

SESIÓN DE CONTINUIDAD

Seguridad de los sistemas corporativos, una cuestión estratégica

La seguridad de los sistemas corporativos es un aspecto cada vez más valorado por las empresas, pero también más complejo. El número de personas que debe acceder a los sistemas de una organización ha aumentado de forma exponencial y ya no sólo se limita a los empleados, sino que abarca a clientes, proveedores y administración. Para ayudar a las empresas a hacer frente a esta complejidad, el e-Business Center organizó una sesión de continuidad que contó con la participación de Juan Pérez Vilaplana, director de tecnología de PwC, y Manuel Cortés y Diego Sacristán, gerentes de seguridad de PwC.



Ponente/s: Brian Subirana, profesor del IESE; Juan Pérez Vilaplana, director de tecnología de PwC; Manuel Cortés y Diego Sacristán, gerentes de seguridad de PwC
Fecha: 19/05/2003

Cada vez más, las empresas se enfrentan a la necesidad de permitir el acceso a sus sistemas a un número mayor de usuarios. Así lo puso de manifiesto Juan Pérez Vilaplana, director de tecnología de PwC, durante su intervención en una sesión de continuidad que el e-Business Center dedicó a la seguridad. En la jornada, que contó con el profesor del IESE Brian Subirana como moderador, también participaron los gerentes de seguridad de PwC, Manuel Cortés y Diego Sacristán. Ambos coincidieron con Pérez Vilaplana en que la integración de los sistemas de las empresas con los de sus clientes y proveedores ha complicado la gestión de la seguridad.

Así, si antes bastaba con controlar a los propios empleados, el nuevo entorno de negocios obliga a gestionar la identidad de los clientes (B2C), las empresas y accionistas (B2B), y la administración (B2E). El banco Citibank, por ejemplo, ha pasado de gestionar 6.000 a 20.000 usuarios.

Además, la noticia de la violación de los sistemas de la empresa puede dañar seriamente la reputación corporativa, un aspecto que ha adquirido una gran importancia en los últimos años. Y, dado que el robo de la identidad es uno de los delitos más cometidos en Estados Unidos, los directivos han comenzado a considerar la seguridad como un tema clave en su gestión.

Una cuestión estratégica

La seguridad de la empresa es un tema estratégico que afecta de forma directa a la dirección general de la empresa y no al departamento de sistemas, por mucho que implique la implantación de tecnología. En los últimos años, los directivos han ido tomando conciencia de ello y cada vez es más frecuente la creación de presupuestos de seguridad al margen del presupuesto de TI.

Las empresas deben abordar unas medidas de seguridad acordes con los riesgos a los que se enfrentan. Por ello, el primer elemento de una estrategia de seguridad es determinar el riesgo a controlar. Después, es necesario establecer una metodología de elección de los nuevos dispositivos de seguridad y de las nuevas tecnologías; definir una política de comunicación del plan de seguridad; delimitar las métricas de implantación del proceso; determinar el modelo de negocio de la empresa y adecuarlo a las políticas de seguridad.

Una vez definida la estrategia y la implantación de la misma, las empresas deben establecer los pasos a seguir en caso de que se produzca un problema de seguridad, pues de nada sirve una buena estrategia si no se prevé cómo responder ante una situación inesperada. Estos planes deben actualizarse con periodicidad, estar dotados de suficientes recursos y determinar los mecanismos para saber qué se ha incumplido.

Gestión de la identidad

Hay que tener en cuenta que la seguridad no pasa sólo por denegar el acceso a los sistemas de la empresa, sino también por habilitar el permiso para que los usuarios que deben acceder a ciertas áreas puedan hacerlo. De hecho, el principio del mínimo privilegio –permitir el mínimo acceso posible a los usuarios— ralentiza los procesos corporativos. Por otra parte, la fuerza de inclusión – permitir el máximo acceso posible a los usuarios— llevada a su máximo extremo es igual de negativa.

Los expertos de PwC aconsejan utilizar una tecnología de gestión de la identidad que permita identificar al usuario del sistema, facilitando un acceso individualizado en función del tipo de usuario y del momento de acceso. El sistema debería permitir, con un único proceso de autenticación, acceder a todas las aplicaciones predefinidas. De este modo, el usuario del sistema debe introducir una única vez su identidad y contraseña para entrar en distintas aplicaciones.

Los beneficios de este sistema son múltiples. Reducción de los costes por la administración centralizada del sistema y la gestión delegada; un mejor y más fácil cumplimiento de la normativa legal; reducción de errores debido a la utilización de estándares y soluciones flexibles; mejor accesibilidad para el usuario por la sincronización de contraseñas; gestión centralizada y administración delegada para la adaptación del sistema a las necesidades y situaciones concretas de la organización.

Problema cultural

De todas formas, el problema de la seguridad es más cultural que tecnológico. La percepción de inseguridad es sólo eso, una sensación. Por ejemplo, Microsoft tiene una herramienta, denominada Passport, cuyo objetivo es almacenar todas las contraseñas de los usuarios con el fin de que éstos deban proporcionarlas una única vez para realizar cualquier acción en la Red. El principal obstáculo al que se enfrenta Passport no es tecnológico, sino legal, ya que ha topado con la política de privacidad de la Comunidad Europea. Según PwC, las fugas de información propietaria podrían evitarse con la formación, la cultura y la asignación de responsabilidades, además de la tecnología.

España

En España, la Ley Orgánica de Protección de Datos ha sido un auténtico dinamizador del sector. Las sanciones impuestas por el incumplimiento de su normativa han resultado ser el mejor impulso para poner en marcha políticas de seguridad encaminadas a la protección de datos de carácter personal, tanto de clientes como de empleados.

A grandes rasgos, España dispone de excelentes técnicos en materia de seguridad, con un nivel perfectamente equiparable a los mejores países del entorno. Sin embargo, organizativamente las empresas no consiguen introducir una cultura de respeto por la seguridad o destinar recursos suficientes para ponerla en marcha de forma viable. La gran mayoría no realiza actividades de gestión y procesos de revisión de las políticas de seguridad existentes. Por otra parte, la comunicación de las políticas de seguridad no es siempre la correcta, e incluso en ocasiones es inexistente, a pesar de disponer de un plan de seguridad perfectamente detallado.