

Política de Seguridad de la Información - KAMINA

1. NUESTRO COMPROMISO

En KAMINA, la seguridad de la información es un pilar fundamental de nuestra operación. Nos comprometemos a proteger la confidencialidad, integridad y disponibilidad de la información relacionada con:

- Clientes
- Cedentes
- Deudores
- Proveedores
- Colaboradores
- Socios estratégicos

Nuestra gestión de seguridad se basa en principios internacionales alineados con la norma **ISO/IEC 27001** y la legislación ecuatoriana aplicable, incluida la **Ley Orgánica de Protección de Datos Personales (LOPD)**.

2. PRINCIPIOS FUNDAMENTALES

Nuestra Política de Seguridad se fundamenta en los siguientes principios:

- **Confidencialidad:** La información solo es accesible para personas autorizadas.
- **Integridad:** La información se mantiene precisa, completa y protegida contra alteraciones indebidas.
- **Disponibilidad:** Los sistemas y datos están accesibles cuando se requieren.
- **Legalidad:** Cumplimos con la normativa vigente.
- **Responsabilidad compartida:** Todos somos responsables de proteger la información.
- **Mejora continua:** Revisamos y fortalecemos nuestros controles de manera periódica.

3. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

KAMINA cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) que incluye:

- Clasificación formal de la información (Pública, Uso Interno, Restringida, Confidencial).
- Control de accesos basado en autorización y autenticación.
- Registro y monitoreo de accesos.
- Gestión de incidentes de seguridad.
- Políticas de contraseñas seguras y control de privilegios.
- RespalDOS periódicos y pruebas de continuidad del negocio.
- Evaluación y control de proveedores con acceso a información.

4. SEGURIDAD EN LA RELACIÓN CON PROVEEDORES

Todos los proveedores y terceros que tengan acceso a información o sistemas de KAMINA deben:

- Cumplir con los requisitos de seguridad establecidos contractualmente.
- Proteger la información conforme a su nivel de clasificación.
- Implementar controles adecuados para prevenir accesos no autorizados.
- Reportar de inmediato cualquier incidente de seguridad.
- Cumplir con la normativa de protección de datos personales.

El incumplimiento de estos lineamientos puede dar lugar a sanciones contractuales y acciones legales.

5. PROTECCIÓN DE DATOS PERSONALES

KAMINA protege los datos personales conforme a la LOPDP y demás regulaciones aplicables. Esto incluye:

- Tratamiento lícito y transparente de datos.
- Uso limitado a fines autorizados.
- Medidas técnicas y organizativas de seguridad.
- Gestión de incidentes y notificación cuando corresponda.

6. GESTIÓN DE INCIDENTES

Contamos con un proceso formal para:

Aplica a las empresas del grupo Kamina, entre otras KAMINECU S.A. y KAMINAECUADOR S.A.S.

- Detectar incidentes de seguridad.
- Contener y mitigar riesgos.
- Preservar evidencia.
- Comunicar a las partes interesadas cuando sea necesario.
- Implementar acciones correctivas y preventivas.

Promovemos una cultura de reporte oportuno y mejora continua.

7. CAPACITACIÓN Y CULTURA DE SEGURIDAD

Nuestro equipo recibe formación periódica en:

- Seguridad de la información
- Prevención de ciberamenazas
- Protección de datos personales
- Buenas prácticas tecnológicas

El factor humano es considerado la primera línea de defensa.