POLÍTICA

De Seguridad de la Información

Versión	Fecha de modificación/creación	Modificación hecha por:	Sección, página(s) y texto revisado:
1	01-junio-2020	Gabriel Alejandro Díaz Sánchez	Creación del Documento
2	23-noviembre-2020	Carlo Iván Puerto González	Ajustes de redacción
3	14-marzo-2023	Gabriel Alejandro Díaz Sánchez	Modificación de alcance
4	27-marzo-2024	Omar Bonilla Hernández	Actualización de firma por el nuevo GSI

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción:

1. La información puede existir en diversas formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en proyecciones o en forma oral en las conversaciones.

2. La seguridad de la información es la protección de la información contra una amplia gama de amenazas con el fin de garantizar la continuidad del negocio, minimizar los riesgos empresariales y maximizar el retorno de las inversiones yoportunidades de negocio.

2. Alcance

La presente política aplica para todos los colaboradores de las 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 Gestión Empresarial S.C.
5.- K2 Soluciones Técnicas Especializadas

Las cuales, en adelante, se englobarán bajo el nombre de “Grupo Interesse”

Así como las partes interesadas externas como: clientes, proveedores, asociados, socios de negocios, etc.

3. Objetivo

Para el correcto desarrollo de los procesos de negocio de Grupo Interesse y la adecuada prestación de sus servicios, es importante que los sistemas de información y todos losdatos de nuestros colaboradores, asegurados y clientes estén protegidos adecuadamente.

Una protección fiable permite a la organización percibir mejor sus intereses y llevar a cabo eficientemente sus obligaciones en seguridad de la información. La inadecuada protección afecta al rendimiento general de una empresa y puede afectar negativamente a la imagen, reputación y confianza de los clientes, afectando el crecimiento estratégicode nuestras actividades.

El objetivo de la seguridad de la información es asegurar la continuidad del negocio en la organización y reducir al mínimo el riesgo de daño mediante la prevención de incidentesde seguridad, así como reducir su impacto potencial cuando sea inevitable.

Para lograr este objetivo, la organización ha desarrollado una metodología de gestióndel riesgo que permite analizar regularmente el grado de exposición de nuestros activos importantes frente a aquellas amenazas que puedan aprovechar ciertas vulnerabilidades e introduzcan impactos adversos a las actividades de nuestro personal o a los procesos importantes de nuestra organización.

El éxito en el uso de esta metodología parte de la propia experiencia y aportación detodos los colaboradores en materia de seguridad, y mediante la comunicación de cualquier consideración relevante a sus Socios Coordinadores en las reuniones periódicasque tengan con ellos, con el objeto de identificar posibles cambios en los niveles de protección y evaluar las opciones más eficaces en costo/beneficio de gestión del riesgo encada momento, y según el caso.

Los principios presentados en la presente política fueron desarrollados por el Grupo Estratégico de Seguridad de la Información (GESI) con el fin de garantizar que las futuras decisiones se basen en preservar la confidencialidad, integridad y disponibilidad dela información relevante de la organización. La organización cuenta con la colaboraciónde todos los colaboradores en la aplicación de las políticas y directivas de seguridad propuestas.

El uso diario de las computadoras por los colaboradores determina el cumplimientode las exigencias de estos principios y un proceso de inspección para confirmar que se respetan y cumplen por parte de toda la organización. Adicionalmente a esta política sedisponen de políticas específicas para las diferentes actividades realizadas de manera cotidiana.

Todas las políticas de seguridad vigentes permanecerán disponibles en el repositoriode Drive que se publicó debidamente y se actualizarán regularmente. El objetivo de lapolítica es proteger los activos de información de la organización en contra de todas las amenazas y vulnerabilidades internas y externas, tanto si se producen de manera deliberada como accidental.

Los Objetivos de la presente política son:

1. Crear una cultura de seguridad de la información en la organización.
2. Crear un nuevo diferenciador al certificar nuestros procesos como seguros.
3. Generar confianza entre nuestros clientes.
4. Certidumbre jurídica.
5. Asegurar la continuidad del negocio.
6. Administrar adecuadamente los riesgos.

El cumplimiento de esta política y de cualquier otra política o procedimiento incluidos dentro del repositorio de documentación del SGSI, es obligatorio y atañe a todos los colaboradores de la organización. La violación a esta política puede conllevar un acta administrativa, la rescisión del contrato laboral o incluso derivar en una demanda penal, dependiendo de la gravedad del incumplimiento o violación.

Las visitas y personal externo que accedan a nuestras instalaciones no están exentas del cumplimiento de las obligaciones indiciadas en la documentación del SGSI, y los colaboradores internos observarán su cumplimiento.

En cualquier caso, de duda, aclaración o para más información sobre el uso de esta política y la aplicación de su contenido, por favor, consulte por teléfono o e-mail al responsable del SGSI.

4. Principios

1. Grupo Interesse afronta la toma de riesgos y tolera aquellos que, con base en la información disponible, son comprensibles, controlados y tratados cuando es necesario.
2. Todos los colaboradores de Grupo Interesse serán responsables de la seguridad dela información que tenga a su disposición para el desempeño de su trabajo.
3. La violación o sospecha de violación a las medidas o controles de seguridad de información deben reportarse de inmediato al Socio Coordinador o a los responsables de la seguridad, para su análisis y acciones correspondientes.
4. Compromiso para satisfacer los requisitos aplicables de la Seguridad de la Información. La Dirección de Grupo Interesse se asegurará de que existan los recursos humanos, materiales y tecnológicos para la gestión operativa de los controles relacionados con la seguridad de la información y en los procesos de gestión para su implantación y mantenimiento. La dirección general y el personal que se designe para dicho fin debe coordinar la revisión anual del cumplimiento delos objetivos y las métricas de seguridad de la información.
5. Se tendrán en cuenta aquellas posibilidades de fraude relacionadas con el uso abusivo de los sistemas de información dentro de la gestión global de los sistemas de información.
6. Los riesgos en seguridad de la información serán objeto de seguimiento y se adoptarán medidas relevantes cuando existan cambios que impliquen un nivel de riesgo no aceptable.

7. Las situaciones que puedan exponer a la organización a la violación de las leyes y normas legales no serán toleradas.
8. Compromiso para la mejora continua. La Dirección General y el personal quese designe para dicho fin, debe coordinar la revisión mensual del cumplimientode los objetivos y las métricas de seguridad de la información. Así como el registro y ejecución de actividades que permitan la mejora continua del SGSI conforme se detecten.

5. Responsabilidades

1. La Dirección General es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la organización.
2. Cada líder de área o línea de negocio es responsable de garantizar que las personas que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la organización.
3. El responsable de seguridad asesora al equipo directivo proporciona apoyo especializado al personal de la organización y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.
4. Cada miembro del personal tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

6. Gestión de Riesgos de Seguridad de la Información

El propósito del sistema de gestión de la seguridad de la información (SGSI) de Grupo Interesse, es prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se implementarán cuando menos medidas mínimas de seguridad, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, de ser posible deben estar claramente definidos y documentados en los perfiles de puesto.

El personal de acuerdo con sus responsabilidades debe monitorear su operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

Para garantizar el cumplimiento de la política de seguridad de la información la administración de Grupo Interesse podrá:

- Autorizar los activos de información antes de entrar en operación.

- Evaluar la seguridad, incluyendo evaluaciones de los cambios de configuración realizados.

- Solicitar cuando sea necesario la revisión por parte de terceros expertos con el fin de obtener una evaluación independiente.

- Establecer protocolos para el intercambio de información relacionada con incidentes.

- Respecto de todos los sistemas de TI sujetos a esta Política realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se realizará cuando menos una vez al año o bien; cuando ocurra un incidente muy grave de seguridad; o cuando se reporten vulnerabilidades muy graves.

7. Tabla Complementaria (Evaluación de Riesgos)

Las siguientes directrices servirán de apoyo para la identificación y evaluación de los riesgos cuando resulte necesario:

A. Se identificarán los riesgos estratégicamente importantes obvios y ocultos pero peligrosos;

B. Se asegurará de que las actividades y los procesos operativos diarios estén diseñados, dirigidos y tengan recursos para gestionar esos riesgos;

C. Se adaptará y responderá a los cambios para hacer frente a los nuevos riesgos y reducir continuamente la exposición a los mismos.

D. Los colaboradores darán aviso a su superior para la identificación de riesgos (revisión de activos, grupos de activos, procesos, tipos de información), verificando la presencia de amenazas y vulnerabilidades comunes y registrando los controles que actualmente se tiene implementados para administrarlos.

E. Se categorizará cada riesgo identificado como muy alto; alto; medio; bajo, teniendo en cuenta su evaluación de probabilidad y las consecuencias.

F. Se deberá documentar los criterios que especifiquen, para cada categoría de riesgo, qué tipo de acción debe tomarse y el nivel o prioridad que se le asigna.

8. Tratamiento de Riesgos

Respecto de cada riesgo identificado en la evaluación de riesgos se deberá determinar su tratamiento de la siguiente manera:

• Eliminación: Eliminar la fuente del riesgo.
• Transferencia del riesgo: Externalizar la actividad a un tercero que tenga mayor capacidad para gestionar el riesgo.
• Aceptar el riesgo: Si no hay un tratamiento del riesgo práctico disponible para la organización, o si se considera que el costo del tratamiento de riesgo es mayor que el costo del impacto puede tomar la decisión de aceptar el riesgo. Esto debe ser aprobado por la Dirección General o la administración de Grupo Interesse.

9. Terceras Partes

Todos los colaboradores de Grupo Interesse tienen la obligación de conocer esta Política de Seguridad de la Información, que es de cumplimiento obligatorio dentro del alcance identificado.

Los terceros prestadores de servicios o cualquier persona con la cual Grupo Interesse intercambie información, dentro del alcance, firmará un acuerdo para proteger la información intercambiada. Si se utilizan terceros que accedan a los sistemas o tecnologías de información de Grupo Interesse, se les hará conocedores de esta política y en su caso quedará sujeta a estos lineamientos, debiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos, con la aprobación de los responsables de la información o los servicios afectados antes de seguir adelante.

10. Vigencia y aceptación de la política de seguridad de la información

Esta política estará vigente desde la fecha de su firma y permanecerá vigente de manera indefinida, en tanto no sea modificada por la Dirección General de Grupo Interesse.

El aseguramiento de que todas las personas que influyen en la seguridad de la información conocen la política, se conseguirá gracias a su difusión, por parte del departamento de recursos humanos a todos los niveles de la organización, así como por medio de la distribución de los documentos que aplican a cada nivel en los distintos puestos de trabajo.

En el momento de la incorporación de un colaborador(a) (interno(a) o externo(a) a Grupo Interesse, éste aceptará la política de seguridad de Grupo Interesse comprometiéndose a su cumplimiento.

Omar Bonilla Hernández.
Elaboró:

DocuSigned by:
Omar Bonilla
ADE008A3283C4D4...

Carlo Iván Puerto González.
Revisó:

DocuSigned by:
Carlo Puerto
0A16768B592F494...

Luis Mauricio Torres Esquinazi
Autorizó

DocuSigned by:
Luis Mauricio Torres Esquinazi
B707B4F4E3D348F...