POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

1. INTRODUCCIÓN

El **GRUPO BRAVO** conformado por ECUAMINERALES / KEIKO / MINMETEC ECUADOR / TRANSVICTORIA mediante este documento dispone las políticas adoptadas para garantizar la seguridad y confidencial de la información, acceso controlado y la protección específica de datos personales.

2. MARCO LEGAL

Nuestra política se basa en La Ley Orgánica de Protección de Datos Personales (Registro Oficial Suplemento 459 del 26-mayo-2021)

Así también, constituye base legal, toda la normativa pertinente, de vigencia actual en el ordenamiento jurídico ecuatoriano, incluyendo el Reglamento a la Ley Orgánica de Protección de Datos Personales, resoluciones vinculantes emitidas por la Superintendencia de Protección de Datos y demás instrumentos jurídicos aplicables.

3. POLÍTICAS

3.1. POLÍTICA DE CONTROL LÓGICO

Objetivo: Limitar el acceso a personas autorizadas, según su función y bajo el principio de mínimo privilegio.

CÓDIGO	DEFINICIÓN	GESTIÓN DE ACCESO / CONTROL DE ACCESOS	
PDP-CL-01	Acceso a sistemas y redes	1	Cuando se requiera acceso temporal a los sistemas, será con autorización documentada y revocación al vencer el plazo. (Bitácora de accesos).
		2	Acceso permanente: Para empleados, basado en perfiles de acceso definidos por rol (Inventario de cuentas y accesos).
		3	Segregación de redes: Implementar VLANs para separar servicios críticos de red administrativa, empleados y WIFI de visitantes.
PDP-CL-02	Acceso a sistemas críticos.	4	Implementación de autenticación multifactor (MFA) para acceso a sistemas críticos.
		5	Prohibición de compartir credenciales.
		6	Cambio periódico de contraseñas, usuarios administrativos cada 3 meses y usuarios finales cada 6 meses.

3.2. POLÍTICA DE GESTIÓN DE LA INFORMACIÓN

Objetivo: Proteger la información mediante respaldos y garantizar la confidencialidad.

CÓDIGO	DEFINICIÓN	RESPALDOS DE INFORMACIÓN / CONFIDENCIALIDAD	
PDP-GI-01	Respaldo de información	1	Los respaldos de sistemas críticos se ejecutarán periódicamente de forma automática.
		2	Se realizará verificación periódicas de validez de respaldos.
		3	Cada empleado es responsable de su información.
		4	Existirán al menos dos copias de las bases de datos, una en ubicación externa y otra en almacenamiento local/interno.
		5	Los respaldos que contengan datos personales o sensibles se protegerán mediante cifrado.
PDP-GI-02	Confidencialidad de la información	7	Todos los empleados firmarán un ACUERDO DE CONFIDENCIALIDAD (NDA) al inicio de la relación laboral.
		8	Todo proveedor o tercero que acceda a datos personales deberá firmar un ACUERDO DE CONFIDENCIALIDAD (NDA) y/o un CONVENIO PARA EL

			ENCARGO DE TRATAMIENTO DE DATOS PERSONALES (DPA) antes de recibir acceso.

3.3. POLÍTICA DE PROTECCIÓN DE DATOS BIOMÉTRICOS

Objetivo: Establecer lineamientos de seguridad para datos biométricos tratados, conforme a la LOPDP.

CÓDIGO	DEFINICIÓN	MEDIDAS ESPECÍFICAS	
PDP-DB-01	Control de accesos a datos biométricos	1	Acceso al equipo biométrico solo a personal autorizado (previa firma de ACUERDO DE CONFIDENCIALIDAD (NDA) y CONVENIO PARA EL ENCARGO DE TRATAMIENTO DE DATOS PERSONALES (DPA).
		2	Registro obligatorio de todos los accesos. (Bitácora de accesos).
PDP-DB-02	Cifrado de datos biométricos	3	Las bases de datos que contengan plantillas biométricas deberán estar cifradas mediante algoritmos seguros (AES-256 o superior).
		4	Las comunicaciones entre lectores biométricos y servidores deberán ir cifradas.
PDP-DB-03	Seguridad física	5	Seguridad a los equipos que almacenan o procesan datos biométricos.
		6	Protección física de los lectores biométricos.
PDP-DB-04	Minimización de datos	7	Los equipos biométricos deben almacenar únicamente plantillas (hash numérico) no imagen.
PDP-DB-05	Retención y eliminación	8	Al desvincular al empleado, el dato biométrico debe ser eliminado de forma segura (máximo 30 días después de la salida).

3.4. POLÍTICA DE ACCESO Y CONTROL DE LA INFORMACIÓN

Objetivo: Limitar el acceso a los recursos de información mediante gestión de usuarios, privilegios y autenticación robusta.

CÓDIGO	DEFINICIÓN	ACCESO / PRIVILEGIOS / AUTENTICACIÓN / TERMINACIÓN	
PDP-AC-01	Cuentas de usuario	1	Se mantendrá un inventario de cuentas de usuario (Inventario de cuentas y accesos).
		2	Queda prohibido el uso de cuentas personales para gestiones de la empresa.
		3	Queda prohibido compartir cuentas.
PDP-AC-02	Principio de menor privilegio	4	Los privilegios de acceso serán asignados según las funciones del puesto (Definición de privilegios).
		5	Se realizará una revisión anual de los privilegios asignados para verificar su necesidad.
		6	Todo cambio en privilegios deberá ser documentado y autorizado.
PDP-AC-03	Autenticación (contraseñas)	7	Complejidad de contraseñas será con un mínimo 8 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.
		8	Prohibición de contraseñas en blanco o por defecto.
		9	Activar la AUTENTICACIÓN MULTIFACTOR (MFA) siempre que sea posible
PDP-AC-04	Terminación de la relación laboral o contractual	10	Revocación inmediata de todos bitácora de accesos.
		11	Actualización del inventario de cuentas.

3.5. POLÍTICA PARA DISPOSITIVOS MÓVILES (BYOD Y MDM)

Objetivo: Regular el uso de dispositivos móviles personales para fines laborales, mitigando el riesgo de fuga de datos.

CÓDIGO	DEFINICIÓN	MEDIDAS ESPECÍFICAS	
PDP-DM-01	Dispositivos móviles	1	Todos los dispositivos móviles (personales o de empresa) que accedan a datos personales o correo corporativo deberán tener solución MDM (MOBILE DEVICE MANAGEMENT).

		2	Borrado remoto en caso de pérdida o robo.
PDP-DM-02	WhatsApp	3	No compartir por WhatsApp información sensible de (datos financieros, crediticios, contraseñas)
		4	Obtener consentimiento previo del cliente para contacto comercial.
		5	Al finalizar la relación con el cliente, eliminar los chats que contengan datos personales.
PDP-DM-03	Política general para EQUIPO PERSONAL USADO PARA EL TRABAJO (BYOD)	6	Permitir, en caso necesario, el borrado remoto de información corporativa si el dispositivo se pierde o al finalizar la relación laboral.
		7	Mantener las últimas actualizaciones de seguridad del sistema operativo.
		8	Tener activado el bloqueo.

3.6. POLÍTICA DE CONSENTIMIENTOS Y BASE LEGAL

Objetivo: Garantizar que todo tratamiento de datos personales cuente con una base legal válida, priorizando el consentimiento informado, explícito y revocable.

CÓDIGO	DEFINICIÓN	MEDIDAS ESPECÍFICAS	
PDP-CS-01	Consentimiento para empleados	1	Todo empleado deberá firmar un formulario de consentimiento
PDP-CS-02	Consentimiento para clientes	2	Para clientes se obtendrá un consentimiento para servicios de postventa, seguimiento comercial, marketing, uso de imagen y geolocalización para logística.
		3	Para clientes de crédito a más de consentimiento general de clientes, se obtendrá consentimiento para consulta a burós, gestión de cobranza y verificación de referencias.
		4	El consentimiento se obtendrá mediante un formulario físico o digital al momento del primer contacto con el cliente o en la solicitud de compra.
PDP-CS-03	Consentimiento para prospectos y hojas de vida	5	Al recibir una hoja de vida o en la entrevista, se solicitará al candidato la firma de un consentimiento para evaluar y almacenar sus datos durante 180 días y posterior eliminación segura de no es seleccionado.
PDP-CS-04	Consentimiento para uso de imagen en redes sociales	6	Antes de publicar cualquier foto o video de clientes, se obtendrá una autorización expresa de uso de imagen.
		7	No se publicarán imágenes de menores sin autorización de sus padres o tutores.
PDP-CS-05	Derecho de revocación	8	Todos los formularios de consentimiento incluirán un explicación clara que indique al titular la forma revocar su consentimiento en cualquier momento.

3.7. POLÍTICA DE ATENCIÓN A DERECHOS ARCO

Objetivo: Establecer procedimientos claros para que los titulares puedan ejercer sus derechos (Acceso, Rectificación, Cancelación, Oposición, Portabilidad).

CÓDIGO	DEFINICIÓN	PROCEDIMIENTO	
PDP-ARCO-01	Canal de atención	1	Se habilitará el correo datos.personales@ecuamineralesgb.com como canal de atención exclusivo.
		2	También se aceptarán solicitudes físicas en las oficinas de la empresa.
PDP-ARCO-02	Plazos de respuesta	3	Toda solicitud será respondida en un plazo máximo de 15 días hábiles.
PDP-ARCO-03	Procedimiento interno	4	El DELEGADO DE PROTECCIÓN DE DATOS (DPD/DPO) recibirá la solicitud, verificará la identidad del titular, y coordinará con el área correspondiente para recabar la información o ejecutar la acción.
		5	Se mantendrá un registro de todas las solicitudes ARCO con sus fechas y resoluciones.

PDP-ARCO-04	Obligación del personal	6	Todo empleado que reciba o atienda de cualquier manera una consulta sobre datos personales deberá dirigirla a RESPONSABLE o DELEGADO DE PROTECCIÓN DE DATOS (DPD/DPO)

3.8. POLÍTICA DE GESTIÓN DE INCIDENTES

Objetivo: Establecer procedimientos claros gestionar vulneraciones de seguridad.

CÓDIGO	DEFINICIÓN	PROCEDIMIENTO	
PDP-INC-01	Detección y reporte interno	1	Todo empleado que detecte una posible vulneración (pérdida de dispositivo, acceso no autorizado, filtración, robo de información) debe reportarlo inmediatamente al RESPONSABLE o DELEGADO DE PROTECCIÓN DE DATOS (DPD/DPO).
PDP-INC-02	Evaluación y contención	2	Se evaluará la naturaleza de la vulneración, datos afectados, número de titulares involucrados, riesgo para los derechos y libertades.
		3	Se implementarán medidas de contención inmediatas.
PDP-INC-03	Notificación a la Autoridad	3	Si la vulneración constituye un riesgo para los derechos de los titulares, se notificará a la Superintendencia de Protección de Datos en un plazo máximo de 5 días desde que se tuvo constancia (Art. 43 LOPDP).
PDP-INC-04	Notificación al titular afectado	4	Si el riesgo es alto, se notificará al titular afectado en un plazo máximo de 3 días (Art. 46 LOPDP).
		5	La notificación incluirá: naturaleza de la vulneración, datos afectados, medidas adoptadas, recomendaciones.
PDP-INC-05	Registro y medidas correctivas	6	Todo incidente será registrado en el formulario de Gestión de Incidentes (Doc. Gestión de incidentes).
		7	Se implementarán medidas correctivas para evitar recurrencia.

3.9. POLÍTICA DE RELACIÓN CON ENCARGADOS DE TRATAMIENTO (PROVEEDORES)

Objetivo: Regular contractualmente el acceso a datos personales por parte de proveedores y terceros, cerrando las brechas identificadas en el GAP.

CÓDIGO	DEFINICIÓN	MEDIDAS	
PDP-EC-01	Identificación de encargados	1	Se mantendrá un listado actualizado de todos los proveedores que actúan como ENCARGADOS de tratamiento.
PDP-EC-02	Contratos con encargados (DPA)	2	Todo encargado de tratamiento deberá firmar un CONVENIO PARA EL ENCARGO DE TRATAMIENTO DE DATOS PERSONALES (DPA) y un ACUERDO DE CONFIDENCIALIDAD (NDA).
PDP-EC-03	Transferencias internacionales	3	Cualquier transferencia de datos a servidores en el extranjero deberá contar con garantías adecuadas. Y conocer la ubicación exacta de los servidores.

3.10. TIEMPOS DE RETENCIÓN Y ELIMINACIÓN DE DATOS

Objetivo: Establecer plazos máximos de conservación de datos personales y procedimientos de destrucción segura.

TIPO DE DATO	TIEMPO DE RETENCIÓN
Hojas de vida de candidatos no seleccionados	180 días
Datos laborales de empleados activos	Vigencia de la relación laboral
Datos laborales de empleados desvinculados	Según Normativas aplicables
Datos de salud ocupacional (exámenes médicos)	10 años (normativa de seguridad y salud)
Plantillas biométricas (huella)	Hasta finalizar la relación laboral
Datos de clientes inactivos	Según Normativas aplicables
Datos crediticios (buró, deudas)	Según Normativas aplicables

Grabaciones de videovigilancia	30 días (salvo vinculación a una investigación lega)
Datos de navegación web (cookies)	Según Política de Cookies