

	GRUPO INTERESSE	
	SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	
19/09/2025	Clave del documento: 02_politica_general_ISO/IEC27001	Versión 6.0

Versión	Fecha de creación/modificación	Modificación hecha por:	Descripción de la revisión:
1	01-06-2020	Gabriel Alejandro Díaz Sánchez	Creación del documento
2	23-11-2020	Gabriel Alejandro Díaz Sánchez	Ajustes de redacción
3	14-03-2023	Carlo Iván Puerto González	Modificación de alcance
4	27-03-2024	Omar Bonilla Hernández	Actualización firma por el nuevo GSI
5	18-03-2026	Omar Bonilla Hernández	Actualización de formato y documento

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

La información puede existir en múltiples formatos: impresa, escrita en papel, almacenada electrónicamente, transmitida por correo o medios digitales, proyectada en presentaciones o compartida de manera oral.

La seguridad de la información consiste en protegerla frente a una amplia gama de amenazas, con el fin de garantizar la continuidad del negocio, reducir los riesgos y maximizar el valor de las inversiones y oportunidades.

2. Alcance

Esta política aplica a todos los colaboradores de las siguientes razones sociales:

1. Interesse Vita Agente de Seguros y de Fianzas S.A. de C.V.
2. Grupo Interesse Agente de Seguros y de Fianzas S.A. de C.V.
3. K2 Soluciones Tecnológicas S.C.
4. K2 Administración y Gestión Empresarial S.C.
5. K2 Soluciones Técnicas Especializadas.

En adelante, todas ellas se englobarán bajo el nombre “Grupo Interesse”.

Asimismo, es aplicable a todas las partes interesadas externas que tengan relación con la organización, tales como clientes, proveedores, asociados y socios de negocio.

Adicionalmente, Grupo Interesse se adhiere al [Aviso de Privacidad Integral](#) publicado en nuestro sitio web, mediante el cual se garantiza que los datos personales de colaboradores, clientes, proveedores y terceros serán tratados de manera confidencial y conforme a lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Dicho aviso forma parte esencial de la presente Política de Seguridad de la Información.

3. Objetivo

El propósito de esta política es asegurar que los sistemas de información y los datos de colaboradores, clientes y asegurados estén adecuadamente protegidos, garantizando la continuidad de los procesos de negocio y la prestación eficiente de los servicios de Grupo Interesse.

Una protección sólida contribuye a preservar los intereses de la organización, cumplir sus obligaciones en materia de seguridad y mantener la confianza de clientes y socios. La falta de medidas adecuadas podría impactar negativamente la imagen, reputación y crecimiento estratégico de la empresa.

Los objetivos específicos son:

1. Fomentar una cultura de seguridad de la información en la organización.
2. Diferenciarnos en el mercado mediante la certificación de procesos seguros.
3. Generar confianza entre clientes, asociados y socios de negocio.
4. Asegurar el cumplimiento legal y regulatorio.
5. Garantizar la continuidad del negocio.
6. Administrar de manera eficaz los riesgos de seguridad.

El cumplimiento de esta política y de toda la documentación asociada al SGSI es obligatorio para todos los colaboradores. Su incumplimiento podrá derivar en sanciones administrativas, rescisión laboral o, en casos graves, responsabilidades legales.

Las visitas y personal externo deberán cumplir igualmente con las disposiciones del SGSI, bajo la supervisión de los colaboradores responsables.

4. Principios

1. Grupo Interesse asume y gestiona únicamente riesgos comprendidos, controlados y tratados de forma adecuada.
2. Todos los colaboradores son responsables de proteger la información a la que tengan acceso en el desempeño de sus funciones.
3. Toda violación o sospecha de violación a las medidas de seguridad debe reportarse de inmediato al Socio Coordinador o al responsable de Seguridad.
4. La Dirección se compromete a proveer los recursos humanos, materiales y tecnológicos necesarios para garantizar la seguridad de la información.
5. Los riesgos de fraude y uso indebido de los sistemas de información serán gestionados de forma integral.
6. Los riesgos serán monitoreados permanentemente y se tomarán medidas oportunas ante niveles de riesgo no aceptables.
7. La organización no tolerará situaciones que impliquen incumplimiento de leyes o normativas aplicables.
8. Grupo Interesse mantiene un compromiso de mejora continua, revisando periódicamente los objetivos, métricas y controles del SGSI.

5. Responsabilidades

1. Dirección General: Responsable de asegurar la adecuada gestión de la seguridad de la información en toda la organización.
2. Líderes de área: Deben garantizar que su personal cumpla con las normas establecidas.
3. Responsable de Seguridad: Asesora, da soporte especializado y reporta el estado de la seguridad de la información.
4. Colaboradores: Deben aplicar las medidas de seguridad en todas las actividades relacionadas con su función.

6. Gestión de Riesgos de Seguridad de la Información

El SGSI de Grupo Interesse tiene como propósito prevenir que la información y los servicios se vean afectados por incidentes de seguridad. Para ello:

- Se aplicarán medidas mínimas de seguridad y controles adicionales según los riesgos identificados.
- Los roles y responsabilidades estarán claramente definidos en los perfiles de puesto.
- El personal deberá monitorear continuamente su operación para detectar anomalías y actuar en consecuencia.
- Se realizarán análisis de riesgos anuales o en casos extraordinarios (incidentes graves o vulnerabilidades críticas).

7. Evaluación de Riesgos

La evaluación de riesgos se basará en:

- A. Identificación de riesgos evidentes y ocultos.
- B. Diseño y asignación de recursos para gestionar dichos riesgos.
- C. Adaptación continua frente a cambios que generen nuevas amenazas.
- D. Participación activa de colaboradores en la identificación de riesgos, amenazas y vulnerabilidades.
- E. Clasificación de riesgos como muy altos, altos, medios o bajos.
- F. Documentación de criterios de tratamiento y priorización de acciones.

8. Tratamiento de Riesgos

Cada riesgo identificado deberá ser tratado mediante una de las siguientes opciones:

- Eliminación: Suprimir la fuente del riesgo.
- Transferencia: Externalizar la actividad a un tercero especializado.
- Aceptación: Cuando el tratamiento no sea viable o su costo sea mayor que el impacto, previa aprobación de la Dirección.

9. Relación con Terceros

Todos los terceros que intercambien información con Grupo Interesse deberán firmar un acuerdo de confidencialidad y cumplir con esta política.

Si un tercero accede a sistemas o tecnologías de información, deberá desarrollar procedimientos operativos que aseguren el cumplimiento de estos lineamientos. En caso de incumplimiento, se requerirá un informe de riesgos y su tratamiento antes de continuar con la operación.

10. Vigencia y Aceptación

Esta política entra en vigor a partir de su aprobación y permanecerá vigente de manera indefinida, salvo modificación por la Dirección General.

Su difusión estará a cargo de Capital Humano y se asegurará que todo colaborador, interno o externo, la conozca y acepte desde su incorporación, comprometiéndose a su cumplimiento.

Elaboró:

Omar Bonilla

Omar B. H.

8cad-06e0b6359226

Omar Bonilla Hernández.

Revisó:

Carlo Puerto

Carlo Puerto

8cad-06e0b6359226

Carlo Iván Puerto González.

Autorizó

Luis Mauricio Torres

Mauricio Torres E.

8cad-06e0b6359226

Luis Mauricio Torres Esquinazi