I. OBJETIVO

Establecer la Política de Seguridad de la Información y continuidad de negocio dentro del Grupo Industrial Saltillo, S. A. B. de C. V. (GIS).

II. ALCANCE

Esta Política es de aplicación general para todas las empresas que conforman GIS.

III. DESCRIPCIÓN DE LA POLÍTICA

1. Marco de referencia de la Seguridad de la Información

Para la debida administración de la seguridad de la información, GIS basa esta política en los estándares ISO/IEC 27001, *TISAX*, NIST CSF, como marco de referencia.

2. Objetivos de Seguridad de la Información

GIS protege la confidencialidad, integridad y disponibilidad de la información propia, de clientes y de terceros autorizados que administra, así como la continuidad de sus procesos operativos y de negocio; administrando los riesgos a un nivel aceptable e implementando controles en base a buenas prácticas de seguridad, cumpliendo con el marco normativo, legal, regulatorio y contractual aplicable; GIS desarrolla, implementa, mantiene y mejora continuamente el Sistema de Gestión de Seguridad de la Información.

IV. MODELO DE GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN

El modelo de Gobierno de Seguridad se basa en el Sistema de Gestión de Seguridad de la Información, cuyos objetivos, en relación con la seguridad de información son:

1. **Identificar** los riesgos de manera sistemática.
2. **Proteger** de las amenazas, mediante el desarrollo de las tecnologías de seguridad aplicables.
3. **Detectar** amenazas mediante el uso de múltiples fuentes de inteligencia para poder gestionarlas de manera proactiva.
4. **Responder** a los incidentes de Ciberseguridad a través de protocolos corporativos:

a) limitando su impacto en la compañía
b) asegurando la continuidad de las operaciones que dependen de los servicios de la TI

5. **Recuperar y restaurar** cualquier capacidad o servicio que se haya visto afectado debido a un evento de Ciberseguridad.

V. USO DE LA INFORMACIÓN

Cada colaborador debe poder acceder únicamente a la información que necesite para su trabajo y ninguna persona no autorizada debe poder acceder a esta.

La información y los activos utilizados para resguardarla existen para lograr el objetivo del negocio y deben ser utilizados únicamente para este propósito.

VI. PROTECCIÓN DE LA INFORMACIÓN

El colaborador debe aplicar y entender los lineamientos definidos por GIS para la protección de la información.

VII. RESTRICCIÓN DE LA INFORMACIÓN

Los colaboradores, clientes y terceros autorizados deben tener acceso solamente a la información que les sea estrictamente necesaria para realizar las actividades relacionadas con los trabajos asignados.

VIII. DIVULGACIÓN DE LA INFORMACIÓN

El acceso a la información confidencial o restringida otorgado a los Colaboradores de GIS, no le confiere la autoridad para permitir el acceso a terceros dentro y fuera de GIS, ni para su divulgación a cualquier persona.

IX. SANCIONES

La violación de los principios de esta Política, lineamientos o procedimientos subsecuentes derivará en la aplicación de las medidas disciplinarias conforme al Código de Ética de GIS vigente.

X. GLOSARIO DE TÉRMINOS

Concepto	Definición
Activo de Información	Es la información en sí misma que posee valor para nuestra organización y debe protegerse en cualquier formato (digital, papel, audio, video, etc.). Su pérdida, alteración o divulgación no autorizada puede afectar la confidencialidad, integridad o disponibilidad de la información, lo que a su vez podría impactar significativamente a la empresa. El valor de la información resulta, entre otras cosas, del beneficio económico o del compromiso legal (por ejemplo, por leyes, contratos con los clientes) que la información crea en una situación determinada, y de los costos en los que se debe incurrir. Por ejemplo: Bases de datos: Información de producción, proveedores, datos de usuarios o clientes, etc. Documentos: Contratos, manuales de procedimientos, políticas internas, informes (digitales o físicos), diseños de productos, listas de clientes, secretos comerciales, reportes financieros, estrategias de negocio.

	Propiedad intelectual: Código fuente, algoritmos. Comunicaciones: Correos electrónicos, mensajes instantáneos que contienen información valiosa.
Activo de Soporte	Recurso que almacena, procesa o transporta activos de información, o que permite su uso: hardware, software, redes, ubicaciones/facilidades, personal, servicios internos y de terceros, medios físicos, etc. VDA ISA 6.0.x/TISAX los define así: "los activos de soporte (electrónicos y físicos) se usan para almacenar, procesar y transportar los activos de información". ¿Por qué distinguir Activo de Información de Activo de Soporte? Orientación del riesgo: el impacto se valora sobre el activo de información; los activos de soporte heredan o contribuyen al riesgo por su relación con la información. Controles adecuados: orientar controles técnicos/organizativos al soporte correcto, por ejemplo, cifrado en base de datos, control de acceso en SaaS (Software as a Service), *hardening* de PLC (Controlador Lógico Programable). Evidencia trazable en auditoría: facilita probar que la clasificación, propietarios y medidas de seguridad están alineadas con el valor del activo y su cadena de soporte.
Acceso Lógico	Es el acto de acceder a la información almacenada en un Sistema de Información.
Amenaza	Causa potencial de un incidente no planeado, el cual puede resultar en daño a un Activo de Información.
Disponibilidad	Aseguramiento de que la información estará accesible y utilizable bajo el requerimiento de una entidad autorizada.
Información	Datos que poseen significado. Comprende bases de datos, archivos de datos, contratos y acuerdos, documentación de sistemas, Información de investigación, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, planes de continuidad, evidencia de auditoría, información archivada, entre otros.
Incidente de Seguridad	Un incidente de Seguridad de Información es un evento que concreta una amenaza al explotar una vulnerabilidad y que causa una afectación en una o más propiedades de la información de algún activo de información, las cuales pueden ser:

	• Integridad • Disponibilidad • Confidencialidad
Integridad	Garantía de la exactitud y completitud de la Información y los métodos de su procesamiento.
Riesgo	Consecuencia de una Amenaza en relación con el Activo de Información.
Seguridad de la Información	Preservación de la Confidencialidad, Integridad y Disponibilidad de la información.
SGSI	Sistema de Gestión de Seguridad de la Información.
Tecnología de Información (TI)	Tecnología requerida para la adquisición, almacenamiento, manipulación, administración, control, intercambio, transmisión, recepción, procesamiento, análisis o despliegue de datos o información. Incluye equipos de cómputo, comunicaciones, equipo auxiliar, *software* comercial o desarrollado en casa, servicios y recursos relacionados adquiridos o arrendados, o bajo la responsabilidad de la Empresa.
Tercero / Tercera Persona	Empleado o representante de una organización diferente a GIS.
Colaborador	Persona o entidad que utilizan o requieren el acceso a un Sistema de Información para realizar una o varias tareas. El usuario puede ser un empleado o un tercero (proveedor, consultor, usuario externo).

XI. POLÍTICAS Y PROCEDIMIENTOS RELACIONADOS

1. GIS-SEG-002 Clasificación, Administración, Respaldo y Recuperación de la Información
2. GIS-SEG-003 Control de Accesos a Sistemas de Tecnología de la Información
3. GIS-SEG-004 Control de Accesos Remotos a Infraestructura de GIS
4. GIS-SEG-005 Asignación de Uso de Contraseñas
5. GIS-SEG-006 Uso de Servicio de Correo Electrónico
6. GIS-SEG-007 Uso de Navegación de Internet
7. GIS-PROC-SEG-001 Clasificación, Etiquetado y Manejo de la Información

Esta Política fue aprobada por el Comité de Seguridad de la Información en su sesión celebrada el 19 de enero de 2023.

Esta Política fue ratificada por el Comité de Seguridad de la Información en su sesión celebrada el 18 de febrero de 2025.

Esta Política fue ratificada por el Comité de Seguridad de la Información en su sesión celebrada el 25 de noviembre de 2025, continúa siendo efectiva para el año 2026.