McEwen Copper - Proyecto Minero Los Azules

Política de Seguridad y Privacidad de la Información del Sitio Web

Documento público

Versión: 1.2 | Fecha de publicación: 05/02/2026

Este documento describe las prácticas de seguridad y privacidad aplicables al sitio web del Proyecto Minero Los Azules y su interacción con los usuarios.

1. Objetivo

Establecer los lineamientos generales de seguridad y privacidad aplicables al sitio web del Proyecto Minero Los Azules (en adelante, el "Sitio"), incluyendo la protección de la información publicada por la Empresa y la información que los usuarios puedan proporcionar o cargar a través del Sitio.

2. Alcance

Esta Política aplica a la navegación y uso del Sitio, a los formularios de contacto y a cualquier funcionalidad que habilite el envío de información, documentación o contenidos por parte de los usuarios (por ejemplo, adjuntos, mensajes, postulaciones u otros).

Esta Política no aplica a sitios web de terceros a los que se pueda acceder mediante enlaces o integraciones desde el Sitio. Cada tercero posee sus propias políticas y prácticas.

3. Identificación del responsable

El responsable del Sitio y del tratamiento de la información recopilada mediante el mismo es McEwen Copper (Andes Corporación Minera S.A. - Proyecto Minero Los Azules) (en adelante, la "Empresa").

Canales de contacto:

- Consultas generales y solicitudes de privacidad (incluye canal de Encargado/LGPD/privacidad de datos personales cuando corresponda): consultasysugerencias@mcewencopper.com
- **Reportes de incidentes o vulnerabilidades de seguridad:** cybersecurity@mcewencopper.com

4. Marco de referencia

La Empresa gestiona la seguridad de la información mediante un enfoque basado en riesgos y buenas prácticas generalmente aceptadas, inspirado en los principios de un Sistema de Gestión de Seguridad de la Información (SGSI), tomando como referencia los estándares ISO/IEC 27001 y, cuando resulte pertinente, controles alineados con ISO/IEC 27002.
En materia de protección de datos personales, la Empresa tiene en consideración la normativa aplicable en función de la naturaleza del tratamiento y de su alcance territorial, incluyendo la Ley Nº 25.326 (Argentina), la Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) de Brasil y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (Reglamento General de Protección de Datos – RGPD), sin perjuicio de otras disposiciones legales que pudieran resultar exigibles en cada jurisdicción.
Esta Política se complementa con los Términos y Condiciones del Sitio. En caso de contradicción, prevalecerán los Términos y Condiciones para los aspectos contractuales y de uso, y la presente Política para los aspectos de seguridad y privacidad.

5. Principios de seguridad y privacidad

La Empresa adopta los siguientes principios:

- Confidencialidad: acceso a la información solo por personas autorizadas y para fines legítimos.
- Integridad: protección contra alteraciones no autorizadas o accidentales, manteniendo la exactitud y consistencia de la información.
- Disponibilidad: acceso oportuno a la información y a los servicios del Sitio, con medidas de continuidad cuando corresponda.
- Minimización de datos: recopilación de la información estrictamente necesaria para cumplir con finalidades legítimas.
- Transparencia: información clara sobre qué datos se recopilan, cómo se usan y con quién se comparten.
- Seguridad desde el diseño y por defecto: incorporación de controles de seguridad y privacidad en el diseño, desarrollo y operación del Sitio.

6. Categorías de información involucradas

En el marco del Sitio pueden existir las siguientes categorías de información:

- Información publicada por la Empresa en el Sitio (textos, imágenes, documentos, comunicados, materiales corporativos).
- Información técnica y registros de seguridad (por ejemplo, fecha y hora de acceso, dirección IP, tipo de navegador, eventos de seguridad y registros de auditoría).
- Datos personales provistos por el usuario (por ejemplo, nombre, correo electrónico, teléfono, empresa, país, contenido del mensaje).
- Archivos o documentación cargada por el usuario cuando el Sitio habilite dicha funcionalidad (por ejemplo, CV, cartas, formularios, evidencia o adjuntos).
- Contenidos aportados por terceros (por ejemplo, comentarios u otra información compartida públicamente por usuarios, si el Sitio habilitara dichas funcionalidades).

7. Medidas de seguridad aplicadas al Sitio

La Empresa aplica medidas técnicas y organizativas razonables, acordes al riesgo, para proteger la información y reducir la probabilidad e impacto de incidentes. Estas medidas pueden incluir, entre otras:

- Gestión de accesos: controles de autenticación, autorización y privilegio mínimo para administrar el Sitio y sus sistemas asociados.
- Cifrado en tránsito: uso de mecanismos de comunicación segura (por ejemplo, HTTPS/TLS) para la transmisión de datos entre el usuario y el Sitio.
- Cifrado y/o protecciones en reposo: medidas de protección para bases de datos, respaldos y repositorios, cuando corresponda según el nivel de riesgo.

- Monitoreo y registros: recolección y análisis de logs para detectar actividades anómalas, fraudes, abuso o intentos de acceso no autorizado.
- Gestión de vulnerabilidades: actualización y mantenimiento de componentes, corrección de fallas, revisiones periódicas y/o pruebas de seguridad.
- Respaldo y continuidad: copias de seguridad y procedimientos de recuperación para reducir el impacto de fallas o incidentes.
- Seguridad en proveedores: selección y gestión de terceros (por ejemplo, hosting o servicios en la nube) con requisitos de seguridad acordes.
- Seguridad del desarrollo y cambios: controles de revisión, pruebas y aprobación de cambios antes de publicar nuevas versiones del Sitio.
- Gestión de incidentes: procedimientos para la detección, contención, análisis y respuesta ante incidentes de seguridad.

Si bien la Empresa implementa medidas para proteger el Sitio, ningún sistema es completamente infalible. Por ello, la Empresa no garantiza que el Sitio esté libre de vulnerabilidades o de accesos indebidos.

8. Privacidad y tratamiento de datos personales

Cuando el usuario interactúa con el Sitio, la Empresa puede recolectar y tratar datos personales. Dicho tratamiento se realizará con medidas de seguridad razonables y considerando la normativa aplicable en materia de protección de datos personales, incluyendo la Ley Nº 25.326 (Argentina) y, cuando corresponda por la naturaleza o el alcance territorial del tratamiento, la Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) de Brasil y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (Reglamento General de Protección de Datos – RGPD).
Cuando resulte aplicable, la Empresa inscribirá y mantendrá actualizadas las bases de datos personales correspondientes ante el registro u organismo de control competente, conforme lo previsto por la normativa local.

8.1. Datos personales que podemos recopilar

Dependiendo del uso del Sitio, se podrán recopilar:

- Datos identificatorios y de contacto: nombre y apellido, correo electrónico, teléfono, empresa u organización, cargo, país u otros datos que el usuario incluya voluntariamente.
- Datos de interacción: contenido de mensajes enviados mediante formularios, consultas, comentarios (si existieran), y comunicaciones con la Empresa.
- Datos técnicos y de seguridad: dirección IP, identificadores de dispositivo, datos de navegador, cookies y registros de eventos asociados a la seguridad y operación del Sitio.

- Documentación y adjuntos: información contenida en archivos que el usuario envíe o cargue (por ejemplo, CV o documentación de soporte).

8.2. Finalidades del tratamiento

La Empresa podrá tratar los datos personales para:

- Responder consultas y gestionar solicitudes realizadas por el usuario.
- Gestionar procesos de contacto, comunicaciones y, cuando aplique, evaluaciones de postulaciones o solicitudes vinculadas al proyecto.
- Administrar y mejorar el Sitio, incluyendo análisis de uso, diagnóstico de errores y optimización del rendimiento.
- Proteger la seguridad del Sitio y de los usuarios, prevenir abusos, fraudes o ataques, y permitir la investigación de incidentes.
- Cumplir obligaciones legales y atender requerimientos de autoridades competentes, cuando corresponda.

8.3. Bases que habilitan el tratamiento

Según el caso y la normativa aplicable, la Empresa podrá basarse en: (i) el consentimiento del titular; (ii) la atención de una solicitud del usuario y/o la ejecución de una relación precontractual o contractual; (iii) el interés legítimo del titular y/o de la Empresa, ponderado con los derechos del titular; (iv) el cumplimiento de obligaciones legales y/o requerimientos de autoridad competente; y/o (v) el ejercicio regular de derechos en procesos administrativos o judiciales, la prevención del fraude y la protección de la seguridad del Sitio, de los usuarios y de los sistemas.

8.4. Destinatarios y terceros proveedores

Los datos personales podrán ser accedidos por personal autorizado de la Empresa y, cuando sea necesario, por proveedores que prestan servicios para operar el Sitio (por ejemplo, hosting, almacenamiento, envío de correos, soporte técnico o analítica), quienes actuarán siguiendo instrucciones de la Empresa y con medidas de seguridad razonables.

La Empresa también podrá divulgar información cuando exista una obligación legal, una orden de autoridad competente, o cuando sea necesario para ejercer o defender derechos.

8.5. Transferencias internacionales

Al utilizar servicios tecnológicos y/o proveedores ubicados fuera del país de residencia del usuario, pueden producirse transferencias internacionales de datos. En esos casos, la Empresa procurará implementar salvaguardas y mecanismos adecuados según la normativa aplicable y el nivel de riesgo (por ejemplo, acuerdos contractuales, medidas técnicas y organizativas, y/o verificación de niveles adecuados de protección), incluyendo los criterios previstos en la Ley Nº 25.326 (Argentina) y en la LGPD (Brasil).

8.6. Plazos de conservación

La Empresa conservará los datos personales durante el tiempo necesario para cumplir con las finalidades informadas y/o mientras exista una obligación legal de conservación. Los registros técnicos y de seguridad se conservarán por períodos razonables para fines de auditoría, prevención de fraude y respuesta a incidentes.

8.7. Derechos de los titulares

El usuario, como titular de los datos, puede ejercer sus derechos conforme a la normativa aplicable. Para ello, puede escribir a consultasysugerencias@mcewencopper.com. La Empresa podrá requerir información razonable para verificar la identidad del solicitante y prevenir fraudes.

- Acceso/confirmación: solicitar información sobre los datos personales tratados.
- Rectificación/actualización: corregir datos incompletos, inexactos o desactualizados.
- Supresión/eliminación: solicitar la eliminación cuando corresponda, sujeto a obligaciones legales o intereses legítimos de terceros.
- Oposición y/o revocación del consentimiento: cuando el tratamiento se base en consentimiento u otras bases que admitan oposición.
- Portabilidad (Brasil/LGPD): solicitar la portabilidad conforme la reglamentación aplicable.
- Información sobre destinatarios: conocer con quiénes se comparten o ceden datos, cuando corresponda.

Plazos legales (referenciales): en Argentina, el derecho de acceso debe ser atendido dentro de los diez (10) días corridos de la intimación fehaciente y la rectificación/actualización/supresión dentro de los cinco (5) días hábiles de recibido el reclamo. El derecho de acceso puede ejercerse gratuitamente a intervalos no inferiores a seis (6) meses, salvo interés legítimo.

En Brasil (LGPD), la confirmación de existencia o el acceso a datos personales se proveerá, a solicitud del titular, en formato simplificado, de manera inmediata; o, mediante una declaración clara y completa, dentro de hasta quince (15) días contados desde la solicitud, sin perjuicio de otros plazos y condiciones reglamentarias aplicables.

Ley Nº 25.326 (Argentina) – leyenda: “El titular de los datos personales tiene la facultad de ejercer el derecho de acceso a los mismos en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto, conforme lo establecido en el artículo 14, inciso 3 de la Ley Nº 25.326”.

Asimismo, el usuario puede presentar reclamos ante la Agencia de Acceso a la Información Pública (AAIP), autoridad de control en Argentina, y/o ante la Autoridade Nacional de Proteção de Dados (ANPD) en Brasil, según corresponda.

En función de la legislación aplicable y del alcance territorial del tratamiento, dichos derechos podrán incluir, entre otros, el derecho de acceso o confirmación sobre la existencia de datos personales tratados; la rectificación o actualización de datos inexactos, incompletos o desactualizados; la supresión o eliminación de los datos cuando corresponda, sujeta a obligaciones legales o intereses legítimos; la

oposición al tratamiento y/o la revocación del consentimiento, cuando este constituya la base legal; la portabilidad de los datos, cuando resulte aplicable; y el derecho a solicitar información sobre los destinatarios o terceros con quienes se compartan los datos, conforme a lo previsto en la Ley Nº 25.326 (Argentina), la Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) de Brasil y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (Reglamento General de Protección de Datos – RGPD), sin perjuicio de otras normas que resulten aplicables en cada jurisdicción.

8.8. Cookies y tecnologías similares

El Sitio puede utilizar cookies y tecnologías similares para funcionar correctamente, recordar preferencias, mejorar la experiencia del usuario y obtener métricas de uso. El usuario puede configurar su navegador para aceptar, rechazar o eliminar cookies. La desactivación de cookies puede afectar el funcionamiento del Sitio.

8.9. Menores de edad

El Sitio no está dirigido a menores de edad. Si la Empresa tomara conocimiento de que se han recopilado datos personales de menores sin la autorización correspondiente, podrá eliminar dichos datos y/o solicitar información adicional para validar la autorización.

9. Información aportada por usuarios y terceros - exclusiones y responsabilidades

El Sitio puede habilitar funcionalidades que permitan a usuarios o terceros enviar o cargar información. En esos casos, aplican las siguientes reglas y exclusiones:

- Responsabilidad del contenido: el usuario es el único responsable por la información y/o contenidos que envíe, cargue, publique o comparta mediante el Sitio.
- Información de terceros: el usuario declara que cuenta con los derechos y autorizaciones necesarias para aportar información (incluyendo datos personales) de terceros. La Empresa no asume responsabilidad por aportes realizados sin autorización.
- No envíe información sensible: salvo que se solicite expresamente y sea estrictamente necesario, el usuario no debe enviar datos sensibles o de especial protección (por ejemplo, información médica, biométrica, financiera, sobre origen racial o étnico, opiniones políticas, convicciones religiosas, vida sexual u otros similares). Si el usuario los envía voluntariamente, lo hace bajo su exclusiva responsabilidad y asumiendo los riesgos asociados.
- Contenido público: si el Sitio habilitara espacios de publicación pública (por ejemplo, comentarios), el usuario debe considerar que cualquier información compartida podrá ser vista, copiada, indexada por motores de búsqueda o reutilizada por terceros, sin control de la Empresa.
- No obligación de monitoreo: la Empresa puede, pero no está obligada a, revisar, moderar o monitorear los contenidos de terceros. La Empresa podrá remover, bloquear o limitar contenidos a su criterio, especialmente si pudieran resultar ilegales, infractores, ofensivos, engañosos o riesgosos.

- Exactitud y veracidad: la Empresa no garantiza la exactitud, integridad o actualidad de los contenidos aportados por terceros y no asume responsabilidad por su uso, interpretación o consecuencias.
- Malware y archivos: la Empresa podrá aplicar controles razonables (por ejemplo, filtros o escaneo) para reducir el riesgo de malware en archivos cargados. Sin embargo, la Empresa no garantiza que los contenidos aportados por terceros estén libres de virus u otros elementos dañinos. El usuario debe utilizar medidas de protección adecuadas en su dispositivo.
- Pérdida de confidencialidad: debido a la naturaleza de Internet, no es posible garantizar confidencialidad absoluta en toda transmisión. El usuario acepta que el envío de información mediante el Sitio puede implicar riesgos inherentes a la transmisión digital.
- Interrupciones y disponibilidad: la Empresa podrá realizar tareas de mantenimiento o enfrentar interrupciones por causas técnicas o de terceros. La Empresa no garantiza disponibilidad continua e ininterrumpida del Sitio.
- Uso indebido por terceros: la Empresa no se responsabiliza por el uso indebido que terceros puedan hacer de información que el usuario publique o comparta (por ejemplo, recolección automatizada de datos públicos, capturas de pantalla, reenvíos o republicaciones).
- Exclusión de responsabilidad: en la máxima medida permitida por la ley, la Empresa no será responsable por daños directos o indirectos derivados de contenidos aportados por terceros o del uso que se haga de dicha información.

10. Enlaces e integraciones de terceros

El Sitio puede contener enlaces o integraciones (por ejemplo, redes sociales, mapas, reproductores, widgets) provistos por terceros. La Empresa no controla las prácticas de seguridad o privacidad de dichos terceros. Se recomienda al usuario revisar sus políticas antes de interactuar con dichos servicios.

11. Reporte de incidentes y ejercicio de derechos

Si el usuario detecta una vulnerabilidad, incidente de seguridad o sospecha de compromiso del Sitio, puede reportarlo a cybersecurity@mcewencopper.com. Para solicitudes de privacidad o ejercicio de derechos relacionados con datos personales, puede contactarse a consultasysugerencias@mcewencopper.com.

La Empresa evaluará los reportes recibidos y adoptará medidas razonables para gestionar el incidente, incluyendo acciones de contención, remediación y mejoras preventivas, cuando corresponda.

12. Actualizaciones de esta Política

La Empresa podrá modificar esta Política para reflejar cambios normativos, técnicos u operativos. La versión vigente será la publicada en el Sitio. Las modificaciones entrarán en vigor desde su publicación.

13. Ley aplicable y jurisdicción

Ley aplicable y jurisdicción

La presente Política se rige por las leyes de la República Argentina. Cualquier controversia relacionada con su interpretación, validez, ejecución o con el uso del Sitio se regirá por lo dispuesto en los Términos y Condiciones y será sometida a los tribunales ordinarios competentes de la Provincia de San Juan, República Argentina.

Normativa aplicable en materia de protección de datos personales

Sin perjuicio de lo establecido en la cláusula anterior, el tratamiento de los datos personales y el ejercicio de los derechos de los titulares podrán quedar sujetos a normativa específica de protección de datos personales en función del lugar de residencia del titular o del alcance territorial del tratamiento. En particular, podrán resultar aplicables, según corresponda, la Ley Nº 25.326 de la República Argentina, la Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) de la República Federativa del Brasil y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos – RGPD), sin perjuicio de otras disposiciones legales que resulten exigibles en cada jurisdicción.

Anexo A. Recomendaciones de seguridad para usuarios

Para reducir riesgos durante la navegación, se recomienda:

- Mantener actualizado el navegador y el sistema operativo del dispositivo.
- Utilizar redes confiables y evitar ingresar datos en redes Wi-Fi públicas no seguras.
- No compartir contraseñas ni códigos de verificación. Desconfiar de correos o mensajes que soliciten credenciales (phishing).
- Verificar que la URL corresponda al Sitio y que la conexión sea segura (https).
- Evitar enviar información sensible o confidencial por formularios o canales no solicitados.