POLÍTICA DE CIBERSEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN

Código: POL-CIB-001
Versión: 1.0
Fecha de emisión: 21 de octubre de 2025
Vigencia: Indefinida
Revisión: Anual o cuando se produzcan cambios normativos relevantes
Aprobada por: Gerencia General – CHIER SpA

1. Objetivo

Establecer los lineamientos generales para la protección de los sistemas informáticos, la información y los datos gestionados por Servicios Mineros e Industriales CHIER SpA (en adelante, "la Empresa"), garantizando la confidencialidad, integridad y disponibilidad de la información, en concordancia con la legislación chilena vigente y las buenas prácticas internacionales de seguridad de la información.

2. Alcance

Esta política aplica a todos los trabajadores, contratistas, asesores y colaboradores que utilicen sistemas, equipos o información perteneciente a la Empresa, cualquiera sea su ubicación física o modalidad de trabajo.

3. Principios generales

a. Confidencialidad: La información corporativa y de terceros debe ser protegida contra el acceso no autorizado.

b. Integridad: La información debe mantenerse completa, precisa y sin alteraciones indebidas.

c. Disponibilidad: Los sistemas e información críticos deben estar disponibles cuando sean necesarios para la operación.

d. Legalidad y cumplimiento: Toda gestión de datos e información se realizará conforme a la Ley N°19.628 sobre Protección de la Vida Privada y demás normas aplicables.

e. Responsabilidad compartida: Cada usuario es responsable de resguardar el uso adecuado de los recursos informáticos de la Empresa.

4. Directrices de seguridad

4.1. Acceso a sistemas y equipos

- Todo acceso a sistemas informáticos deberá realizarse mediante credenciales personales e intransferibles.
- Las contraseñas deben mantenerse confidenciales, con un mínimo de 8 caracteres y combinación alfanumérica.
- Se prohíbe compartir claves o utilizar credenciales de otro usuario.

4.2. Protección de la información

- Los documentos corporativos deberán almacenarse exclusivamente en las plataformas institucionales o servidores autorizados.
- No se debe copiar, descargar o distribuir información sensible sin la debida autorización.
- La información que contenga datos personales deberá ser tratada conforme a la Ley 19.628, asegurando el principio de finalidad y proporcionalidad.

4.3. Uso de correo electrónico y redes

- El correo institucional se utilizará únicamente para fines laborales.
- Se debe evitar abrir archivos o enlaces de origen desconocido.
- Queda estrictamente prohibido el uso de redes públicas o no seguras para acceder a información corporativa.

4.4. Dispositivos personales y móviles

- Los equipos personales que se utilicen para trabajo remoto deben contar con antivirus actualizado y mecanismos de bloqueo.
- En caso de pérdida o robo de un dispositivo con información corporativa, el trabajador deberá informar inmediatamente al área administrativa o de sistemas.

4.5. Copias de seguridad y respaldo

- La Empresa mantendrá copias de respaldo periódicas de los sistemas y documentos críticos.
- Se verificará periódicamente la recuperación efectiva de la información respaldada.

4.6. Gestión de incidentes

- Todo evento que afecte la seguridad de la información (acceso no autorizado, pérdida de datos, malware, etc.) deberá ser reportado de inmediato al encargado designado por la Empresa.
- Se registrará el incidente y se aplicarán medidas correctivas y preventivas.

5. Capacitación y concientización

La Empresa promoverá instancias de capacitación anual en materias de ciberseguridad, uso responsable de la información y prevención de incidentes informáticos, orientadas a fortalecer la cultura organizacional en torno a la protección de datos.

6. Responsabilidades

- **Gerencia General:** Aprobar y supervisar el cumplimiento de esta política.
- **Encargado de Sistemas:** Implementar las medidas técnicas y coordinar la respuesta ante incidentes.
- **Trabajadores y Colaboradores:** Cumplir con los lineamientos establecidos, resguardar la información bajo su responsabilidad y reportar eventuales vulneraciones.

7. Vigencia y revisión

Esta política entra en vigencia desde su aprobación por la Gerencia General y será revisada al menos una vez al año, o cuando existan cambios normativos, tecnológicos o contractuales que así lo requieran.

Servicios Mineros e Industriales CHIER SpA

Aprobado por Gerente General