MINERA VALLE CENTRAL S.A.

Política de Sistema de Gestión de Seguridad de Información (SGSI)

Elaborado por Subgerente de Ingenieria y TI	**Revisado por** Gerente de Continuidad Operacional	**Aprobado por** Gerente General

Tabla de Contenidos

1. IDENTIFICACIÓN DEL DOCUMENTO

Identificación del documento	Política Sistema de Gestión de Seguridad de Información (SGSI)
Documento(s) relacionado(s)	
Responsable de aprobación (anual)	Directorio - Comité de Gerencia
Dueño funcional	Gerente de Continuidad Operacional
Período de revisión	Anual
Actualización	Anual

2. CONTROL DE VERSIONES

Versión	Descripción del cambio	Solicitado por:	Realizado por:	Aprobado por:	Fecha Aprobación	Vigente a partir de:
1.0			Gerencia Continuidad Operacional			

3. DEFINICIONES

- **Información:** Es un recurso cuyo origen se genera al interior de la organización a través de los distintos procesos de negocio donde se registran, se procesan y se almacenan datos operacionales, comerciales y financieros. Todo este gran cúmulo de datos, denominados recursos de información, al igual que otros activos comerciales importantes, esencial para la continuidad del negocio y en consecuencia necesita ser protegida adecuadamente. Como resultado del creciente flujo de información a través de las redes, "La Información" se expone a un número cada vez mayor y a una variedad más amplia de amenazas y vulnerabilidades.

- **Seguridad de la Información:** Es la protección de la información (durante todo su ciclo de vida y en todos sus formatos) respecto de un rango amplio de amenazas, procurando asegurar la continuidad del negocio, minimizar el riesgo operacional y salvaguardar la imagen de la Empresa.

- **ISO/IEC 27002; 2013:** Es un estándar en el cual de establecen las mejores prácticas para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional.

- **Software malicioso:** También denominado "malware", incluidos los virus, gusanos, troyanos o ransomwares. Éstos ingresan a la red a través de correos electrónicos de los trabajadores, la utilización de Internet, computadoras portátiles o de dispositivos de almacenamiento, y explotan las vulnerabilidades del sistema.

- **CSIRT:** Equipo de Respuesta ante Incidentes de Seguridad, es un equipo multidisciplinario de especialistas en Seguridad de la Información, encargado de realizar las acciones

necesarias para proteger, contener, controlar y erradicar un incidente de Seguridad de la Información.

- **Respaldo:** Repositorio cuya finalidad es la preservación, protección y custodia de la información sujeta a requisitos de disponibilidad de largo plazo. Este repositorio puede estar implementado en diversas plataformas, por ejemplo, en la nube, que garanticen la disponibilidad en tiempo y forma para cumplir con los requerimientos del negocio.

4. OBJETIVO

El propósito de esta Política de Sistema de Gestión de Seguridad de Información es definir las directrices de la protección de los recursos de la información de todas las posibles amenazas, internas o externas, deliberadas o accidentales, mediante la implementación de un Sistema de Gestión de Seguridad de Información (SGSI).

La implementación efectiva de esta política es importante para mantener y demostrar la confidencialidad, integridad, y disponibilidad de los recursos de Minera Valle Central (MVC).

5. ALCANCE

Este documento contiene los lineamientos mínimos que debe considerar MVC para la implementación y mantención del Sistema de Gestión de Seguridad de Información, de forma de garantizar que la seguridad de la información es gestionada correctamente, haciendo uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial y formando parte del Gobierno Corporativo de Minera Valle Central.

La presente política es de aplicación general, comprende a toda la empresa, y considera el involucramiento y compromiso de todo el Equipo Humano, independientemente de su rango, función o localización, así como de sus proveedores y sus Empresas Colaboradoras.

6. REFERENCIAS

Los siguientes documentos se consideran como referencia en la presente Política:

- Series ISO 9000, 31000, 27001, 27002, 27032, 22301.
- BSI 25999 Business Continuity Management.
- Information Technology Infrastructure Library, ITIL4.
- Objetivos de Control para la Información y Tecnologías Relacionadas, COBIT 5 For Risk.
- Marco de Ciberseguridad del National Institute of Standards Technologies, NIST.
- Center for the Internet Security, CIS Controls.
- 20/30389105 DC BS ISO/IEC 27555. Information security, cybersecurity and privacy protection.
- 20/30383968 DC BS ISO 22329. Security and resilience. Emergency management.
- 19/30387733 DC BS ISO/IEC 19566-4. Information technologies.
- 19/30363856 DC BS ISO/IEC 27102. Information technology. Security techniques.
- BS 31111:2018 Cyber risk and resilience.
- PD ISO/IEC TS 27110:2021 Information technology, cybersecurity and privacy protection.
- Políticas de Gobierno Corporativo MVC www.mineravallecentral.cl

7. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El propósito del SGSI es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información consiste en la **preservación de su confidencialidad, integridad y disponibilidad** y de los sistemas implicados en su tratamiento, dentro de la organización. Así pues, estos tres términos constituyen la base de la seguridad de información:

- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** Acceso y utilización de la información y de los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes en la organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

MVC y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a los recursos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallas técnicas.

El SGSI establece políticas y procedimientos en relación con los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de tolerancia al riesgo que la propia organización ha decidido asumir.

7.1 Estructura Organizacional de SGSI

7.1.1 Directorio y/o Gerente General

1. Aprobar la Política Sistema de Gestión de Seguridad de Información.
2. Asignar recursos al SGSI en todas sus fases.

3. Aprobar los criterios de aceptación de riesgos y sus correspondientes niveles (Apetito de Riesgo).
4. Asegurar que se realicen auditorías internas.
5. Velar por el establecimiento, implementación, operación, monitoreo, control, revisión, mantenimiento y mejora continua del SGSI.

7.1.2 Comité de Seguridad de Información

Mediante la aprobación de este documento se funda y define el Comité de Seguridad de Información como la instancia para la revisión, supervisión, análisis y evaluación de los temas relacionados con la Seguridad de Información. De ser necesario se evalúa la necesidad de recursos, se establecen y/o revisan las políticas, objetivos y alcances del SGSI y se revisan necesidades específicas.

- **Frecuencia de sesión:** Bimensual.

Miembros permanentes del Comité de Seguridad de Información

1. Gerente de General.
2. Gerente de Continuidad Operacional.
3. Gerente de Administración y Finanzas.
4. Gerente de Producción.
5. Subgerente de Sustentabilidad.
6. Subgerente de Ingeniería y TI.

- **Quórum:** El comité puede sesionar con 3 miembros como mínimo.
- **Registro:** Agenda y el Acta del Comité de Seguridad de Información firmada por los participantes.
- **Reporte:** Resumen ejecutivo de cada sesión al Directorio.

Miembros no permanentes o invitados

Pueden participar de acuerdo a los contenidos de la tabla o agenda de la sesión o cuando lo deseen, sin restricción: Subgerentes; Jefes de Departamento, Supervisores, Asesores externos, Trabajadores/as en general, sin derecho a voto.

Responsabilidades del Comité de Seguridad de Información

1. Aprobar las políticas que permiten la adecuada implementación del SGSI, señaladas en la Estructura Documental del SGSI.
2. Aprobar el establecimiento de objetivos y planes del SGSI.
3. Asumir la responsabilidad y obligación de rendir cuentas con relación a la eficacia del SGSI.
4. Asegurar de que se establezcan las políticas de Seguridad de la Información y que éstas sean compatibles con el contexto y la dirección estratégica de la organización.
5. Aprobar roles y responsabilidades de seguridad de la información.
6. Asegurar de la integración de los requisitos del SGSI en los procesos de negocio de la organización.
7. Promover el uso del enfoque a procesos y el pensamiento basado en riesgos.
8. Asegurar de que los recursos necesarios para el SGSI estén disponibles.
9. Comunicar la importancia de una gestión de la Seguridad de Información eficaz y conforme con los requisitos del SGSI.
10. Asegurar de que el SGSI logre los resultados previstos.

11. Comprometer, dirigir y apoyar a las personas, para contribuir a la eficacia del SGSI promoviendo la mejora y apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo en la forma en la que aplique a sus áreas de responsabilidad.
12. Supervisar la implementación, operación, monitoreo, revisión, mantención y mejora del SGSI.
13. Supervisar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.
14. Asegurar que todo el personal relevante esté consciente de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

Este Comité forma parte de la Gestión Estratégica o Revisión Gerencial de MVC y tiene como base los temas relacionados con:

- El estado de las acciones desde anteriores revisiones por la dirección.
- Cambios en las cuestiones externas e internas que sean pertinentes al SGSI.
- La información sobre el comportamiento de la SGSI, incluidas las tendencias relativas a:
- El grado en que se han logrado los objetivos de la Seguridad de Información;
- El desempeño de los procesos relacionados a la Seguridad de Información;
- Las no conformidades y acciones correctivas;
- Los resultados de seguimiento y medición;
- Los resultados de las auditorías;
- Desempeño de los proveedores externos;
- La adecuación de los recursos;
- La eficacia de las acciones tomadas para abordar los riesgos y las oportunidades;
- Las oportunidades de mejora;
- Cualquier necesidad de cambio en el SGSI;
- Las necesidades de recursos.

7.1.3 Oficial de Seguridad de la Información (OSI)

1. Desarrollar y mantener las Políticas del SGSI.
2. Reportar la implementación, operación, monitoreo, revisión, mantención y mejora del SGSI.
3. Supervisar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.
4. Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
5. Administrar y coordinar diariamente el SGSI.
6. Desarrollar el Plan de Seguridad de la Información.
7. Ejecutar la evaluación de riesgos en seguridad de la información que abarque toda la organización.
8. Desarrollar los procedimientos de seguridad que fortalezcan las políticas de seguridad informática.
9. Guiar a la administración de la organización ante incidentes de seguridad mediante un Plan para Responder y atender notificaciones de incidentes y problemas.
10. Crear y mantener una base de datos para el registro de incidentes en la red, la cual debe poder ser accedida por los miembros del grupo de seguridad.
11. Coordinar la realización periódica de auditorías a las prácticas de seguridad informática, así como, dar seguimiento al corto plazo de las recomendaciones que hayan resultado.
12. Ser el punto de referencia para todos los procesos de seguridad y ser capaz de guiar y aconsejar a los usuarios de la institución sobre cómo desarrollar procedimientos para la protección de los recursos de software y hardware.
13. Evaluar la eficacia de las acciones realizadas.
14. Proveer resultados de auditorías y revisiones del SGSI.
15. Proveer técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
16. Realizar seguimiento y proveer información sobre el estado de acciones preventivas y correctivas.
17. Supervisar la gestión de vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
18. Resultados de las mediciones de eficacia.

7.1.4 Departamento de Tecnologías de Información

1. Implementar políticas y procedimientos del SGSI que corresponda.
2. Monitorear y controlar la implementación de las Políticas del SGSI que corresponda.
3. Crear, desarrollar e implementar planes de acción para corregir desviaciones a las Políticas del SGSI que corresponda.
4. Realizar seguimiento a las acciones correctivas que corresponda.
5. Informar resultados de la implementación, monitoreo, control y seguimientos a planes de acción al OSI.

7.2 Estructura documental de SGSI

7.2.1 Políticas

1. **Política de Sistema de Gestión de Seguridad de Información**, aprueba Directorio y/o Gerente General.
2. **Norma de Gestión de Activos de Información**, aprueba Comité de Seguridad de Información.
3. **Norma de Gestión de Seguridad de Información en las Operaciones**, aprueba Comité de Seguridad de Información.
4. **Norma de Gestión de Control de Accesos**, aprueba Comité de Seguridad de Información.
5. **Norma de Seguridad en las Comunicaciones**, aprueba Comité de Seguridad de Información.
6. **Norma de Protección de Datos**, aprueba Comité de Seguridad de Información.
7. **Norma de Gestión de Incidentes de Seguridad,** aprueba Comité de Seguridad de Información.
8. **Norma de Capacitación de Seguridad**, aprueba Comité de Seguridad de Información.
9. **Norma de Seguridad de Software**, aprueba Comité de Seguridad de Información.

Las siguientes normas se desarrollarán y aprobarán según MVC avance en la implementación del SGSI.

1. Norma de Gestión de Seguridad de Información en Recursos Humanos.
2. Norma de Seguridad Física y del Entorno.
3. Norma de Gestión de la Adquisición, desarrollo y mantención de sistemas tecnológicos.
4. Norma de Gestión de la Continuidad del Negocio.
5. Norma de Gestión de Seguridad de Información en Proveedores
6. Norma de Criptografía.

7.2.2 Declaración de Aplicabilidad (SOA, Statement of Applicability, en su sigla en inglés)

Documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

La evaluación de riesgos de Seguridad de Información se realizará utilizando los criterios de la Política de Riesgos y el Procedimiento de Evaluación de Riesgos y Oportunidades.

8. Reglas de la Política

Todo el Equipo Humano de MVC, sea este permanente o temporal (o empresas colaboradoras que se vinculan por sus funciones con sistemas de información de MVC) tiene la obligación de proteger los recursos de información, los sistemas y la infraestructura tecnológica de la organización, actuando siempre de forma responsable y profesional, manteniendo pleno conocimiento de lo establecido por la presente política, que pasa a formar parte de las Políticas de Gobierno Corporativo MVC y de Reglamento Interno de Orden, Higiene y Seguridad MVC.

Todos los recursos de información deberán poseer un dueño designado, quien será responsable de asegurar que los mismos se encuentren debidamente inventariados y clasificados según su sensibilidad y criticidad. Será también su responsabilidad el realizar una revisión periódica de dicha clasificación y de las autorizaciones de acceso a los mismos.

Todos los recursos de información deberán ser protegidos en función de su clasificación y según lo definido por la evaluación de riesgos correspondiente.

Todo proyecto que involucre recursos de información deberá, desde su concepción, incorporar los requerimientos de seguridad definidos por los dueños de los activos afectados. El proceso de incorporación y validación de la seguridad deberá estar integrado a la administración de proyectos desde la etapa de diseño.

Todo el personal de MVC tiene la responsabilidad de notificar incidentes de seguridad y potenciales debilidades que pudieran detectarse a través de los canales definidos por el Comité de Seguridad de la Información (informática@mineravallecentral.cl).

Será responsabilidad del Oficial de Seguridad de la Información la implementación de un programa adecuado de sensibilización y capacitación. Este programa deberá estar disponible para todo el personal de MVC incluyendo trabajadores/as permanentes, temporales y externos.

MVC declara su decisión de mejorar continuamente los procesos y niveles de seguridad a través de un seguimiento permanente de los controles y procedimientos implantados. Del mismo modo declara su intención de asegurar la existencia de planes de contingencia que permitan garantizar la continuidad de la operación de la compañía y de sus clientes.

MVC declara su decisión de cumplir con la normativa y legislación vigente en temas de Seguridad de la Información y con los requerimientos contractuales establecidos por los clientes con relación a la misma.

El Comité de Seguridad de la Información de MVC será responsable de la gestión de los temas de la Seguridad de la Información y tendrá la autoridad para su implantación y control.

Las Políticas que componen el SGSI se revisarán y actualizarán en forma anual.

9. Sanciones

El incumplimiento de lo dispuesto en esta política general constituye una falta grave y podrá resultar en medidas disciplinarias, según se define en el Reglamento Interno de Orden, Higiene y Seguridad MVC, pudiendo aplicarse una amonestación escrita hasta la desvinculación del trabajador/a dependiendo del incumplimiento de la falta.

10. Aprobaciones

La presente Política, ha sido aprobada por el Gerente General con fecha 27 de Septiembre de 2022.

BIOMETRICS

RUT 10332847-0
BENJAMIN MANUEL ALEJANDRO
CAMPOS ORDAZ
COD. TRX YWI0Yjg1OO0YxNzkwMTU2
2022/09/27 19:44:18 UTC
bcampos@mineravallecentral.cl

FIRMA ELECTRONICA
Ley N°19.799

RUT 10355911-1
CHRISTIAN MARCELO
CACERES MENESES
COD. TRX OGJhNjM2O0YxODAxNzQ0
2022/09/29 19:34:01 UTC
ccaceres@mineravallecentral.cl

FIRMA ELECTRONICA
Ley N°19.799

RUT 15524446-1
JUAN JOSE
GONZALEZ NUÑEZ
COD. TRX MGU0NWQzO0YxNzkwOTQ1
2022/09/27 21:19:49 UTC
juan.gonzalez@mineravallecentral.cl

FIRMA ELECTRONICA
Ley N°19.799