	Asesorías y Gestión De Procesos S.A.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código:	SGSI004.1
Versión:	1.3
Fecha de la versión:	22-05-2019
Oficial Interno de Seguridad:	Carlos Vidal
Aprobado por:	Mauricio Droguett
Nivel de confidencialidad:	Público

Control de cambios

Fecha	Versión	Oficial Interno de Seguridad	Descripción de la modificación
05-08-2018	0.1	Carlos Vidal	Descripción básica del documento
10-10-2018	1.0	Carlos Vidal	Definición Política de seguridad de la información
12-02-2019	1.1	Carlos Vidal	Cambio de logo de la organización
27-03-2019	1.2	Carlos Vidal	Modificación en apartado 2, 4.4, 4.5, 4.6 y 7
22-05-2019	1.3	Carlos Vidal	Modificación en secciones 2 y 4.8

Índice

1. Objetivo, alcance y usuarios

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas generales para el Sistema de Gestión de la Seguridad de la Información de Asesorías y Gestión de Procesos S.A (AGP)

Esta Política se aplica a todo el Sistema de Gestión de Seguridad de la Información (SGSI), según se define en el Documento del Alcance del SGSI.

Los usuarios de este documento son todos los empleados de AGP. como también terceros externos a la organización.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos 4.4, 5.2, 5.3, 6.2, 7.1 y 7.4
- Norma ISO/IEC 27001, Anexo A.6.1.3, A.6.1.4, A7.2.2
- Documento sobre el contexto y el alcance
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Lista de requisitos legales, normativos, contractuales y de otra índole
- Plan de la Continuidad del Negocio
- Procedimiento para gestión de incidentes

3. Terminología básica sobre seguridad de la información

Confidencialidad: característica de la información por la cual solo está disponible para personas o sistemas autorizados.

Integridad: característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida.

Disponibilidad: característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de gestión de seguridad de la información: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

4. Gestión de la seguridad de la información

4.1. Objetivos y Panel de indicadores

Los objetivos generales para el sistema de gestión de seguridad de la información están definidos en el Panel de indicadores y objetivos. El Gerente General es el responsable de revisar estos objetivos generales del SGSI y de establecer nuevos.

Los objetivos para controles individuales de seguridad o grupos de controles pueden ser propuestos por Alta dirección o el Jefe de Tecnología y Sistemas, y son aprobados por el Gerente General y quedan registrados en el “Panel de indicadores y objetivos”.

Todos los objetivos deben ser revisados al menos una vez al año.

4.2. Acta de revisión por la gerencia

Asesorías y Gestión de Procesos medirá el cumplimiento de todos los objetivos. El Jefe de tecnología y sistemas es el responsable de definir el método para medir el cumplimiento de los objetivos; la revisión se realizará al menos al menos una vez al año y el Gerente de Tecnología y Sistemas analizará y evaluará los resultados y los reportará a la Gerencia como material para la revisión por parte de la Dirección.

El registro y evidencia de estas revisiones quedará en el documento: “Acta de revisión por la gerencia SGSI” el que se almacenará en la biblioteca del sitio “Gerencia” de la intranet de la organización.

La periodicidad de estas actas debe realizarse al menos una vez al año.

4.3. Requisitos para la seguridad de la información

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información, como también con las obligaciones contractuales.

En la Lista de obligaciones legales, normativas, contractuales y de otra índole se detalla una lista de requisitos legales, normativos, contractuales y de otra índole.

4.4. Controles de seguridad de la información

El proceso de escoger los controles (protección) está definido en la metodología de evaluación y tratamiento de riesgos.

Los controles seleccionados y su estado de implementación se detallan en la Declaración de aplicabilidad.

4.5. Continuidad del negocio

La Gestión de la continuidad del negocio está reglamentada en el Plan de la continuidad del negocio.

4.6. Roles y Responsabilidades

Los roles y responsabilidades están definidos en el organigrama y descriptor de cargos
En el descriptor de cargos se describen las competencias, las competencias se complementan con el Plan de capacitación y concienciación.

Las responsabilidades para el SGSI son las siguientes:

1. El Gerente de Tecnología y Sistemas es el responsable de garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política y de garantizar que todos los recursos necesarios estén disponibles.
2. El Jefe de Tecnología y Sistemas es el responsable de la coordinación operativa del SGSI, como también de informar su desempeño.
3. La Gerencia General debe revisar el SGSI al menos una vez por año o cada vez que se produzca una modificación significativa; y debe elaborar minutas de dichas reuniones. El objetivo de las verificaciones por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGSI.
4. El Jefe de Recursos Humanos implementará programas de capacitación y concienciación de empleados sobre seguridad de la información.
5. La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.
6. Todos los incidentes o debilidades de seguridad deben ser informados al Jefe de tecnología y sistemas.
7. El Gerente Comercial definirá qué información relacionada con la seguridad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo. Las necesidades de comunicación internas y externas estarán documentadas en el “Instructivo de Comunicaciones”.
8. El Jefe de Recursos Humanos es el responsable de adoptar e implementar el Plan de capacitación y concienciación, que corresponde a todas las personas que cumplen una función en la gestión de la seguridad de la información.

4.7. Comunicación de la Política

El Gerente Comercial debe asegurarse de que todos los empleados de Asesorías y Gestión de Procesos S.A., como también los participantes externos correspondientes, estén familiarizados con esta Política a través de difusiones y /o capacitaciones

4.8. Contacto con autoridades

Deben existir procedimientos para contactar a las autoridades pertinentes y reportar las incidencias relativas a la seguridad de la información

Nro.	*Nombre de la organización*	*Nombre*	*Cargo / unidad organizativa*	*Teléfono móvil*	*Teléfono fijo*	*Correo electrónico*	*Nro. de reemplazo*
21.	SAMU 131: Ambulancia	Gonzalo Cartagena y Paulo Alvarez	Encargado de RRHH y Prevencionista de Riesgos		131		
22.	Voluntarios de Bomberos	Gonzalo Cartagena y Paulo Alvarez	Encargado de RRHH y Prevencionista de Riesgos		132		
23.	Carabineros: Emergencia policiales	Gonzalo Cartagena y Paulo Alvarez	Encargado de RRHH y Prevencionista de Riesgos		133		
24.	Policía de Investigaciones	Gonzalo Cartagena y Paulo Alvarez	Encargado de RRHH y Prevencionista de Riesgos		134		
25.	Asociación Chilena de Seguridad	Gonzalo Cartagena y Paulo Alvarez	Encargado de RRHH y Prevencionista de Riesgos		1404		
26.	RB CLIMATIZACIÓN SPA	Vladimir Garrido	Asistente de tecnología y sistemas	+569 6541 0244		Reinoso.clima@gmail.com	

27.	GTD Teleductos	Vladimir Garrido	Asistente de tecnología y sistemas Y Jefe de Tecnología y Sistemas.		800390 800	soportetecnico@grupogtd.com	+56 224139 030 +56 224139 205 +56 223900 600
28.	Movistar	Vladimir Garrido	Asistente de tecnología y sistemas Y Jefe de Tecnología y Sistemas. Asistente de tecnología y sistemas		600 600 3200		800 214 242
29.	Encargado de mantenimiento de cableado estructurado	Vladimir Garrido	Asistente de tecnología y sistemas	+56995 398271		vgarrido@agpsa.cl	
30.	Enel	Vladimir Garrido	Asistente de tecnología y sistemas		600 696 0000		

4.9. Contacto con grupos de interés especial

Los grupos de interés especial mejoran el conocimiento y las prácticas relativas a la seguridad de la información.

El Jefe de Tecnología y sistemas es el responsable de revisar nuevos temas que puedan ser de interés para Asesorías y Gestión de Procesos S.A. y su SGSI. Actualmente estos grupos son:

- Firewall.cx
- www.segu-info.com.ar
- Grupo de linkedin ISO27001-SGSI Spanish Group

5. Determinación de Recursos y Entrega de Recursos del SGSI

A través del presente, el Gerente General declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

La determinación y entrega de los recursos estará dada en razón a las necesidades que requiere el SGSI tanto a los recursos relacionados a las personas (tiempo de trabajo, capacitación, etc.) y recursos de inversión (mantención de infraestructura, tecnología, recursos externos, etc.). Cada Jefe de Área o Procesos es responsable de la gestión y solicitud de los recursos, los cuales pueden ser solicitados en las reuniones de coordinación o vía mail.

6. Validez y gestión de documentos

Este documento es válido hasta el 10-10-2020.

El propietario de este documento es el Jefe de Tecnología y Sistemas, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de empleados y participantes externos que cumplen una función en el SGSI pero que no están familiarizados con el presente documento.
- No cumplimiento del SGSI con las leyes y normas, las obligaciones contractuales y con los demás documentos internos de la organización.
- Ineficacia de la implementación y mantenimiento del SGSI.
- Responsabilidades ambiguas para la implementación del SGSI.

7. Apéndices

- Organigrama
- Descriptor de cargos
- Panel de indicadores y objetivos
- Acta de Revisión por la gerencia SGSI
- Instructivo de Comunicaciones

Jefe de Tecnología y Sistemas
Carlos Vidal