POLÍTICA DE GOBIERNO TECNOLÓGICO Y CIBERSEGURIDAD

Nombre del Documento	Política de Gobierno Tecnológico y Ciberseguridad		
Área Responsable	Gerencia de Transformación y Tecnología		
Encargado	Gobierno y Control Tecnológico - Subgerencia de Tecnología		
Revisado por	Compliance Officer	Fecha de creación	11-07-2025
Aprobado por	Gerente General Yodo y Nutrición Vegetal	Fecha de aprobación	20 de enero de 2026
Oficializado por	Pablo Altimiras	Entrada en vigencia	20 de enero de 2026

Control de Versiones			
Versión	Última Actualización	Aprobado por	Descripción
1.0	N/A	Firmado por: Pablo Altimiras 9B24FABB44D744F...	Creación de Política

Inicial RA

Inicial LT

1. Objetivo

Con el objetivo de establecer un marco seguro, eficiente y sostenible para la gestión de los Recursos Tecnológicos de la organización, Sociedad Química y Minera de Chile S.A. ("SQM"), ha elaborado la presente Política de Gobierno Tecnológico y Ciberseguridad. Ésta busca asegurar que las personas responsables, apoyadas por procesos, herramientas y capacidades, apliquen prácticas que minimicen los riesgos, protejan y potencien el valor de la organización.

En esta Política, los términos en mayúscula inicial tendrán el significado que se indica en el Anexo N°1 y, en caso de no encontrarse definidos, se entenderán conforme a su sentido natural y obvio.

2. Alcance

La presente Política aplica a todos los colaboradores y externos de SQM, que interactúen con Recursos Tecnológicos, así como a sus filiales, y compañías en que SQM tenga una participación igual o superior al 50%, salvo aquellas filiales que componen la División Litio-Potasio, Litio Internacional, y las sociedades Soquimich Comercial S.A., y Ajay-SQM Chile S.A., las cuales se regirán por sus políticas y procedimientos propios.

3. Principios Rectores

Toda la gestión de Recursos Tecnológicos a efectos de cumplir con los compromisos señalados precedentemente debe regirse por los siguientes principios:

3.1 Gobierno Tecnológico.

El Gobierno Tecnológico debe asegurar que todas las decisiones, iniciativas y Recursos Tecnológicos se gestionen de manera transparente, alineada a los objetivos estratégicos y conforme a criterios de eficiencia, control, priorización y uso responsable.

3.2. Riesgo Tecnológico.

La gestión del riesgo tecnológico debe ser proactiva, continua y proporcional, orientada a anticipar, evaluar, controlar y mitigar los impactos que el uso, adopción o falla de la tecnología pueda generar en la seguridad de las personas, la información, el cumplimiento normativo, la operación, la reputación y la rentabilidad. Todas las decisiones tecnológicas deben alinearse con el apetito de riesgo corporativo y sustentarse en análisis de riesgo documentados, oportunos y trazables.

3.3. Ciclo de Vida.

La gestión del Ciclo de Vida de toda tecnología debe ser integral, sostenible y basada en control, asegurando que, desde su concepción hasta su retiro, se

ejecuten procesos de evaluación, actualización, mejora continua, mantenimiento y revisión de riesgos que garanticen su funcionamiento seguro, eficiente y alineado a los objetivos estratégicos.

3.4. Seguridad Digital y Cultura.

La ciberseguridad debe incorporarse desde el diseño y durante todo el Ciclo de Vida de cada recurso tecnológico, asegurando la protección de la información, la continuidad operativa y la prevención de incidentes. La organización debe promover una cultura sólida de ciberseguridad basada en capacitación continua, concientización, comportamiento responsable y participación activa de todos los Usuarios, reafirmando la responsabilidad compartida en la protección de los activos tecnológicos y de información.

3.5. Compatibilidad e Interoperabilidad.

Toda tecnología que incorpore a SQM debe ser diseñada, adquirida e implementada garantizando su compatibilidad con la arquitectura tecnológica vigente y su interoperabilidad con los sistemas existentes, asegurando continuidad operativa, eficiencia, escalabilidad y cumplimiento de estándares corporativos. Cada solución tecnológica deberá alinearse a los lineamientos de arquitectura, integrarse mediante mecanismos seguros y soportar la evolución del ecosistema tecnológico de la organización.

3.6. Usuarios y Conducta Responsable.

Los Usuarios de Recursos Tecnológicos son responsables de utilizarlos de manera segura, diligente y conforme a la normativa vigente, contribuyendo activamente a la protección de la información, a la continuidad operativa y a la gestión del riesgo tecnológico. Su conducta debe alinearse a los estándares corporativos, participar en los procesos de mejora continua, cumplir las obligaciones de reporte oportuno de incidentes o anomalías y colaborar con los mecanismos de monitoreo y control establecidos por la organización. La participación consciente y el comportamiento seguro de los Usuarios constituyen elementos esenciales del modelo de gobernanza tecnológica de SQM.

3.7. Proporcionalidad.

Las medidas de seguridad, control y gestión aplicadas a los Recursos Tecnológicos deben ser proporcionales a su criticidad, sensibilidad, relevancia operativa y nivel de riesgo asociado, asegurando un equilibrio entre protección, eficiencia operativa y continuidad del negocio. Toda decisión tecnológica deberá basarse en análisis de riesgo que permitan aplicar controles adecuados, evitando tanto la sobreprotección como la insuficiencia de medidas que puedan comprometer la seguridad, el cumplimiento normativo o el desempeño de SQM.

3.8. Legalidad.

Todas las decisiones, procesos y controles tecnológicos deberán alinearse con la normativa nacional e internacional aplicable, incluyendo, sin que sean las únicas, la Ley N°21.663 (Marco de Ciberseguridad), el Decreto Supremo N°295, y las disposiciones emitidas por la Agencia Nacional de Ciberseguridad (ANCI), así como la regulación sectorial correspondiente. En caso de discrepancia, prevalecerán las definiciones y obligaciones establecidas por la normativa legal sobre cualquier definición interna.

4. Normas Específicas de Conducta

4.1. Todo recurso tecnológico debe ser concebido, diseñado, implementado y operado integrando medidas de seguridad desde su origen, asegurando que la protección de la información, la prevención de vulnerabilidades y la continuidad operativa sean consideradas en todas sus etapas, desde la definición inicial hasta su retiro.

4.2. Es obligatorio realizar evaluaciones de riesgo de manera periódica y previa a cualquier cambio, gestionar los accesos siempre con segregación de funciones y mantener controles y monitoreo continuo que permitan detectar, prevenir y responder oportunamente a desviaciones o incidentes de seguridad.

4.3. La Gerencia de Transformación y Tecnología es la responsable de implementar controles, y revisiones periódicas que permitan identificar, mitigar y monitorear riesgos. Asimismo, garantizará la entrega de información de manera oportuna y transparente para la evaluación de auditorías externas o internas que sean necesarias.

4.4. La incorporación, modificación y evolución de Recursos Tecnológicos debe realizarse siguiendo los lineamientos de arquitectura, seguridad, operación y calidad definidos por la organización. Los Equipos Responsables deberán validar que los cambios cumplen dichos lineamientos, documentar las decisiones técnicas y asegurar que su ejecución mantenga la coherencia, escalabilidad y sostenibilidad del ecosistema tecnológico.

4.5. Está prohibido desarrollar, adquirir, integrar, entrenar o poner en operación soluciones de inteligencia artificial, así como cualquier otro Recurso Tecnológico sin la evaluación y aprobación previa de la Gerencia de Transformación y Tecnología.

4.6. Está prohibido divulgar, transferir, almacenar o procesar información sensible sin autorización y sin los controles establecidos, debiendo reportar de inmediato cualquier acceso indebido, filtración, pérdida o incidente relacionado con dicha información.

4.7. Toda adquisición o contratación de tecnología, en especial las soluciones de inteligencia artificial, debe ser evaluada y aprobada previamente por la Gerencia de Transformación y Tecnología, verificando los riesgos operacionales, de

seguridad, cumplimiento normativo y costo–beneficios asociados. Ningún área podrá adquirir, contratar o comprometer Recursos Tecnológicos sin esta aprobación previa. Los Equipos Responsables deberán documentar la evaluación realizada y asignar responsables para la administración, operación y mejora continua del recurso tecnológico adquirido.

4.8. Está estrictamente prohibido operar servicios tecnológicos sin cumplir con los procedimientos y controles mínimos de continuidad definidos por la organización.

4.9. Todo requerimiento tecnológico debe ser evaluado y documentado previamente por el área responsable, considerando su impacto, riesgos operacionales, ciberseguridad y cumplimiento normativo. Ningún requerimiento podrá avanzar a desarrollo, adquisición o implementación sin esta evaluación previa.

4.10. Todo colaborador interno que participe en procesos, servicios o Recursos Tecnológicos debe reportar oportunamente cualquier oportunidad de mejora, desviación, ineficiencia o incidencia que identifique, utilizando los canales y procedimientos definidos por la organización. Asimismo, deberá colaborar con los Equipos Responsables en la implementación de mejoras aprobadas. Ningún hallazgo o anomalía detectado podrá omitirse o quedar sin reporte.

4.11. Todo colaborador que gestione procese o acceda a datos corporativos o personales debe proteger su confidencialidad, integridad y disponibilidad, aplicando controles proporcionales al nivel de sensibilidad de la información durante su uso, almacenamiento, retención y eliminación. Se prohíbe almacenar, transferir o eliminar datos sin las medidas y autorizaciones definidas por la organización. Los Equipos Responsables deberán documentar la clasificación de la información y las medidas aplicadas según los lineamientos vigentes

4.12. Todo contrato, acuerdo o relación con Terceros que involucren servicios tecnológicos, acceso a sistemas o tratamiento de información deberá incorporar cláusulas específicas de seguridad, confidencialidad, cumplimiento normativo y protección de datos, así como causales de término anticipado en caso de incumplimiento. Ningún servicio o proveedor podrá contratarse, renovarse u operar sin estas cláusulas. Los Equipos Responsables deberán validar y documentar que los contratos cumplen los lineamientos vigentes antes de su suscripción.

4.13. Toda las decisiones, procesos y controles tecnológicos deberán alinearse con la normativa nacional e internacional aplicable, incluyendo la Ley N° 21.663 (Marco de Ciberseguridad), el Decreto Supremo N° 295 y las disposiciones emitidas por la Agencia Nacional de Ciberseguridad (ANCI), así como la regulación sectorial correspondiente. En caso de discrepancia, prevalecerán las definiciones y obligaciones establecidas por la normativa legal sobre cualquier definición interna.

4.14. Todo contrato con Terceros que involucre servicios tecnológicos, acceso a sistemas o tratamiento de información deberá incorporar cláusulas específicas de seguridad, confidencialidad, protección de datos y cumplimiento normativo, conforme a la Ley N° 21.663 y demás normativa aplicable. Los proveedores

deberán contar con políticas de seguridad alineadas a estándares internacionales (ISO 27001, NIST) y someterse a auditorías periódicas definidas por SQM para verificar su cumplimiento.

4.15. Todo proveedor deberá notificar a SQM cualquier incidente de ciberseguridad que pueda tener efectos significativos, en los plazos establecidos por la normativa vigente, proporcionando toda la información necesaria para cumplir con el esquema de reporte ante la ANCI. Asimismo, deberá informar incidentes menores que afecten activos informáticos de SQM en un plazo máximo de 2 horas desde su detección y entregar un informe final con las medidas aplicadas.

5. Canal de Denuncias

Todos los colaboradores deberán canalizar la información de la que dispongan, o las denuncias respecto a cualquier actividad prohibida por esta Política, o incumplimiento a la misma, a través del Canal de Denuncias.

Las vías de comunicación del Canal de Denuncias son: (i) a través del sitio web http://denuncias.sqm.com ; (ii) a través de los demás mecanismos indicados en el Código de Ética de SQM disponible en el link https://mi.sqm.com/etica".

6. Cumplimiento de la Política

Todo colaborador interno o externo tiene la responsabilidad de velar por el fiel cumplimiento de esta Política, así como de la demás normativa interna asociada. Cualquier infracción a la normativa anteriormente indicada podrá dar lugar a medidas disciplinarias respecto del colaborador, de acuerdo con lo establecido en el Código de Ética, la legislación vigente y el RIOHS de SQM, pudiendo incluso determinarse su desvinculación en casos de gravedad o reincidencia.

Los colaboradores que tengan dudas respecto de si una determinada conducta podría infringir lo dispuesto en esta Política, o demás normativa vinculada, deberán consultar a la Gerencia de Transformación y Tecnología y abstenerse de actuar mientras no reciban respuesta a dicha consulta.

7. Referencias

7.1. Código de Ética de SQM

7.2. Reglamento Interno de Orden, Higiene y Seguridad (RIOHS).

Anexo 1
Definiciones

"Ciclo de Vida" Conjunto de etapas por las que atraviesa un recurso tecnológico, desde su exploración y adquisición, pasando por su operación y mantenimiento, hasta su retiro, asegurando su gestión sostenible y eficiente.

"Equipos Responsables" Se entiende por Equipos Responsables a las áreas, unidades o equipos designados formalmente por la organización para dirigir, administrar, operar, mantener y supervisar los Recursos Tecnológicos y de seguridad de la información. Estos equipos actúan dentro de su ámbito de competencia, asegurando la correcta implementación del Gobierno Tecnológico, la gestión de riesgos, la protección de la información y el cumplimiento normativo.

"Gobierno Tecnológico" Modelo de gestión liderado por la Gerencia de Transformación & Tecnología, orientado a asegurar la alineación entre los objetivos de la organización y la correcta administración de los Recursos Tecnológicos, estableciendo roles, responsabilidades y mecanismos de control.

"Recursos Tecnológicos" Conjunto de activos, herramientas, sistemas, infraestructuras, plataformas, aplicaciones, datos, servicios digitales y capacidades tecnológicas, tanto internas como provistas por Terceros, que son utilizados por la organización para soportar sus procesos operativos, estratégicos y de gestión, y cuyo uso debe ajustarse a las políticas, normas y controles definidos por la organización.

"Riesgo Tecnológico" Posibilidad de que el uso, adopción o falla de la tecnología cause impactos negativos en la organización, afectando la seguridad de las personas, la información, el cumplimiento normativo, la reputación o la rentabilidad.

"SQM" Sociedad Química y Minera de Chile S.A.

"Tercero": cualquier persona que no mantenga una relación laboral con la Empresa o con alguna entidad que no pertenece o no es controlada por la Empresa, incluso en parte, que la Empresa contrató o contratará para suministrar servicios o productos a la Empresa o para realizar actividades comerciales con o en representación de la Empresa.

"Usuarios" Personas internas o externas a la organización que interactúan con Recursos Tecnológicos, patrocinan su uso, definen su operatividad, impulsan la mejora continua y evalúan su impacto en el negocio.

Anexo 2
Marco de Referencia Normativo

El presente anexo identifica los principales estándares, marcos de referencia y buenas prácticas internacionales que sirven de base para la definición de los principios rectores, normas de conducta y lineamientos establecidos en la Política de Gobierno Tecnológico y Ciberseguridad.

1. ISO/IEC 38500 – Gobierno Corporativo de Tecnologías de Información

   Estándar internacional que proporciona principios para el gobierno corporativo de las tecnologías de información, orientando a la alta dirección en la evaluación, dirección y monitoreo del uso de la tecnología.
   Este marco establece la separación entre gobierno y gestión, promoviendo la responsabilidad, la alineación estratégica, el desempeño, la conformidad y el comportamiento humano en el uso de la tecnología.

2. ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información

   Estándar internacional para establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la identificación, evaluación y tratamiento de riesgos.
   Proporciona un enfoque sistemático para proteger la confidencialidad, integridad y disponibilidad de la información.

3. ISO/IEC 27002 – Controles de Seguridad de la Información

   Marco complementario a ISO 27001 que define un conjunto de controles de seguridad organizados en personas, procesos y tecnología.
   Refuerza el rol del comportamiento humano y la responsabilidad individual en la protección de la información.

4. ISO 31000 – Gestión del Riesgo

   Estándar internacional que establece principios y directrices para la gestión del riesgo en las organizaciones, aplicable a riesgos estratégicos, operacionales, tecnológicos y reputacionales.
   Promueve un enfoque proporcional y contextualizado del riesgo.

5. COBIT 2019 – Marco de Gobierno y Gestión de Tecnologías de Información

   Framework de buenas prácticas para el gobierno y la gestión de TI, ampliamente utilizado por áreas de auditoría y control interno.
   Integra objetivos de gobierno, procesos de gestión, métricas y responsabilidades.

6. NIST Cybersecurity Framework (CSF)

   Marco de referencia desarrollado por el National Institute of Standards and Technology (NIST) para gestionar la ciberseguridad mediante las funciones de identificar, proteger, detectar, responder y recuperar. Permite una visión integral del Ciclo de Vida de la seguridad.

7. NIST Special Publications (SP 800 Series)

   Conjunto de publicaciones técnicas que proporcionan controles de seguridad, lineamientos de continuidad y gestión de sistemas de información, ampliamente utilizadas como referencia técnica y de auditoría.

8. ISO 22301 – Continuidad del Negocio

   Estándar internacional que establece los requisitos para un Sistema de Gestión de Continuidad del Negocio, orientado a asegurar la resiliencia organizacional frente a incidentes disruptivos.

9. Sarbanes-Oxley Act (SOX)

   Regulación que exige la implementación de controles internos efectivos sobre los sistemas que soportan información financiera y procesos críticos del negocio.
   Incluye requisitos sobre trazabilidad, segregación de funciones y control de accesos.