POLITICA DE SEGURIDAD INFORMATICA Y CIBERSEGURIDAD

En Consorcio Qutub Minar SAS, entendemos que la información es uno de nuestros activos más valiosos y un pilar fundamental para la prestación de nuestros servicios en el desarrollo de software y la creación de aplicaciones tecnológicas. El propósito de la siguiente política de seguridad de la información tiene como objetivo establecer las directrices y controles para la protección de la información que se gestiona en el sistema, esto ayuda a minimizar los riesgos asociados a accesos no autorizados, pérdida de información y amenazas cibernéticas.

Dando cumplimiento a las normativas vigentes, Consorcio Qutub Minar SAS define el modelo de política de seguridad de la información y la seguridad digital, que brinda los principios y responsabilidades en materia de seguridad de la información, proporcionando un marco de referencia para la prevención, detección y respuesta ante incidentes de seguridad.

Esta política es de cumplimiento obligatorio para todos los usuarios, administradores, desarrolladores, clientes y terceros que tienen acceso a nuestra información. La implementación de esta política asegura el cumplimiento de normativas vigentes y buenas prácticas de seguridad, alineadas con estándares de calidad.

El objetivo de esta política de seguridad de la información es proteger la información. los sistemas, los equipos de cómputo y todo lo relacionado a la infraestructura tecnológica de Consorcio Qutub Minar SAS de cualquier acceso no autorizado, pérdida de información, alteración de información o infraestructura de cualquier otra amenaza que pueda surgir en la operatividad y manejo de los sistemas de la empresa y que puedan comprometer la seguridad de la información.

Esta política de seguridad de la información es aplicable a todos los activos de información de Consorcio Qutub Minar SAS que componen los sistemas de información, redes, servidores, bases de datos, aplicaciones, dispositivos corporativos o personales que tengan acceso a información confidencial utilizada dentro de la empresa. Cualquier excepción a esta política deberá ser evaluada y aprobada por el Departamento de TI y personal administrativo.

Normas y reglas de aplicación:

Control de accesos: Sólo el personal autorizado puede acceder a sistemas y datos sensibles.

Auditorías y evaluaciones de riesgos: Se realizan de forma periódica para mitigar vulnerabilidades.

Actualización de software y sistemas: Se aplicarán parches de seguridad y mantenimiento constante.

Gestión de incidentes: Se establecerán procedimientos claros para la identificación y resolución de amenazas.

Concienciación y capacitación: Se capacitará regularmente a los empleados en buenas prácticas de ciberseguridad, fomentando una cultura de seguridad en toda la organización.

Seguridad en bases de datos: Implementación de cifrado, segmentación de accesos y auditoría de consultas.

Disponibilidad y redundancia: Uso de mecanismos de replicación y almacenamiento seguro.

El incumplimiento de esta política podrá dar lugar a sanciones disciplinarias conforme a la normativa interna y las regulaciones legales vigentes. La presente política será revisada y actualizada periódicamente para asegurar su eficacia y adaptación a los nuevos desafíos tecnológicos.

Jorge Villate C.
Gerente General
Fecha: 25 de Febrero de 2025

CONTROL DE CAMBIOS

VERSIÓN	FECHA	CAMBIOS REALIZADOS	REALIZA	REVISA	APRUEBA
1	25/02/2025	Creación documento	Sara Vertel	Andres Delgado	Jorge Villate Isaza