

Gestión de Riesgos de Terceros: una nueva disciplina para las empresas

Las empresas hoy en día operan como parte de un ecosistema, donde actores que son entidades legalmente independientes, y ubicados en zonas geográficas distintas, se deben coordinar para generar el resultado deseado: el producto o servicio que espera el cliente final. Cada participante es un eslabón de una cadena, y su objetivo debe ser no convertirse en el eslabón más débil que hace que la cadena se rompa.

Cuando nos integramos a una cadena de suministro, nuestro cliente nos exige diversos requisitos para asegurar que nuestro producto o servicio será entregado en tiempo y forma. Aparte de comprobar nuestra capacidad técnica y financiera, la preocupación es que no sucedan cosas que nos impidan cumplir con la entrega en el momento establecido. Esos riesgos pueden tener una gran cantidad de causas, muchas de ellas relacionadas con los criterios de sostenibilidad que abarca el ESG.

Es por eso que nuestros clientes nos exigen demostrar que tenemos una gestión confiable de los temas ambientales, sociales y de gobernanza, la cual evita que se presenten problemas que interrumpan nuestra operación o afecten la imagen de nuestros clientes. Y así como nuestros clientes nos exigen a nosotros, nosotros debemos hacer lo mismo con nuestros proveedores.

Implementar un sistema de gestión de riesgos de terceros requiere dedicar recursos e implementar procesos que involucran a varias áreas de la organización. Los pasos son los siguientes:

1. Involucrar a los actores principales: Compras, Finanzas, TI y Legal, coordinados por una función central de GRC (Gobernanza, Riesgos y Cumplimiento)
2. Crear un registro centralizado de proveedores con perfil completo, incluyendo en lo posible las “cuartas partes”, o sea los proveedores de nuestros proveedores.
3. Determinar qué tan crítico es cada proveedor para nuestras operaciones.
4. Recopilar información de los proveedores a través de cuestionarios adaptados a la categoría y relevancia de cada proveedor
5. Identificar y priorizar riesgos: matriz de probabilidad × impacto
6. Identificar los controles adecuados, validarlos y revisar la evidencia
7. Monitorización continua de amenazas cibernéticas, listas globales de sanciones, análisis financiero y cumplimiento fiscal, información regulatoria y legal.

No es una tarea fácil. En una encuesta hecha por la consultora Process Unity, más de la mitad de las empresas emplean 40 o más horas hombre para la evaluación de un proveedor. El proceso dura más de cuatro meses, tan solo porque muchos proveedores se tardan en responder y hay que estarlos activando. El promedio de la cantidad de proveedores evaluados es un 25% del total.

El uso de la inteligencia artificial ayuda a acelerar el proceso y genera una información más completa. Un 40% de las empresas ya lo están probando. No solo nos ayuda a evaluar la evidencia. También evita la aplicación de extensos cuestionarios, hace un monitoreo continuo y nos ayuda a anticipar los riesgos con un modelado predictivo.

Pero claro, implementar correctamente las herramientas de inteligencia artificial es un reto adicional. Pero todo ello es indispensable para poder competir en el entorno actual.

Si quieres saber mas sobre este tema, contáctame: thomas.karig@tkonsult.com.mx