



Informe sobre Tendencias de GRC y Gestión de Riesgos para 2025 y su Impacto en la Ciberseguridad

Introducción

El Gobierno, Riesgo y Cumplimiento (GRC) se ha convertido en un componente fundamental para las organizaciones que buscan navegar un entorno empresarial cada vez más complejo y regulado. Para el corriente año 2025, se prevé que varias tendencias emergentes afecten la forma en que las empresas gestionan el GRC y los riesgos asociados, especialmente en el ámbito de la ciberseguridad. Este informe analiza estas tendencias clave y cómo pueden influir en la postura general de ciberseguridad de las organizaciones.

Tendencias Clave

Un cambio hacia una cultura organizacional que prioriza la gestión del riesgo en todos los niveles. Esto implica no solo la formación y concienciación de los empleados sobre la ciberseguridad, sino también la inclusión de métricas de riesgo en las evaluaciones de desempeño y en la toma de decisiones estratégicas. Promover una mentalidad centrada en la gestión del riesgo permitirá a las organizaciones responder de manera más efectiva a las amenazas emergentes.

Las decisiones informadas por datos serán cruciales para la gestión del riesgo. La recopilación sistemática e integración de datos provenientes tanto del entorno interno como externo proporcionará una visión más holística del panorama de riesgos, permitiendo respuestas más rápidas ante incidentes cibernéticos.

La incorporación de la automatización en los procesos de cumplimiento permitirá a las organizaciones reducir la carga operativa y minimizar errores humanos. Herramientas avanzadas de automatización facilitarán la monitorización continua, el seguimiento de auditorías y la generación de informes, lo que permitirá un enfoque más proactivo en la gestión del cumplimiento normativo.

El futuro de la ciberseguridad en el marco de GRC estará marcado por un aumento en la colaboración entre organizaciones, industrias y sectores. Compartir información sobre amenazas y mejores prácticas puede mejorar la preparación y respuesta ante incidentes. Las asociaciones público-privadas jugarán un papel fundamental en la creación de estándares y protocolos comunes que fortalezcan la ciberseguridad a nivel macro.

La rápida evolución de las amenazas cibernéticas exigirá que las organizaciones inviertan en capacidades robustas de respuesta a incidentes. Esto incluye la creación de equipos dedicados que puedan actuar rápidamente en caso de un incidente, así como la implementación de simulacros y ejercicios que preparen a la organización para una respuesta efectiva. La gestión de crisis será un componente vital en el marco GRC.

La implementación de estas tendencias transformará la manera en que las organizaciones abordan la ciberseguridad. Algunas implicaciones clave son:

Mejora de la Proactividad y Reactividad: La integración de tecnología avanzada permitirá anticipar y responder rápidamente a las amenazas, reduciendo el tiempo de



exposición a incidentes cibernéticos.

Reducción de Costos y Recursos: La automatización y un enfoque basado en datos permitirán optimizar los recursos destinados a la gestión del GRC, facilitando el cumplimiento normativo sin sacrificar la eficiencia operativa.

Mayor Resiliencia Organizacional: Fomentar una cultura organizacional, apoyado desde las esferas Directivas de la organización, centrada en el riesgo ayudará a desarrollar una mayor resiliencia ante los incidentes cibernéticos, transformando las amenazas en oportunidades de aprendizaje y mejora continua.

Base Sólida para la Innovación: Con un enfoque claro y efectivo en GRC y ciberseguridad, las organizaciones estarán mejor posicionadas para innovar y aprovechar nuevas oportunidades de negocio con confianza.

Conclusión

Durante 2025, el entorno de GRC y gestión de riesgos seguirá evolucionando en respuesta a las nuevas amenazas y regulaciones. Se espera un endurecimiento normativo relacionado con la protección de datos, privacidad e integridad operativa impulsada por legislaciones como GDPR o CCPA expandiéndose globalmente. Las organizaciones tendrán que implementar mejores controles dentro del marco GRC para garantizar el cumplimiento normativo sin comprometer su agilidad operativa, por lo cual aquellas organizaciones que adopten estas tendencias estratégicas no solo estarán mejor preparadas para enfrentar los desafíos de ciberseguridad, sino que también podrán impulsar su crecimiento y agilidad en un mercado cada vez más competitivo. Una integración sólida de GRC en la cultura empresarial y la tecnológica será fundamental para garantizar la sostenibilidad y el éxito en el futuro.

Atte. Hector M. Amodeo
Socio Gerente Comercial
ImperiaSTI SRL