POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

REM Tools entiende el valor único y crítico de los datos de nuestros clientes. Por ello, la protección y la confidencialidad de la información son fundamentales para nuestras operaciones. Mantenemos un compromiso que se refleja en el esfuerzo constante para asegurar que nuestras plataformas y servicios digitales cumplan con altos estándares de seguridad. Esto nos permite ser un socio confiable para todos nuestros clientes.

*La finalidad de la Política de Seguridad de la Información de **REM Tools** es cumplir con los principios fundamentales y normas internacionales para la administración de la seguridad de la información. Enfocándonos en salvaguardar la confidencialidad, integridad y disponibilidad de los recursos de información y tecnológicos que son propiedad de la organización o están bajo su custodia. El objetivo esencial es asegurar que las distintas áreas de negocio de **REM Tools** hagan inclusión de prácticas de seguridad a través del tratamiento de riesgos tecnológicos presentes en nuestro entorno adoptando una postura de prevención que nos permita mitigar cualquier impacto.*

La Dirección de **REM Tools** está decididamente comprometida con el Sistema de Gestión de la Seguridad de la Información, priorizando las necesidades y expectativas de todos nuestros clientes, inversionistas y autoridades. Esto nos facilita asegurar y demostrar que nuestra tecnología y administración se ajusta a los siguientes principios y objetivos:

Principios

Confidencialidad: Todo dato en el entorno digital de **REM Tools** está protegido de personas NO autorizadas.

Integridad: REM Tools garantiza que todos los datos estén completos, sean exactos y válidos, previniendo cualquier tipo de manipulación no autorizada.

Disponibilidad: REM Tools mantiene un entorno digital seguro y persistente ante cualquier incidente o escenario de contingencia con el único objetivo de no comprometer o afectar los intereses de nuestros clientes.

Objetivos

1) Identificar, clasificar y tratar al menos el 90% de los riesgos críticos de seguridad.

2) Evaluar en al menos un 80% los controles de protección de los activos de información críticos.

3) Fomentar una cultura de seguridad para el 100% del personal involucrado en el manejo de información sensible.

La estrategia de seguridad de **REM Tools** se basa en la Norma internacional ISO/IEC 27001:2013. Hemos establecido y formalizado un conjunto de políticas, procedimientos y mejores prácticas de seguridad para proteger los activos de información de la organización frente a amenazas, internas o externas, deliberadas o accidentales, enfocándonos principalmente en la prevención de ciberfraudes y ciberataques.

La Dirección ha dispuesto de los medios y recursos necesarios para establecer e implementar las medidas de control necesarias. Las Políticas de Seguridad se mantienen actualizadas y adecuadas al entorno de riesgo de **REM Tools**. Así mismo, se mantiene la directriz de mejorar de forma continua la capacidad técnica a través de la formación del personal.

La Dirección ha formalizado un compromiso con sus clientes en garantizar el puntual cumplimiento a los objetivos de seguridad de la información, así como a dar cumplimiento a los requisitos legales y regulatorios que le apliquen.

Nota: Esta Política se comunicará a todas las partes interesadas internas y externas dentro del alcance del SGSI para su consulta.