POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
Sistema de Gestión de Seguridad de la Información - Grupo ATS 2026

Código: **GATS-POL-05-03**
Versión: **v.1** Fecha de versión: **05/06/2026**

Elaboró: **Auditor Interno** Fecha de elaboración: **05/06/2026**
Aprobó: **Dirección General** Fecha de aprobación: **05/06/2026**

5.2 Política de Seguridad de la Información

Política de Seguridad de la Información de Grupo ATS

Grupo ATS establece la presente Política de Seguridad de la Información con el propósito de proteger la información generada, procesada, almacenada y transmitida por la organización y sus clientes, garantizando los principios de confidencialidad, integridad, disponibilidad y privacidad de la información.

La organización mantiene un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con los requisitos de ISO/IEC 27001:2022 y con los criterios aplicables de SOC 1 y SOC 2, asegurando controles adecuados sobre los servicios tecnológicos y procesos críticos del negocio.

1. Alcance

5.2.1 Alcance de la Política de Seguridad de la Información

La presente política aplica a:

- Todos los procesos, activos de información, sistemas, infraestructura tecnológica y servicios administrados por Grupo ATS.
- Los sistemas SaaS operados por la organización, incluyendo:
  - IDSE Cloud
  - Auditor SUA
  - MiNómina en Línea
- Infraestructura tecnológica:
  - Servidores
  - Bases de datos
  - Redes
  - Servicios en la nube
  - Equipos de usuario
  - Plataformas de respaldo y recuperación
- Todos los colaboradores internos y externos.
- Proveedores, socios comerciales y terceros que tengan acceso a información o activos de Grupo ATS.
- Información en cualquier formato: digital, físico, verbal o electrónico.

2. Compromiso de la Organización

Grupo ATS se compromete a:

2.1 Confidencialidad

Proteger la información contra divulgación, acceso o uso no autorizado mediante controles de acceso, autenticación, cifrado y clasificación de la información.

2.2 Integridad

Preservar la exactitud, consistencia y confiabilidad de la información mediante controles de validación, monitoreo, segregación de funciones y protección contra modificaciones no autorizadas.

2.3 Disponibilidad

Garantizar que la información y los servicios críticos estén disponibles para los usuarios autorizados cuando sean requeridos, mediante controles de continuidad, redundancia, respaldo y recuperación ante desastres.

2.4 Cumplimiento Normativo y Contractual

Cumplir con:

- Requisitos legales y regulatorios aplicables en México y otras jurisdicciones aplicables.
- Obligaciones contractuales con clientes y terceros.
- Requisitos de privacidad y protección de datos personales.

- Estándares internacionales de seguridad de la información, incluyendo ISO/IEC 27001:2022.
- Criterios de Servicios de Confianza (Trust Services Criteria) aplicables a SOC 2:
    - Seguridad
    - Disponibilidad
    - Confidencialidad
    - Integridad del procesamiento
    - Privacidad
- Requisitos de control interno relevantes para SOC 1 relacionados con procesos que puedan impactar la información financiera de los clientes.

2.5 Gestión de Riesgos

Mantener un proceso continuo de identificación, evaluación, tratamiento y monitoreo de riesgos de seguridad de la información y riesgos tecnológicos.

2.6 Mejora Continua

Mejorar continuamente la eficacia del SGSI y del entorno de control interno mediante auditorías, revisiones, monitoreo, análisis de incidentes y acciones correctivas.

3. Directrices de Seguridad

3.1 Gestión de Riesgos

Realizar evaluaciones periódicas de riesgos sobre activos de información, servicios tecnológicos y procesos críticos para implementar controles adecuados de mitigación.

3.2 Gestión de Accesos

Implementar controles de acceso basados en el principio de mínimo privilegio y necesidad de conocimiento, incluyendo autenticación robusta, segregación de funciones y revisiones periódicas de privilegios.

3.3 Gestión de Incidentes de Seguridad

Mantener procesos formales para:

- Detección y reporte de incidentes.
- Respuesta y contención.
- Investigación y análisis forense cuando aplique.
- Comunicación interna y externa.
- Acciones correctivas y preventivas.

3.4 Protección de Infraestructura y Datos

Proteger los sistemas e información mediante mecanismos como:

- Cifrado de datos en tránsito y almacenamiento.
- IDS/IPS y monitoreo de seguridad.
- Antivirus y protección endpoint.
- Gestión de vulnerabilidades.
- Gestión de parches.
- Respaldo y recuperación.
- Monitoreo y registro de eventos (logs).

3.5 Continuidad del Negocio

Mantener planes de continuidad del negocio y recuperación ante desastres para minimizar interrupciones operativas y garantizar la resiliencia de los servicios críticos.

3.6 Gestión de Proveedores y Terceros

Evaluar y monitorear a proveedores y terceros que procesen o tengan acceso a información de Grupo ATS, asegurando el cumplimiento de requisitos de seguridad y confidencialidad.

3.7 Capacitación y Concientización

Desarrollar programas continuos de capacitación y sensibilización en seguridad de la información, privacidad y cumplimiento para todo el personal y terceros relevantes.

3.8 Monitoreo y Auditoría

Realizar monitoreo continuo y auditorías periódicas para verificar el cumplimiento de políticas, procedimientos, controles internos y requisitos regulatorios aplicables.

3.9 Gestión de Cambios

Grupo ATS establece un proceso formal de gestión de cambios para modificaciones realizadas sobre infraestructura tecnológica, aplicaciones, configuraciones de seguridad, bases de datos y servicios productivos.

Todo cambio deberá:

- Ser documentado y evaluado previamente.
- Analizar riesgos e impactos potenciales.
- Ser autorizado por personal competente.
- Ser probado antes de su implementación en producción.
- Mantener evidencia de aprobación e implementación.
- Contar con mecanismos de reversión cuando sea aplicable.

Los cambios de emergencia deberán ser documentados y revisados posteriormente para validar su correcta implementación.

3.10 Gestión de Registros y Evidencias

La organización mantendrá controles para la creación, almacenamiento, protección, recuperación, retención y disposición de registros relacionados con el SGSI.

Los registros deberán conservarse durante los periodos definidos por requisitos legales, regulatorios, contractuales y operativos aplicables.

3.11 Monitoreo y Retención de Registros de Seguridad

Los eventos de seguridad relevantes serán registrados y monitoreados para apoyar la detección de incidentes, investigaciones, cumplimiento normativo y actividades de auditoría.

Los registros de auditoría incluirán, cuando sea aplicable:

- Accesos a sistemas.
- Actividades administrativas.
- Cambios en configuraciones.
- Eventos de seguridad.
- Actividades críticas de procesamiento.

Los registros serán protegidos contra alteración, pérdida o acceso no autorizado y conservados conforme al periodo de retención definido por la organización.

3.12 Controles Relacionados con Información Financiera de Clientes

Para los servicios que puedan impactar la información financiera de los clientes, Grupo ATS implementará controles internos orientados a garantizar:

- Exactitud de la información procesada.
- Integridad de las transacciones.
- Autorización adecuada de actividades críticas.
- Segregación de funciones.
- Trazabilidad de operaciones.
- Gestión controlada de cambios en aplicaciones y procesos.

Estos controles contribuyen al cumplimiento de los requisitos aplicables de SOC 1.

3.13 Gestión de Proveedores Críticos

Los proveedores que procesen, almacenen o tengan acceso a información sensible serán evaluados antes de su contratación y monitoreados periódicamente durante la relación comercial.

La evaluación podrá considerar:

- Riesgos de seguridad.
- Requisitos contractuales.
- Acuerdos de confidencialidad.
- Certificaciones o reportes independientes de control (SOC, ISO u otros).
- Cumplimiento regulatorio y legal.

Los resultados serán documentados y considerados dentro del proceso de gestión de riesgos de terceros.

4. Responsabilidades

Director General

Responsabilidades:

- Aprobar la Política de Seguridad de la Información y demás documentos estratégicos del SGSI.
- Proporcionar los recursos humanos, tecnológicos y financieros necesarios para la implementación, operación y mejora del SGSI.
- Impulsar una cultura organizacional orientada a la seguridad de la información, cumplimiento normativo y mejora continua.
- Definir y aprobar los objetivos estratégicos del SGSI.
- Supervisar el cumplimiento de ISO/IEC 27001, SOC 1, SOC 2 y demás requisitos aplicables.
- Aprobar planes de tratamiento de riesgos, continuidad del negocio y recuperación ante desastres.
- Participar en la Revisión por la Dirección del SGSI.
- Supervisar el desempeño general de las áreas relacionadas con seguridad de la información.
- Garantizar que los riesgos críticos sean gestionados adecuadamente.

Auditor Interno

Responsabilidades:

- Implementar, coordinar, administrar y supervisar el SGSI.
- Gestionar la identificación, evaluación, tratamiento y seguimiento de riesgos de seguridad de la información.
- Coordinar auditorías internas y externas.
- Supervisar el cumplimiento de controles de seguridad de la información y controles internos.

- Mantener actualizada la Declaración de Aplicabilidad (SoA).
- Mantener actualizado el sistema documental del SGSI.
- Dar seguimiento a hallazgos, observaciones y acciones correctivas.
- Coordinar el monitoreo del cumplimiento de requisitos legales, regulatorios y contractuales.
- Gestionar indicadores del SGSI y reportarlos a la Dirección.
- Coordinar programas de concientización y capacitación en seguridad de la información.
- Coordinar la gestión de incidentes desde la perspectiva de cumplimiento y seguimiento.

Gerente de Desarrollo

Responsabilidades:

- Implementar y operar los controles técnicos de seguridad de la información.
- Administrar servidores, infraestructura tecnológica y servicios en la nube.
- Gestionar accesos lógicos, cuentas de usuario y privilegios tecnológicos.
- Supervisar el desarrollo seguro de software.
- Gestionar cambios tecnológicos y configuraciones de activos.
- Ejecutar actividades de monitoreo tecnológico y revisión de eventos de seguridad.
- Gestionar incidentes técnicos de seguridad de la información.
- Mantener planes de respaldo, recuperación y continuidad tecnológica.
- Supervisar la disponibilidad, integridad y confidencialidad de los sistemas.
- Implementar medidas de protección para infraestructura, bases de datos y aplicaciones.

Gerente Comercial

Responsabilidades:

- Asegurar la implementación de controles de seguridad dentro de los procesos comerciales.
- Proteger la información de clientes, prospectos y distribuidores.
- Supervisar la correcta gestión de contratos, cotizaciones y renovaciones.
- Verificar el cumplimiento de requisitos contractuales relacionados con seguridad de la información.
- Reportar incidentes, riesgos o incumplimientos detectados en el área comercial.
- Gestionar los riesgos asociados a los procesos comerciales.
- Garantizar el adecuado tratamiento de información confidencial de clientes.

Gerente de Gestión de Clientes

Responsabilidades:

- Asegurar la implementación de controles de seguridad en los procesos de atención a clientes.
- Gestionar adecuadamente la información de clientes durante capacitaciones, soporte y renovaciones.
- Dar seguimiento a solicitudes, tickets y requerimientos de clientes.
- Reportar incidentes, vulnerabilidades o incumplimientos detectados.
- Mantener la confidencialidad de la información administrada.
- Gestionar riesgos relacionados con la operación y soporte a clientes.

Experto en Inteligencia Artificial

Responsabilidades:

- Desarrollar soluciones de IA alineadas a los requisitos de seguridad de la información.
- Implementar automatizaciones y modelos de IA de forma segura.

- Proteger la información utilizada en procesos de inteligencia artificial.
- Evaluar riesgos tecnológicos asociados a soluciones de IA.
- Documentar desarrollos, configuraciones y modelos implementados.
- Reportar vulnerabilidades o incidentes relacionados con herramientas de IA.
- Promover el uso responsable y seguro de tecnologías de inteligencia artificial.

Asistente Administrativo

Responsabilidades:

- Apoyar el control documental y administrativo del SGSI.
- Coordinar reuniones, convocatorias y seguimiento de acuerdos relacionados con el SGSI.
- Gestionar documentación, registros y evidencias administrativas.
- Mantener la confidencialidad de la información administrada.
- Apoyar el seguimiento de tareas derivadas de auditorías, revisiones y acciones correctivas.
- Reportar incidentes o incumplimientos detectados.

Colaboradores

Responsabilidades:

- Cumplir la Política de Seguridad de la Información y los controles aplicables.
- Proteger la información y activos asignados.
- Utilizar adecuadamente los recursos tecnológicos de la organización.
- Reportar incidentes, vulnerabilidades, eventos de seguridad o incumplimientos detectados.
- Participar en capacitaciones y actividades de concientización.
- Cumplir los procedimientos y políticas del SGSI aplicables a sus funciones.

Distribuidores, Proveedores, Consultores y Terceros

Responsabilidades:

- Cumplir las políticas, procedimientos y controles de seguridad aplicables.
- Respetar los acuerdos de confidencialidad suscritos con Grupo ATS.
- Proteger la información a la que tengan acceso.
- Reportar incidentes, vulnerabilidades o incumplimientos detectados.
- Cumplir los requisitos contractuales relacionados con seguridad de la información.
- Utilizar la información únicamente para los fines autorizados.
- Colaborar en auditorías o revisiones cuando sea requerido por contrato.

5. Revisión y Mejora

La presente política será revisada al menos una vez al año o cuando ocurran cambios significativos en:

- La operación del negocio.
- La infraestructura tecnológica.
- Los requisitos legales, regulatorios o contractuales.
- Los riesgos de seguridad identificados.
- Los requisitos de ISO/IEC 27001, SOC 1 o SOC 2.

Toda actualización deberá ser aprobada por la Dirección General y comunicada a las partes interesadas correspondientes.

6. Contexto de la Organización y Partes Interesadas

Grupo ATS identifica y monitorea de forma continua las necesidades y expectativas de las partes interesadas relevantes para el Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo clientes, usuarios, colaboradores, proveedores, socios comerciales, autoridades regulatorias, organismos certificadores y accionistas.

La organización considera los factores internos y externos que puedan afectar la capacidad para alcanzar los resultados previstos del SGSI y mantiene mecanismos periódicos de revisión para asegurar que dichos factores sean evaluados y tratados adecuadamente.

El alcance del SGSI es definido, documentado, mantenido y revisado periódicamente considerando los servicios, procesos, ubicaciones, tecnologías, activos de información y requisitos aplicables de negocio.

7. Declaración de Aplicabilidad (SoA)

Grupo ATS mantiene una Declaración de Aplicabilidad (Statement of Applicability - SoA) documentada, la cual identifica los controles de seguridad de la información aplicables, su justificación de inclusión o exclusión, estado de implementación y relación con los riesgos identificados.

La SoA es revisada periódicamente como parte del proceso de gestión de riesgos y mejora continua del SGSI.

8. Cumplimiento

El incumplimiento de esta política podrá derivar en acciones disciplinarias, contractuales o legales conforme a la normatividad interna y legislación aplicable.

Grupo ATS se reserva el derecho de monitorear y auditar el cumplimiento de esta política y de los controles asociados para garantizar la protección de la información y la continuidad de los servicios.

_____
Javier Aaron Quezada Mendoza

Historial de Revisión			
Este documento se emite bajo la guía de Calidad. Este documento o cualquier parte del mismo no se duplicarán ni se comunicará a los proveedores o clientes sin el consentimiento del departamento de calidad de Grupo ATS			
Versión	**Preparado por**	**Fecha (día/mes/año)**	**Descripción del cambio**
v.1	Lic. Maria de los Angeles Barajas Jaquez Auditor Interno SGSI	**05/06/2026**	Nueva Creación