Lineamiento Corporativo para el Uso Responsable de IA Generativa y Chatbots”

EXT-26-001

APROBADO POR:	APROBADO POR:
ANDRES PINTO	**GERSON SALAS**
Gerente de Tecnología y Digitalización	Gerente de Energia y Automatización
Firma: Andres Pinto Andres Pinto (Nov 26, 2025 09:57:14 GMT-3)	Firma: Gerson Salas Gerson Salas (Nov 26, 2025 10:03:27 GMT-3)
OFICIALIZADO POR: Gerson Salas Gerson Salas (Nov 26, 2025 10:03:27 GMT-3)	**OFICIALIZADO POR:**
ALBERTO LLONA	**CARLOS DIAZ**
COMPLIANCE OFFICER	GERENTE GENERAL
Firma: Alberto Llona Alberto Llona (Jan 16, 2026 13:45:55 GMT-3)	Firma:

1. Objetivo

Establecer los lineamientos para la evaluación, adopción, desarrollo, implementación y uso responsable de soluciones basadas en Inteligencia Artificial Generativa (IA-G) y chatbots, asegurando la protección de la información, el cumplimiento normativo y ético, así como un uso seguro, eficiente y alineado con los objetivos estratégicos y la protección de los intereses de la compañía.

2. Alcance

Este documento aplica a:

- Todas las áreas de la compañía que evalúen desarrollen, integren o utilicen soluciones de Inteligencia Artificial Generativa, chatbots, Machine Learning (ML), modelos de desarrollo cuántico, entre otros, ya sea con herramientas propias o de terceros.
- Proyectos internos, externos o de terceros que involucren estas tecnologías.
- Casos de uso que incluyan automatización de conversaciones, generación de contenido, análisis predictivo, entre otros.

3. Principios Rectores

- **Ética:** Priorizar la transparencia, no discriminación, privacidad y explicabilidad.
- **Seguridad:** Proteger los datos sensibles y evitar exposición a riesgos cibernéticos o de compliance.
- **Seguridad de la Información:** Conjunto de procedimientos, herramientas y estrategias para proteger la confidencialidad, integridad y disponibilidad de la información, ya sea en activos digital o físico.
- **Orígenes de Datos**: Las soluciones de IA deben estar conectadas con fuentes de datos confiables y autorizadas por la gerencia de tecnología. Todos estos orígenes deben vivir en la infraestructura OnPremise/Cloud de la compañía.
- **Valor de Negocio:** Toda solución debe responder a una necesidad concreta y medible.
- **Interoperabilidad**: Buscar integración adecuada con los sistemas existentes.
- **Gobernanza tecnológica:** Toda solución debe ser evaluada y/o aprobada por la Gerencia de Tecnología.
- **No Discriminación:** Se debe evitar que los algoritmos generen sesgos o discriminación hacia personas por género, etnia, religión u otros factores sensibles.
- **Privacidad:** Se deben respetar los principios de minimización de datos y consentimiento informado.

- **DevSecOps:** Desarrollo, Seguridad y Operaciones y es una metodología que integra la seguridad en cada etapa del ciclo de vida del desarrollo de software, en lugar de solo en la fase de pruebas.

4. Desarrollo y Adopción de Nuevas Soluciones de IA (Obligaciones)

- **Informe de caso de uso:** Se debe documentar el objetivo, los riesgos, las fuentes de datos involucradas y el valor esperado para la compañía o área de negocio con el fin de entregar eficiencia en el proceso.
- **Evaluación Técnica previa:** Toda iniciativa debe ser revisada por el de Tecnología y/o Seguridad de la Información con el fin de que se encuentre alineada con una necesidad específica del negocio, aportando eficiencias, retorno y beneficios concretos que justifiquen su implementación.
- **Alineamiento con Ciberseguridad:** Cumplimiento obligatorio de las políticas corporativas de seguridad y privacidad.
- **Evaluación legal y de compliance:** Si la solución maneja datos personales y sensibles, se debe coordinar con el área legal.
- **Costos asociados:** La solución debe considerar y asumir todos los costos asociados a la nueva implementación, estos son; Infraestructura tecnológica; licencias y suscripciones; integración con otros sistemas; mantenimiento y soporte; almacenamiento interno o externo; otros costos asociados a la implementación como controles de protección y seguridad que deben ser implementados para el cumplimiento normativo.
- **Medición y Evaluación Continua:** Toda solución de Inteligencia Artificial implementada deberá contar con mecanismos que permitan su evaluación periódica mediante indicadores clave de desempeño (KPIs). La medición será obligatoria y deberá ser reportada al Centro de Excelencia IA.
- **Transparencia del proveedor:** Se debe validar cómo el proveedor gestiona el entrenamiento, uso y almacenamiento de datos. Las soluciones expuestas deben contar con soluciones de seguridad y cumplimiento, además de evaluar sus políticas de uso de datos, entrenamiento de modelos y propiedad intelectual.
- **Aseguramiento en la cadena de suministros:** Todo proveedor debe garantizar y cumplir los lineamientos definidos en este documento, las políticas de seguridad de la información y los que establezca el CoE. Con el fin de garantizar la auditabilidad, protección de los datos, y controles que la organización considere necesarios para el cumplimiento del SGSI, SGI y/o normativas nacionales e internacionales que nos aplican.
- **Controles de Seguridad de la información y Ciberseguridad:** Toda solución basada en Inteligencia Artificial, deberá cumplir con los controles mínimos de Seguridad de la Información, entre ellos: Clasificación y Protección de Datos; Control de acceso; Evaluación de Riesgos; Protección y detención de amenazas y vulnerabilidades; Gestión de Incidentes; Continuidad operativa; entre otros. Lo anterior, cumpliendo a las obligaciones que SQM Salar tiene con las regulaciones SOX, ISO27001, Tisax, Leyes nacionales e internaciones, entre otros.

5. Limitantes

- **Uso de información confidencial:** Prohibido el uso de información sensible o estratégica en plataformas sin control corporativo.
- **Soluciones no evaluadas:** No se permite el uso de herramientas de IA no evaluadas o sin respaldo técnico.
- **Delegación total de decisiones:** Ninguna solución de IA debe tomar decisiones autónomas sin supervisión humana si estas impactan a personas, clientes o procesos críticos.
- **Transparencia del modelo:** Prohibido el uso de modelos que no permitan trazabilidad o explicación de resultados.
- **Restricción de atención al cliente:** No se deben usar chatbots para atención de clientes sin validación legal y de experiencia de usuario.
- Queda prohibido el uso de IA o chatbots para procesar información clasificada o categorizada como confidencial, sensible o privada sin las medidas de seguridad adecuadas definidas por la Política General de Seguridad de la Información (SGSI-POL-001).
- Toda solución deberá cumplir con la Ley de Protección de Datos Personales vigente (por ejemplo, Ley 19.628 / Ley 21.719 en Chile o GDPR si aplica internacionalmente).
- Se deben aplicar controles como cifrado, control de acceso, registro de logs y monitoreo continuo.
- Restricciones y Prohibiciones sobre la solución a implementar:
    - Automatizar decisiones críticas y operativas (ej. contrataciones, sanciones, aprobaciones financieras) sin supervisión humana.
    - Generar contenido engañoso, manipulado o que pueda dañar la reputación de personas u organizaciones.
    - Entrenar modelos de IA usando información confidencial de la organización sin permiso del área de Seguridad de la Información y custodio del negocio.

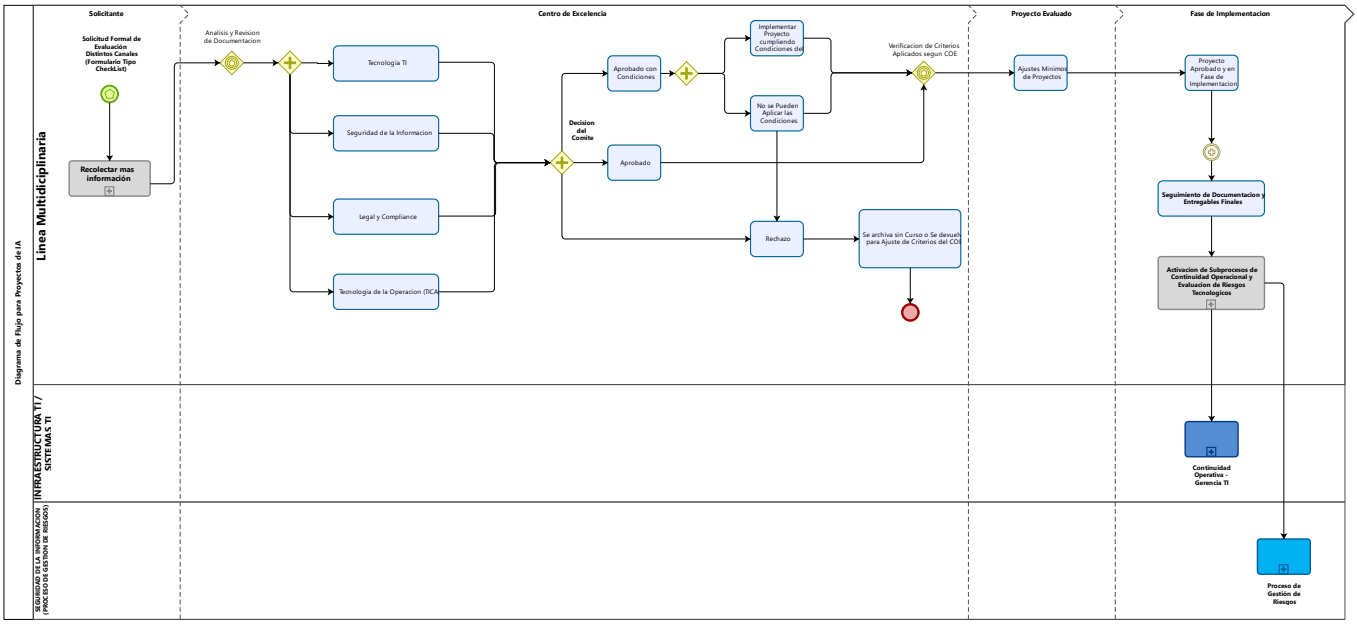
6. Reglas para Evaluación

Antes de implementar una solución de IA-G o chatbot, se deben cumplir los siguientes requisitos:

1. El caso de uso debe estar alineado a un objetivo de negocio concreto.
2. No deben existir riesgos críticos reputacionales, legales, operativos o de ciberseguridad.
3. Definir el origen de los datos, su tratamiento, almacenamiento y medidas de protección.
4. Procesar datos personales solo con la autorización del titular.
5. Contar con la aprobación del custodio de los datos y de seguridad de la información para su uso.
6. Se prohíbe almacenar resultados de IA en dispositivos personales o plataformas no autorizadas.
7. El modelo debe poder explicar su toma de decisiones.
8. La solución debe ser escalable e interoperable
9. Contar con responsables designados para su monitoreo y mejora continua.
10. Toda implementación debe incorporar la medición de su eficiencia, adopción y costos.

7.Procedimiento de Aprobación

7.1 Diagrama de Flujo



Diagrama_Propuesto_IA_Flujo_v2.svg

7.2 Solicitud formal: El área interesada debe ingresar una solicitud documentada que incluya:

- ✓ Objetivos del proyecto.
- ✓ Descripción de la solución de IA a implementar.
- ✓ Datos a utilizar y fuentes previstas.
- ✓ Riesgos potenciales identificados.
- ✓ Recursos requeridos (humanos, tecnológicos, financieros).

7.3 Revisión multidisciplinaria:

- ✓ Tecnología de Información (IT): validación de arquitectura, compatibilidad e integración con tecnología corporativa.
- ✓ Tecnología Operativa (OT): validación de la analítica de datos de la operación en su uso y modelamiento.
- ✓ Seguridad de Información: revisión de riesgos, controles de seguridad y privacidad.
- ✓ Legal y Compliance: verificación de cumplimiento normativo, contractual y ético.

- ✓ Riesgos/Continuidad Operativa: análisis de impacto en procesos críticos.

7.4 Informe de evaluación: Documento consolidado con:

- ✓ Riesgos detectados y mitigaciones.
- ✓ Nivel de madurez de la solución.
- ✓ Recomendación final (aprobar, aprobar con condiciones o rechazar).

7.5 Decisión del Centro de Excelencia IA: Este revisa el informe y emite:

- ✓ Aprobación (con o sin condiciones).
- ✓ Rechazo (con justificación).

7.6 Criterios de aprobación (se verifican antes de la decisión final): El proyecto debe demostrar:

Reducción de tiempos operativos.

Mejora en la experiencia de los usuarios.

Cumplimiento normativo y de seguridad sin incidentes.

- ✓ Alineación con los objetivos estratégicos de digitalización.
- ✓ Otros Beneficio cuantificables del proyecto.

8. Centro de Excelencia de Inteligencia Artificial (IA)

Para asegurar la correcta implementación, seguimiento y mejora continua de las soluciones de Inteligencia Artificial, se deberá conformar un **Centro de Excelencia IA**. Este tendrá las siguientes responsabilidades:

- **Supervisar** que toda iniciativa cumpla con los lineamientos definidos en este mandato.
- **Revisar y aprobar** casos de uso propuestos por las distintas áreas.
- **Evaluar riesgos** éticos, legales, operacionales y tecnológicos de las soluciones.
- **Promover buenas prácticas**, aprendizaje continuo y actualización de políticas.
- **Asegurar la trazabilidad**, monitoreo y rendición de cuentas sobre el uso de estas tecnologías.
- **Hacer seguimiento** de las iniciativas, mejoras o proyectos aprobados, y con ello validar el cumplimiento de los alineamientos acordados.

8.1 Composición sugerida del Centro de Excelencia:

- **Líder Centro de Excelencia**: para asegurar alineación estratégica y visión innovadora (Propuesta Gerente General o Gerente Digitalización y Tecnología)
- **Representante de Tecnología (TI/CTO)**: para evaluar factibilidad técnica e interoperabilidad.
- **Responsable de Ciberseguridad (CISO)**: para velar por la seguridad y gestión de riesgos.
- **Representante del área Legal y Compliance**: para validar cumplimiento normativo y ético.
- **Representante del área usuaria solicitante**: para representar la necesidad del negocio.
- **Representante de TICA**: para representar la gobernanza, alineación estratégica y visión del uso de los datos y tecnologías pertenecientes a la OT

El Centro de Excelencia debe reunirse de forma **periódica**, y generar **actas de evaluación, recomendaciones y seguimientos** de cada proyecto de IA-G aprobado.

9. Recomendaciones Generales

- Se recomienda preferir soluciones que permitan trazabilidad y explicabilidad.
- Las pruebas de concepto (PoC) deben tener objetivos claros, duración acotada y responsables asignados.
- Involucrar desde etapas tempranas a las áreas de TI, transformación digital, legal y ciberseguridad.
- Garantizar la concientización, sobre el uso responsable de la inteligencia artificial a todos los colaboradores de la compañía, así como también profundizando en los lineamientos declarados en este documento y los que defina el CoE, hacia los usuarios que implementen soluciones basadas en IA.

10. Supervisión, Auditoría y Riesgos

- La solución debe ser capaz de adoptar los controles mínimos de seguridad de la información, ciberseguridad, protección de datos, entre otros.
- Se realizarán auditorías periódicas sobre el uso de IA en la organización.
- Toda herramienta o modelo de IA deberá estar registrada y monitoreada por el área de TI o Seguridad de la Información.
- Se fomentará una revisión continua de riesgos éticos y de ciberseguridad.
- La solución debe contar con trazabilidad y logs de acciones en configuración como en accesos y otros si aplicase, con el fin de facilitar cualquier revisión interna o externa.
- Cada implementación deberá someterse a una evaluación de riesgos conforme “Metodología de Gestión de Riesgos de Seguridad e la Información” con el objetivo de identificar, tratar y monitorear los riesgos de IA de forma temprana.
- Los incidentes de seguridad de la información relacionados con soluciones basadas en IA, deberán gestionarse según el “Procedimiento de Gestión de Incidentes de Seguridad de la Información” garantizando la recuperación y resiliencia con el menor impacto posible para la organización.

11. Cumplimiento del Documento

Todo colaborador tiene la responsabilidad de velar por el fiel cumplimiento de este documento, 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 Salar, 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 este documento, o demás normativa vinculada, deberán consultar a la Gerencia de Tecnología y Digitalización y abstenerse de actuar mientras no reciban respuesta a dicha consulta.

12. Glosario

Se definen uniformes los términos técnicos utilizados en el documento:

- **IA Generativa (IA-G):** Modelos de IA capaces de crear contenidos (texto, imágenes, audio, video o código) a partir de instrucciones en lenguaje natural.
- **Chatbot:** Agente conversacional, con o sin IA-G, que interactúa con usuarios para resolver consultas, ejecutar flujos o proveer información.
- **Alineación/Guardrails:** Controles técnicos, de seguridad y de cumplimiento que encauzan el comportamiento del modelo a los límites definidos por la organización.
- **Datos personales / sensibles:** Información definida por la legislación vigente y por las definiciones a nivel compañía
- **SGSI:** Sistema de Gestión de Seguridad de la Información conforme a la Salar_SGSI-POL-001 Politica General Seguridad de la Información.
- **DevSecOps:** Integración de seguridad en todas las etapas del ciclo de vida del desarrollo.
- **CoE IA:** Centro de Excelencia de IA definido en la sección 8 del presente documento.

13. Referencias

1. Google AI, Our AI Principals, https://ai.google/principles/#our-ai-principles-in-action
2. Microsoft Responsible AI Standard, v2, General Requirements, June 2022. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft-Responsible-AI-Standard-General-Requirements.pdf?culture=en-us&country=us
3. Políticas de Uso, Open AI. https://openai.com/es-ES/policies/usage-policies/
4. Recommendation on the Ethics of Artificial Intelligence, Unesco. 2021. https://unesdoc.unesco.org/ark:/48223/pf0000381137

14. Documentos Relacionados

- Salar_SGSI-POL-001 Política General Seguridad de la Información.
- Salar_SGSI-POL-002 Política General de Seguridad de Datos.
- Salar_SGSI-POL-003 Política General de Control de Acceso.
- Salar_SGSI-POL-004 Política General de Gestion de Incidentes.
- Salar_SGSI-POL-007 Política General de Seguridad en la Nube.
- Política Corporativa de Gestión de Riesgos.
- Metodología de Gestión de Riesgos de Seguridad de la Información.
- Procedimiento de Gestión de Incidentes de Seguridad de la Información.

15. Razón del cambio

Este documento debe ser revisado y/o actualizado al menos cada 12 meses o cada vez que ocurra un cambio relevante en proceso. Dejando el registro y trazabilidad de las modificaciones en este apartado.

Versión	Razón del cambio de esta versión	Fecha
1.0	Versión Inicial	14 – 10 - 2025