POWER LAWYERS
DE REPÚBLICA DOMINICANA
2023

RIZEK ABOGADOS

CIBERSEGURIDAD: PLAN Y DEFENSA

República Dominicana ha implementado normativas en ciberseguridad, incluyendo la ley núm. 53-07 de Crímenes y Delitos de Alta Tecnología, el reglamento de seguridad cibernética adoptado por la Junta Monetaria en 2018 para entidades financieras, y el Reglamento de Ciberseguridad para el acceso a internet, emitido por el Consejo Directivo del INDOTEL en 2021.

Jessica
ARTHUR JIMÉNEZ
Asociada Senior
Rizek Abogados

José Alfredo
RIZEK VIDAL
Socio Gerente
Rizek Abogados

María Virginia
IRIZARRY
Asociada Junior
Rizek Abogados

Luis Guillermo
FERNÁNDEZ
Asociado Senior
Rizek Abogados

¿Cuál ha sido la experiencia de Rizek Abogados en casos relacionados con la ciberseguridad y seguridad de la información? Nuestra firma ha acumulado una notable experiencia asesorando corporaciones, entidades de intermediación financiera, entidades gubernamentales e inversionistas con el objetivo, entre otros, de salvaguardar y proteger los datos personales que manejan; y que ellos a su vez puedan identificar las alertas de ciberseguridad que permitan prevenir cualquier ataque que pueda afectar el desenvolvimiento de sus operaciones diarias.

¿Qué servicios ofrecen en materia de ciberseguridad? Hemos acompañado a nuestros clientes en el diseño, implementación y ejecución de estrategias de gestión de riesgos y prevención de la cibercriminalidad y de protección de datos personales. Asimismo, en caso de intentos de ataques a los sistemas informáticos o intromisión en la privacidad de la información generada por nuestros clientes, brindamos asesoría legal especializada para la detección, mitigación y control de riesgos y, eventualmente, la debida representación legal para la identificación y persecución de los infractores.

¿Cuáles niveles de especialización han alcanzado en leyes ciberseguridad? Como política formal de la oficina, fomentamos su capacitación continua en las respectivas áreas de negocios de nuestros clientes, lo que nos permite adelantarnos a las modificaciones y actualizaciones de las reglas técnicas y normativas. Esto nos habilita a mejor resguardar y prever las posibles eventualidades riesgosas que pudieran padecer nuestros representados.

¿Qué pasos implementan para que sus clientes estén conformes con las leyes de ciberseguridad aplicables? Participamos activamente en las consultas públicas, propuestas legislativas y, en ocasiones, como miembros de las comisiones de expertos que influyen de manera directa en la revisión de los distintos proyectos que son sometidos al Congreso Nacional o que son propuestos por los organismos autónomos y especializados del Estado dominicano en la materia.

¿Qué acciones legales son aplicadas al momento de que una persona es víctima de un ataque cibernético o robo de datos? Conforme a la Ley 53-07, en caso de que alguien acceda de manera ilegal a un sistema informático, telemático o de telecomunicaciones que contenga información personal de usuarios de empresas o proveedores de servicios en el territorio dominicano, se expone a la condena del pago de 1 a 200 salarios mínimos vigentes y tres meses a un año de prisión.

¿Cómo aplican las auditorías de seguridad y riesgos cibernéticos? Se trata de dos procesos fundamentales en el ámbito de la ciberseguridad, diseñados para identificar y abordar posibles vulnerabilidades y riesgos en los sistemas de tecnología de la información. Las primeras se realizan a través de revisiones exhaustivas de sistemas, redes y procesos de la entidad u organización respectiva, para evaluar su nivel de seguridad y garantizar el cumplimiento de las políticas y regulaciones establecidas. La evaluación de riesgos cibernéticos identifica amenazas y vulnerabilidades en corporaciones o entidades comerciales, analizando la probabilidad e impacto en los activos digitales y la seguridad del negocio. Utilizando un enfoque basado en riesgos, se desarrollan estrategias de mitigación y se asegura una gestión eficaz de la seguridad cibernética. La entidad se somete a monitoreo y verificación constante para detectar, corregir y mitigar los riesgos, asegurando una gestión eficaz de la seguridad cibernética. Su finalidad es poder mantener una postura de seguridad de la organización y garantizar la preparación para combatir las amenazas que continuamente se desarrollan y cambian en el entorno digital.

Las regulaciones de privacidad y ciberseguridad implican recoger información sobre la arquitectura de los sistemas, políticas controles internos, y ejecutar pruebas técnicas como análisis de penetración y escaneo de vulnerabilidades.

RIZEK
ABOGADOS

Ave. Gustavo Mejía Ricart
No. 106, Torre Piantini,
Suite 802, Santo Domingo, RD.
(809) 547-4748
www.rizekabogados.com
@Rizekabogados

El objetivo de una auditoría de seguridad es identificar y mejorar brechas y vulnerabilidades en los controles de seguridad.