

Lo que tu empresa debe saber sobre las oportunidades en cyber compliance

La falta de conocimiento técnico sobre sistemas expone al compliance officer al darwinismo del mercado laboral

La recomendación de controles sobre activos informáticos para el cumplimiento de normativas sobre protección de datos y de contratos sobre la disponibilidad y calidad de servicios abre oportunidades laborales concretas. El ***compliance officer*** adquiere un rol privilegiado para ayudar al departamento de sistemas y tecnologías a articular controles en políticas y contratos en soporte. Asimismo, el ***compliance officer*** contribuye a cuantificar los riesgos de incumplimientos sobre leyes de privacidad y de servicios esenciales, y sobre contratos de servicios de datos, infraestructura ***cloud***, licencias de ***software***, desarrollo de aplicaciones y tecnologías en general. La extensión de la visibilidad y aportes del ***compliance officer***en las funciones de sistemas y de seguridad informática requiere un nuevo conocimiento sobre riesgos, procesos, y controles de cyber seguridad.

A través de regulaciones sobre infraestructuras y servicios críticos, la **Comunidad Europea** y otros reguladores han multiplicado sus requerimientos en la última década. Inicialmente desde los sectores de energía y trasporte, la estrategia de regulación ha avanzado sobre servicios financieros, infraestructura de comunicaciones e internet, salud, agua y residuos, y servicios gubernamentales. De esta forma, los proveedores de servicios públicos críticos deben seguir crecientes obligaciones con responsabilidad proactiva para asegurar la continuidad de sus operaciones frente a la sociedad. Es esperable que esta tendencia incrementará la responsabilidad proactiva para prevenir interrupciones de servicios y sobre la seguridad de datos. También es esperable la extensión de regulaciones a otros sectores como la industria alimenticia, la agricultura, la educación, los servicios de defensa y seguridad informática, y la gestión de edificios de utilidad pública.

Desde Chile hasta China, las regulaciones sobre privacidad de datos personales también han crecido exponencialmente como áreas de interés para los ***compliance officers***. Especialmente a partir de la regulación Europea de protección de datos adoptada en 2016 para convertirse actualmente en el "*Golden Standard*", los servicios de asesoramiento y nuevas contrataciones han expandido el horizonte de los especialistas de ***compliance*** con vocación práctica y conocimiento técnico en protección de datos. Este nuevo perfil requiere la traducción de obligaciones sobre privacidad en procedimientos claramente articulados sobre controles de sistemas y cláusulas contractuales sobre procesadores de datos y proveedores en la terciarización de servicios informáticos.

En respuesta a la pandemia de COVID19, la función de ***compliance*** ha debido liderar el diseño y la comunicación de procedimientos para proteger dispositivos terminales y móviles como consecuencia del ***work from anywhere***. Asimismo, la función de compliance ha debido actualizar nuevos contratos de eCommerce y de adquisición de servicios cloud para el trabajo remoto. En especial al trabajar remotamente, la minimización del riesgo de los sistemas en las sombras ***(shadow IT)***por la instalación indebida de software no licenciado o aplicaciones web en muchos casos gratuitas, ha hecho que los ***compliance officers*** mejoren los protocolos de solicitud de compra de software y el bloqueo de servicios web como Dropbox y Google Documents.

Los riesgos de ir detrás de las constantes vulnerabilidades de los activos informáticos y los cambios en las estrategias de ataques de hackers y otros delincuentes, requieren que el ***compliance officer*** proponga, implemente, comunique y audite el cumplimiento de controles en sistemas basados en políticas de seguridad, contratos y regulaciones. Las crecientes tercerizaciones de servicios y modelos de software y almacenamiento en la nube, aumentan exponencialmente la exposición a estos riesgos. Las habilidades de los ***compliance officers*** para ir más allá del cumplimiento en papel y la mera escritura de políticas generales permiten canalizar decisiones de negocios sobre alternativas efectivas en costes que minimicen incumplimientos y protejan activos como la propiedad intelectual.

El ***compliance officer*** también ha ayudado a la cuantificación de impactos regulatorios y contractuales ante factores de riesgos vinculados a activos informáticos en diferentes escenarios. Al asesorar al negocio sobre compensaciones y penalidades máximas y mínimas sobre contratos y regulaciones, como los artículos del reglamento Europeo de protección de datos, la función de cumplimiento permite utilizar metodologías cuantitativas de evaluación de riesgos de ***compliance.*** Esto permite dejar atrás metodologías sesgadas

que desprecian a los datos, como las evaluaciones en "*rojo, amarillo y verde*", matrices 5*5 y sistemas arbitrarios de scoring. Estas metodologías cualitativas han sido refutadas por la ciencia durante más de una década convirtiéndolas actualmente en negligencia y mala práctica inefectivas para la defensa corporativa.

El entendimiento del contexto de ***cybercompliance***permite a los consultores ofrecer nuevos servicios diferenciados en el mercado y a los ***compliance officers*** internos dar un paso para llegar a ser un asesor influyente en los negocios. Aducir la falta de conocimiento técnico en sistemas, controles sobre procesos informáticos o protección de datos hace que la función de ***compliance*** no proteja sus organizaciones. Además, deja a los ***compliance officers*** a merced del darwinismo del mercado laboral y sin poder ofrecer servicios de consultoría demandados y bien pagos.

Fuente: *cincodías*