POLÍTICAS

De Seguridad de la Información

Número de versión	Fecha de modificación/creación	Modificación hecha por:	Sección, página(s) y texto revisado:
0.1	01/Junio/2020	Gabriel Alejandro Díaz Sánchez.	

Tabla de Contenido

1. OBJETIVO 2

2. ALCANCE 2

3. REFERENCIAS 2

4. LINEAMIENTOS 2

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 3

6. VIGENCIA Y ACEPTACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 3

7. TABLA COMPLEMENTARIA (EVALUACIÓN DE RIESGOS) 5

8. TRATAMIENTO DE RIESGOS 6

9. TERCERAS PARTES 7

10. VIGENCIA Y ACEPTACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 7

1. OBJETIVO

Definir la política de seguridad de la información a seguir para obtener un nivel de seguridad que permita la óptima operación y confiabilidad de las soluciones desarrolladas e implementadas por las sociedades integrantes de Grupo Interesse, en lo sucesivo Interesse. Dichas políticas deberán cumplirse con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información de Interesse.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con habilidad y rapidez a los incidentes.

2. ALCANCE

Esta política aplica para todos los colaboradores de las sociedades integrantes de Grupo Interesse así como las partes interesadas como clientes, proveedores, asociados, etc.

Las empresas integrantes de Grupo Interesse son:
Grupo Interesse Agente de Seguros y de Fianzas, S.A. de C.V.
Interesse Agente de Seguros y de Fianzas, S.A. de C.V.
Interesse Vita, Agente de Seguros y de Fianzas, S.A. de C.V.

Los lineamientos y directrices desarrolladas a partir de estas políticas deben aplicarse en todas las fases del ciclo de vida de la información: generación, distribución, almacenamiento, procesamiento, transporte, acceso, consulta y destrucción; para todos los sistemas, infraestructuras tecnológicas y las instalaciones que los soportan

3. REFERENCIAS

- Norma ISO 27001:2013.
- Glosario de términos.

4. LINEAMIENTOS

- Interesse depende de los sistemas TI (Tecnologías de Información) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.
- Esta Política de Seguridad de la Información complementa las políticas de Interesse en la protección de datos personales con base en los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad

y responsabilidad, establecidos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

- La política estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información.
- Todos los trabajadores de Interesse tienen la obligación de conocer esta Política de Seguridad de la Información, que es de cumplimiento obligatorio dentro del alcance identificado. La violación a esta política puede conllevar un acta administrativa, para documentar la mala práctica realizada por el empleado, menor, media o grave, dependiendo de la gravedad del incumplimiento o violación puede generar en su caso la rescisión del contrato laboral.
- La política debe actualizarse cada vez que se identifique un nuevo riesgo, exista un cambio en la operación o cualquier otra situación que así lo requiera.
- Los términos, abreviaturas y definiciones se encuentran en el glosario de términos.

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Interesse reconoce que los recursos humanos, la información y los activos de tecnología de información (T.I.) son esenciales para la continuidad de las operaciones de la empresa.

  La Dirección General o la Administración de Interesse debe asegurarse de que existan los recursos humanos, materiales y tecnológicos para implementar planes y programas en aspectos de seguridad de la información.
- La administración y el personal que se designe para dicho fin, debe coordinar la revisión anual del cumplimiento de los objetivos y las métricas de seguridad de la información.

  Un activo de información es un elemento reconocible que almacena datos, registros, información en cualquier medio. La información y los activos soportan una parte importante de la operación diaria de Interesse, por lo cual, toda la información creada como parte de la operación y funcionamiento de la Empresa, ya sea generada con activos de T.I., de forma manual o verbal, es propiedad de Interesse.
- Los principios que deben ser atendidos por los departamentos dentro de su alcance para garantizar la seguridad de la información son:
  - **Confidencialidad**: solo las personas autorizadas para ello deben conocer los datos. Se limita el nivel de la visibilidad de la información a únicamente que tengan acceso a ésta.
  - **Integridad**: la información tiene que ser completa, válida, veraz, exacta y no estar manipulada.
  - **Disponibilidad**: la información ha de ser accesible de forma que los usuarios autorizados para ello puedan disponer de ella cuando la necesiten y garantizar su protección.

Para apoyar al cumplimiento de la misión y objetivos de Interesse, incrementando y manteniendo el nivel de confianza que se tiene en la empresa, todos los que forman parte de ésta son responsables de la seguridad de la información y de los activos de T.I.

- La persona responsable del activo debe salvaguardar la integridad, disponibilidad y confidencialidad del activo, hacer uso del activo únicamente para los propósitos y actividades de Interesse; reportar cualquier incidente o problema relacionado con el activo de información y realizar lo necesario para mantener el activo de información en buenas condiciones que garantice y cumplan su función.
- Es importante que la seguridad de la información sea un requisito de calidad inherente a las actividades y/o procesos del negocio y nunca deberá ser una función adicional o no prioritaria.

- Los recursos para el procesamiento de la información son prioritarios para el desarrollo de los procesos de negocio y el adecuado cumplimiento de sus funciones; por lo que, es responsabilidad del personal, el salvaguardar de cualquier alteración o modificación no autorizada, daño o destrucción que límite su disponibilidad para el adecuado desarrollo de sus actividades.

- Es política de Interesse proteger su información y sus activos de tecnología de información, permitiendo el acceso, uso y revelación de dicha información solamente conforme con sus intereses institucionales y la legislación aplicable.

- La información sensible y crítica para Interesse, es aquella que se encuentra en programas, funciones o actividades y cuya pérdida, interrupción o mal uso pueden tener un impacto significativo en los productos y servicios ofrecidos por Interesse y/o que pueden dañar materialmente la capacidad de la empresa para cumplir con sus objetivos.

- Cualquier uso no autorizado de la información y/o de los activos de tecnología de información propiedad de Interesse para propósitos personales o cualquier otro propósito no relacionado con la empresa, está estrictamente prohibido. Únicamente se permitirá a los empleados el uso de información y de los activos de tecnología de información para los cuales están explícitamente autorizados.

- Cada empleado de Interesse, sin importar su nivel y su permanencia en la empresa, deberá cumplir con los lineamientos de seguridad establecidos por el mismo.

- Para garantizar la disponibilidad de los servicios críticos, los departamentos o la administración de Interesse dentro del alcance deben desarrollar planes de continuidad de los sistemas TI como parte de su plan general de continuidad de negocio y actividades de recuperación.

- La violación o sospecha de violación a las medidas o controles de seguridad de información deben reportarse de inmediato a los jefes superiores y/o a los responsables de la seguridad de tecnología de información, para su análisis y acciones correspondientes.

6. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN:

El propósito del sistema de gestión de la seguridad de la información (SGSI) de 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 monitorizar 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 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 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:

• Evasión: dejar de realizar la actividad o procesar diferente la información que está expuesta al riesgo.
• Eliminación: Eliminar la fuente del riesgo.
• Cambio de probabilidad: reducir los incidentes de seguridad de la información.
• Cambio en las consecuencias: Disminuir el impacto si ocurre un incidente.
• 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 Interesse.

9. TERCERAS PARTES

Todos los trabajadores de 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 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 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 administración de 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 empleado(a) (interno(a) o externo(a) a Interesse, éste aceptará la política de seguridad de Interesse comprometiéndose a su cumplimiento.

Gabriel Alejandro Díaz Sánchez.
Elaboró:
DocuSigned by:
Gabriel Díaz
91877EFDA5E2459...
10/07/2020
Carlo Puerto González.
Revisó:
DocuSigned by:
6F99492A637D415...
10/07/2020
José Francisco Torres Olmos.
Autorizó:
DocuSigned by:
CA5BDFEFAF0F439...
10/07/2020