La necesaria transformación digital del compliance

La transformación digital de las compañías no es un capricho ni una moda pasajera a la que subirse. Los nuevos negocios y los negocios digitales nativos no necesitan transformarse porque ya fueron concebidos de esa manera.

Pero el resto de empresas e industrias están trabajando en ese proceso de transformación digital para mejorar en competitividad, rentabilidad, generación de valor y adaptación al entorno actual.

Sin duda, la crisis del *Covid-19* ha producido una aceleración espectacular en tales procesos de Transformación Digital de todas las compañías. Nos ha supuesto nuevas formas de trabajar, la promoción del tele-trabajo, otra manera de atender a clientes, otra manera de relacionarse con proveedores... Todo ello, por supuesto, ha tenido una incidencia directa en muchas áreas de las compañías, donde *compliance* y riesgos no pueden quedarse fuera de juego.

De hecho, considero que se están enfrentando y se van a enfrentar a una nueva realidad donde deberán acompañar al negocio y las áreas corporativas a finalizar con éxito esa travesía de la transformación digital. Las empresas trabajarán para que la tecnología, los procesos y las ersonas estén alineadas con los objetivos estratégicos que se marquen, y *compliance* deberá orientar muy bien sus esfuerzos a mitigar los nuevos riesgos, proteger los activos intangibles de las organizaciones y absorber los cambios organizativos y legales de manera eficiente

En este sentido, creo que los retos de las áreas de *compliance* en los próximos años pueden aglutinarse teniendo en cuenta los siguientes aspectos:

En primer lugar, resulta necesario dimensionar y definir correctamente la función y su alcance, y utilizar sus recursos de manera inteligente para mitigar los mayores riesgos de la organización

El contexto en el que debe hacerse es absolutamente retador, ya que nos enfrentaremos a una avalancha de nuevas normativas y estándares: normativa de trabajo a distancia, de medidas Covid, resoluciones en protección de datos, directiva y futura ley sobre protección de denunciantes y mecanismos de funcionamiento de canales de denuncia, ley de *sandbox* financiera, futura ISO 37301 por la que se podrán certificar sistemas de *compliance*, novedades en prevención de blanqueo de capitales, promoción de planes y normas sobre inteligencia artificial, transformación digital, ciberriesgos, ciberseguridad, etcétera.

Además, el área debe tener capacidad de ser escalable en su operación diaria, ya que la tendencia de crecimiento parece clara en cuanto a investigaciones internas, seguimiento de controles, gestión de derechos y denuncias, nuevas obligaciones normativas, ambiente de auditoría, etc.

Sin olvidar el contexto económico adverso con restricciones económicas, congelación presupuestaria, escaso crecimiento en recursos propios.

Por ello, es más necesario que nunca repensar la estructura y recursos del área y realizar un plan de eficiencia que dedique de manera inteligente los recursos que se tienen para cumplir de la mejor manera y mitigar los mayores riesgos de cada organización

Otro de los grandes retos de los próximos años reside en la importancia del IT Compliance. Hablamos de transformación digital y de ampliar las capacidades informáticas y de datos de las organizaciones, por lo que evidentemente se va a incrementar la actividad digital del mundo de los negocios más aún.

Va a resultar fundamental que las áreas de *compliance* se refuercen con expertos en *tecnología e IT compliance,* ya que será necesario tener conocimientos y soltura en elementos como la identidad digital, las investigaciones y *forensic* digitales, intimidad en entornos informáticos, métodos para preservar evidencias electrónicas, algoritmia para la toma de decisiones, la gestión de incidentes de seguridad, las obligaciones de protección de datos, la comunicación de brechas de seguridad a las Autoridades competentes, las garantías y la protección de los derechos digitales, los instrumentos de denuncia a Fiscalía y Fuerzas y Cuerpos de Seguridad del Estado especializados en cibercrimen, criptomonedas, fraudes electrónicos, pólizas de ciberseguros, etcétera.

A todo ello hay que sumar la importancia de los controles y la monitorización en compañías y organismos que reciban ayudas públicas de los planes de recuperación para poder justificar correctamente la inversión y sus costes. Muchas de estas normas tienen un impacto frontal en las tareas de las áreas de compliance y riesgos, y evidentemente en los sistemas de gestión implantados en cada organización.

Finalmente, no debemos olvidarnos de la transformación digital de la propia función de compliance. Compliance no solo deberá acompañar al negocio en su transformación digital, sino también trabajar en su propia transformación digital, automatizando tareas, construyendo mejores reports, operando los sistemas de control de manera más eficaz, definiendo mejores métricas e indicadores, etc. La industria legaltech y regtech está evolucionando y creciendo de manera rápida y su objetivo es claro: ayudar a los profesionales jurídicos (en sentido amplio) a utilizar todas las capacidades tecnológicas posibles para mejorar su trabajo, su rendimiento y su visibilidad, aprovechando al máximo la automatización para que el profesional aporte el valor que la computación no puede.

Fuente: Expansión