DIOMEDIA

Las pymes son propensas a fraudes comunes.

Fraudes:

El gran peligro que deben combatir las pymes

Experto recomienda implementar medidas de prevención, tales como la creación de canales de denuncia o la distribución de tareas al interior de la empresa.

Las últimas cifras de la Sociedad de Fomento Fabril (Sofofa) revelan que en nuestro país el 98% de las empresas son pymes, creándose en promedio 351 compañías al día, según datos de RedCapital. Dichas compañías se enfrentan a diario con una diversidad de inconvenientes. Uno de ellos es el riesgo de fraude, vulneración que, a pesar de dejar consecuencias graves en cualquier tipo de organización, en una pyme genera un impacto que puede generar hasta su quiebra.

Si bien las pymes son propensas a los fraudes comunes que afectan a cualquier empresa, las malversaciones son la vulneración más recurrente. "Una pyme es mucho más propensa a lo que se conoce como malversaciones, que en el fondo se refiere a las apropiaciones de recursos de la pyme. Esto es pérdida de inventarios, o cuentas por cobrar en que los pagos se desvían. Estas acciones pueden prevenirse con medidas muy simples, pero bastante poderosas", señala Héctor Osorio, socio de PKF Chile Finanzas Corporativas.

En la misma línea, el experto indica que la clave está en evitar que se produzca lo que los expertos llaman el triángulo del fraude. Aquí se utiliza la misma lógica del bombero: para que no se genere fuego, hay que evitar que se produzca el triángulo del fuego; es decir, que simultáneamente exista un combustible, un detonante y oxígeno.

Osorio recalca que la gran misión del gestor de la pyme es tener mucho cuidado con las oportunidades; es decir, con los accesos que se les da a las personas. "No puede haber una persona que maneje la bodega sin supervisión o que un solo profesional controle la cuenta corriente, aunque sea el propio dueño.

Se debe tener un control. El que lleva las cuentas, debe ser distinto del que gira cheques. Los contadores llaman a dicho proceso control por oposición. En la pyme esto puede ser muy difícil de ejecutar porque a veces hay pocas personas entre las cuales distribuir la tarea, pero es parte de un proceso que hay que realizar", comenta.

Dentro de las medidas más fáciles, poderosas y de bajo costo que puede implementar una pyme para disminuir el riesgo de fraudes es la creación de un canal de denuncia. Según el sondeo anual Global Fraud Study de la Association of Certified Fraud Examiners, un 40% de los fraudes corporativos en 2018 se detectó por medio de un canal de denuncias, siendo más de la mitad de ellos reportados por colaboradores de la organización.

El canal de denuncia da la sensación de que yo tuve la oportunidad de decir algo sin exponerme y suele ser lo más efectivo para detectar delitos. Y es muy barato y fácil de implementar.

"Se genera un correo que automáticamente le llega al principal responsable de la organización y las personas pueden participar anónimamente, fundamentando muy bien, aportando todos los antecedentes que permitan una investigación coherente", concluye Héctor Osorio.

Ciberseguridad ciudadana:

Cuidado, se puede estar a un clic del peligro

Las personas enfrentan una doble amenaza en materia de ciberseguridad. Por un lado, la que se vincula con información personal; y, por otro, la que se relaciona con el funcionamiento de la ciudad y los servicios básicos.

DIOMEDIA

Los ciberdelincuentes siempre intentan, de alguna manera, robar información que les puede ser útil para obtener dinero.

En Chile los ataques a dispositivos móviles durante este año han aumentado en más de un 50%, siendo las personas un blanco cada vez más buscado por los ciberdelincuentes. "Con el aumento de aparatos como notebooks, teléfonos inteligentes y tablets, además de la facilidad para conectarlos a internet, ha aumentado también la posibilidad de ser víctimas de ataques", dice Iván Toro, gerente general de ITQ Latam.

Lo anterior, señala el ejecutivo, debido básicamente a que las personas "estamos y vivimos conectados a internet. Nos informamos, nos comunicamos y nos entretenemos en la web; realizamos transacciones bancarias, pagos de servicios, revisamos sitios web, y también estamos conectados a redes sociales. Esto es caldo de cultivo para los cibercriminales", asegura Toro.

Hugo Soto, investigador del Centro de Estudios del Futuro, CEF, de la Usach, aclara que los riesgos que en este ámbito enfrentan los ciudadanos se pueden clasificar en dos grandes tipos: delitos ciberdependientes, que son aquellos que solo pueden ser cometidos por medio del uso de computador y/o tecnologías de la información, tales como el contagio de virus y otros software maliciosos, hackeos, secuestro del equipo o denegación de servicios. Y, por otra parte, existen los ciberposibilitados, es decir, delitos tradicionales cuyo alcance y escala se amplifica mediante el uso de computador y tecnologías de la información, tales como fraudes, robos y acoso sexual.

"Hay que tener conciencia de que los ciberdelitos son la principal amenaza de seguridad ciudadana en el futuro próximo. De hecho, en el caso de Chile ya la última encuesta de seguridad ciudadana del Ministerio del Interior reportó que en 2018 hubo más víctimas de ciberdelitos (6.0%) que de robo de casas (4.7%) e incluso asaltos (5.6%)", advierte el investigador del CEF.

César Pallavicini, gerente general de Pallavicini Consultores, agrega que la seguridad pública depende hoy de diversas tecnologías de televigilancia interconectadas por redes con centrales de monitoreo, globos y cámaras de video. Por lo anterior, las municipalidades y el Estado deben hacer contratos de servicios con empresas que les otorguen garantía de que tienen sistemas de gestión de Seguridad de la información (incluida la ciberseguridad) y de continuidad operacional. Ello minimiza el riesgo de ataques cibernéticos.

"Por la crisis social que tenemos ahora, los ciberataques —según el CSIRT— aumentaron en forma exponencial desde el 18 de octubre recién pasado. Así, por nuestra integridad y futuro, es necesario tener planes de prevención y contingencia en caso de un acto de vandalismo o ciberataque, que garanticen la seguridad de las personas y el suministro de servicios básicos", advierte Pallavicini.

Pallavicini enfatiza que la ciberseguridad es parte de la Seguridad de la Información. En ese contexto, dice, las ciudades inteligentes están conectadas, son sostenibles y eficientes gracias a las nuevas tecnologías. "Esto nos lleva a un modelo complejo de gestión de la seguridad, que precisa una visión global y transversal de los riesgos, además de abarcar —de manera integral— todos los servicios que este ecosistema 4.0 ofrece a sus ciudadanos", concluye.

CONSEJOS DEL CENTRO DE ESTUDIOS DEL FUTURO, CEF, DE LA USACH

- Estar consciente de la "huella digital", es decir, todo lo que se comunica online queda almacenado en alguna parte.
- No acceder a un sitio por medio de links o enlaces enviados por e-mails. Escribir la dirección directamente en la url.
- Al hacer una transacción en línea fijarse que aparezca un candado en el lado izquierdo del navegador y tiene que decir https.
- Mantener actualizado el software.
- Usar passwords y claves robustas.
- Usar solo redes conocidas. No hacer transacciones en redes públicas.
- Borrar e-mails sospechosos.
- Instalar antivirus en todos los dispositivos.