

Los riesgos en la información

Nuestra dependencia de la tecnología nos obliga a tener una atención especial a los riesgos que puedan ocasionar la pérdida total o parcial, temporal o definitiva de información clave para la operación de suministros. Es común olvidar este tipo de riesgos, ya que la información la damos por hecho y no nos parece posible que pueda simplemente desaparecer o faltar.

Imagina un escenario donde se pierde todo el historial de compras o de pagos, donde no se sabe cuánto se le debe a un proveedor o que está pendiente de llegar, o peor aún, imagina que alguien externo tiene acceso a las fórmulas secretas de tu producto que están en manos de un proveedor o a través de tu sistema. ¿Qué harías si te llamara un proveedor indicándote que ha perdido toda la información de tus órdenes y especificaciones y se ve imposibilitado en cumplir con los compromisos contraídos?



Algunas organizaciones han trabajado fuertemente en mejorar su seguridad de información basado en el apoyo de proveedores externos, por lo que en estos casos el manejo de riesgo se puede orientar a los procesos de seguridad que estos proveedores tienen sobre la información ya sea nuestra o de ellos.

Inspirado en un artículo llamado "[20 questions you should ask to ensure you're doing enough on cyber-supply chain risk management](#)" publicado por Phil Huggins, he formulado 10 preguntas para facilitar la identificación de este tipo de riesgos en el área de compras.

- 1) ¿Existe alguna operación crítica de nuestro negocio que dependa de la información de un proveedor en particular?
- 2) ¿Nuestra capacidad de lograr una recuperación rápida de un problema de TI depende de la colaboración de algunos proveedores?
- 3) ¿Tenemos demasiada dependencia del desempeño de área de TI de algún proveedor?
- 4) ¿Tienen nuestros proveedores identificados los posibles ataques a su información y tienen claros, documentados y probados los procesos para reducirlo y enfrentarlos?
- 5) ¿Auditamos y retroalimentamos las estrategias de nuestros proveedores para administrar sus riesgos asociados con recolección, almacenaje, resguardo y transmisión de información crítica?
- 6) ¿Nosotros o algún socio puede usar su poder de compra para facilitar acceso económico a productos o servicios que disminuyan el riesgo de pérdida o mal uso de la información de la relación comercial?
- 7) ¿Nuestros proveedores de los servicios de tecnología de información, tiene en el nivel de protección adecuado?
- 8) ¿Está nuestra área de tecnología de información consciente de los riesgos que impactan al área de compras y los atiende con la prioridad adecuada?
- 9) ¿Incluimos en los contratos aspectos de seguridad de la información?
- 10) ¿Estamos preparados y hemos realizado simulacros asociados con un evento de interrupción o pérdida de información?

Cualquier respuesta negativa a estas 10 preguntas representa una amenaza potencial para la cual hay que tomar medidas lo antes posible.