



De izda. a dcha.: José Manuel Huidobro, director de BIT; Jesús Sánchez, Responsable Comercial de la Administración Central de McAfee; Carlos Jiménez, Presidente de Secuware; María Campos, *Country Manager* de Stonesoft y Mario Arienza, *Systems Engineer* de Fortinet.

Seguridad, factor clave en las TIC

La seguridad en la Información se ha convertido en un elemento crítico hoy en día. Se trata de un factor que ha evolucionado de ser considerado como un gasto inevitable a una inversión clave que permite mantenerse en el mercado y garantiza el crecimiento de cara al futuro.

El avance de la tecnología móvil, con los teléfonos inteligentes, PDA y otros dispositivos que se están implantándose con éxito en el mercado, es un punto de inflexión para que se logre por fin una concienciación global de la seguridad, y se perciba como un elemento a integrar dentro de las organizaciones, y no sólo como un “parche” puntual en caso de ataque.

España es uno de los países más evolucionados en este campo, gracias, entre otras cosas, a la progresiva implantación del DNle (Documento Nacional de Identidad electrónico), similar al tradicional y cuya principal novedad es que incorpora un pequeño circuito integrado (chip), capaz de guardar de forma segura información y de procesarla internamente.

En esta mesa se han sentado para debatir sobre el futuro y la evolución del mercado de la “seguridad en la Información” cuatro de las principales empresas del sector en España.

bit ¿Creéis que las empresas, las Administraciones Públicas y los ciudadanos son conscientes de la importancia de la seguridad?

María Campos. Sí, existe una concienciación. Sin embargo, en este aspecto hay que hacer una distinción entre gran empresa y PYME.

Si nos comparamos con otros países, España está por detrás en una serie de comportamientos. Este es el caso de muchas de las grandes empresas españolas, que todavía no tienen un CSO (responsable de seguridad) y pocas elaboran planes directores de seguridad, de continuidad de negocio, de monitorización de la red, test periódicos de intrusiones, etc, aunque sí exista cierta implantación de productos.

Jesús Sánchez. Para mí sí existe esa concienciación y cada vez va calando más, tanto en cuenta privada como en la Administración Pública.

Por otra parte, en cuenta privada se suma una mayor estructuración en la articulación de un proceso de gestión de seguridad. En cuanto a la Administración Pública, esta menos estandarizada la figura del CSO / CSIO a nivel general en los diferentes organismos, recayendo esta responsabilidad en los responsables de sistemas y comunicaciones.

Además, la adopción cada vez más común de aspectos normativos (ISO 17799, 27001), y necesidades de cumplimiento regulatorio (LOPD; Basilea II, SOX y otros) están provocando una mayor concienciación respecto al desarrollo de Programas de Gestión de la Seguridad de la Información.

Carlos Jiménez. Pues yo pienso que no son muy conscientes del proble-

ma. Intentan aplicar los mismos criterios de la vida normal a la protección de sistemas informáticos y no se dan cuenta que un ordenador funciona mil veces más rápido que una persona y, por tanto, para cuando se quieran dar cuenta de un ataque de Internet es probable que hace muchos microsegundos que se haya terminado.

Por todo ello es muy importante la prevención y no aplican ese mismo criterio porque están acostumbrados a una política reactiva, a reaccionar cuando pasa algo. Hay que tener una mayor concienciación en prevención de la que hay actualmente.

Corporación, PYME y Administración Pública

bit ¿Hay que hacer una distinción importante en este sentido entre la empresa privada y la Administración Pública?

Carlos Jiménez. La Administración Pública en base al despliegue del DNI electrónico ha hecho un esfuerzo de actualización en todos sus sistemas, pero sobre todo mejora la identificación. Hoy en día se pueden hacer muchos trámites que hace un año no se podía hacer, pero esto no se hace en aras de la seguridad sino de cara al ciudadano.

También pienso que hay una gran diferencia entre una gran empresa y una PYME. En el caso de la segunda, suele creer que con un antivirus, un *firewall*, etc. se resuelve toda la problemática, cuando habría que enfocarlo en mejorar la formación y la educación de los responsables.

Mario Arienza. Para mí hay claramente tres velocidades y se marcan por el uso de las Tecnologías de la Información en la empresa. Por un

lado estarían la gran cuenta, banca y grandes nombres de la industria, donde la seguridad está consolidada. Después, estaría la Administración Pública, que sería la velocidad intermedia y poco a poco van adoptando más medidas de seguridad.; bajo mi punto de vista goza de buena salud.

Ya por último, se encontraría la PYME, aquí te encuentras un amplio espectro. Hay algunas que están concienciadas porque tienen una cultura tecnológica propia y puedes encontrar desde un CSO hasta equipos dedicados a la seguridad, y luego están otros que, por no haber adoptado la tecnología como herramienta para fomentar su negocio, tampoco han adoptado la seguridad.

Para mí la implementación de la tecnología y la adopción de medidas de seguridad casi van de la mano.



Jesús Sánchez

“La solución en una segunda etapa es controlar a aquellos que tienen el acceso, tanto a través de la Red como de soportes físicos”



María Campos

“Seguridad y continuidad de negocio son dos conceptos completamente indisolubles”

Factores críticos

bit Desde vuestro punto de vista, ¿qué factores consideraréis más críticos para la seguridad de la Información?

Jesús Sánchez. Tal vez el factor crítico a la hora de desarrollar el programa de seguridad sea conocer qué seguridad se necesita. Es decir, conocer tus activos críticos para el negocio, y la infraestructura IT que soporta los procesos es vital, para saber la repercusión en la operativa de tu negocio de cualquier impacto que se pueda tener sobre esos activos y, por tanto, poder identificar las medidas necesarias.

Todos estos factores, al final, te llevan a saber el nivel de riesgo y evaluar las medidas que lo mitiguen a umbrales aceptados por la organización. Hablar de seguridad sin saber lo que necesitas en función de cómo se ve afectado el negocio es caminar sin rumbo. La adopción de tecnología, de manera previa a saber

las medidas de seguridad que tienes que adoptar, ha derivado en decisiones erróneas.

Carlos Jiménez. Yo estoy de acuerdo. Hay que detectar los puntos críticos de la organización, que son aquellos sin los cuales no podría funcionar el negocio, porque no se puede aplicar seguridad a todo por igual.

Existe una cultura desde hace años en la que el usuario se siente unido a la máquina, pero hay que tener en cuenta que el negocio está compuesto de muchas de esas máquinas unidas. El problema es que la seguridad sigue sin formar parte del diseño.

María Campos. Yo creo que es necesaria la integración de la seguridad en la organización de la empresa a todos los niveles. Es decir, no hay que percibir la seguridad como un proceso aparte.

Así, del mismo modo que las Tecnologías de la Información nos habilitan las relaciones comerciales y la expansión de los negocios, la seguridad debe ser un proceso clave en todas esas relaciones.

Mario Arienza. Desde mi punto de vista, la seguridad es adoptada de forma reactiva. Primero está el gran principio de seguridad que es “no hay que gastarse en proteger tu inversión más de lo que la inversión te va a producir” y muchas veces eso lleva a la dejadez, hasta acabar con sistemas vulnerables.

También hay que hacer énfasis en las políticas de seguridad. Los sistemas deben estar diseñados de manera que se adapten en la organización y que incluyan la seguridad como parte del diseño.

Probabilidad y riesgo

bit ¿Es rentable invertir en seguridad? ¿Qué opináis de la seguridad en red y la continuidad del negocio, en cuanto a gestión del riesgo?

Carlos Jiménez. La probabilidad del riesgo no se puede medir, porque es algo muy impulsivo, igual no te han atacado nunca y de pronto sucede un día. Esto obliga a prevenir basándose en las partes críticas del negocio, aquellas que hacen que no funcione si se paran.

En el caso de un ataque informático por Internet, el problema es que la diseminación de ese ataque puede producir muchísimos daños y la suma ser tan importante como una agresión específica.

María Campos. Desde mi punto de vista, seguridad y continuidad de negocio son dos conceptos completamente indisolubles. Tan importante es permitir a las personas adecuadas acceder a los recursos a los que están autorizadas como permitir eso en el momento oportuno.

Evidentemente esto dependerá del perfil de empresa y del tamaño. Entre la PYME está muy difundido el concepto de que no necesitan seguridad o “cuando tenga un problema reaccionaré”, y son minoría aquellos que apuestan por la prevención.

Sin embargo, en este mundo, cada vez más globalizado y con fronteras de trabajo menos definidas gracias a la movilidad, con necesidades de acceso no sólo de los empleados sino de los socios y clientes, el tener un sistema caído durante minutos supone una pérdida de dinero importantísima. Por eso no se entiende la seguridad sin asociarla a la continuidad, fiabilidad y alta disponibilidad.

Mario Arienza. Quizá la clave sea los planes directores de seguridad y el enfoque que se hace de ellos. Hay que darse cuenta que también es seguridad cuando un sistema deja de funcionar, es decir: el plan de contingencia o el plan de continuidad de negocio ha de estar dentro del plan director de seguridad.

Seguridad es todo aquello que nos hace parar, bien sea por causas externas debido a un ataque que nos haga un tercero o por causas internas, paradas de servicio que están asociadas a la tecnología en sí. Por eso el plan director tiene que ampliar sus miras.

Jesús Sánchez. La continuidad del negocio es uno de los dominios dentro del ámbito de la gestión de seguridad.

Es importante realizar un análisis de riesgo en el que se incorporen probabilidades e impactos, que en algunos puntos es prácticamente incalculable, como es el caso del ataque de un *hacker*. No obstante el análisis del riesgo nos permite tener un inventariado de activos, que no se ciñe a un servidor, un *router*, etc. El activo es en primera instancia la información y los procesos, y éstos están sustentados en tecnología. Por eso hay que incidir en los controles necesarios para alinear la seguridad con el negocio.

La seguridad como factor integral

bit Se entiende que no hay que considerar, por tanto, la seguridad como una parcela independiente...

Jesús Sánchez. Si tomamos en cuenta las normativas de referencia (ISO 27001) y los controles que debe incluir un Sistema de Gestión de la Seguridad de la Información (SGSI), estos son de ámbito jurídico, de ges-

ción y técnicos, por los que la seguridad afecta a todos los ámbitos de la organización.

En el caso de los técnicos, representan aproximadamente un 55% del total de los controles y algunos cubren las tres facetas.

bit ¿Es importante basarse en estándares de planificación y gestión de seguridad o es preferible que cada empresa lo haga a su medida?

Mario Arienza. Si siguen ciertas recomendaciones el problema quizá sea la unificación. Creo que en este momento no hay una unidad como tal.

Si nos adscribimos al panorama de la gran empresa y la normativa ISO tenemos una vía clara. Aunque en el momento que llegamos al mundo PYME es mucho más complejo implementar todas las medidas, porque son demasiado complejas para la operativa del día a día. En este sentido hay una serie de normas pero no queda claro las que imperan sobre otras. Por eso no hay unidad, por lo menos en la pequeña y gran empresa.

bit Supongo que en el ámbito de la Defensa la normativa sobre seguridad será distinta...

Carlos Jiménez. No creo que surja por la necesidad, ni por una interiorización de la misma, sino porque es una norma impuesta y hay que cumplir con la Ley.

Pero se puede dar el caso de que haya quien prefiera pagar la multa y eso es por falta de conciencia.

Es parecido al carné por puntos. En realidad deberías ser prudente al conducir porque te puedes matar, no porque te vayan a quitar luego los puntos. Creo que hace falta interiorizar más la necesidad de seguridad.

María Campos. Yo estoy de acuerdo, pero también creo que es necesario un marco de referencia. Así que, en mi opinión, hemos tenido una evolución muy positiva, porque se ha pasado de un Código de Buenas Prácticas a la ISO en sí.

Al final todas estas regulaciones funcionan como catalizadores. Por eso, cuando analizamos las prioridades nos damos cuenta que la nº 1 siempre es cumplir con la normativa y legislación vigente, como la protección de datos, privacidad de la información, etc.

El problema de la fuga de información

bit Otro aspecto es la pérdida de datos y fuga de información. ¿Es significativo esta problemática de robo de información en las empresas?



Carlos Jiménez

“La probabilidad del riesgo no se puede medir, porque es algo muy impulsivo, igual no te han atacado nunca y de pronto sucede un día”



Mario Arienza

“La implementación de la tecnología y la adopción de medidas de seguridad casi van de la mano”

Carlos Jiménez. Hemos pasado en informática de una cultura en la que el usuario hacía lo que le daba la gana con el ordenador y podía llegar a cualquier tipo de información. Luego pasamos a intentar poner control a eso, pero todavía queda muchísimo por hacer.

Precisamente ahora tenemos los teléfonos inteligentes (*smart phones*) o incluso CD que tienen una capacidad de almacenamiento de varios GB y cualquiera se puede llevar en dos minutos un volumen de información que hace cinco años representaba el servidor completo. Así que existe esa necesidad de control, porque hoy por hoy se puede producir una fuga ingente de información.

María Campos. Estoy de acuerdo. De hecho yo creo que a día de hoy los mayores peligros potenciales y los mayores peligros existentes vienen de la red interna. Por eso los fabricantes estamos poniendo espe-

cial interés en la protección de Intranet. Porque ahora es fácil saltarse los perímetros que hemos estado construyendo durante tantos años y olvidarnos de lo que está pasando dentro.

Creo que las amenazas existentes dentro la red interna son incluso mayores a día de hoy que las que pueden venir desde el exterior. Por ello es donde tenemos que poner mayores esfuerzos, porque controlar el tráfico interno es uno de los mayores quebraderos de cabeza.

Mario Arienza. Yo coincido con esa opinión en que hoy por hoy es el gran reto. Hacer saltar los sistemas de seguridad desde el punto de vista tecnológico en que controlamos estados prácticamente binarios a sistemas que son capaces de protegerse con comportamientos heurísticos es hacia donde van todas las inversiones.

Hay que tener en cuenta que, en último término, las amenazas están siempre provocadas por personas y ese es el terreno que se debe proteger. Hay que securizar, pero desde un punto de vista más heurístico, lo cual es más difícil que un sistema de SI-NO. Este es el camino que empezamos a recorrer.

Dispositivo único de seguridad

bit ¿Cómo se podría implementar un Sistema de Gestión Integral de la Seguridad? ¿Es posible un único dispositivo que incluya cortafuegos de redes, prevención y detección de intrusiones en red y antivirus gateway?

Mario Arienza. Hay un punto de unión en tu empresa en el cualquier ataque externo puede ser recibido. Por eso hay que hacer especial énfasis

en protegerte de todo lo que pueda entrar. Pero no es un enfoque global sino seguridad perimetral.

Lo que se hace con los sistemas perimetrales, desde el punto de vista global, es proteger de todos los ataques que puedan entrar, enfocando la seguridad en el punto más crítico.

Un equipo con seguridad perimetral no protege internamente, por ejemplo: en el caso de ataque de un empleado de la propia compañía.

Jesús Sánchez. *Firewall*, antivirus, sistemas de prevención no dejan de ser sistemas diseñados para hacer una contención de impacto. Lo importante es la capacidad de las soluciones que proveamos para poder incorporarlas dentro de los procesos.

De esta forma, puedo decidir que necesito un control de Red y que, por tanto, hay que implementar una solución de control de intrusiones a la misma.

Probablemente todos los que estamos aquí podemos dar una solución para intrusiones de Red con pequeños diferenciales en los valores añadidos, pero el hecho de implementar un dispositivo de este tipo lo que hará será dar una serie de alertas y, por tanto, un trabajo. El diferencial de estos dispositivos vendrá cuando se puedan integrar dentro de los procesos.

En cuanto a la problemática de fuga de información, la tecnología está avanzando y las soluciones se implementaban en un principio controlando los controles de acceso. La solución en una segunda etapa es controlar a aquellos que tienen el acceso, tanto a través de la Red como de soportes físicos.

Identificación electrónica

bit En la actualidad se está intentando implantar masivamente en España el DNI electrónico, así como otros sistemas como: la firma electrónica, PKI (Public Key Infrastructure) y prestadores de servicio de certificación. ¿En qué manera contribuirán a mejorar la seguridad?

Carlos Jiménez. El e-DNI significa la posesión de la tarjeta con un *chip* que no se puede copiar ni duplicar, lo que garantiza es que no puede ser utilizado por otro fraudulentamente. Esto no pasa con el DNI corriente, que se puede falsificar. Es muy importante que cuando te lo quitan se puede denunciar y se invalida el *chip* para siempre. Por eso, si posees ese documento te permite identificarte con total seguridad y no existe ningún sistema mejor para esa finalidad.

La alternativa, es decir; la biometría, puede ser más cómoda, pero tu huella puede ser escaneada y, por tanto, copiada. Por eso yo creo que antes o después integrarán un *chip* en tu cuerpo para que lo tengas integrado, pero eso ya lo veremos dentro de muchos años.

Jesús Sánchez. Creo que en este caso hay mucho que agradecer a la Administración Pública por su tremendo impulso a favor del uso de una tecnología existente que hasta este momento estaba fracasando.

Yo creo que igual que en otros casos miramos a otros países, en este es encomiable el apoyo de la Administración para el uso del PKI (Public Key Infrastructure) en todos los mecanismos de identificación.

bit ¿Cómo se encuentra la industria española de seguridad y qué apoyos creéis que necesita?

Carlos Jiménez. Hay factores que ha permitido que España se desarrolle antes que otros países, por ejemplo: la lucha contra ETA. En EE.UU. no despertaron en este sentido hasta el 11-S. Otro punto sería el control de fronteras, ya que tenemos la más complicada del mundo, porque separa África de Europa.

Todos estos diferenciales ha hecho que España se desarrolle mucho en este aspecto. En la Plataforma Española de Seguridad (eSEC) hay 146 empresas nacionales, y muchas de estas empresas han conseguido exportar tecnología a otros países.

Resumiendo, yo creo que la industria de tecnología de seguridad en nuestro país goza de buena salud.

Certificación y seguridad

bit Hay empresas de certificación de seguridad que imparten cursos que permiten que salgas con un título o diploma para poder certificar, ¿qué os parece?

Carlos Jiménez. Todos tienen la carrera, lo cual no garantiza que puedas tener el mejor encaje en una empresa o en un puesto en concreto. Es un título más y si lo tienes mejor por una cuestión de formación y cultura, pero no garantiza nada.

A mí me parece que un problema en general de toda la tecnología es que la gente que la utiliza no se plantea para qué la utiliza, lo que provoca una cultura de "ir hacia delante" que hace que los sistemas sean cada vez más inestables y difíciles de proteger, a la vez que más complejos, ya que incluso puede que tengan características que no necesitas.

Mario Arienza. Estoy de acuerdo, una certificación no certifica que alguien es operativo y es capaz de operar un sistema. Para mí es importante que una persona vaya más allá, no sólo que aplique una regla sino que tenga el sentido común más allá de las propias certificaciones.

Por eso, para mí sería una condición necesaria pero no suficiente para los técnicos de seguridad.

María Campos. Yo también estoy muy en la línea de las opiniones anteriores. En este asunto, como en todas las facetas de la vida, es necesaria la coherencia. El tener de la noche a la mañana a tu personal certificado no te garantiza tampoco que vayas a ser capaz de unos despliegues al máximo nivel.

Lo que hace falta es una experiencia que se acumula y se aplica a unas situaciones concretas. Estoy de acuerdo con que todos apliquemos unos estándares y hablemos el mismo idioma, pero la certificación te garantiza una pequeña parte de lo que es el conjunto. La certificación es una condición necesaria, pero el despliegue global en todos los ámbitos requiere más que eso.

El reto de la telefonía móvil

bit ¿Qué opináis de la seguridad que hay en la actualidad respecto a los teléfonos móviles?

Carlos Jiménez. Hay una diferencia entre la seguridad física y la seguridad lógica. En el primer caso se trata de una cuestión perimetral, como una muralla que aísla una fortaleza, pero desde hace unos años esto es inviable.

Ahora hay que asumir que tu enemigo está a tu lado, aunque esté físi-

camente en China, pero gracias a la tecnología está cerca. Por lo tanto, hay que tener una actitud “paranoica”, porque cualquiera puede ser tu atacante. De hecho, el 70% de los ataques son internos, no externos.

Ya es todo mezclado, no hay dentro y fuera, no hay móvil y fijo, por lo tanto alguien con *Wi-Fi* puede atacarte y estar a tu lado. Por lo tanto, no sabes quién es tu enemigo a ciencia cierta, por lo que la estrategia tiene que basarse más en aquello que confías que en lo que desconfías.

María Campos. Yo también estoy muy en la línea de las opiniones anteriores. En este asunto, como en todas las facetas de la vida, es necesaria la coherencia. El tener de la noche a la mañana a tu personal certificado no te garantiza tampoco que vayas a ser capaz de unos despliegues al máximo nivel.

Lo que hace falta es una experiencia que se acumula y se aplica a unas situaciones concretas. Estoy de acuerdo con que todos apliquemos unos estándares y hablemos el mismo idioma, pero la certificación te garantiza una pequeña parte de lo que es el conjunto. La certificación es una condición necesaria, pero el despliegue global en todos los ámbitos requiere más que eso.

Jesús Sánchez. En el ámbito móvil hay falta de concienciación. Los móviles se han convertido en una llave con una gran capacidad de almacenamiento y en una forma de compartir información. Así, puedo tener en el teléfono móvil información sensible y estar en el coche con el *bluetooth* y puede ser un terminal abierto a todo el mundo.

Mario Arienza. Quizá se ha primado en el diseño para mejorar la



movilidad sobre la seguridad. Así la problemática está en la base.

Inversión y rentabilidad

bit ¿Os parece que es rentable invertir en seguridad?

María Campos. Hay que verlo como una inversión y no como un gasto, que es como lo perciben muchas organizaciones. Se ha hablado de la prevención y ese es el único modo.

Tenemos que tener en cuenta que si estamos utilizando unas tecnologías que nos ayudan a expandir nuestro negocio, la seguridad tiene que ser una parte central si queremos mantenernos. Comprar una serie de productos no es suficiente, hay que integrar la seguridad en la organización de la empresa y considerarla dentro del plan de negocio.

Jesús Sánchez. La única manera de que las organizaciones lo vean como una inversión es que el responsable de seguridad sepa arrojar esas métricas a nivel directivo. La

dirección entenderá el impacto y coste que tendrá en el negocio.

De esta manera se podrá percibir el retorno de esa inversión. Hay que acercar la gestión de seguridad al negocio.

Mario Arienza. Yo incluso iría un paso más allá, es decir: integrar la seguridad en el propio negocio para que las medidas de seguridad me ayuden a vender un producto. Así, el hecho de tener implantado una norma sea atractivo para mis clientes. La seguridad también forma parte de la filosofía del negocio como valor añadido.

Carlos Jiménez. El auge de inversiones en seguridad sigue creciendo, lo que significa que es realmente rentable. La seguridad sirve para dar confianza, ya que de ella depende tu negocio. También hay que tener en cuenta que en el caso de la seguridad es importante la colaboración de la industria para trabajar en equipo, para no tener tecnologías aisladas. ♦