

## Cómo ajustar la seguridad de los sistemas de cómputo

Artículo original:  
HOW TO TIGHTEN COMPUTER SECURITY  
En:  
CORPORATE BOARD MEMBER  
JANUARY/FEBRUARY 2002

Antes del 11 de septiembre, los directores rápidamente encerraban en círculos los montos propuestos de dinero destinados a tecnologías y hacían un llamado a los altos ejecutivos a discontinuarlos. Los encargados del área de tecnologías de información se comunicaban en dialectos que pocos directivos comprendían, y esto no ayudó que los departamentos de tecnología estuvieran siempre requiriendo por costosas mejoras y recursos actualizados.

Ahora los directivos y su gente de tecnologías de información están en la misma página. De hecho, los miembros de los directorios de las corporaciones están siendo empujados a pasar más tiempo en atender la construcción de los sistemas de seguridad de sus compañías. Ellos acostumbraban preguntar "¿Realmente necesitamos esto?", dice Peter G. Neumann, director científico de los laboratorios de computación de SRI Internacional e influyente experto en tecnologías de seguridad. Ahora ellos preguntan: ¿estamos haciendo lo suficiente?



Los directivos no están preocupados solamente de la violencia física. Un habilidoso hacker puede dañar los sistemas computarizados de una compañía, corrompiendo, impidiendo el acceso o llenando los sitios web, bases de datos, redes financieras y comunicaciones internas. Aquí es donde los directivos necesitan estar preguntando a sus encargados de tecnologías de información -y algunas de las respuestas que deben estar haciendo:

### ¿Cuál es nuestro plan de seguridad de información?

El directivo suele preguntar por un documento escrito que describa, en un inglés comprensible, cómo la compañía se está protegiendo su tecnología (incluyendo hardware, software e infraestructura), qué es lo que se planea hacer si un empleado tiene acceso al hardware y el trabajo en red es interrumpido, y como continuará haciendo negocios si su sitio web es dañado o desmantelado por un ataque cibernético. "La meta es que los datos de inteligencia de la compañía estén físicamente descentralizados pero lógicamente centralizados", dice Kevin Mandia, coautor del libro Respuesta al Incidente: Investigando el Crimen Cibernético y director de informática forense en Foundstone Inc., una firma de seguridad. "Los mismos datos deben existir en muchas y diferentes partes pero estar accesibles desde cualquiera de ellas".

### ¿Cómo estamos endureciendo o protegiendo nuestros sistemas?

En términos técnicos, endurecer significa reducir los accesos no autorizados a los servidores de red, la que es administrada por comandos internos de los empleados y los enlaces externos de visitantes de un sitio web. Este proceso fortalece el cortafuegos (firewall), el software de seguridad que bloquea los accesos no autorizados. Otra parte del proceso de endurecimiento involucra tener todos los servidores en la red usando sensores de detección de intrusos para que el departamento de tecnologías de información pueda monitorear la actividad y los agujeros de seguridad sean reconocidos y reportados rápidamente. Mandy Andress, presidente y fundador de la firma de seguridad ArcSec Technologies y autor de Sobreviviendo a la seguridad, empuja a las compañías a instalar los últimos "parches más populares", nuevos códigos que cierran los agujeros de seguridad en el sistema. Las compañías también necesitan bloquear los hoyos que puedan comprometer sus sitios web.

Una aplicación de escaneo web, por citar un ejemplo, identificará todos los agujeros de seguridad y dará la alerta.

### ¿Cuál es nuestro plan de recuperación ante desastres?

Las compañías cuyos sistemas son dejados fuera de servicio necesitan estar involucradas en el tema. Una forma de hacer esto es contratar a una firma de recuperación frente a desastres. Así, un equipo completo mantiene un segundo conjunto de computadores en tus oficinas o plantas, copias de todo lo que tu sistema hace, y regularmente transmite los datos a otro sitio. Si un hacker te deja fuera de servicio, este sistema de backup absolutamente necesario se activará cuando tu sistema caiga. En suma, muchas grandes compañías ahora se protegen a sí mismas contra el colapso de sus líneas terrestres con la instalación de sistemas inalámbricos que puedan transmitir datos de un edificio de oficinas a otro, o a un sitio de recuperación frente a desastres.

### Tenemos espacio para una oficina con copias de seguridad, backups, con computadoras?

Deberías tenerla. Tu empresa necesita duplicar sus computadoras más importantes y otros sistemas de hardware en un lugar donde los empleados puedan volver a trabajar rápidamente, usando los datos que tu contratista de recuperación frente a desastres te provea. Esto implica que debes invertir en una gran cantidad de laptops o computadoras de escritorio, y también en modems telefónicos en caso de que tus líneas T (líneas telefónicas) queden inoperativas. Asegúrate de que este lugar tenga las suficientes líneas de seguridad y enchufes, y toma otros pasos usuales basados en el tipo de tu compañía y la naturaleza de su trabajo. Haz esto ahora, no cuando el desastre ocurra. Y no olvides los muebles, como mínimo debes contar con mesas y sillas.

Ahora es un buen tiempo para impulsar a los empleados a empezar a almacenar copias de la información de sus computadoras cada noche y dejar de programar a sus computadoras para que les recuerden sus claves de acceso. Estos dos puntos de seguridad pueden parecer como trabajo hecho, pero no lo son. Ellos protegen la propiedad intelectual de la compañía.