POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN
(CALIDAD, SERVICIOS INFORMÁTICOS, SEGURIDAD DE LA INFORMACIÓN, ANTISOBORNO, CONTINUIDAD DEL NEGOCIO, INFORMACIÓN DE LA PRIVACIDAD, SEGURIDAD EN SERVICIOS Y PROTECCIÓN DE PII EN LA NUBE)

GRD RADICAL CORPORATION C.L. **(GRUPO RADICAL)**, es una empresa privada con operaciones a nivel nacional e internacional, dedicada a brindar servicios y soluciones tecnológicas en ciberseguridad, infraestructura y data center; con capacidad colectiva para añadir valor y mejorar la satisfacción del cliente, gestionando todo el ciclo de vida de nuestros productos y servicios al garantizar la confidencialidad, integridad y disponibilidad de la información, gestionando la continuidad del negocio, evitando caso de soborno, asegurando la privacidad de la información y sus servicios en entornos cloud.

GRD RADICAL CORPORATION C.L. mantiene su compromiso con la implementación, el mantenimiento y la mejora continua de su Sistema Integrado de Gestión (SIG), tomando como referencia los requisitos aplicables de las normas internacionales ***ISO 9001:2015-****Sistema de gestión de la calidad*; ***ISO 20000-1:2018-****Tecnologías de la información - Sistemas de Gestión del Servicio;* ***ISO 27001:2022-*** *Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información;* ***ISO 37001:2016-****Sistema de gestión antisoborno;* ***ISO 22301:2019-*** *Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio;* ***ISO 27701:2019-****Técnicas de Seguridad - Extensión a ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información de privacidad;* ***ISO 27017:2015*** *Tecnología de la información — Técnicas de seguridad — Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube*, **ISO 27018:*2019*** *Código de prácticas para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII.* Así también se considera los marcos de referencia, estándares y requisitos aplicables relacionados con SOC, CSIRT, DCOS y SIM3, así como la legislación vigente y demás obligaciones legales, reglamentarias, contractuales y normativas que correspondan a sus actividades y al alcance del SIG. En este marco, la organización orienta sus esfuerzos al cumplimiento de los objetivos de calidad, gestión de servicios, seguridad de la información, privacidad y protección de datos personales, prevención del soborno, continuidad del negocio y seguridad de los servicios en la nube. Para ello, promueve la gestión de riesgos y oportunidades, el cumplimiento de los requisitos aplicables, la optimización de los procesos y el fortalecimiento de sus capacidades, con el propósito de mejorar continuamente el desempeño del SIG, la satisfacción de las partes interesadas y la sostenibilidad de la organización.

La Alta Dirección de nuestra empresa ratifica además su compromiso para que:

- Proporcione un marco de referencia para el establecimiento, revisión y logro de los objetivos del SIG;
- Cumpla con los requisitos y normas aplicables del SIG, alineando los procesos internos con estándares internacionales y regulaciones locales.
- Promueva la mejora continua del SIG y los servicios, incorporando prácticas para el tratamiento ético de la información, respetando los principios de confidencialidad, integridad y disponibilidad.
- Explique las consecuencias de no cumplir con las políticas del SIG.
- Asigne responsables de los Sistema de Gestión, así como la autoridad y responsabilidad para la supervisión de la implementación, mantenimiento, mejora y la toma de medidas administrativas y sanciones con el personal que incumpla con las políticas, procedimientos del SIG.
- Promueva el desarrollo de una cultura ética profesional en todo su personal y contratistas.
- Promueva el planteamiento de inquietudes de buena fe o sobre la base de una creencia razonable, en confianza y sin temor a represalias.
- Cumpla con el desarrollo de la Política Antisoborno, Política de Seguridad y Privacidad de la Información y la Política de Continuidad del Negocio.

Esta política está disponible como información documentada, se comunica en el idioma apropiado dentro de la organización, a los socios de negocios y demás partes interesadas según corresponda.