confiable nuestra infraestructura de Sociedad Digital o si quiere Sociedad de la Información.

en nuestros acuerdos con fabricantes de PCs, móviles, PDAs, etc.

¿Y este esfuerzo se ve recompensado?
Creemos que sí por el siguiente motivo. Al ser la seguridad una propiedad implícita de los Sistemas de Información, nuestra actividad nos hace estar incluidos en un número cada vez mayor de proyectos, tanto por demanda de los usuarios finales, como por iniciativa y requerimiento de los propios fabricantes de hardware.

¿Con qué tipo de fabricantes tienen acuerdos?
Estamos trabajando con los mayores fabricantes de PCs del mundo como Dell, para que sus plataformas incluyan desde fábrica nuestra solución de seguridad. Concretamente para la utilización del DNI electrónico, con lo cual su oferta será implícitamente segura para la utilización de este avance que es el DNI electrónico. También tenemos acuerdos con importantes integradores como IECISA, INDRA, etc.

Para el DNI electrónico está claro. Sin embargo, ¿todo el mundo va a utilizar el DNI electrónico como llave del PC?
El ejemplo del DNI electrónico es extrapolable a la tarjeta de identificación de la empresa, la tarjeta de salud, es decir, para una infinidad de usos que, como usted decía antes, desenmascaran al usuario final cuando utiliza los recursos de la Sociedad Digital.

¿Es el usuario enmascarado, es decir no identificado, el responsable de los fraudes?
Así es. Se ha convertido en una cifra estándar admitida desde hace años, que más del 80% de los fraudes, violaciones de información, fugas de información y problemas serios de seguridad de los Sistemas de Información proceden del mal uso, abuso o negligencia, del usuario final. Por lo tanto, si la plataforma de trabajo de una organización o una empresa, o incluso individual, es segura, y quien accede a ella es identificado de manera segura, toda esa problemática desaparece.

¿Cómo podemos incorporar el DNI electrónico a nuestras vidas?
Es tan sencillo como que cuando tú enciendes un ordenador, lo primero que te dice es: ¿Y tú quién eres? Y tienes que meter tu DNI electrónico. Con este objetivo en Secuware fabricamos un sistema operativo de seguridad, que se llama SSF, que es el que permite que se pueda utilizar el DNI electrónico de forma segura en los ordenadores.
Nos parece esencial que los ordenadores de la Administración Pública estén protegidos. Nos parece esencial impedir que cualquiera que pasa por un pasillo se pueda meter en el ordenador de alguien. Y creemos que el DNI electrónico es la vía para hacerlo. Algunos servicios electrónicos del futuro, por ejemplo la votación electrónica, serán impensables si no tenemos un sistema para identificar a las personas. La tecnología de Secuware ha permitido que el DNI electrónico sea la llave del PC.

En este sentido, ¿qué papel cree que juega España dentro del sector tecnológico a nivel europeo?
Desde Secuware creemos que una gran oportunidad para España en el sector de la Sociedad de la Información es, precisamente, el de la seguridad. Porque empresas punteras como la nuestra, que ya existe, y están además agrupadas en la Plataforma de Seguridad y Confianza, es una iniciativa pionera en Europa.
En Europa se crearon plataformas hace tiempo orientadas a la movilidad y a los contenidos, que tienen un fiel reflejo en España con plataformas equivalentes. Pero en materia de seguridad en Sociedad de la Información, España es el líder y debemos aprovechar esa coyuntura, ya que en el sector de la Seguridad Informática no existe una plataforma europea.

¿Cuál es la visión del equipo técnico de I+D en Secuware?

Afortunadamente contamos con un grupo técnico altamente cualificado y que une a su capacidad de Innovación y Desarrollo un sentido pragmático para el resultado de su trabajo. Ellos saben mejor que nadie la diferencia entre un juguete y una plataforma de trabajo empresarial o individual. Entienden la seguridad, como ya he dicho, como un valor inherente al sistema, igual que lo puede ser el funcionamiento correcto de una aplicación o la gestión del acceso a los datos, etc.
Nosotros desarrollamos un sistema operativo de seguridad, puesto que la oferta que había en el mercado era básicamente un sistema orientado al manejo flexible de información que requería ser complementado con la seguridad.
En Secuware trabajamos desde hace años en conseguir ordenadores que no se rompan. Ordenadores que no se estropeen. Que no tengas que cambiar de ordenador al cabo de dos años únicamente porque ahora va mucho más lento que el día en que lo compraste.

“...en materia de seguridad en Sociedad de la Información, España es el líder y debemos aprovechar esa coyuntura...”

¿Y cuál es el resultado final?

Gracias a este esfuerzo, Secuware es hoy un referente en materia de seguridad. Mantenemos acuerdos con los líderes mundiales de la industria y estamos abriendo nuestras operaciones en EEUU e Hispanoamérica, con notables expectativas.

De hecho muchos equipos de los líderes mundiales en PCs como Dell, o de comunicaciones como Cisco, pueden llevar nuestras soluciones desde su salida de fábrica.

Carlos Jiménez

Presidente de Secuware | 39 años Ingeniero Superior de Telecomunicaciones | El único que ha simultaneado cinco especialidades durante la carrera

- Creó el primer antivirus de ordenador hace 16 años.
- Fundó en 1989 Anyware Seguridad Informática S.A., primera empresa española de I+D+i para seguridad de ordenadores. Su filial de California (Anyware Software Corporation) fabricó el segundo antivirus más descargado de Internet entre 1995 y 1998. En 1998 vendió Anyware a McAfee (multinacional americana) por 11 millones de euros, que utilizó para financiar su segundo proyecto: Secuware.
- En 1998 el CNI le expresa la necesidad de proteger los ordenadores de la Administración Pública, especialmente el Ministerio de Defensa e Interior, y fabrica desde Secuware el producto de cifrado Crypt2000 que actualmente protege la información de todos los ordenadores de la Agencia Tributaria y varios Ministerios y de las principales empresas publicas y privadas: Telefónica, Iberdrola, FNMT, Banco de España, etc.
- Colaborador asiduo de los medios de comunicación, ha aparecido en múltiples ocasiones en programas de noticias (TVE, A3TV, Tele5, Canal +, TM) y medios escritos (El País, El Mundo, ABC) para comentar los diferentes incidentes de seguridad informática ocurridos. Ha impartido clases en diferentes universidades españolas (UPM, UPV, Autónoma de Madrid...) y extranjeras (París, Milán, UCLA y Berkeley en USA). Semanalmente colabora con Radio Intereconomía en el programa “Profesionales en Internet”.
- Vicepresidente del Club de Amigos de la Sociedad de la información presidido por Crisanto Plaza, donde comparte su visión con la de los presidentes y directores generales de las compañías más importantes del país.
- Miembro de la comisión de expertos del Ministerio de Ciencia y Tecnología, participó en la redacción del Plan de I+D+i 2004-2007 con la “Acción estratégica sobre seguridad y confianza en los planes nacionales de electrónica, informática y Sociedad de la Información”.
- Asesor invitado por la OTAN a participar en la conferencia sobre terrorismo de los directores generales de armamento.
- Otras áreas en las que ha hecho aportaciones son la decodificación del Genoma Humano, la generación de números aleatorios por software o la gestión de contenidos digitales, por ejemplo.
- Carlos Jiménez es una mezcla de empresario y comunicador aunque él prefiere definirse como un técnico al que se le puede entender. Es considerado un experto en Seguridad Informática, ordenadores personales y redes, y uno de los diez mayores expertos mundiales en virus informáticos y ciberterrorismo.

Más Información: www.secuware.com

autelsi

ASOCIACIÓN ESPAÑOLA DE USUARIOS
DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Seguridad y Negocio:

Experiencias y Claves para Directivos

Con la colaboración de:

red.es

Patrocinadores:

CROSSBEAM SYSTEMS

enterasys

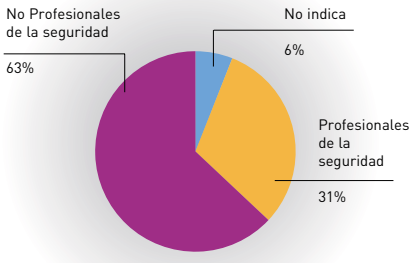
Networks that Know

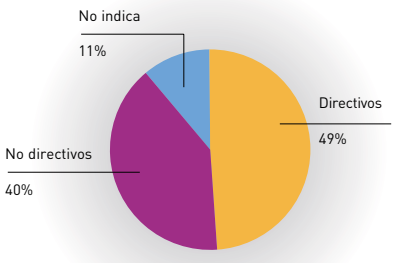
f5

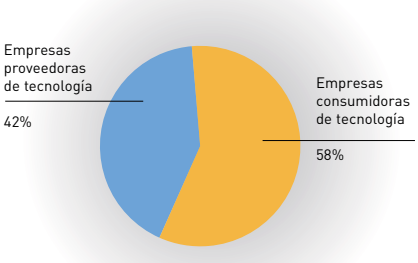
SECURE COMPUTING

SECUWARE

Perfil de los asistentes







Marco actual en la gestión de la Seguridad de los Sistemas de Información

"Si piensas que la tecnología puede resolver tus problemas de Seguridad, entonces no entiendes el problema y no entiendes la tecnología"

"Secrets & Lies" de Bruce Scheneier

Francisco Lázaro durante su exposición.

Comencemos con un hecho poco cuestionable; el entorno TIC (Tecnología de la Información y Comunicaciones) ya ha sido metabolizado dentro de las estructuras organizativas corporativas, y ha pasado de considerarse una importante función de apoyo, a admitirse como una función principal. Parte de esa metabolización es la presencia de los responsables de los Sistemas de Información en las mesas de los consejos. Asimismo, la necesidad imperativa del cumplimiento legal o los Planes de Contingencia de Negocio han forzado el trabajo en equipo del departamento TIC con otras áreas de negocio (y viceversa). De la regularización y el cumplimiento legal se derivan conceptos fundamentales como: privacidad, transparencia, separación de funciones, responsabilidad y pruebas electrónicas, en las que las TIC tienen mucho que aportar. Todo ello nos permitiría pensar que por fin se ha alcanzado la meta de "alinear la tecnología de la información con el negocio" y que, por tanto, el proceso de Seguridad estaría también alineado con los fines y objetivos del negocio.

Pero somos muchos los que pensamos que todavía queda un largo camino por recorrer. Centrándonos en el proceso de la Seguridad de los Sistemas de Información nos encontramos que hay ciertos aspectos en los que hay que trabajar para alcanzar esa simbiosis con el negocio. Por un lado, las empresas, sus dirigentes, delegan la responsabilidad en este campo y no ejercen el control de la gestión de la Seguridad de la Información. Por otro lado, los responsables de Seguridad ejercen su trabajo desde su conocimiento técnico, sin proporcionar información compresible hacia la alta dirección, y sin establecer un marco de gestión que aglutine los procesos y que le permita dar visibilidad a su trabajo. Por resumir en términos mercantilistas "unos no compran y los otros no venden".

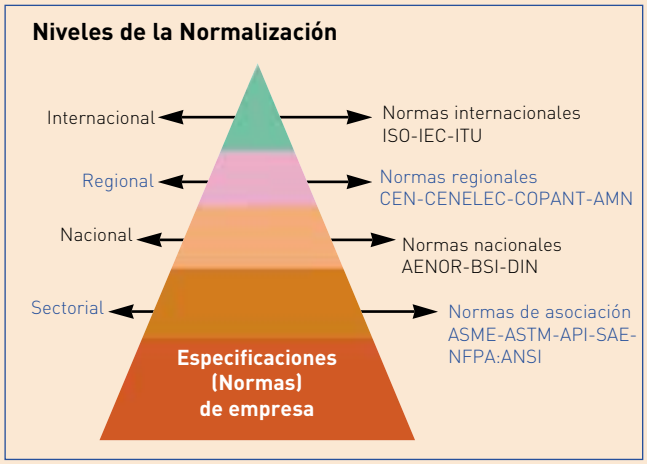
Si la Seguridad de su red corporativa está basada en la compra e instalación de firewalls, antivirus, sistemas de detección de intrusos y otras soluciones hardware/software, deberemos saber que los

incidentes de Seguridad seguirán produciéndose y que se seguirá teniendo la visión del departamento de Seguridad de la Información como un costoso parque interno de bomberos.
La falta de visión global en el plan de Seguridad nos lleva a afrontar cada situación de Seguridad desde el constante "reinventar la rueda" y acometiendo las acciones porque creemos que tenemos que hacerlas, pero sin saber realmente qué representa para el negocio y cómo ayuda no sólo a preservar el valor de los activos de la empresa (entre los que se encuentra la información), sino a crear valor (al participar del cumplimiento de los objetivos del negocio).
En los últimos 6 años y a nivel internacional se ha ido elevando y popularizando una serie de conceptos, que permitirán que se encuentren en un espacio común la Seguridad de la Información y el negocio:

- Desarrollar un Sistema de Gestión de la Seguridad de los Sistemas de Información (SGSI en castellano o ISMS en inglés).
- Establecer como punto clave el Análisis y Gestión del Riesgo. Es decir, incluir dentro de la Seguridad de los Sistemas de Información una metodología habitual en otros procesos de negocio.
- Promover y tomar como referencia normas internacionales en este campo, como por ejemplo ISO/IEC 27001 o ISO/IEC 17799; con el fin de no reinventar, dentro de casa aquellos aspectos relevantes en los que expertos a nivel mundial han alcanzado consenso sobre prácticas que se ya se han demostrado como eficaces.
- Incluir dentro de los límites de la Seguridad de los Sistemas de Información conceptos referentes al Buen Gobierno (como COBIT) o a buenas prácticas (como ITIL) para proporcionar servicios de soporte y provisión con calidad (ISO/IEC 20000).
- Presentar información comprensible a la alta dirección. El proceso de medición para obtener medidas (métricas e indicadores) se yergue como un facilitador de esa labor, incluso para ser metabolizada su información dentro del cuadro de mando del negocio.

Normas ISO y UNE

Las **normas** son especificaciones técnicas, de carácter voluntario, consensuadas y elaboradas con la participación de las partes interesadas (fabricantes, usuarios, consumidores, laboratorios, administración, centros de investigación, etc.) y aprobadas por un organismo reconocido.
En el ámbito internacional existen dos organismos de normalización formados por cuerpos nacionales de normalización: la **Comisión Electrotécnica Internacional (IEC),** responsable de la elaboración de normas internacionales sobre electrotecnia y electrónica, y la **Organización Internacional de Normalización (ISO)** que cubre el resto de sectores de actividad.
ISO e IEC comparten la responsabilidad de la elaboración de las normas relativas a las tecnologías de la información. Sus normas reciben el prefijo ISO/IEC.
International Organization Standardization (ISO www.iso.org) es una organización mundial no gubernamental, que representa a 145 países. Los miembros de ISO o IEC son los organismos que representan la normalización de un país. En España, tal responsabilidad recae sobre AENOR.
Las siglas deberían ser IOS pero se adoptó ISO, que como prefijo griego "iso" significa "igual o igualdad", que es exactamente lo que se espera de los resultados de un proceso normalizado.
La actividad de AENOR comenzó en el año 1986, mediante una Orden Ministerial. En ella, fue reconocida como la única entidad aprobada para desarrollar las tareas de **normalización** en nuestro país (Normas UNE). AENOR es miembro de pleno derecho, y representa a nuestro país, en los organismos internacionales, europeos y regionales de normalización (ISO, IEC, IEC, CEN, CENELEC, ETSI, COPANT).
En la estructura de AENOR existen unos órganos técnicos, denominados Comités Técnicos de Normalización (AEN/CTN), que estudian y plantean las necesidades de cada sector y elaboran y aprueban los proyectos de normas que posteriormente se publican como normas UNE. AENOR mantiene CTNs "espejos" de los Comités Técnicos de Normalización de ISO, con la misma denominación y objetivos que los de ISO.
El Subcomité 27 (SC27), Técnicas de Seguridad, del CTN Tecnologías de la información tiene la responsabilidad de redactar las normas referentes a la Seguridad de la Información, como por ejemplo: ISO/IEC 27001, ISO/IEC17799.



Así pues, para materializar el concepto "alinear la Seguridad de la Información con el negocio" deberemos trabajar en los siguientes aspectos claves:

- **Preservar y generar valor.** Partiendo de la cadena de valor, desbrozamos los procesos de negocio, definimos los procesos tecnológicos que los soportan e identificamos los mapas de sistemas para esos procesos. Al combinarlos con los objetivos de negocio y con el cumplimiento legal estamos en condiciones de realizar el Análisis y Gestión de Riesgos; es decir, sabemos cuantificar la importancia de los activos que tenemos que proteger y las acciones que debemos tomar para cumplir, de una forma eficaz y eficiente, con los objetivos que el negocio nos ha marcado. En definitiva, preservar y generar valor.
- **Gestionar la Seguridad.** La Seguridad de la Información es un proceso continuo y estratégico. Por ser continuo debe ser gestionado, buscando la mejora a través del ciclo (PDCA —Plan, Do, Check, Act—) y por ser estratégico es responsabilidad de la alta dirección. La inclusión de dicha gestión en los comités existentes es la expresión de ese alineamiento.
- **Buenas prácticas,** para ser efectivos y eficaces. Con una visión multidisciplinar de Seguridad y con criterios de calidad, servicio y excelencia, para poder satisfacer las expectativas que el negocio fija a Sistemas de Información. La Seguridad de la Información como "sólo tecnología" es una visión condenada al fracaso. Las salvaguardas se conforman con controles organizativos, políticas, procesos y recursos. Por ejemplo, la firma por la alta dirección de la política de Seguridad se presenta como un hito clave, pues es la expresión del respaldo de cualquier acción posterior que se encuadra en las directrices plasmadas en el documento.
- **Medir el desempeño.** La gestión necesita de pruebas objetivas y repetibles que nos permitan conocer qué nivel de implantación hemos alcanzado y cómo mejoramos en la eficacia y en la eficiencia de los controles y salvaguardias seleccionadas. En este campo y a nivel internacional, se está elaborando una norma para establecer una metodología de medición de la Seguridad de la Información: la futura ISO/IEC 27004. España, a través del SC27 está trabajando intensamente en su redacción y edición, baste citar como ejemplo de este esfuerzo que Paloma Llaneza es la coeditora internacional de dicha norma.
- **Comunicar:** se identifican dos sentidos de información:
  - *Descendente* (desde el negocio —alta dirección— hacia la Seguridad de la Información). Los objetivos del negocio y los requerimientos regulatorios y legales deben llegar a toda la organización. Cada empleado debería saber cómo su trabajo debe ser orientado para lograr la consecución de los objetivos del negocio. O dicho de otra forma, como empleado debo saber como las acciones de Seguridad que desarrollo ayudan a alcanzar las metas.
  - *Ascendente* (desde la Seguridad de Información hacia el negocio). En relación con la Seguridad de la Información, las acciones orientadas a los RRHH son: concienciación, formación y capacitación. Las dos primeras entran de lleno en el concepto de "comunicar". Pero hay más aspectos que deben ser cubiertos, en relación con la función que los recursos humanos desempeñan:

    a) *Para todo el personal;* usuarios, empleados, subcontratados, responsables y gestores de la Seguridad de la Información: concienciación, formación y capacitación. En este nivel, adquiere una especial importancia el conocimiento de la política de seguridad.
    b) *Gestores de la Seguridad de la Información:* información para la mejora del proceso de Seguridad, por ejemplo con la medición (medidas, métricas e indicadores) de la eficacia y eficiencia de los controles de Seguridad.
    c) *Alta dirección.* Información para la toma de decisiones. Su desconocimiento en esta área, por falta de información, no puede llevar aparejada otra actitud que la indiferencia por el proceso de Seguridad. Los diferentes departamentos y áreas de la organización compiten por el presupuesto, la información es un elemento clave para presentar cómo la inversión y el gasto en Seguridad de la Información se transforma en generación y preservación de valor.

En definitiva, la imagen que el negocio tenía de la Seguridad de la Información como algo oscuro, costoso e ininteligible está tornándose a una visión compresible del proceso y, por lo tanto, gestionable.

Francisco Lázaro [Consultor en Seguridad de la Información y Jefe de Internet de Renfe]

Virtualización de servicios de seguridad en Telefónica Empresas

El entorno competitivo al que se ha de enfrentar una organización que ofrece servicios de alojamiento, como es el caso de Telefónica Empresas, es altamente variable y volátil. Es fundamental disponer en estos entornos de soluciones que puedan ofrecer los servicios diseñados por la organización para sus clientes pero que, al mismo tiempo, puedan cambiar rápidamente con el tiempo para ofrecer nuevos servicios si fuera necesario. En este proceso conceptos como virtualización y seguridad cobran una dimensión fundamental.

Telefónica Empresas es la línea de negocio de Telefónica S.A. dedicada a las soluciones para grandes empresas surgida a la raíz del rediseño del Grupo Telefónica en otoño 2004. Telefónica Empresas ofrece, dentro de las soluciones para grandes empresas, servicios de hosting y ASP incluyendo dentro de éstos, también, una oferta en servicios gestionados de seguridad perimetral (MSS), que van desde la posibilidad de contratación de sistemas cortafuegos y de detección de intrusos, dedicados o compartidos y gestionados por personal especializado de Telefónica. Estas soluciones de seguridad se ofrecen dentro de las infraestructuras propias de Telefónica, que cuenta con centros de procesos de datos, llamados Telefónica Internet Centers (TIC), en distintas ciudades de España y donde se hospedan los servicios de las empresas cliente y se les provee de conexión a Internet.

Redes privadas de clientes

Uno de los proyectos recientemente abordado por Telefónica en sus TIC es el despliegue de una infraestructura destinada a proveer servicios a clientes con redes propias conectadas a los TIC. Este servicio se conoce como "Módulo de Conectividad Privada"o MCP. Se trata de un problema complejo, pues los clientes, en función de sus necesidades, podrán disponer o no de servidores corporativos alojados en el TIC, y podrán querer, o no, acceder a servicios adicionales ofertados dentro de los TIC.

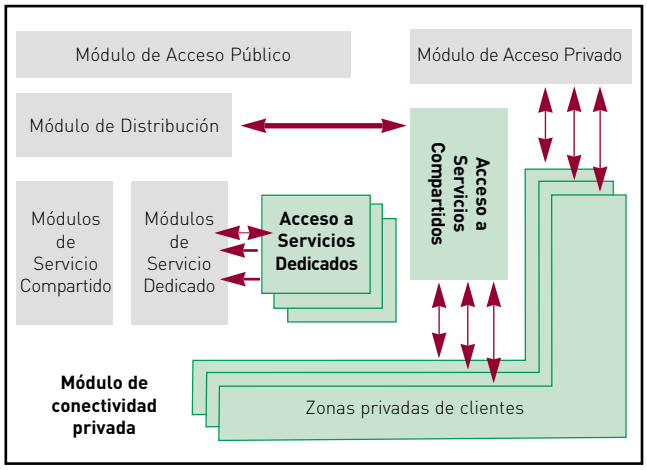
En la figura adjunta se muestra el modelo lógico de este módulo. Como se puede observar, la introducción de un nuevo elemento en una infraestructura compleja como es la de los TIC de Telefónica introduce un elevado número de interacciones con servicios y sistemas preexistentes lo que incrementa, aún más, la complejidad del problema *(Ilustración 1)*.

Además, a la hora de diseñar un servicio de estas características, se debe exigir un alto nivel de seguridad en un entorno compartido que garantice la privacidad de la información de distintas redes privadas de distintos clientes. Una solución técnica que permita implementar este servicio debe, además, poder ofrecer unos altos niveles de disponibilidad, necesidad propia de los grandes clientes empresariales, así como una elevada flexibilidad para permitir a Telefónica un crecimiento escalonado en función de la evolución de la demanda, así como la posibilidad de ofrecer nuevos servicios con un coste adicional. Se trata, en fin, de buscar una solución que pueda adaptarse a los cambios futuros desconocidos.

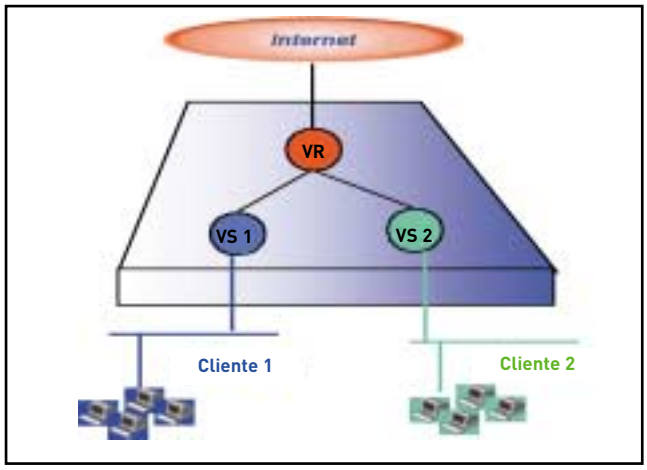
Uno de los problemas tecnológicos surge de la interconexión de una red propia de un cliente a un entorno compartido, surgirán necesariamente problemas de solapamiento al utilizar los distintos clientes rangos comunes de direcciones IP habitualmente asignados de los rangos reservados por la IANA y descritos en el RFC 1918 (Address Allocation for Private Internets). Problema que obliga, además, a la utilización de traducción de direcciones (NAT, Network Address Translation).

Implementación

La solución tecnológica adoptada por Telefónica se basa en la utilización de cortafuegos virtuales en una plataforma común para todos los clientes pero que, a todos los efectos, se comporta como si se tratara de un sistema individual por cliente. La utilización de sistemas virtuales evitan recurrir a equipamiento dedicado sin pérdida de funcionalidad, reduciendo los costes y permitiendo ofrecer los servicios de una forma más competitiva. Además, ofrece la posibilidad de



Modelo lógico del Módulo de Conectividad Privada.



Cortafuegos virtuales sobre un mismo hardware.

implementar políticas de seguridad independiente y distintos tipos de mecanismos de NAT.
El término de cortafuegos virtual es un término relativamente reciente en la tecnología de seguridad perimetral. Básicamente consiste en que un único sistema hardware, a través de un software de cortafuegos específico, es capaz de gestionar el tráfico de forma que éste se trata por un sistema de cortafuegos distinto (distintas reglas, distintas tablas de estados), en función de alguna de sus características (puerto entrante, VLAN, etc.). Al efecto es como si en lugar de un único cortafuegos en el sistema hardware se dispusieran de tantos cortafuegos "virtuales" como se deseara para tratar el tráfico. Esto permite: implementar políticas de seguridad separadas por cada "cliente" (red conectada) y limitar el consumo de recursos de forma individual a cada "cliente" *(Ilustración 2)*.
El uso de cortafuegos virtuales permite obtener las ventajas de un entorno de hardware dedicado por cliente (imposición de límites a los recursos consumidos por cliente y gestión individualizada) con las ventajas (reducción de costes) de un entorno de hardware compartido.
Tras una prospección tecnológica en busca de una posible solución, ésta se decantó por la utilización del sistema de cortafuegos Check Point Firewall-1 VSX sobre plataforma Crossbeam X80.
Esta plataforma hardware, ya mencionada en esta misma revista, está basada en la utilización de tarjetas individuales (equivalentes a servidores independientes) dentro de un mismo chasis con una muy alta conectividad (hasta 64 puertos FastEthernet o 32 Gigabit) y disponibilidad.

Una tecnología de cortafuegos virtuales permite a Telefónica dotar a sus clientes de sistemas virtuales independientes, de forma que pueda garantizar que las distintas redes no puedan comunicarse entre sí, que las políticas de seguridad de los distintos clientes estén separadas. Uno de los vicios ocultos de políticas de seguridad compartidas es que los cambios en la política de seguridad global solicitados por un cliente pueden tener efectos insospechados en la política definida para otros clientes, lo que complica la gestión y hace necesaria que este tipo de políticas sufran una auditoría y revisión continua. Con una política de seguridad dedicada se evitan estos males. Sería incluso posible delegar la gestión de estas políticas a los propios clientes si éstos lo requirieran, bien a través de la plataforma de gestión de Provider-1 o de desarrollos específicos. Esta posibilidad es impensable en entornos en los que la política de seguridad es común.

Conclusiones

La tecnología de cortafuegos virtuales está siendo utilizada hoy en día por grandes proveedores para ofrecer a sus clientes funcionalidades equivalentes a entornos de hardware dedicado con un importante ahorro de costes.
La decisión por parte de Telefónica de utilizar Crossbeam, una plataforma introducida el año pasado en España y, por tanto, relativamente nueva, como plataforma hardware preferente no ha sido "a ciegas", sino tras realizar pruebas pilotos en los que ha demostrado su validez.

Juan Miguel Pérez Velasco [Telefónica Empresas. Director Asociado Plataformas Comunes y Servicios de Seguridad. Telefónica Soluciones]

Redes basadas en políticas

Las universidades tradicionalmente han sido pioneras en la construcción de redes de comunicaciones y en el uso de Internet, que se ha convertido en un recurso estratégico para el cumplimiento de su misión, la investigación y la docencia. La Universidad Complutense es la universidad presencial más grande de España con 90.000 estudiantes de títulos oficiales, 5.000 profesores y 3.500 trabajadores. Actualmente dispone de una red corporativa que se extiende por sus dos campus (Ciudad Universitaria y Somosaguas) y a varios edificios en el centro de Madrid con más de 18.000 puntos activos de acceso a la red cableada y 210 puntos de acceso inalámbrico, que dan cobertura en el exterior y en zonas comunes del interior de los edificios. Aproximadamente unos 4.000 de estos puntos se concentran en aulas de informática y mediatecas de libre acceso. Esto genera una problemática muy importante de cara a la seguridad por la amplitud en el número de usuarios que, además, tienen necesidades e inquietudes muy diversas.

Manuel Hernández Urrea.

Las redes basadas en políticas son la solución para mantener segura una red corporativa. La estrategia tradicional de la seguridad perimetral implica la necesidad de realizar un difícil ejercicio para el establecimiento de un perímetro que separe a los "buenos" de los "malos". Este ejercicio resulta imposible en redes corporativas universitarias de gran tamaño. Frente a esto, las redes basadas en políticas permiten controlar y gestionar la seguridad de la red con la máxima granularidad posible.
Una política de red es un conjunto de reglas que son aplicadas al tráfico de un puerto para garantizar, limitar o bloquear el acceso a los diferentes recursos que ofrece la red. Éstas políticas, a su vez, se pueden explotar mediante diferentes formas de uso.

Control de aulas y laboratorios

La forma más sencilla y que involucra menos elementos es el uso de políticas asociadas al puerto físico de conexión a la red. En la Universidad Complutense las aulas informáticas y los laboratorios son gestionados con políticas asociadas al puerto. Mediante una pequeña aplicación desarrollada hace dos años en la universidad, la aplicación *Prof-e*, el profesor decide en cada momento el comportamiento de la red en un aula o laboratorio de informática. El profesor a través de un navegador web elige el modo de funcionamiento del aula: *normal* (aula libre), *clase*, *examen* (en varios modos) y *aislamiento*. *Prof-e* se comunica con el gestor de políticas que aplica la que

> **"...hay que destacar que las redes basadas en políticas permiten reaccionar rápidamente ante problemas de seguridad"**

corresponde a ese modo de funcionamiento en todos los puertos de red a los que están conectados los equipos del aula. A partir de ese momento, el tráfico de los equipos es tratado según las reglas activas de la política asignada obteniendo acceso a diferentes recursos ofrecidos en la red.

Políticas basadas en la identidad del usuario

Si bien la gestión de identidad es un proceso organizativo complejo y que involucra a muchas áreas de la organización que están fuera de los departamentos de informática, una vez resuelto se puede utilizar para el control de acceso a la red y así crear un entorno de trabajo personalizado para cada usuario.
Cuando un usuario se conecta a la red, ésta envía las credenciales del usuario a los servidores de gestión de identidad, que devuelven la política que se debe aplicar a ese punto de red concreto. Por tanto, una vez identificado el usuario y dependiendo de su función dentro de la universidad, se le asigna una política de red que le permite acceder a los recursos adecuados. Otra ventaja importante de esta forma de uso de las políticas de red es facilitar la movilidad de los usuarios dentro de la red corporativa.
Aquellos usuarios que no están autenticados, ya sea porque sus credenciales no son correctas o carecen de ellas, pueden ser tratados como invitados dentro de la red, ofreciéndoles una conectividad básica y limitada o se puede bloquear completamente su acceso.

Políticas asociadas al estado del equipo

La identificación del usuario no es suficiente para eliminar todas las amenazas. Es necesario, también, identificar y, sobre todo, verificar el *estado de salud* del equipo que utiliza para conectarse a la red. Según el resultado de esta verificación, se asigna una política determinada en función del riesgo que supone. Si el equipo cumple con los requisitos de seguridad establecidos (parches actualizados, antivirus corporativo instalado y actualizado, etc.), se aplica la política definida para ese usuario. Si el equipo no cumple los requisitos, la política que se aplica es de cuarentena. Esta política desvía el tráfico del usuario a una página web cautiva en un servidor de reparación que dispone de las instrucciones y herramientas para poder resolver el problema.

Todos los grandes fabricantes de equipamiento de red y fabricantes de software como Microsoft están desarrollando actualmente soluciones de este tipo para el control de acceso a la red.
Se utilizan, según el entorno, diversos métodos para la verificación del *estado de salud* de los equipos:

- Soluciones basadas en agente que, por ser más intrusivas, son adecuadas para un entorno de puesto de trabajo gestionado donde existirán herramientas automáticas de distribución y actualización de software.
- Soluciones basadas en herramientas de escaneo de vulnerabilidades a través de la red en aquellos entornos donde el puesto de trabajo no se puede gestionar centralizadamente.

Respuesta dinámica ante incidentes

Teniendo en cuenta que la red es una pieza imprescindible para la continuidad del negocio, hay que destacar que las redes basadas en políticas permiten reaccionar rápidamente ante problemas de seguridad.
La universidad, como todas las organizaciones, dispone de herramientas de seguridad que vigilan permanentemente el tráfico que circula por la red para detectar posibles anomalías (virus, gusanos, ataques de DoS, etc.). Cuando una de estas herramientas detecta un incidente de seguridad, la red localiza el puerto del usuario y mediante el gestor de políticas corrige el problema en tiempo real, aplicando una política de cuarentena o bloqueo en ese puerto.
Por supuesto, el despliegue de este tipo de soluciones se debe realizar con la prudencia necesaria para que los falsos positivos no generen las perdidas de servicio que queremos evitar.

Manuel Hernández Urrea [Director del Área de Seguridad, Redes e Infraestructura de los Servicios Informáticos Universidad Complutense de Madrid (www.ucm.es)]

Soluciones para acceso remoto seguro a aplicaciones y recursos corporativos

Existe en la actualidad un número creciente de organizaciones que necesitan dar acceso a aplicaciones y datos corporativos a su personal que trabaja temporal o permanentemente fuera de las oficinas centrales. En este caso se encuentra, por poner algunos ejemplos, el personal en delegaciones remotas, la fuerza de ventas, directivos que se desplazan con frecuencia, personal técnico de campo, distribuidores y *partners* en general.

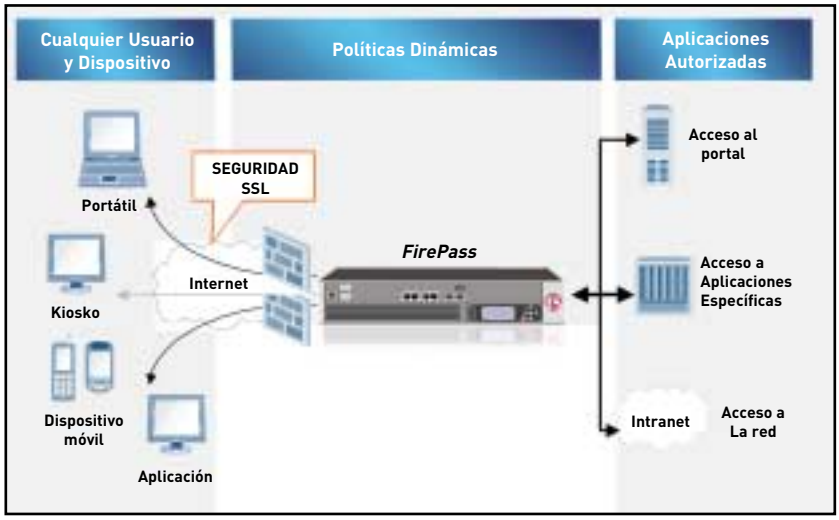
José María Legido.

Esta necesidad de dar acceso a recursos corporativos desde el exterior debe tener en cuenta estrictos requisitos de seguridad, en caso contrario, estaríamos exponiendo activos de información de la organización de manera innecesaria. Por ello, se han utilizado de manera habitual redes privadas virtuales (VPN) con protocolo IPSEC que, si bien son muy adecuadas para la conexión entre sedes con localización geográfica diferente, adolecen de ciertos inconvenientes cuando se trata de dar acceso desde el exterior a personas de nuestra organización.

Para ilustrar estos problemas, así como la mejor manera de resolverlos, se plantea en este artículo, a modo de ejemplo, la existencia de una organización ficticia, que consta de una sede principal y varias subsedes. Esta organización cuenta con una fuerza de ventas que accede desde el exterior a sistemas corporativos mediante un servidor de acceso remoto (RAS), a través de la línea telefónica. Sus directivos disponen de ordenadores portátiles equipados con clientes VPN, de manera que pueden acceder a la red local cuando se encuentran fuera de la oficina.

Finalmente, esta empresa ficticia cuenta con un gran número de distribuidores repartidos en diferentes continentes, que son los que venden los productos de esta empresa ficticia al público en general. La empresa pone a disposición de estos distribuidores un cliente VPN con el que conectarse a una aplicación específica, con la que se gestionan los pedidos y los pagos a los distribuidores.

Tras analizar el estado de esta configuración de acceso, se detectan dos problemas principales en la arquitectura de esta organización. El primero de ellos es un nivel de seguridad insuficiente, que conlleva a una arquitectura compleja para solventarlo. Dado que las VPN IPSEC permiten el acceso desde el exterior a toda la red, se hace necesario poner separaciones entre segmentos de red, entre aplicaciones, etc., para restringir el acceso a recursos concretos, lo que complica la arquitectura de red de la organización. Eso implica problemas, tanto de recursos como de plazos, a la hora de desplegar nuevos servicios accesibles desde el exterior. El segundo problema está asociado a los costes operacionales de la actual infraestructura de la organización. El acceso por RAS requiere la contratación de un servicio específico por parte de un operador de telecomunicaciones, además de los costes de telefonía que supone cada conexión realizada. Por otro lado, el mantenimiento de los clientes VPN, especialmente los de los distribuidores, supone un coste elevado para el call center de la organización,



> **"La seguridad, cada vez más, se está viendo como un elemento que aporta valor y numerosas ventajas competitivas"**

ya que éste tiene que atender a los continuos problemas de configuración que experimentan dichos distribuidores. La solución planteada por SGI para resolver los problemas de esta organización pasan por la implantación de un dispositivo Firepass de F5. Este dispositivo es una VPN con protocolo SSL, que aporta una serie de ventajas sustanciales sobre las VPN clásicas basadas en IPSEC.

La primera ventaja es la facilidad de acceso. Cualquier dispositivo equipado con un navegador web puede conectarse a la VPN SSL, y tras autenticarse adecuadamente, acceder a los recursos autorizados. Se eliminan así los clientes VPN IPSEC y los sistemas RAS, así como los costes asociados a su adquisición, operación y mantenimiento. La segunda ventaja es la flexibilidad de implantación de políticas de acceso, que permite dar acceso a recursos internos de la organización según el perfil de usuario y el tipo de dispositivo desde el que se accede. Esta característica es fundamental a la hora de establecer la política de seguridad de acceso según las necesidades requeridas por la organización. Finalmente, el dispositivo dispone de conectores específicos que facilitan la integración con recursos concretos (servicios web, aplicaciones específicas, terminal server, sistemas host, etc.) de la organización, y que permiten desplegar nuevos servicios al exterior muy rápidamente, sin necesidad de securizarlos ni establecer mecanismos complicados de acceso. Cabe destacar también otras funcionalidades importantes del dispositivo Firepass, entre las que destacan la aceleración SSL, que reduce el tiempo de conexión a recursos internos, la capacidad de comprobar que los equipos remotos disponen de configuraciones adecuadas (antivirus, parches), denegando la conexión a dispositivos no seguros, y la capacidad de gestión de equipos remotos de manera centralizada, lo que facilita el despliegue de nuevas configuraciones.

Una vez implantada la VPN SSL, nuestra organización ficticia experimenta una drástica reducción de los costes de gestión de su infraestructura de acceso, así como un notable incremento de productividad por parte de usuarios y personal administrador. En el primer caso, desaparecen los costes de operación del RAS, ya que todos los accesos se hacen a través de Internet. Además, el consumo de recursos del call center decrece considerablemente, ya que desaparecen los costes ocultos asociados al mantenimiento de la configuración de clientes VPN. Por lo que respecta al incremento de productividad, no sólo se proporciona a los usuarios un interfaz único, independiente del tipo de acceso, sino que éstos observan una mejora muy apreciable con respecto a la disponibilidad y rendimiento de servicios. Asimismo, los usuarios administradores ven reducida su carga de trabajo asociada a la administración del sistema implantado.

Como conclusión, y basándonos en la experiencia de SGI en implantaciones parecidas a la que aquí se ha descrito, destacamos la conveniencia de aplicar este tipo de soluciones en organizaciones que necesiten dar acceso remoto a distintos perfiles de usuarios con privilegios diferentes, securizar el acceso remoto a aplicaciones y recursos compartidos y dar acceso remoto seguro a nuevas aplicaciones de manera rápida y sin costes añadidos.

José María Legido [Director de la Delegación de Barcelona SGI Soluciones Globales Internet]

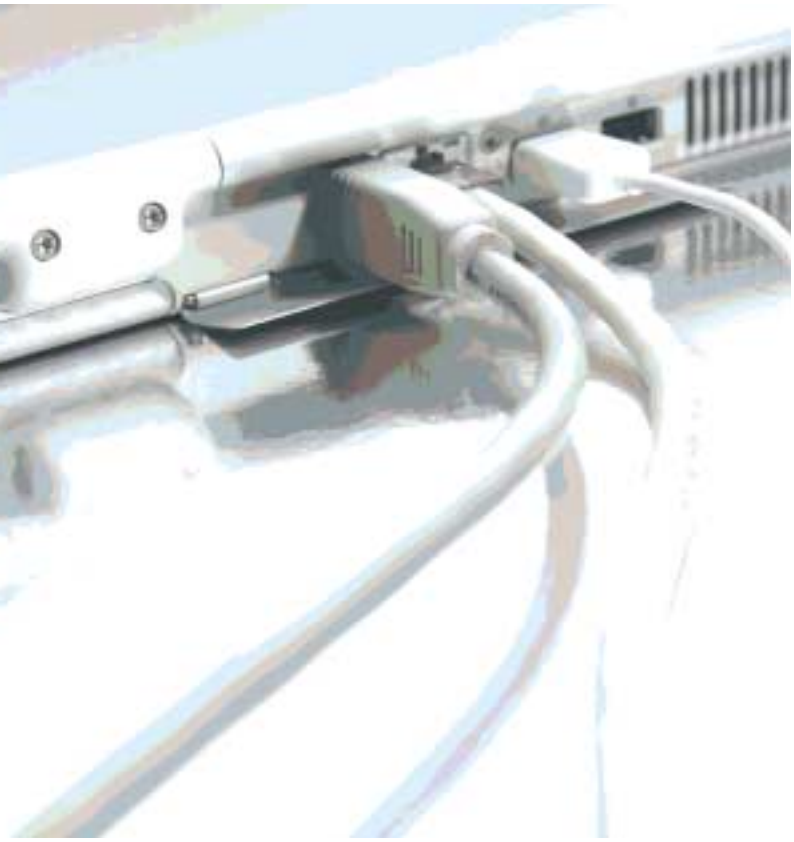
Seguridad a nivel de aplicación. Modelo positivo

Hace veinte años, el Departamento de Defensa de los Estados Unidos encargó al Departamento de Seguridad de Honeywell —hoy Secure Computing—, la preparación de un dispositivo de seguridad para proteger sus redes internas con las siguientes características.

En primer lugar, que tuviera una protección para los servidores y que esta protección tuviera en cuenta a las venideras futuras tecnologías de acceso desde el exterior —como es el caso hoy en día de Internet—.

En segundo lugar, una protección para los servidores de aplicación.

Tercero, que estuviera integrado dentro de una caja negra, en la que nadie (no autorizado) pudiera ver ni tocar nada, y con un sistema operativo que se auto-protegiera.



Con estas premisas, nació el f*irewall más antiguo del mercado SideWinder G2* y que hoy en día protege a más de *18.000 organizaciones a nivel mundial.*
Hay que entender los modelos de seguridad que existen en la actualidad.
En primer lugar, tenemos un *modelo de seguridad negativo,* que es reactivo porque permite que todo el tráfico fluya a través de él y luego identifica lo malo comparándolo con unos patrones de firmas que tiene introducidas. Como ejemplo, mencionaré los sistemas antivirus o los sistemas IPS.
A día de hoy, estas aplicaciones tienen menos tiempo de respuesta. En el momento en que se detecta una amenaza, hay que crear la firma, bajarla a estos dispositivos e integrarla.
Por otro lado, también tenemos el *modelo de seguridad positivo.* Nos vale para protegernos de las amenazas que no se conocen. Basta simplemente con configurar una contramedida, para entender todos los requerimientos del tráfico legítimo que hay que dejar pasar. ¿Qué hacemos con el que no sea legítimo?... ¿lo denegamos?... ¿no dejamos pasar nada más?...

> **"... actualmente estamos hablando de una tecnología con un modelo negativo porque mi servidor va a estar expuesto a unos ataques durante dos o tres meses —inaceptable para cualquier organización."**

En nuestro caso hipotético, los clientes van a acceder a nuestra página web. Tenemos que tener claro cuál es el tráfico que hay que dejar pasar y así reducir drásticamente cualquier posibilidad de amenaza que pueda causar daños dentro de nuestra organización, eliminando con ello cualquier tipo de ataque.

"Todos las organizaciones necesitamos protección siempre, no sólo en los accesos, sino también de aplicaciones."

Actualmente, la tecnología utilizada a nivel de firewall o de protección de aplicaciones es un sistema que no está analizando todo el paquete web, sino que solamente mira la cabecera de esos paquetes. Abre las conexiones, permite cualquier tipo de tráfico y lo va comparando, ignorando cuál es el tráfico exclusivo para esas aplicaciones web.
En el caso de la tecnología que implementa el SideWinder G2, vamos a permitir exclusivamente el tráfico web y dentro de esto, el análisis de anomalías de tráfico que van a llegar a nuestra aplicación web.
El cliente quiere estar seguro de que su aplicación está totalmente protegida, ya que los datos internos de su compañía van a estar también protegidos.
Vamos a analizar esas anomalías y vamos a asegurarnos de que la información que entra es exclusivamente la necesaria.
Por otro lado, tenemos que ver dónde está ubicado nuestro servidor web. Vamos a camuflar nuestra red y nadie va a saber dónde y cómo están esos servidores. Nos vamos a asegurar de que el retorno de la información que nos están pidiendo no sea mayor del necesario, puesto que debemos garantizar la confidencialidad del resto de datos que tenemos dentro del servidor web o dentro de nuestra organización.
Para entender cómo funcionan —a nivel de firmas— las vulnerabilidades, desde que una vulnerabilidad sale a la luz hasta que se propaga a través de Internet suelen pasar dos o tres días. De ahí que hasta que un fabricante saca una firma, por ejemplo de antivirus, y el equipo lo descarga pueden pasar más de dos días.
Y cuando la vulnerabilidad está dentro de un dispositivo que protege esos servidores, en el momento en el que el fabricante aprueba la contramedida o parchea su propio sistema operativo, estamos hablando de dos o tres meses.
Por lo tanto, actualmente estamos hablando de una tecnología con un modelo negativo porque mi servidor va a estar expuesto a unos ataques durante dos o tres meses —inaceptable para cualquier organización—.

A día de hoy (después de 20 años), SideWinder G2 no ha tenido que sacar parches de seguridad. Nadie ha conseguido entrar en sus sistemas. ¿Cómo han conseguido esto?, pues separando todas las funcionalidades de que dispone en "compartimentos estanco".
Si tenemos aplicaciones en Oracle, SAP Citrix, etc., o tenemos aplicaciones web o de correo electrónico, cada una de ellas van a estar en departamentos diferentes y aisladas unas de las otras. Con lo que si alguien consiguiese atacar a una determinada aplicación/servicio, el resto de aplicaciones no se verían comprometidas.
¿Cómo va a garantizar SideWinder G2 la seguridad de nuestro servidor Web? Primero, va a entender cuál es el propósito y funcionamiento de esa aplicación. Segundo, va a permitir que el usuario pida la información que el cliente quiere mostrar. Con una tolerancia cero para cualquier dato que sea desconocido.
Con esta tecnología que controla desde el nivel cuatro al siete de la pila OSI (*), cualquier tipo de tráfico que llegue a nuestro servidor web va a ser pasado por distintos filtros, llamados "Application Pathways" (**), de forma y manera que cualquier tráfico desconocido va a ser filtrado de una manera totalmente diferente. Es decir, rechaza todo lo desconocido, de esta manera estaremos protegidos en todo momento.

Resumiendo

- Todos las organizaciones necesitamos protección siempre, no sólo en los accesos, sino también de aplicaciones.
- La clave está en evitar los fallos de seguridad contra ataques desconocidos.
- Disponer una tecnología híbrida, es decir, que combine las necesidades actuales (ej. UTM) y con una tecnología que sea capaz de analizar el tráfico a nivel de aplicación.
- Un sistema operativo invulnerable con técnicas de codificación de software que protejan todo el software alojado de uso erróneo y contengan todos los procesos de la máquina.

Alberto Arbizu [Director de Ventas para Iberia Secure Computing]

El valor de la seguridad en la empresa

En los últimos años los avances tecnológicos y el continuo alineamiento de las TIC a las funciones del negocio han proporcionado mejoras significativas en la ejecución y operación de las funciones y procesos empresariales, sin embargo, han contribuido a la aparición de nuevas y complejas amenazas que ponen de manifiesto la vulnerabilidad de los sistemas de información.

Empresarios, ejecutivos y profesionales han notado un cambio importante en el concepto de la seguridad, ha pasado de ser una actividad simplemente funcional a una actividad operativa con un gran impacto sobre los procesos empresariales. Estudios realizados por la Information Systems Security Association (ISSA) y la Information Systems Audit and Control Association (ISACA) indican que la mayoría de los ejecutivos pertenecientes a empresas de los Estados Unidos —con una facturación de entre 1 y más de 100 millones de dólares— manifiestan la importancia del alineamiento de la seguridad a las funciones y procesos empresariales, considerando como puntos clave a tener en cuenta para la convergencia de la seguridad y negocio:

- La rápida expansión del ecosistema de la empresa.
- El valor de la información (activos intangibles).
- Las nuevas tecnologías de protección.
- Las nuevas normas y regímenes reguladores.
- La necesidad de reducir costes.

Éstos y otros puntos están modificando los conceptos generales de la seguridad, básicamente están forzando al cambio en el papel que desempeñan los profesionales de seguridad al otro lado de la cadena de valor, alineando sus actividades a las del negocio para mejorar el valor de la empresa. Por todo ello, cada vez más los responsables de Seguridad reconocen la necesidad de extender sus funciones a toda la organización, más allá del ámbito de los sistemas y tecnologías de la información[1]. Un incidente reciente en el Sumitomo Mitsui Bank de Londres, en el que unos hackers intentaron robar 220 millones de libras, pone de manifiesto esta necesidad, aunque el banco tenía fuertes medidas de seguridad en TI, ocurrió un fallo en la seguridad física, suplantaron la identidad de los conserjes para poder instalar unos dispositivos que les permitieron obtener información sobre los inicios de sesión. Esta situación enfatiza la necesidad de unir todos los elementos de seguridad con un enfoque global a toda la organización.

En el panorama actual, la aparición de comités de evaluación de riesgo ha contribuido a detectar el impacto e incremento del riesgo empresarial a nivel de negocio. La seguridad, cada vez más, se está viendo como un elemento que aporta valor y numerosas ventajas competitivas.

Para que la convergencia entre seguridad y negocio sea eficaz, la seguridad debe extenderse a personas, procesos y tecnología desde una perspectiva que englobe todas las actividades de la organización, lo que permitirá identificar, prevenir y responder a cualquier tipo de amenaza.

La seguridad no debe verse desde una perspectiva unitaria —elementos y acciones de seguridad por separado—, porque las consecuencias ante un fallo y/o vulnerabilidad pueden ser catastróficas. Tres días fueron suficientes para que el virus de correo electrónico Mydoon[2] se extendiera a más de 200

[1] Watson, James. "Physical and IT Security Must Go Together", Computing, may 4, 2005. http://www.vnunet.com/computing/news/2071716/physical-security-together

[2] Herman, Wendy. "Network Security-Trusted Communications." Nortel Networks. http://www.nortel.com/corporate/pressroom/feature_article/2004d/10_25_04_security.html

Para que la convergencia entre seguridad y negocio sea eficaz, la seguridad debe extenderse a personas, procesos y tecnología desde una perspectiva que englobe todas las actividades de la organización, lo que permitirá identificar, prevenir y responder a cualquier tipo de amenaza.

países y ocasionase unas pérdidas aproximadas de 22,6 billones de dólares, el virus de correo electrónico I Love You[3] afectó a miles de empresas y 45 millones de ordenadores causando pérdidas aproximadas de 2,1 billones de dólares. Además de los gastos a los que las compañías tienen que enfrentarse para solucionar los efectos ante un fallo, vulneración o catástrofe inminente, también pueden causar, a medio o largo plazo, daño sobre la imagen y reputación de la marca.

La convergencia de seguridad está impulsando a las empresas a tener una visión más allá de las dimensiones funcionales para poder incluir todos los elementos de seguridad dentro de un mismo ciclo de vida, creando la necesidad de disponer de una base sólida y unificada que incluya a las personas, procesos y estrategias, y la prevención, detención, respuesta y recuperación ante cualquier fallo, amenaza o vulneración.

La mayoría de las empresas se están dando cuenta de la necesidad que tienen de abandonar la visión actual, sobre funciones y elementos individuales del ciclo de vida de la seguridad, para centrarse en el ciclo de vida de seguridad global de la empresa y del negocio. Llevar a cabo esta transformación puede incrementar la ventaja competitiva de la organización.

Juan Luis Iglesias [Director de Sistemas de DAEMON QUEST]

[3] Paul Festa and Joe Wilcox, Experts estimate damages in the billions for bug. http://news.com.com/2100-1001-240112.html

El Centro de Alerta Temprana sobre Virus y Seguridad Informática llega al INTECO

La seguridad informática es una de las áreas prioritarias dentro del Plan Avanza 2006-2010 (www.planavanza.es) con el que el Gobierno busca alcanzar la convergencia con Europa y entre las Comunidades Autónomas en cuanto a desarrollo de la Sociedad de la Información. La seguridad es uno de los elementos que contribuyen al fomento de la e-Confianza entre ciudadanos y empresas. Este objetivo es precisamente una de las prioridades del Centro de Alerta Temprana sobre Virus y Seguridad Informática, creado en la empresa del Ministerio de Industria Turismo y Comercio Red.es (www.red.es), e integrado ahora en el Instituto Nacional de Tecnologías de la Información (INTECO) (www.inteco.es).

El Centro lleva trabajando en este ámbito desde hace varios años en los que ha logrado convertirse en centro de referencia de habla hispana en materia de Seguridad Informática. Sus actividades se verán reforzadas a partir de ahora con su integración en el INTECO, filial de Red.es, y con la creación del Centro Nacional de Respuesta a Incidencias en Tecnologías de la Información en el seno del propio Instituto.

Actuaciones

Para generar en la sociedad la confianza necesaria para el desarrollo de las Tecnologías de la Información y la Comunicación (TIC), en general, y de Internet, en particular, el Centro ofrece:

- Servicios como informes gratuitos distribuidos a través del correo electrónico.
- Información detallada y estadísticas en la página web: alerta-antivirus.red.es.
- Herramientas gratuitas de ayuda al usuario para protegerse tanto de virus y software malicioso como de otras prácticas fraudulentas a través de la red.
- Foros de discusión, buzones de consulta y sugerencias, información a través de las páginas de Teletexto y alertas en el IRC-Hispano.
- Además, el Centro de Alerta Antivirus colabora con la comunidad php-nuke, y cuenta con una red de sensores integrada por más de 80 agentes.

Más de 2.500 millones de correos procesados

Actualmente el Centro es capaz de procesar, a través de la red de sensores, unos siete millones de e-mails diarios, lo que supone aproximadamente el 8% del correo electrónico nacional. La red está compuesta por más de 80 agentes, entre los que se incluye la Administración Central (ministerios, el Senado, etc.), las Comunidades Autónomas, ayuntamientos, diputaciones, juntas, etc., y la Red Académica

Universitaria RedIRIS, así como empresas privadas proveedores de servicios de Internet.
De esta manera, la red de trabajo genera unas series estadísticas: diarias, semanales, mensuales y anuales que en el último año se traducen en más de 2.560 millones de correos procesados. La media de detección de correos infectados de virus informáticos se sitúa en la actualidad en un 5,5%, lo que da una buena razón para continuar con esta labor.

Información, el mejor antivirus

El Centro de Alerta Temprana sobre Virus y Seguridad Informática insiste en que el mejor antivirus es la información. Conocer unas normas básicas sobre Seguridad Informática y estar al día de las incidencias que se producen es la mejor manera de evitar, y resolver si se plantea, cualquier incidencia.
Por esta razón, el Centro envía sus alertas gratuitas a los más de 225.000 usuarios que se han suscrito a este sistema. La información de seguridad se distribuye tanto mediante fuentes RSS —que además pueden incluirse en cualquier página web—, como por correo electrónico, en forma de alertas y de informes. Hasta el momento 115.000 usuarios reciben avisos cuando se producen incidencias puntuales sobre virus muy peligrosos (mydoom, blaster, sasser, bagle, sober, etc.) y oleadas de *phising* (correos con los que se pretenden obtener ilícitamente datos bancarios de los internautas). En cuanto a los informes, 110.000 suscriptores reciben diariamente datos sobre los alias y descripción de los virus, links a páginas de Seguridad Informática, boletines de seguridad, conferencias, nuevas secciones, etc.
La información se difunde también en televisión, a través del Teletexto —con presencia en TVE1, La 2, Antena 3, Tele 5 y en las cadenas autonómicas—, y en el chat IRC Hispano. El sistema permite alertar a entre 15.000 y 20.000 usuarios conectados. A través de la colaboración con la comunidad php-nuke, más de 500 sititos web ofrecen los datos del Centro de Alerta Antivirus en dos módulos de información: virus informáticos y vulnerabilidad de aplicaciones.

Útiles gratuitos

La información y documentación sobre Seguridad Informática que se envía en estas alertas está también disponible en la web del Centro, que da acceso además a una base de datos de vulnerabilidades y parches, y a herramientas y útiles gratuitos para prevenir los principales riesgos de la red.
La página cuenta con más de 500.000 visitantes mensuales que provienen de España, Hispanoamérica, Estados Unidos y Europa. En los casi cinco años de historia, la página ha sido visitada por más de 13 millones de usuarios.
Entre las herramientas a las que da acceso la página del centro se cuentan cortafuegos y antivirus gratuitos y antivirus en línea. Con esta última sección se ofrece al usuario la posibilidad de revisar su equipo sin necesidad de instalar ningún programa en su ordenador. El antivirus se ejecuta directamente desde alguna de las direcciones web a las que da acceso alerta-antivirus.red.es. En caso de que se detectara la presencia de algún tipo de software malicioso, puede recurrirse a la sección especializada en herramientas gratuitas de desinfección.

Anti-fraude

Para combatir el fraude en Internet, se ofrece en primer lugar una explicación detallada de los principales sistemas empleados: *phising, pharming y key-loggers.*
En el caso del *phising* (el intento de obtener información personal principalmente de acceso a servicios financieros), se proporcionan algunos consejos para distinguir correos y webs falsas, así como herramientas que permiten medir el grado de seguridad que ofrece cada página. De esta manera se ayuda también a combatir el *pharming,* es decir, la redirección de la página solicitada por el usuario a otra predeterminada por el atacante, en la que se pedirá al usuario que introduzca sus datos. Para evitar los *key-loggers,* una subclase de "troyanos" que registran las pulsaciones efectuadas sobre el teclado para robar información, el Centro recomienda la emplear antivirus actualizados.
El Centro también facilita herramientas gratuitas contra el *spam,* las ventanas emergentes y los marcadores, así como escaneadores de puertos y tests de velocidad.

Instituto Nacional de Tecnologías de la Información
Mayo de 2006

Argumentos

La seguridad en sentido amplio, es decir, empresarial tal y como yo lo entiendo, no es un tema sencillo de tratar. Cuando nos reunimos responsables de Sistemas de Información, nuestra tendencia natural es considerar la seguridad desde una única perspectiva y, sin embargo, cuando nos encontramos en el Comité de Dirección, surgen inevitablemente las consecuencias de dicha perspectiva en forma de incomprensión, más o menos generalizada, ya que quizás sea por la historia de la propia tecnología y nuestra actitud centrada en los sistemas, ya sea porque aunque los departamentos de Sistemas de Información tenemos la obligación de saber casi de todo y los demás sólo de negocio (su) —la tecnología para los tecnólogos—, lo que en definitiva debería verse como una actitud de compañía se ve como una actividad centrada en los Sistemas de Información.

Emilio Casalduero de Alfaro, durante el seminario celebrado el pasado 14 de marzo en el salón de actos del museo Thyssen-Bornemisza.

Esta situación respecto a la seguridad no es única. Si tenemos en cuenta la adaptación a las diferentes legislaciones, LOPD pongamos por caso, o incluso planes de contingencia de negocio, parece que todo puede resolverse acudiendo a los Sistemas de Información, pero es de todos conocido el que cuando se aborda cualquiera de los aspectos antes mencionados como ejemplos, la intervención de negocio es previa, y absolutamente necesaria en la fijación de la política, a la adopción de cualquier medida técnica con realmente pocas excepciones en las que los departamentos de Informática pueden y deben decidir sus políticas.

Así, si consideramos todos los esfuerzos que realizamos en una compañía para resolver los múltiples problemas derivados de la necesidad de compatibilizar el negocio con su entorno, un aspecto queda de manifiesto si simplemente hacemos una lista de los proyectos que tenemos en marcha, dibujamos a qué área de negocio afectan y ponemos en común su objetivo final: proyectos hay muchos, pero objetivos de negocio hay pocos; y si nos paramos a ver qué recursos estamos utilizando, otro aspecto salta inmediatamente a la palestra: para un mismo objetivo tenemos diferentes grupos de trabajo e, invariablemente, formados casi por las mismas personas.

El por qué esto ocurre probablemente debamos buscarlo en los propios organismos rectores de las compañías a su más alto nivel, responsables de la definición de la estrategia de la misma y su plasmación efectiva en cualquier tipo de documento que especifique sus líneas maestras, en el supuesto, claro está, de que reconozcamos que la seguridad es un aspecto de la gestión de índole corporativa y no departamental. Mi criterio en este sentido es que existen una serie de aspectos que se deben de tener en cuenta desde una perspectiva claramente de la alta dirección, es decir, estratégica, entre los cuales se encuentra la seguridad, entendida ésta en su sentido más amplio y considerando entre sus objetivos la propia continuidad de negocio: la seguridad y todos sus mecanismos no los debe establecer una compañía porque la LOPD, por

ejemplo, lo exija[1]—en los aspectos de custodia de los datos de índole personal de sus clientes y su relación con ésta—, sino porque en el entorno actual en que una empresa se encuentra cualquier atentado, interno o externo a su entidad, constituye siempre un peligro potencial a su existencia.

Si una organización no tiene clara su estrategia, si no tiene esta estrategia plasmada en procesos y si estos procesos no están relacionados con los Sistemas de Información en cuanto a "que proceso que servicios lo soportan" y si estos servicios no tienen asociada la mejor arquitectura, de hardware, software y comunicaciones, creo que es francamente difícil hablar de seguridad corporativa, y si —y únicamente— de seguridad en aspectos parciales con el despilfarro de recursos y esfuerzos descrito.

Comenzando por la parte más alta de la pirámide, yo abogaba por la necesidad de la existencia del Balanced Scorecard, aunque lo mismo podría haber abogado por EFQM (aunque lo conozco menos) o cualquier otro método de gestión de orientación a la estrategia. La importancia de cualquiera de estos métodos, los más comunes a mi entender en las organizaciones, es que establecen de una manera intuitiva la relación de las acciones con los resultados —obligando a medir y no considerando en ningún caso aquellos aspectos que no se puedan medir—: las cosas, como dije en mi exposición, se hacen para algo y un aspecto significativo de la propia estrategia que no debiéramos olvidar es la sujeción a las leyes, no sólo por su carácter regulador, sino, y en este caso importante, por ser uno de los mecanismos de defensa con los que cuenta nuestra sociedad. Continuando con el razonamiento, una estrategia se materializa en procesos: para hacer algo, para conseguir un objetivo, las cosas se efectúan de una determinada manera y no de otra, y al final, pero no en último lugar, existe el soporte de los Sistemas de Información a los procesos, resolviendo de manera más o menos eficaz su misión de alinear la técnica con el negocio. Una organización que se oriente en su operativa a procesos —definidos seguro que están, pero descritos al menos en sus líneas maestras es lo exigido— no sólo está más preparada para saber dónde tiene que actuar para su optimización o cambio de acuerdo a las condiciones del entorno, también está mucho mejor preparada para aislar todas aquellas situaciones que presenten un peligro potencial, y evaluar su impacto, estableciendo los mecanismos de seguridad adecuados y los controles de esa misma seguridad —y de ahí la importancia que di a nuestros departamentos de Auditoría Interna en una, no la única, de sus misiones más actuales, cuya labor bajo esta perspectiva se simplifica sobremanera—.

Vayamos ahora con los Sistemas de Información (SI). Si consideramos un proceso, no una aplicación, siempre es posible definir qué servicios conlleva, y la misión de SI es dotar a dicho servicio de la infraestructura necesaria de acuerdo a lo crítico que dicho servicio sea en el proceso al que da soporte, criticidad que en ningún caso la tiene el servicio en sí mismo (disponibilidad, tiempo de recuperación, salvaguarda o posibles ataques a su integridad, etc.), sino, y es necesario insistir, la criticidad que tenga el proceso del que es soporte, proceso a su vez definido por la estrategia de la empresa. Creo que esto es lo que significa alinear tecnología y negocio en el sentido de su contribución a la eficacia y eficiencia de un proceso y de su contribución, como consecuencia, a la estrategia corporativa. Obviamente, contribución significa medir, por lo que los indicadores que se pueden establecer en SI no miden (no deberían) aspectos por sí mismos, sino en función del servicio; no se trata de establecer como objetivo el 99,99% de operación de la máquina X, sino del admitido por el negocio (que a lo mejor es del 55%) del servicio Y prestado por la máquina X o de la infraestructura en su conjunto asociada al servicio Y. No se trata de que las copias de seguridad salven todo (¡cuánto podríamos ahorrar en almacenamiento!), sino aquello necesario y con la cadencia necesaria. No olvidemos además que cualquier daño que ocurra como consecuencia de un atentado a la seguridad debe ser perfectamente evaluable a los efectos judiciales pertinentes, y que esta evaluación debe ser previa al incidente —es decir, tiene que estar medida— y no posterior.

¿Qué podemos hacer —si estamos de acuerdo con la exposición hasta ahora— como responsables de los Sistemas de Información de nuestras compañías? Pues desde luego no es una buena actitud la de, ante

[1] Aunque también, claro está.

la necesidad de alinear (o armonizar o sincronizar) la tecnología y el negocio, refugiarnos en nuestra soledad e intentar actuar solamente en aquellos aspectos en que nos consideramos maestros. Como directores de un departamento, eso es lo que debemos hacer, pero como directores de una corporación no. Como directores de una corporación, nuestra obligación es contribuir a la eficacia y eficiencia de los procesos y al desarrollo de la estrategia corporativa. ¿Cómo?, pues con argumentos que pongan de manifiesto que esta forma de plantear la gestión —si así se acepta— puede ser una forma razonable de resolver algunas de las incongruencias que afectan a nuestro trabajo.
Por paradojas de nuestro mundo actual, nuestras corporaciones están manejando conceptos que pertenecen a nuestro acervo cultural técnico desde hace años, estando quizás mejor preparados no sólo para manejarlos con soltura, sino, y lo que es más importante para lo que nos ocupa, para enseñarlos.
No deja de ser divertido el que los diagramas de flujo sean una forma de expresión manejada a diario y que nuestra obsesión por la medida sea ahora una necesidad corporativa —entre otras habilidades y conocimientos que podría nombrar—. Por tanto, si tenemos el conocimiento es obvio que debemos potenciar nuestra actitud aprendiendo a ejercitar nuestra paciencia, dejando de actuar como si lo que decimos fueran verdades absolutas. Quienes nos escuchan y comparten con nosotros la difícil labor de dirección quizás necesiten que les expliquemos, que les enumeremos, aquellos aspectos de nuestra labor que no son sencillos de comprender para llevar a su ánimo la importancia que tiene para nosotros el que ellos, a su vez, se expliquen, nos escuchen y nos ayuden, todo esto teniendo como marco y directrices las que la propia estrategia de la compañía dicta.
Nuestro trabajo como responsables de SI, que consideramos habitualmente muy creativo, está, por esta misma razón, sujeto a que manejemos de la forma más hábil posible las restricciones que conlleva; y una forma muy correcta de hacerlo es introducir no inteligencia, todo el mundo la tiene —en el supuesto de que sepamos qué es—, sino comportamientos inteligentes, menos común pero que sí que sabemos que es, en nuestra actuación como directivos[2].
Me permitiréis, como conclusión, unas palabras que completen el esquema ya tratado y relativo a la defensa frente a las amenazas con las que una empresa se enfrenta en su entorno. Además de las leyes, existe otro conjunto de mecanismos de defensa que, por no ser obligatorias, o en todo caso dan un poco de prestigio cuando su logotipo se coloca en los documentos o aparece como una referencia en la memoria anual de la compañía, quizás les prestemos menos atención que la debida —y que represente en la intervención con un oscuro cuadro de Van Gogh—.
Estas normas deberíamos aprender a verlas (¡qué difícil es abstraerse del significado histórico de las palabras!) como ayudas importantes para nuestras organizaciones, reconociendo la labor de los diferentes grupos de trabajo que en su definición y difusión participan, entre ellos los de nuestra asociación, trabajando —recordemos, argumentos— para que se aprecie su importancia como una oportunidad real de mejora, e igualmente prestando nuestro tiempo con la adhesión a uno de estos grupos que están realizando una gran labor por nosotros y para nosotros.
Y ahora unas breves notas sobre el *making off*. Me causó una enorme impresión. En la exposición Rembrandt/Caravaggio, que se encontraba en el Van Gogh Museum en Ámsterdam, estaba el cuadro de Caravaggio *La conversión de María Magdalena* y mientras que la audioguía desgranaba la explicación y contemplaba absorto la obra, decidí que dicho cuadro se convertiría en el eje de una exposición que debía realizar, también en otro museo, el Thyssen-Bornemisza de Madrid, con nuestra asociación AUTELSI un par de semanas después. Una visita, pocos días más tarde de la estancia en Ámsterdam, al Thyssen-Bornemisza me convenció para, aplicando el dicho de que "una imagen vale más que mil palabras", ilustrar la presentación con imágenes de cuadros pertenecientes tanto a museos de Madrid, como los recientes de Ámsterdam que había visitado.

Emilio Casalduero de Alfaro [Director de Informática de Fórum Filatélico]

[2] Aplicando dos conceptos que J. A. Marina describe muy bien en sus extraordinarias obras: manejo hábil de las restricciones y comportamiento inteligente. Un comportamiento inteligente no es el que actúa, sino el que actúa para algo, con un fin, a largo plazo y sin dejarse llevar por las recompensas inmediatas.

Clausura del seminario "Seguridad y Negocio"

El 14 de marzo de 2006 en el salón de actos del museo Thyssen celebramos el seminario: "Seguridad y Negocio: Experiencias y Claves para Directivos", organizado por el Grupo de Trabajo de Seguridad de AUTELSI.

Ramón Palacio, Director General de Red.es, y Leandro Pérez Manzanera, Presidente de AUTELSI, en el acto de Clausura.

AUTELSI reunió a 150 directivos (directores generales, directores de Recursos Humanos, directores financieros...) y responsables de la Gestión de Seguridad de sus empresas.
En palabras del Presidente de AUTELSI, Leandro Pérez Manzanera, durante el acto de Clausura, esta jornada cumplió con el objetivo autoimpuesto por la asociación de difundir los conocimientos sobre Tecnologías de la Información y Comunicaciones, abundando en un tema de rigurosa actualidad cuya importancia ha quedado patente en la encuesta de CIOs de AUTELSI, realizada en el último año: la Seguridad.
Clausuró el acto Ramón Palacio, Director General de Red.es, que animó a todos los presentes a aplicar las claves ofrecidas durante la jornada en torno a la gestión de seguridad, tema que

Tras las exposiciones, durante hora y media, se estableció un coloquio con todos los ponentes.

considera esencial para el desarrollo de la Sociedad de la Información, señalando que: "AUTELSI es el único foro que yo conozco que permite compartir experiencias y proponer iniciativas en las que participan las empresas TI, los operadores y los usuarios empresariales de este país".

ACTIVIDADES

espacio autelsi

Es una iniciativa que tiene por objetivo ser un foro de encuentro en el que los profesionales de las TIC podamos compartir nuestros objetivos, problemas, inquietudes y prioridades. El "espacio autelsi" contará con un programa profesional, que incorporará la celebración del XIV Congreso AUTELSI, centrado este año en dos temas de máxima actualidad e interés como son la convergencia de las TIC y la agenda del CIO. Este programa profesional se completará con actividades culturales y deportivas diseñadas para los asistentes y sus acompañantes.

Workshop 2006

El interés mostrado por los asociados ha provocado el realizar en octubre un Workshop interactivo sobre aplicaciones IP. En estos momentos hay un interés máximo sobre qué elegir, para ello tendremos a los más importantes fabricantes, operadores e integradores del mercado español.

Foro para el debate sobre el desarrollo de la Sociedad de la Información

Bajo esta denominación se puso en marcha en mayo, con carácter bimestral, un ciclo de desayunos impulsados por la Comisión de Desarrollo de la Sociedad de la Información AUTELSI, con el objetivo de crear un foro de opinión en los temas relativos a la Sociedad de la Información. Más información: www.autelsi.es.

XIX Encuentro del Grupo de Trabajo CC. AA.-AUTELSI

Siguiendo con los encuentros que AUTELSI organiza conjuntamente con las Comunidades Autónomas, los días 25 y 26 de mayo tuvo lugar en la ciudad de Barcelona el XIX Encuentro del Grupo de Trabajo CC.AA.-AUTELSI.

Grupo de Trabajo para la Seguridad de la Información (SETSI)

Como parte de las actuaciones previstas en el área de "e-Confianza" del Plan Avanza, se ha constituido un Grupo de Trabajo para la Seguridad de la Información. AUTELSI, participa de manera activa en este grupo cuya misión principal es la de asesorar y colaborar con la Dirección General para el Desarrollo de la Sociedad de la Información para potenciar las actuaciones previstas en el Plan Avanza 2006 y en la definición de futuras actuaciones.

PUBLICACIONES

"Elementos Básicos para una Ciudad Digital"

Autor: Grupo de Trabajo de Ciudades Digitales de AUTELSI • **Edición:** Formato electrónico • www.autelsi.es

El Grupo de Trabajo de Ciudades Digitales, de AUTELSI ha elaborado esta guía para abordar un proyecto de ciudad digital. Se recogen sus reflexiones sobre la definición de ciudad digital, haciendo un análisis de los principales proyectos ya desarrollados y, a continuación, se plantea el debate sobre las infraestructuras mínimas y los servicios básicos que se necesitan y ofrecen en un entorno de ciudad digital.

"AUTELSI-Portal PYMES"

Autor: Grupo de Trabajo Pymes de AUTELSI • **Edición:** Formato electrónico • www.autelsi.es

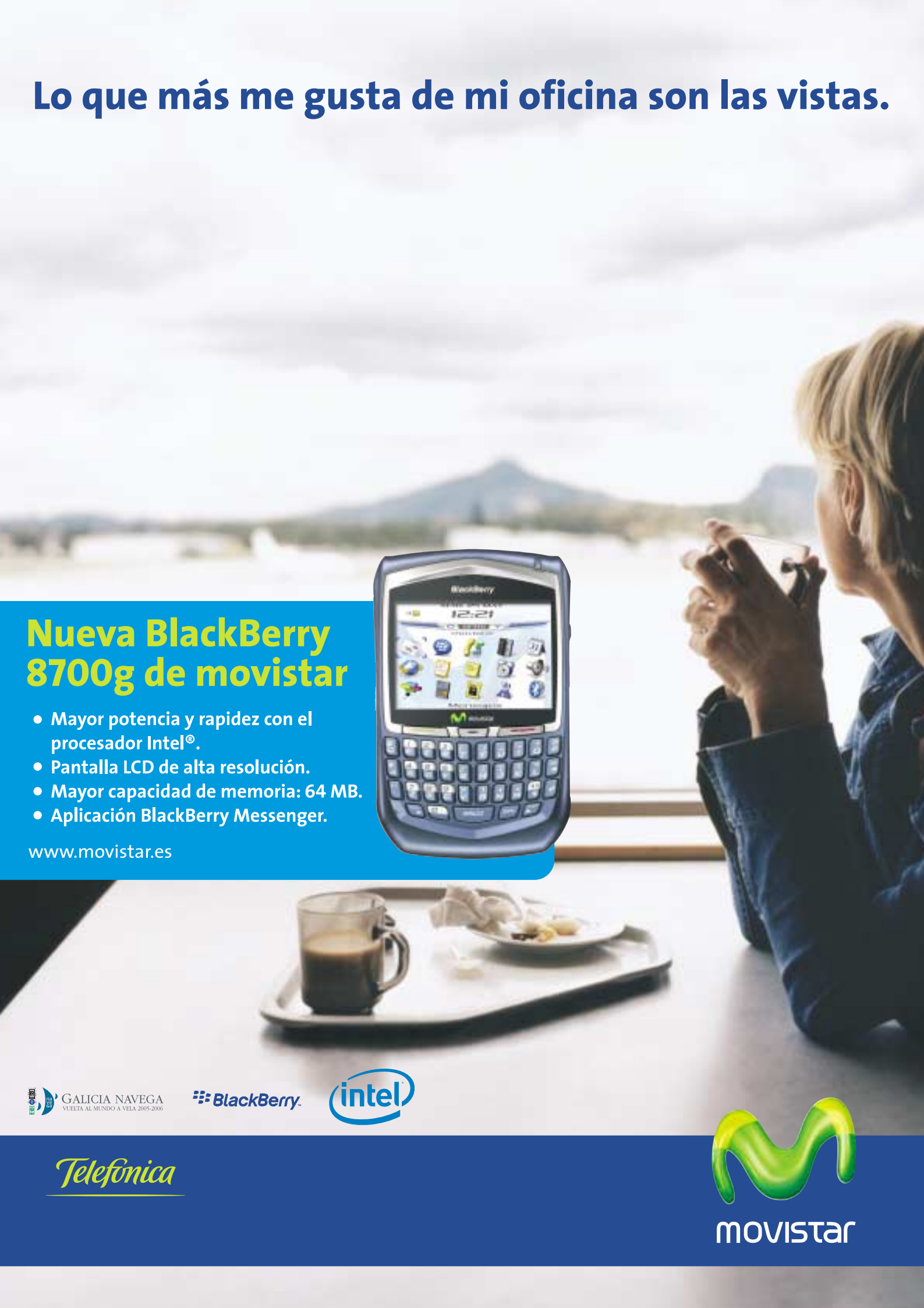
El Grupo de Trabajo PYMES de AUTELSI ha concluido el desarrollo del cuestionario web, que permitirá a las pymes conocer su estatus tecnológico, su nivel respecto a otras empresas de su sector, a la vez que disponer de la información de los asociados AUTELSI, a través de un catálogo de soluciones que éstos ofrecen.

"Guía de Mejores Prácticas de Comercio Electrónico"

Autor: Grupo de Trabajo de Comercio Electrónico de AUTELSI • **Edición:** Formato electrónico • www.autelsi.es

Elaboración y publicación de una *Guía de Mejores Prácticas de Comercio Electrónico* que incluye una guía en el ámbito B2B *(Business to Business)* y otra en el ámbito B2C *(Business to Consumer)* con el objetivo de orientar a los directores generales de las pymes en sus proyectos de comercio electrónico.

Lo que más me gusta de mi oficina son las vistas.



Nueva BlackBerry 8700g de movistar

- Mayor potencia y rapidez con el procesador Intel®.
- Pantalla LCD de alta resolución.
- Mayor capacidad de memoria: 64 MB.
- Aplicación BlackBerry Messenger.

www.movistar.es

GALICIA NAVEGA
VUELTA AL MUNDO A VELA 2005-2006

BlackBerry

intel

Telefónica

movistar