



Cuando falta un miembro clave del personal de TI

Por Michael Mazengia.*

¿Su empresa está preparada para una epidemia de fiebre aviar? ¿Y si se incendiara la oficina matriz? ¿Ha hecho lo necesario para la seguridad de su personal y la de su información? Está claro que planear la continuidad de un negocio es de alta prioridad para muchas compañías, pero tal vez se olvide una amenaza más obvia: la muerte repentina de una persona importante para nuestras operaciones.

Esto obliga a los comités ejecutivos y a los gerentes de Tecnología de Información (TI) a preguntarse: si algo pasara a uno de los empleados clave de TI, ¿se podría seguir operando? El Jefe de TI de Mintz & Partners se enfrentó a este problema cuando un muy importante y estimado miembro del equipo de TI falleció de manera imprevista.

Esta persona era muy competente y se le había dado autonomía en muchas áreas. En las semanas que siguieron a la tragedia, el mayor reto del directivo no fue el de redistribuir las obligaciones de su amigo, sino simplemente descubrir cuáles eran todas. Además, estaba el desafío de dirigir al equipo en su propia crisis emocional y manejar su propio duelo por la pérdida. Lo que aprendió puede aplicarse en cualquier si-

tuación cuando, de manera abrupta, falte un miembro clave del equipo de TI.

Conocimiento

Con el tiempo, las personas acumulan habilidades que no son fácilmente transmisibles. Esto incluye el conocimiento de diferentes programas de *software* y de relaciones de negocio internas y externas. Para minimizar los efectos de cuando alguien deja una compañía, debe mantenerse una base de datos para registrar áreas en las que miembros de Tecnología de la Información hayan desarrollado una pericia particular. Para ello, algunas firmas prefieren usar una herramienta *wiki* (que permite a los usuarios crear, editar y establecer vínculos con páginas *web*), lo cual facilita que cada persona del equipo mantenga su sección.

Los tecnólogos se especializan. Aunque puede ser positivo para el desarrollo de habilidades y la satisfacción en el trabajo, es importante formalizar el reconocimiento de estas especializaciones y asegurar que esto no es un impedimento para que otros puedan desarrollar un conocimiento de trabajo en el área.

¿Qué pasa cuando el equipo es pequeño y la carga de trabajo de la persona no puede absorberse temporalmente por los

otros? Identifique, entre su personal, a tecnólogos que no sean de TI (por ejemplo, tenga en la firma cuando menos un contador con un conocimiento bastante sólido de sistemas de TI en general). Al otorgar a esta persona una función en la continuidad del negocio, puede eliminar muchos de los retos que implica contratar a un trabajador temporal. Las firmas también deberán registrar todas las solicitudes de soporte de TI y su resolución. En poco tiempo, esto creará un almacén de conocimiento al que tendrán acceso los nuevos miembros del equipo de TI. Sin embargo, es importante que esto no se vuelva un trabajo rutinario y que los elementos del grupo registren los detalles relevantes de cada llamada, con la menor cantidad de lenguaje especializado.

Siga el rastro

Para muchas empresas, la información está entre sus activos más valiosos. Muchas firmas almacenan datos fuera del sitio y, si fallece el responsable de hacerlo, la continuidad del negocio puede verse amenazada. Deberá documentarse bien la ubicación y el contenido de todos los datos en el sitio y fuera de éste. Cualquier cambio de personal de TI deberá comunicarse inmediatamente a los proveedores encargados del almacenamiento de datos fuera del sitio.

Al ser la información algo tan crítico para las organizaciones, puede resultar conveniente que el director de operaciones de la firma, el socio director o alguna otra persona de alto nivel, se encargue de la relación con el proveedor del almacenamiento de datos. De este modo, en medio de una tragedia, las principales autoridades de la firma tendrán acceso directo a este activo clave. También es importante auditar datos almacenados de manera asegurada. Por ejemplo, ¿sabe usted algo de la información guardada en las computadoras personales? Aunque su firma tenga aplicaciones sofisticadas en almacenaje centralizado, quizá haya quienes tengan información crítica en sus computadoras; o peor aún, en sus archivos personales de correo electrónico.

Muchos guardamos en nuestra memoria tres, cuatro o más contraseñas. Si se pierde una importante, puede bloquearse el acceso a sistemas críticos para la misión. Por ello, las firmas deben mantener una base de datos segura para rastrear todas las claves, quién las creó y la fecha en que se cambió cada una. Para asegurar que esta base de datos no caduque, deberá revisarse y probarse regularmente, ya sea mensual o trimestralmente.

También, las firmas deberán establecer una base de datos para rastrear todo el equipo de TI que sale y la fecha en que debe regre-

sarse, así como un registro del equipo que está en reparación fuera de las oficinas. Un buen programa de administración de activos puede permitir una identificación rápida y la reasignación de recursos. Si fallece un miembro del equipo de TI, revise sus papeles de trabajo. Por ejemplo, si recibía regularmente facturas, alguna podría estar en un limbo de indefinición si no se ha turnado al departamento de contabilidad interna de la compañía.

Un despido hostil

El caso real que hemos revisado, en el que un miembro del equipo de TI falleció, se relaciona mucho con lo que ocurriría si una empresa tuviera que despedir a algún integrante. En un escenario así, es fundamental estar bien preparado. Antes de un despido, realice una auditoría de todos los nodos de su red de trabajo.

Un empleado malicioso o descontento podría asignar derechos administrativos a un aditamento inocuo, como una impresora, para tener acceso a la red y causar daños. Como prevención, cambie las contraseñas administrativas y los códigos de tableros para las puertas físicas. Cancele las tarjetas de crédito y de llamadas del empleado. Como es posible acceder a las redes desde fuera de una oficina, si tiene usted una *nube* inalámbrica (*wireless cloud*) es preciso cambiar su contraseña. Asimismo, es importante contratar a un consultor independiente antes de despedir a la persona. Esto ayudará a identificar todos los puntos remotos de entrada a la infraestructura de TI de la firma y a manejarlos de manera consecuente.

Plan para la continuidad

Hace más de un año que la firma perdió a su buen amigo. El esfuerzo de manejar el duelo hizo más difíciles los retos de negocios que todos enfrentaban. Aunque se hayan atendido los problemas técnicos, no deberá ignorarse el factor humano. Las personas a quienes se pidió el esfuerzo de trabajar más arduamente para que la empresa siguiera operando, pese a la situación, eran las mismas a quienes afectaba ésta. Permitir un periodo para el duelo es reconocer una necesidad humana y una parte importante para mitigar errores costosos. Es importante un plan de continuidad del negocio para estar seguros de poder manejar la pérdida de un miembro clave del equipo de TI o ante cualquier imprevisto que pudiera ocurrir. 🌸

Texto original: "In the Event of Tragedy" (CAMagazine, mayo 2008). Traducción para Veritas del Colegio de Contadores Públicos de México por Jorge Abenamar Suárez Arana.

*Michael Mazengia es Gerente en TI en Deloitte/Mintz & Partners. michael_mazengia@mintz.com