

Directriz

Seguridad de la Información

DIR-TICA-00

AMSA: DIR-TICA-00

SGSI: A5.1-DIR-SGSI_Directriz Seg.Info.

Gerencia de
Tecnologías de Información, Comunicaciones y Automatización

Vicepresidencia de Finanzas

NOTA DE CONFIDENCIALIDAD

Este documento contiene información propiedad de Antofagasta Minerals S.A. que ha sido preparada estrictamente con el propósito de ser utilizada en las operaciones de la Compañía y no podrá ser proporcionada o revelada parcial o totalmente a terceros sin autorización expresa por parte de la Compañía.

INDICE

1. OBJETIVO.....	3
2. ALCANCE	3
3. TERMINOLOGÍA CLAVE	3
4. POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN.....	4
4.1 Fundamentos.....	4
4.2 Principios	5
4.3 Directrices de Seguridad de la Información.....	6
4.4 Excepciones a la política	10
4.5 Estructura Organizacional de la Seguridad de la Información	11
5. VERSIONES DEL DOCUMENTO	12
6. RUTA DE VALIDACIÓN	12
7. ACCESIBILIDAD	13

1. OBJETIVO

En el Grupo Antofagasta Minerals tenemos como valor corporativo alcanzar mejores resultados siendo austeros, eficientes y cuidando nuestros recursos. Este valor, nos motiva a comprometernos como compañía a proteger los activos de información que forman parte de nuestra plataforma tecnológica.

Nuestra Directriz Corporativa de Seguridad de la Información constituye el marco de referencia para considerar la seguridad de la información como un proceso continuo a través del tiempo y en el que todos los integrantes de la compañía tienen un rol fundamental que desempeñar.

El marco de referencia propuesto establece directrices específicas orientadas a cumplir con los fundamentos generales de disponibilidad, integridad y confidencialidad de la información, de esta forma aseguramos que los usuarios autorizados puedan acceder a los recursos informáticos cuando lo requieran y obtener la información adecuada en el desempeño de sus funciones.

2. ALCANCE

La presente Directriz Corporativa de Seguridad de la Información y las Directrices Específicas que la componen, son aplicables al Grupo Antofagasta Minerals, en específico a los activos de información, la infraestructura tecnológica, las instalaciones físicas relacionadas y las personas que hacen uso de estos activos.

3. TERMINOLOGÍA CLAVE

Directriz Corporativa	: Intenciones y lineamientos formalmente expresadas por la Dirección.
Directriz Específica	: Declaración destinada a alcanzar los objetivos de la Directriz Corporativa al proporcionar orientación y lineamientos en un ámbito acotado e identificable, basado en mejores prácticas aceptadas.
Procedimiento	: Describe una secuencia ordenada de acciones destinada a lograr un objetivo. Entrega las instrucciones específicas para aplicar las directrices y normas en un entorno operativo.
Marco Normativo	: Conjunto de actividades destinadas a organizar y gestionar el conjunto de normas, procedimientos y documentos que formalizan los procesos TICA.
Seguridad de la Información	: Conjunto de actividades destinadas a preservar y asegurar los requerimientos de la compañía con relación a confidencialidad, integridad y disponibilidad de la información.

4. POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN

4.1 Fundamentos

Confidencialidad:

Condición de la información destinada a evitar que la información sea divulgada a personas, entidades o procesos no autorizados, en base a la privacidad y sensibilidad que tienen los datos para la Compañía.

Los controles que se establezcan deben garantizar que la información, sus medios de procesamiento y/o conservación, estén protegidos del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran perjudicarla.

Integridad:

Condición de la información destinada a mantener la consistencia a través de su procesamiento, protegiéndola de errores, destrucción, modificación inadecuada, borrado total o parcial sin autorización.

Los controles que se establezcan deben prevenir que se concreten estas situaciones y, en caso de ser necesario, asegurar la recuperación de la información a un estado consistente y conocido.

Disponibilidad:

Servicio que asegura que la información esté disponible en forma oportuna para las entidades autorizadas cuando la necesiten (en tiempos de acceso considerados aceptables), para cumplir los requerimientos de negocio y/o para minimizar pérdidas sustanciales. Disponibilidad implica además que los recursos, tanto hardware como software, se mantienen funcionando apropiadamente y que estos pueden recuperarse en caso de falla.

Se debe garantizar que la información y la capacidad de su procesamiento, puedan ser resguardadas y recuperadas para las operaciones de negocio habituales y ante cualquier hecho contingente que interrumpa la operatoria o dañe las instalaciones, medios de almacenamiento y/o equipamiento relacionado.

4.2 Principios

Reconocemos la información como factor clave

- **La información** y los principales sistemas que permiten su procesamiento, **son considerados un activo clave** en el desarrollo de la compañía, razón por la que **debemos protegerlos y asegurar su disponibilidad, integridad y confidencialidad**.
- La seguridad de la información es una actividad que **involucra a todos los trabajadores y colaboradores** del Grupo Antofagasta Minerals, quienes deben desarrollar sus actividades cotidianas asumiendo el compromiso diario de proteger la información y la infraestructura tecnológica de la compañía.
- Las empresas del Grupo Minero deben mantener controles destinados a inventariar, clasificar y asignar los activos de información críticos para la Administración.

Procedemos de acuerdo a un esquema formal

- Las principales actividades relacionadas a la seguridad de la información serán formalizadas de acuerdo al esquema normativo y organizacional vigente en la compañía.
- En caso que una situación no esté regulada expresamente por la presente política, actuaremos en base a no exponer la información y reputación de la compañía a riesgos innecesarios.

Somos proactivos al mantener la seguridad de la información

- Todo trabajador o colaborador debe notificar las actividades que afecten o que representen un potencial riesgo contra; la seguridad de la información, los activos y personas relacionadas.

Fomentamos una cultura de seguridad de la información

- Reconocemos y alentamos toda actividad orientada a divulgar las políticas y directrices de seguridad de la información a los trabajadores y colaboradores del Grupo Minero.

Nos comprometemos con el cumplimiento

- Declaramos nuestro compromiso de cumplir con la legislación y normativa vigentes en temas de seguridad de la información.
- El cumplimiento de las directrices y procedimientos relacionados a Seguridad de la Información debe ser verificado por las áreas que la organización ha establecido para tal efecto. El incumplimiento de lo definido será objeto de sanciones disciplinarias en los términos contemplados en la normativa interna de la compañía.

4.3 Directrices de Seguridad de la Información

Es importante que los controles de seguridad de la información sean desarrollados en base a mejores prácticas reconocidas internacionalmente. En este sentido, Antofagasta Minerals ha considerado la estructura propuesta por la norma ISO/IEC 27002 para establecer las siguientes Directrices de Seguridad de la Información:

4.3.1 Marco Normativo y Organización de la Seguridad de la Información TICA

Se debe establecer una estructura coherente y jerárquica de políticas, directrices, procedimientos y normas de la Gerencia TICA, con la finalidad que estos, sean efectivos en la implementación y funcionamiento de la seguridad de la información y permitan que los controles se adapten a los cambios propios de un área tecnológica como la Gerencia TICA.

4.3.2 Seguridad de la Información ligada a los Recursos Humanos

Se debe asegurar que el personal del Grupo Minero y sus colaboradores, estén en conocimiento y cumplan sus responsabilidades de seguridad de la información. Los controles que se establezcan en este ámbito deben procurar proteger los activos de información en todas las etapas que compone el proceso de Recursos Humanos (Contratación, traslados de cargos, desvinculaciones).

4.3.3 Administración de Activos de Información

La información, y todos los activos asociados con su procesamiento, almacenamiento e intercambio, deben ser controlados y protegidos.

Se adoptarán controles destinados a administrar los medios computacionales y mitigar los riesgos que puedan afectarlos. En este sentido, la asignación de recursos informáticos se realizará en coordinación con el área de Recursos Humanos.

4.3.4 Control de Acceso

Será responsabilidad de cada usuario, el eficaz resguardo de la información y las credenciales que se le han otorgado para el acceso a los activos de información del Grupo Minero.

El acceso a los activos de procesamiento, almacenamiento e intercambio de información, que se otorgue a los usuarios, deberá ser autorizado en forma expresa por el propietario del activo o, quien éste designe.

Se adoptarán controles para mitigar la materialización de riesgos de accesos no autorizados a los activos de información considerando nivel de acceso y plazo autorizado por el responsable del área usuaria o dueño del activo.

Se restringirá sólo a lo estrictamente necesario para la continuidad operacional del Grupo Minero, aquellos accesos de administración o de altos privilegios que los activos de información tengan disponibles.

Se restringirá el acceso a programas fuentes y configuraciones de los sistemas computacionales del Grupo Minero, sólo a aquellos usuarios que, por el desempeño de sus funciones lo requieran.

4.3.5 Criptografía

Para los activos de Información clasificados como críticos por la Alta Administración, serán aplicados sistemas criptográficos en la medida que un control compensatorio no satisfaga los niveles de seguridad exigidos por la Administración y no entorpezca el normal desarrollo de las operaciones del Grupo Minero.

4.3.6 Seguridad Física y Condiciones de Operación

Se deben identificar y proteger las áreas críticas en la continuidad operacional de los servicios informáticos.

Se restringirá el acceso físico a las áreas críticas identificadas, sólo al personal que, por desempeño de sus funciones o aseguramiento de la continuidad operacional, requiera acceder.

Se adoptarán controles para mitigar la materialización de riesgos de daños a los activos de información producto de condiciones de operación inadecuadas (de acuerdo a las especificaciones entregadas por los fabricantes), desastres naturales, accidentes o ataques maliciosos.

Los activos de información deben recibir mantenimiento en base a las especificaciones de los fabricantes para asegurar su permanente disponibilidad e integridad.

4.3.7 Gestión de las Operaciones (Tecnología e Infraestructura)

Se debe administrar la operación de los activos de información gestionando, controlando y monitoreando adecuadamente la configuración, capacidad, segregación de accesos y cambios de la infraestructura relacionada.

Se adoptarán controles para mitigar la materialización de riesgos relacionados a software malicioso, explotación de vulnerabilidades técnicas, pérdida y/o modificación no autorizada de datos.

Se mantendrán registros de las actividades realizadas por los responsables de la operación de la infraestructura de operaciones.

4.3.8 Gestión de las Comunicaciones

Se protegerá la información mediante la gestión de la seguridad en la infraestructura de comunicaciones del Grupo Minero.

Se establecerán los controles pertinentes orientados a mantener la seguridad de la información en la transferencia de información interna o externa a las redes de cada compañía.

4.3.9 Adquisición, Desarrollo y Mantenimiento de Sistemas

Se debe definir una metodología formal de desarrollo, pruebas, puesta en producción y mantenimiento de los sistemas computacionales administrados por la Gerencia TICA.

Se debe asegurar que la seguridad de la Información es parte integral de los sistemas de información en todo el ciclo de adquisición, desarrollo y mantenimiento de sistemas.

Todos los desarrollos se deben llevar a cabo en entornos específicamente destinados a ese propósito y separados de los ambientes de producción y prueba. Dicha segregación podrá ser física o lógica, e incluye también al personal involucrado en cada una de dichas etapas.

Se deben proteger los datos de pruebas utilizados en las etapas de adquisición, desarrollo y mantenimiento de sistemas, resguardando la confidencialidad de estos datos.

4.3.10 Relaciones con Proveedores

Los activos de información del Grupo Minero a los que tienen acceso los proveedores serán protegidos para reducir los riesgos de ingresos no autorizados, pérdida de integridad de datos y falencias en la disponibilidad de los servicios TICA.

Serán supervisadas todas las entregas de servicios de proveedores relacionados a los activos de información del Grupo Minero.

4.3.11 Gestión de Incidentes de Seguridad

Se debe establecer un esquema formal de administración de incidentes que afecten la Seguridad de la Información, considerando una categorización de los incidentes en base al impacto que tengan en los procesos que la compañía ha definido como críticos y/o sus sistemas informáticos de apoyo. Se dejará registro de los principales antecedentes del evento (por ejemplo, causas, responsables y soluciones adoptadas).

4.3.12 Gestión de la Continuidad del Negocio

Se establecerá una metodología destinada a hacer frente a desastres informáticos que afecten los sistemas de apoyo a los procesos que la compañía ha definido como críticos. Adicionalmente, la administración podrá definir la necesidad de realizar regularmente pruebas documentadas de los planes destinados a mantener la disponibilidad de dichos sistemas críticos.

4.3.13 Cumplimiento

En lo que a resguardo de la información se refiere, las empresas del Grupo Minero deben cumplir con las regulaciones definidas por Ley que le sean aplicables, la normativa interna y con los compromisos contractuales que hayan suscrito.

Se verificará regularmente el cumplimiento de la presente Política, Directrices y Procedimientos relacionados.

4.4 Excepciones a la política

Antofagasta Minerals reconoce que en el cumplimiento de las normas pueden ocurrir situaciones donde una necesidad del negocio requiera realizar acciones que pudieran estar en conflicto con la presente política. En este caso, debe primar el cumplimiento de las normas legales y luego el uso criterioso de la información a fin de no exponerla a riesgos innecesarios.

4.5 Estructura Organizacional de la Seguridad de la Información

La estructura organizacional define las responsabilidades en materia de Seguridad de la Información de cada uno de los participantes del Gobierno Corporativo TICA y de los usuarios de los servicios informáticos disponibles. En tal sentido se han definido las siguientes responsabilidades:

Comité de la Vicepresidencia

El comité es informado de las principales actividades relacionadas a Seguridad de la Información y de la identificación de riesgos e implementación de los principales controles informáticos. Adicionalmente tiene la facultad de aprobar los planes de seguridad de la información.

Comité de Gerentes TICA

A cargo de abordar una situación excepcional de alto impacto en la seguridad de la información. Regularmente se presentan la identificación de riesgos y los controles que los mitigan.

Gerente Corporativo TICA

Responsable de entregar lineamientos y recursos que permitan el cumplimiento de la política y directrices de seguridad de la información en el Grupo Minero.

Oficial de Seguridad de la Información:

Es responsable de la implementación y cumplimiento de la política y directrices de seguridad de la información en el Grupo Minero.

Coordinadores de Seguridad de la Información

Responsable de la implementación y cumplimiento de la política y directrices corporativas en sus respectivos ámbitos de acción. Adicionalmente están a cargo de monitorear y canalizar las acciones destinadas a resolver incidentes de seguridad trabajando coordinadamente con el Oficial de Seguridad.

Gerentes de Área:

Responsable de resguardar la información que generan, reciben, publican y distribuyen las áreas que se encuentren a su cargo. Asimismo, es responsable de la seguridad de los activos de información que le son asignados (computadores, teléfonos, espacios de almacenamiento, entre otros).

Personal interno y colaboradores:

Responsable de cumplimiento de las políticas y directrices de seguridad en las labores que desempeñan diariamente.

5. VERSIONES DEL DOCUMENTO

Versión	Fecha	Modificaciones	Comentarios
V.1.0	30/05/15	Creación del documento	
V.2.0	25/07/17	Actualización del documento	Revisión y actualización en base al marco normativo vigente.

6. RUTA DE VALIDACIÓN

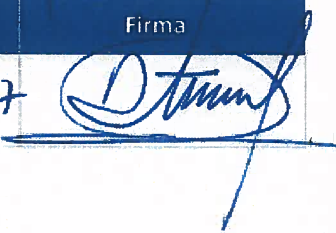
6.1. Elaborado por:

Cargo	Nombre y Apellido	Fecha	Firma
Oficial de Seguridad de la Información	Miguel Angel Elizondo C.	Julio-2017	

6.2. Revisado por:

Cargo	Nombre y Apellido	Fecha	Firma
Gerente Corporativo TICA	Gino Iván M.	28/08/17	

6.3. Aprobado por:

Cargo	Nombre y Apellido	Fecha	Firma
Vicepresidente de Administración y Finanzas	Alfredo Atucha A.	28/08/17	

7. ACCESIBILIDAD

Entidad	Acceso	Comentarios
Directorio AntoPLC		
Equipo Ejecutivo		
Todos los empleados de Grupo Minero	X	
Todos los empleados de AMSA	X	
Gerencia TICA		
Todos los empleados de TICA		
Público/Global	X	

Este documento será revisado a intervalos apropiados y cuando sea necesario para mantenerlo actualizado.

Cambios Menores:

Corresponde a correcciones, cambios o actualizaciones que no afectan la esencia del documento. Estos cambios no requieren aplicar la ruta de validación y será facultad del Oficial de Seguridad de la Información realizarlos y custodiar los documentos originales.

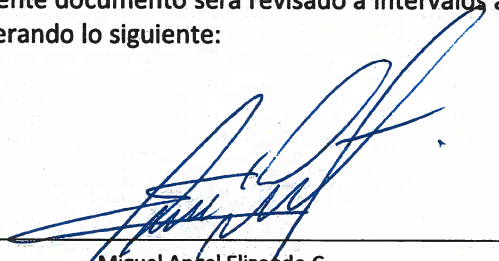
Cambios Significativos:

Corresponde a la intervención mayor del contenido por lo que, en estos casos, se aplicará la ruta de validación que aplique al documento.

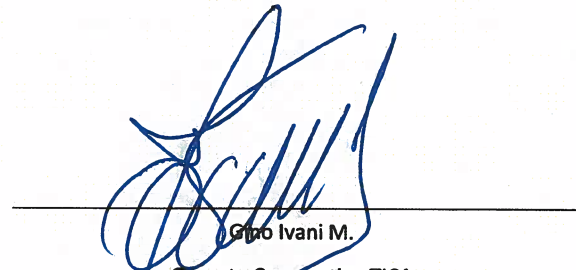
ANEXO: REVISIONES DEL DOCUMENTO - DIRECTRIZ CORPORATIVA SEGURIDAD INFORMACIÓN

Versión	Fecha	Modificaciones	Comentarios
V.1.0	30/05/15	• Creación del documento.	
	25/07/17	• Actualización del documento.	
	23/11/20	• Revisión del documento.	

El presente documento será revisado a intervalos apropiados y/o cuando sea necesario para mantenerlo actualizado, considerando lo siguiente:



Miguel Angel Elizondo C.
Subgerente de Ciberseguridad

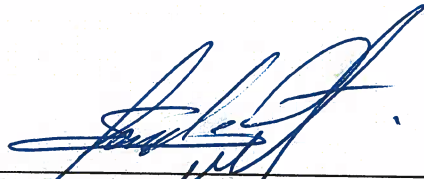


Gipo Ivani M.
Gerente Corporativo TICA

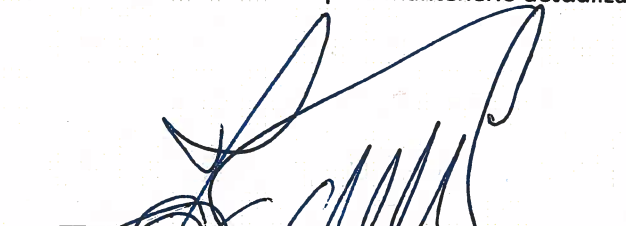
ANEXO: REVISIONES DEL DOCUMENTO - DIRECTRIZ CORPORATIVA SEGURIDAD INFORMACIÓN

Versión	Fecha	Modificaciones	Comentarios
V.1.0	30/05/15	• Creación del documento.	
	25/07/17	• Actualización del documento.	
	23/11/20	• Revisión del documento.	
	30/09/22	• Revisión del documento.	

El presente documento será revisado a intervalos apropiados y/o cuando sea necesario para mantenerlo actualizado, considerando lo siguiente:



Miguel Ángel Elizondo C.
Subgerente de Ciberseguridad

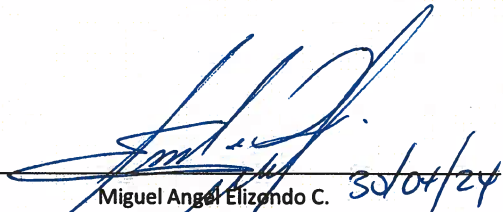


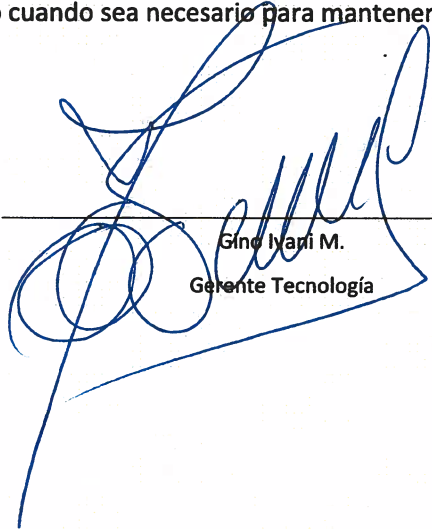
Gina Ivani M.
Gerente Corporativo TICA

ANEXO: REVISIONES DEL DOCUMENTO - DIRECTRIZ CORPORATIVA SEGURIDAD INFORMACIÓN

Versión	Fecha	Modificaciones	Comentarios
V.1.0	30/05/15	• Creación del documento.	
	25/07/17	• Actualización del documento.	
V.2.0	23/11/20	• Revisión del documento.	
	30/09/22	• Revisión del documento.	
	30/04/24	• Revisión del documento.	

El presente documento será revisado a intervalos apropiados y/o cuando sea necesario para mantenerlo actualizado.


Miguel Ángel Elizondo C.
Subgerente de Ciberseguridad


Gino Iván M.
Gerente Tecnología

ANEXO: REVISIONES DEL DOCUMENTO - DIRECTRIZ CORPORATIVA SEGURIDAD INFORMACIÓN

Versión	Fecha	Modificaciones	Comentarios
V.1.0	30/05/15	• Creación del documento.	
	25/07/17	• Actualización del documento.	
V2.0	23/11/20	• Revisión del documento.	
	30/09/22	• Revisión del documento.	
	30/04/24	• Revisión del documento	
	28/12/25	• Revisión del documento y actualización formato (cambio menor)	Establece directrices complementarias anexas para SGSI

En la actual revisión se establecen las siguientes directrices anexas que complementan al documento principal:

4.5.- Aplicable al proceso de ciber resiliencia

El proceso de actualización de las directrices se mantiene vigente (cambiar denominación a “política”) y que las presentes directrices generales y las directrices específicas son aplicables al SGSI del proceso de ciber-resiliencia.

4.6.- Compromiso de la Alta Dirección

La Alta Dirección del Grupo Antofagasta asume su compromiso con el cuidado de la información reconociéndola como un activo clave en su desarrollo y mandata la implementación, operación y mejora continua de un Sistema de Gestión de Seguridad de la Información y Ciberseguridad apropiado y se compromete a la asignación de recursos para tal efecto.

4.7.- Estructura organizacional de la seguridad de la información y ciberseguridad

El Comité de Seguridad de la Información es el órgano ejecutivo que supervisa la operación y la mejora continua del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

El CISO es responsable de la implementación, ejecución y reporte periódico del desempeño del SGSI, fomentar el Cumplimiento, revisión de la presente política y atribuciones para aprobar los documentos que componen el SGSI.

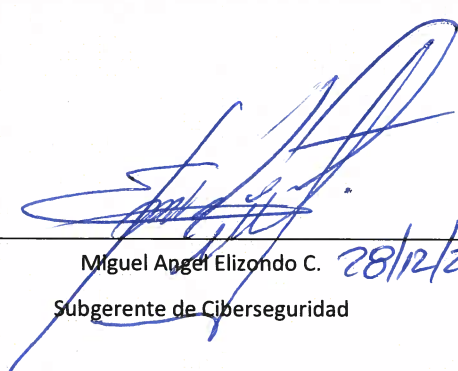
El responsable del proceso de negocio está a cargo de autorizar el acceso y uso de los activos de información que estén a su cargo como de designar a los administradores (dueños), de cada activo de información que se utilice en su área o proceso.

4.8. Objetivos de seguridad de la información y ciberseguridad

El Sistema de Gestión de Seguridad de la Información tiene como objetivo:

- Gestionar los riesgos de seguridad de la información para reducirlos al nivel aceptable definido por el Grupo Antofagasta.
- Garantizar la continuidad operacional de la infraestructura tecnológica del Grupo Antofagasta (Ciber-resiliencia).
- Fomentar una cultura de seguridad de la información y ciberseguridad en el Grupo Antofagasta.
- Prevenir incidentes de ciberseguridad y responder a ellos de forma eficaz, informando a las autoridades competentes cuando corresponda.
- Cumplir con las obligaciones legales, regulatorias y contractuales que le sean aplicables.

El presente documento será revisado a intervalos apropiados y/o cuando sea necesario para mantenerlo actualizado.



Miguel Angel Elizondo C. 28/12/25.
Subgerente de Ciberseguridad



Gino Iván M.
Gerente de Tecnología

28/12/25.

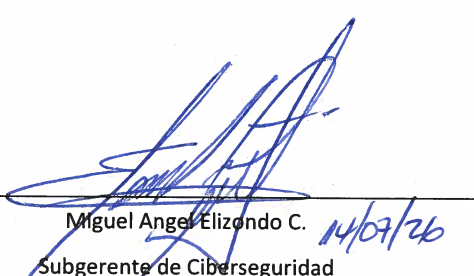
ANEXO: REVISIONES DEL DOCUMENTO - DIRECTRIZ CORPORATIVA SEGURIDAD INFORMACIÓN

Versión	Fecha	Modificaciones	Comentarios
V.1.0	30/05/15	• Creación del documento.	
	25/07/17	• Actualización del documento.	
V2.0	23/11/20	• Revisión del documento.	
	30/09/22	• Revisión del documento.	
	30/04/24	• Revisión del documento	
	22/12/25	• Revisión del documento y actualización formato (cambio menor)	Establece directrices complementarias anexas para SGSI
	14/07/26	• Revisión del documento	Establece directrices complementarias anexa con relación a actualización en Norma ISO27002

4.9. Actualización de Directrices

Antofagasta Minerals ha considerado la estructura propuesta por la norma ISO/IEC 27002 para establecer las Directrices de Seguridad de la Información (generales y específicas), en caso de nuevas versiones de esta norma de referencia, se adoptarán y serán parte de las presentes directrices todas las actualizaciones que sean aplicables al Grupo Antofagasta.

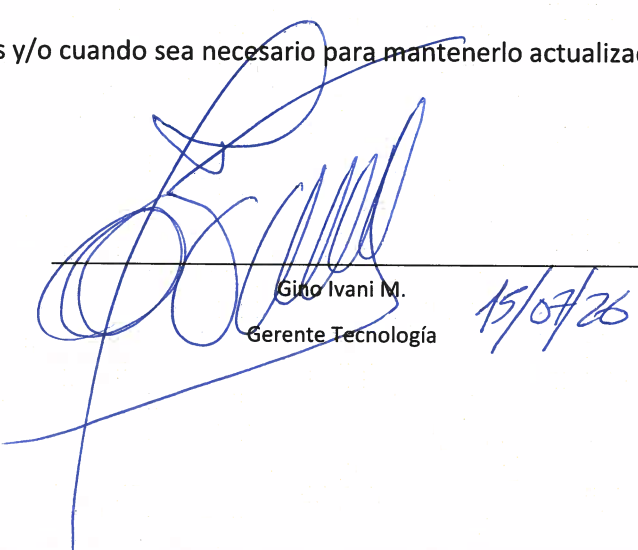
El presente documento será revisado a intervalos apropiados y/o cuando sea necesario para mantenerlo actualizado.



Miguel Angel Elizondo C.

Subgerente de Ciberseguridad

14/07/26



Gino Ivani M.

Gerente Tecnología

15/07/26