El riesgo de crear responsables todopoderosos en la organización

nexus aggity

Hay un gran riesgo que una sola persona o un proveedor sea el responsable de todas las actividades de TI dentro de la organización. ¿Qué puede salir mal?

Un dueño de una PYME me buscó hace algunos meses porque su proveedor de la página de internet, desde donde realizaba ventas de sus productos, había decidido subir los precios de sus servicios. Al comparar con otros proveedores el dueño decidió cambiar a la persona que le llevaba de forma externa la administración de toda esa infraestructura tecnológica. Para responsable de esta PYME era simple, la persona le administraba el correo electrónico y el portal desde donde realizaba ventas y ahora necesitaba cambiarlo. Lo que no sabía es que quien tenía registrado el dominio de internet desde donde operaba, estaba registrado al nombre de este proveedor. El proveedor secuestró el dominio porque la empresa no había aceptado su cambio de costos; la PYME ahora tenía que iniciar un proceso que tomaría mucho tiempo para poder recuperarlo pero que también existía la posibilidad de que no lo recuperara.

Esto es más común de lo que parece. En muchos de los casos, por desconocimiento, se toman decisiones que pueden afectar la operación de la organización. Tan simple como que el dominio de internet no esté en manos de alguien dentro de la organización.

Cada vez escucho más frecuentemente: **“Ya no confío en quien lleva mi área de TI.”** Y de ahí vienen miles de comentarios que van

desde “creo que está leyendo mis correos”, “creo que está robándome dinero por medio de los proveedores”, “está coludido con los proveedores”, “tiene más poder que yo en la organización” o hasta “en cualquier momento me podría afectar a mí y a mi familia con lo que tiene información de mi”.En muchas PYMES, se espera que la misma persona sea responsable de la gestión de datos, redes y comunicaciones, infraestructura, desarrollo de software, cumplimiento y ciberseguridad.

Estamos hablando que no haya una estructura formal y delegada.

Y la verdad, lo entiendo: Las PYMES no pueden tener un ejército de personas dentro del área de TI para poder atender todos los requerimientos que tiene la empresa, pero esto también genera una serie de riesgos que pocas veces los directores o dueños de las PYMES consideran.

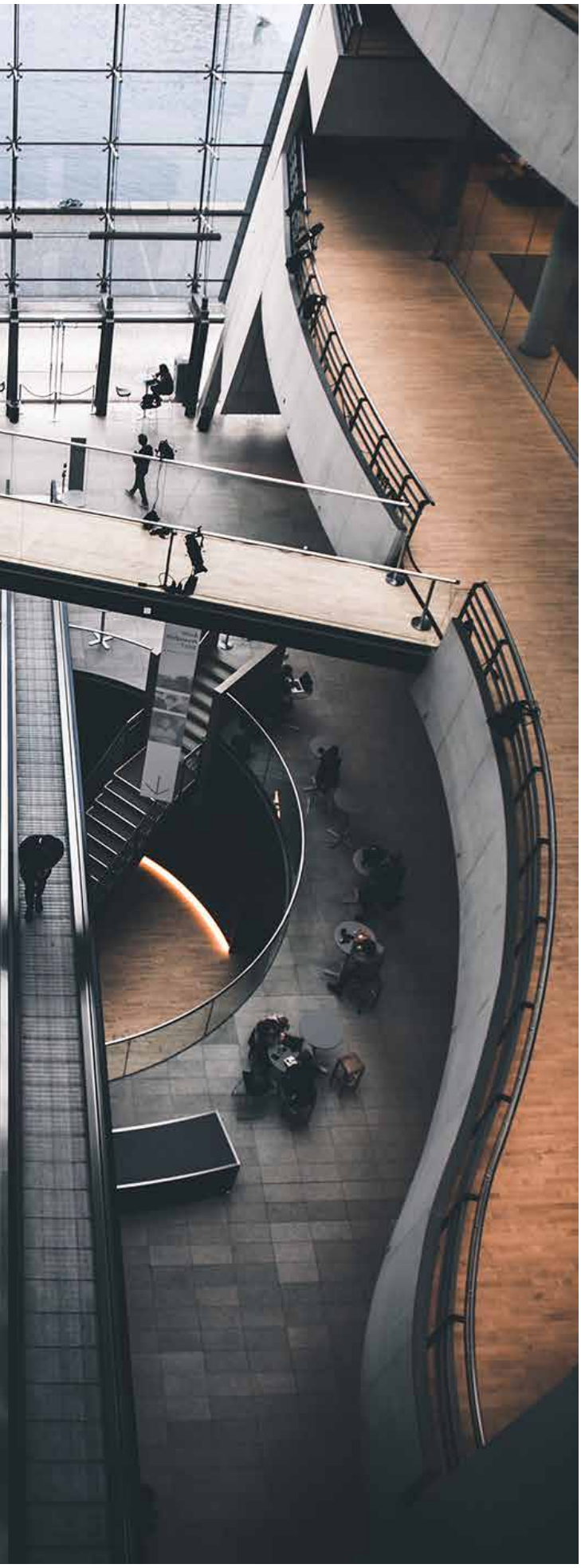
Los más adelantados, piden a su responsable de TI que sea el punto de contacto o administrador de varios proveedores para poder cubrir todas las necesidades antes mencionadas. Lo cual también genera algunos riesgos: que la persona se ponga de acuerdo con el proveedor para afectar económicamente a la organización.

Esto no solo pasa en las PYMES, puede afectar a cualquier organización no importando el tamaño, pero todas tienen algo en común: dejaron que esta persona, responsable de TI, se convirtiera en amo y dios de las redes. Incluso, en algunos casos, le delegaron la responsabilidad de configurar cualquier dispositivo tecnológico que se instaló en casa por qué: "yo no le sé a la tecnología".

Que un proveedor tenga registrado el dominio o que un administrador tenga acceso a todo y pueda usarlo en su beneficio ¿Es un ciberataque? No, le dimos las llaves de todas las puertas a una misma persona, pero nunca lo supervisamos.

Cuando se ha perdido esa confianza o cuando es evidente que se tiene que separar esa persona de la organización, es cuando nos damos cuenta de lo que hemos creado, porque no es tan fácil como citarlo para que deje la organización. Esta persona es la única que sabe cómo opera tecnológicamente la empresa y podría desaparecerla en cuestión de segundos.

"¿Qué puedo hacer?" me decía intranquilo un dueño de una empresa, mientras le explicaba las opciones que tenía y que no podría de la noche a la mañana separar a esta persona. Finalmente, hablamos de la posibilidad de hacer un "Take Over de TI" donde no podríamos separarlo inmediatamente, sino cuando lográramos entender cómo opera la organización para posteriormente pedirle los accesos a todos los sistemas, proveedores, aplicaciones y otros recursos de tecnología para



asegurar la continuidad de la operación.
También está la preocupación de que posterior a su salida, pudiera conectarse remotamente para causar algún daño: borrar información o hacer que algún sistema fallara. Situación que está considerada para que, a su salida, se hagan cambios importantes en la estructura de la red y de los sistemas. En pocas palabras: pensar lo peor para tratar de evitarlo. Se está atendiendo como un incidente y un manejo de crisis, ya está sucediendo.

Pero todo esto se puede evitar. No es un problema técnico, es un problema estratégico que debe ser considerado por los tomadores de decisiones de la organización.

Si a la alta administración, dueños, socios, inversionistas y director general les interesa proteger su reputación y operación, deben considerar estos escenarios de riesgo que en muchos de los casos la ciberseguridad lo considera. El problema radica en que muchas de las organizaciones comienzan a hablar de ciberseguridad hasta después de que sufren un incidente como los mencionados anteriormente o algunos otros que vienen del exterior.

Ciberseguridad no necesariamente es implementar un sistema costoso, sino un procedimiento simple, así como las reglas del juego: definir claramente roles y responsabilidades, implementar controles de acceso para evitar que una sola persona tenga acceso a todo y establecer procedimientos de auditoría (interno o externo).

Obviamente hay más, pero para empezar y para el tamaño de una PYME es un gran comienzo. No es mi intensión voltee a ver a su responsable de TI como el malo de la película, ya que quizá no lo sea, pero piense en el riesgo de dejar de operar porque el o la responsable de TI no está disponible cuando lo requiera.

Autor: Andrés Velázquez
Fuente de información: forbes.com.mx