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

Código de Formato: POL-AG2-SGSI-GENERAL-09 **Estatus normativo:** Vigente.

Índice

1. Introducción

La información es un activo valioso para AG2, y su protección es esencial para mantener la confianza de nuestros clientes, cumplir con los requisitos regulatorios y salvaguardar la continuidad del negocio.

Esta política establece los principios fundamentales que guían nuestro Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con la norma ISO/IEC 27001:2022.

2. Objetivo

Establecer los principios, lineamientos y compromisos generales de AG2 con respecto a la seguridad de la información, para proteger los activos de información frente a amenazas internas o externas, deliberadas o accidentales, garantizando la confidencialidad, integridad y disponibilidad.

3. Alcance

Esta política aplica a:

- Todos los miembros de AG2, incluyendo colaboradores, contratistas y terceros con acceso a la información.
- Todos los activos de información (físicos, digitales, servicios, aplicaciones, infraestructura tecnológica).
- Todos los procesos y servicios incluidos en nuestro alcance del SGSI:
  "El Sistema de Gestión de Seguridad de la Información de AG2 aplica a los servicios de contabilidad general y financiera, incluyendo: registro contable, conciliaciones bancarias, preparación de estados financieros y análisis financieros en general; elaboración y revisión de informes financieros; reporteria de estados de cuenta; cumplimiento normativo ante entidades regulatorias del sistema financiero; servicios de cumplimiento tributario; elaboración, validación y revisión de documentos en XBRL; servicios especializados para estructuras de mercados de capitales; servicios integrales de nómina; portal de cliente y automatización de procesos con base en tecnologías; servicios integrales para SOFOMES; consultoría y asesoría financiera; involucrando a todas las personas, infraestructura, tecnología y procesos internos necesarios para proveer dichos servicios, garantizando la confidencialidad, integridad y disponibilidad de la información, con el fin de brindar entera confianza a las partes interesadas internas y externas, y en cumplimiento con los requisitos legales, reglamentarios y contractuales."

4. Definiciones

- **Sistema de Gestión de Seguridad de la Información (SGSI)**: Conjunto de políticas, procedimientos y procesos diseñados para gestionar y proteger la información, asegurando su confidencialidad, integridad y disponibilidad.
- **Confidencialidad**: Garantizar que la información sea accesible únicamente a personas autorizadas.
- **Integridad**: Proteger la exactitud y completitud de la información.
- **Disponibilidad**: Asegurar que los usuarios autorizados puedan acceder a la información cuando lo necesiten.
- **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información. Incluye autenticidad, no repudio, trazabilidad y fiabilidad.
- **Incidente de seguridad de la información**: Evento o serie de eventos no deseados que comprometen la seguridad de la información y afectan las operaciones de negocio.
- **Activo de información**: Elemento con valor para la organización que requiere protección. Puede ser tangible (hardware) o intangible (datos).
- **Auditoría**: Evaluación sistemática e independiente de procesos, registros o sistemas para verificar conformidad con requisitos normativos y organizacionales.
- **No conformidad**: Incumplimiento de un requisito especificado.
- **Acción correctiva**: Medida adoptada para eliminar la causa de una no conformidad y prevenir su recurrencia.
- **Minuta**: Documento que registra los acuerdos, decisiones y puntos clave tratados en una reunión.

5. Responsabilidades

Los roles y responsabilidades y autoridades del Sistema de Gestión de Seguridad de la Información (SGSI) están definidos en el Organigrama y los Perfiles de Puesto de AG2.

Alta Dirección

La Alta Dirección es responsable de:

- Aprobar, difundir y garantizar el cumplimiento de esta política.
- Asegurar que las responsabilidades asignadas sean acordes al perfil y cargo de cada colaborador.
- Revisar periódicamente el desempeño del SGSI para asegurar su alineación con la estrategia del negocio.
- Designar un Coordinador del SGSI con autoridad y recursos suficientes para liderar su implementación, mantenimiento y mejora.
- Participar en reuniones de revisión del SGSI, conforme a los lineamientos definidos por la norma ISO/IEC 27001:2022.

La Alta Dirección realiza revisiones del SGSI en intervalos planificados para asegurar:

- Su conveniencia, adecuación, eficacia y alineación con la dirección estratégica de la organización.
- Que los elementos de entrada y salida de la revisión estén claramente definidos, e incluyan aspectos como:
  - Seguimiento de acciones previas.
  - Cambios en el contexto interno y externo.
  - Retroalimentación de partes interesadas.
  - Resultados de auditorías, evaluación de riesgos y cumplimiento de objetivos.
  - Identificación de oportunidades de mejora continua.

Los resultados de estas reuniones se documentan en minutas, que incluyen decisiones y acciones derivadas de la revisión.

Colaboradores y terceros

Todos los colaboradores y terceros deben:

- Cumplir con esta política y los lineamientos del SGSI.
- Reportar cualquier incidente de seguridad de la información.
- Participar en actividades de capacitación y sensibilización en seguridad de la información.

Coordinador del SGSI

Nombrado por la Alta Dirección, tiene la autoridad y responsabilidad de: Asegurar la conformidad del SGSI con la norma ISO/IEC 27001:2022.

- Verificar que los procesos cumplen con los resultados planificados.
- Informar a la Alta Dirección sobre el desempeño del SGSI y oportunidades de mejora.
- Promover el enfoque al cliente en toda la organización.
- Mantener la integridad del SGSI durante los cambios organizacionales.
- Coordinar auditorías internas para verificar la eficacia del sistema, el cumplimiento de los requisitos documentales, y detectar desviaciones o no conformidades.
- Gestionar un plan de auditoría considerando la criticidad de los procesos, los resultados previos y los criterios de imparcialidad (los auditores no auditan su propio trabajo).
- Comunicar resultados de auditoría y coordinar acciones correctivas cuando se detecten desviaciones.

Recursos Humanos y Dueños de Proceso

- Son responsables de poner a disposición de los colaboradores la documentación necesaria para que comprendan sus funciones dentro del SGSI.
- El área de Recursos Humanos asegura que el personal cuente con las competencias necesarias para desempeñar su rol, mediante planes de capacitación continua y evaluación de la eficacia de dichas acciones.

Responsables de Área / Dueños de Proceso

- Aplican métodos apropiados de seguimiento y medición de sus procesos, demostrando su capacidad para alcanzar los resultados planificados.
- Implementan correcciones y acciones correctivas cuando no se cumplen los resultados previstos.
- Aseguran la ejecución oportuna de las acciones derivadas de auditorías y evaluaciones internas, incluyendo las relacionadas con el Plan de Continuidad del Negocio (BCP).

6. Marco Normativo y legal

El Sistema de Gestión de Seguridad de la Información (SGSI) de AG2 se rige principalmente por la norma internacional ISO/IEC 27001:2022 y cumple con las disposiciones legales, regulatorias y contractuales aplicables conforme al contexto de la organización.

AG2 considera, entre otras, las siguientes regulaciones:

Normativa nacional relacionada con protección de datos personales, fiscalización y seguridad de la información, como:

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)
- Normativas emitidas por el SAT, SHCP, STPS y otras autoridades aplicables.
- Obligaciones contractuales derivadas de acuerdos con clientes, proveedores y terceros, incluyendo cláusulas de confidencialidad y resguardo de información.
- Normas internacionales como el Reglamento General de Protección de Datos (GDPR), únicamente cuando las operaciones o los servicios de AG2 impliquen el tratamiento de datos personales de residentes en la Unión Europea.

El cumplimiento de estos marcos se evalúa de acuerdo con la naturaleza de los servicios prestados, el tipo de datos procesados y la ubicación de los usuarios o clientes.

7. Comunicación y Disponibilidad de la Política

AG2 garantiza que la presente Política del Sistema de Gestión de Seguridad de la Información (SGSI) sea comunicada, comprendida y aplicada por todo el personal de la organización, incluidos colaboradores, contratistas y terceros que tengan acceso a información o activos relevantes.

Asimismo, AG2 asegura que esta política se mantenga disponible para las partes interesadas externas mediante su publicación en los medios digitales oficiales de la organización, tales como el portal corporativo interno, el Portal de Recursos Humanos y el sitio web institucional, en cumplimiento de lo establecido en la cláusula 7.4 “Comunicación” de la norma ISO/IEC 27001:2022.

La política se difunde de forma controlada, garantizando que todos los colaboradores conozcan su contenido a través de los procesos de inducción, capacitación y sensibilización en materia de seguridad de la información.

De igual manera, se revisa periódicamente para asegurar su vigencia, adecuación y alineación con la estrategia corporativa, los objetivos del SGSI y los requisitos aplicables.

Para facilitar su comprensión y observancia, AG2 mantiene una versión resumida institucional, denominada “Declaración de la Política del SGSI” (véase en punto 8), la cual se publica en sitios visibles y medios digitales oficiales. Esta declaración resume los principios, compromisos y lineamientos esenciales de la presente política, promoviendo su entendimiento por parte de todo el personal y las partes interesadas.

8. Declaración de la política

AG2 está comprometido con salvaguardar la información y ofrecer servicios que garantizan el cumplimiento de objetivos específicos para la seguridad de la información, ciberseguridad y protección a la privacidad en cuanto a la confidencialidad, integridad y disponibilidad de la información a través de un sistema de gestión de seguridad de la información en los servicios de contabilidad general y financiera que incluyen registro contable, conciliaciones bancarias, preparación de estados financieros, análisis financiero, elaboración y revisión de informes, cumplimiento normativo ante entidades regulatorias, servicios tributarios, elaboración y validación de documentos en XBRL, servicios para mercados de capitales, gestión integral de nómina, automatización de procesos, servicios para SOFOMES, y consultoría y asesoría financiera, a fin de garantizar la información, salvaguardar la vida humana, proteger el ambiente, los activos de la empresa y de las partes interesadas; mediante el liderazgo de la Alta Dirección y la asignación de recursos como estrategia prioritaria y buscando la mejora continua, y en cumplimiento de las leyes, normas y aplicaciones contractuales que la empresa tiene como obligación.

9. Compromisos de AG2

La Alta Dirección de AG2 demuestra su liderazgo mediante la **Declaración de Liderazgo**, participación activa en sesiones de revisión, y emisión de minutas o comunicaciones formales.

AG2 se compromete:

En materia de seguridad de la información

- Proteger la información y activos conforme a los principios de confidencialidad, integridad y disponibilidad.
- Establecer, mantener y mejorar el SGSI conforme a ISO/IEC 27001:2022.
- Gestionar los riesgos que puedan afectar la seguridad de la información.
- Cumplir con los requisitos legales, regulatorios y contractuales aplicables.

En cuanto a cultura organizacional

- Promover la capacitación, concientización y responsabilidad de todo el personal.
- Alinear el SGSI con los objetivos estratégicos del negocio.
- Comunicar la política y asegurar su comprensión en toda la organización.
- Fomentar la participación de los colaboradores para reportar cualquier incidente de seguridad de la información.
- Comunicar los lineamientos establecidos en el sistema mediante la firma del "Manifiesto de enterado y responsiva de cumplimiento".

En recursos y operación

- Garantizar la disponibilidad de recursos humanos, técnicos y financieros necesarios.
- Integrar los requisitos del SGSI en procesos, indicadores y objetivos.
- Monitorear y auditar el desempeño del SGSI y sus controles.
- Asegurar la competencia del personal mediante planes de capacitación y evaluación continua.

Infraestructura y soporte tecnológico

- Proporcionar y mantener una infraestructura segura y adecuada, incluyendo:
  - Oficinas,
  - Equipos de hardware y software,
  - Seguridad física y lógica,
  - Servicios en la nube como Microsoft 365,
  - Programas de mantenimiento preventivo y correctivo.

Comunicación y documentación

- Establecer mecanismos de comunicación interna y externa respecto al SGSI.
- Asegurar el control documental conforme a los lineamientos del procedimiento de Control Documental y Lista de Control Documental.
- Difundir políticas y objetivos a través de medios electrónicos oficiales, SharePoint y/o página web.

AG2 implementa un enfoque de mejora continua basado en:

- **Seguimiento a**:
  - Objetivos del SGSI.
  - Desempeño de proveedores.
  - Auditorías internas y externas.
  - Revisión por la Alta Dirección.
  - Incidentes de seguridad.
  - Acciones correctivas y preventivas.

- **Medición de**:
  - Procesos e indicadores.
  - Controles de seguridad implementados.

- **Análisis y evaluación de**:
  - Conformidad de productos y servicios.
  - Eficacia del SGSI y acciones tomadas.
  - Evaluación de riesgos y desempeño de proveedores.
  - Necesidades de mejora.

- **Auditorías y comprobaciones**:
  - Internas periódicas.
  - Verificación de cumplimiento.
  - Seguimiento a observaciones y acciones correctivas.

Los resultados de las evaluaciones y auditorías se comunican a la Alta Dirección para la toma de decisiones estratégicas.

10. Estructura documental del SGSI

El Sistema de Gestión de Seguridad de la Información (SGSI) de AG2 se sustenta en una estructura documental integral, que respalda el cumplimiento de los requisitos de la norma ISO/IEC 27001:2022 y facilita su implementación, operación, mantenimiento y mejora continua.

Esta estructura está compuesta por políticas, procedimientos, formatos y otros documentos de soporte que aseguran la trazabilidad, coherencia y eficacia del sistema.

Todos los documentos del SGSI se gestionan conforme al Procedimiento de Control Documental, el cual regula su creación, revisión, aprobación, publicación y disposición final, garantizando:

- la disponibilidad de versiones vigentes,
- la trazabilidad de cambios,
- la prevención del uso de documentos obsoletos, y
- el cumplimiento de los requisitos normativos aplicables.

Control de cambios

Versión	Fecha	Historial de cambios	Responsable
0.1	02/10/2024	Creación de la política	Lizbeth Aviles
	03/10/2024	Política se libera a responsable de revisión	Miguel Jaime
	04/10/2024	Se obtiene firma de conformidad	Alfonso Chida
1.0	01/08/2025	Se inicia borrador para robustecimiento de política con base em RAM-08 del Control de Seguimiento de Acciones Correctivas y Mejora FOR-AG2-SGSI-GENERAL-42.	Lizbeth Aviles
	25/08/2025	Política se libera a responsable de revisión sin encontrar cambio alguno.	Miguel Jaime
	29/10/2025	Se obtiene firma de conformidad, política se eleva a vigente y se ingresa en medios de comunicación oficiales de AG2.	Alfonso Chida

Autorizaciones

	Puesto(s):	Nombre(s):	Firma(s):	
Responsable de elaboración:	Coordinador del SGSI	Lizbeth Aviles		**Versión:**
Responsable de revisión:	Administración Corporativa	Miguel Jaime		**1.0**
Autorización:	Alta Dirección	Alfonso Chida		
Vigencia de esta versión:			1 año, a partir de la fecha de la última revisión.	