CAS-CHILE®
LÍDER EN SOFTWARE DE GESTIÓN PÚBLICA

CAS-CHILE® Conectando a las **Municipalidades** del País.

Política y Objetivo General de Seguridad de la Información

Uso Público

Política y Objetivo General de Seguridad de la información AMSI-01		
Modificado por: Yoelina Hurtado	Revisado por: Rodrigo Martorell	Aprobado por: Claudio Valdés
Fecha de Implantación: 01/02/2012	Revisión N°: 16	Fecha de Modificación: 13/10/2022
Nivel de Criticidad: Media		

Control de Cambios y Revisiones

Revisión	Fecha de Modificación	Aprobado por	Comentarios/Observaciones
00	01-02-2012	Comité de Seguridad	Creación
01	04-09-2012	Comité de Seguridad	Incorpora los Objetivos Generales a la Política
02	07-09-2012	Comité de Seguridad	Se incorporan los Objetivos Estratégicos
03	03-12-2012	Comité de Seguridad	Se incorporan recomendaciones ortográficas, por parte del área de Comunicaciones Se modifica el Número telefónico en el pie de pagina Se incorpora la clasificación del documento en la portada
04	06-02-2013	Comité de Seguridad	Aprobación de cambios en redacción de la Política, cambios de objetivos y tipo de clasificación
05	14-05-2013	Comité de Seguridad	Se incorpora al final de los textos en número de la revisión y fecha de la última modificación
06	07-10-2014	Comité de Seguridad	Se modificó el Formato del Documento y ortografía
07	28-10-2014	Daniel Valdés	Se modifica la redacción de la política general y junto con esto se agregan 3 objetivos específicos
08	03-08-2015	Claudio Valdés	Se actualiza la política en base a la versión actualizada de la norma ISO 27001:2013, junto con esto se actualizan los objetivos específicos año 2015

09	21-02-2017	Daniel Valdés	Se actualizan los objetivos específicos del sistema de gestión de seguridad de la información para el año 2017
10	09-05-2018	Oficial de Seguridad	Se actualizan los objetivos específicos del sistema de gestión de seguridad de la información para el año 2018
11	17-06-2019	Claudio Valdés	Cambios en la estructura y actualización de objetivos para el año 2019
12	21-11-2019	Claudio Valdés	Se agregan excepciones a la política.
13	12/05/2020	Claudio Valdés	Se actualizan los objetivos y contenidos generales
14	26/11/2020	Claudio Valdés	Se estandariza a UNE – ISO/IEC 27001:2014, según observación n°3 de auditoría interna 2020
15	13/12/2021	Claudio Valdés	Actualización de los servicios incluidos dentro del alcance del sistema.
16	13/10/2022	Claudio Valdés	Actualización de los objetivos específicos del sistema (punto 3.1) y responsables en materia de seguridad de la información en el cual se actualiza responsabilidades del Oficial de Seguridad y se incluye al Encargado de Procesos SGSI (punto 9)

Política General de Seguridad de la Información

CAS-CHILE S.A. de I., es una empresa del mercado de las tecnologías de la información, dedicada al diseño, desarrollo y mantenimiento de Software de gestión pública y municipal. Asimismo, ofrece cursos de capacitación y asesorías para la implementación de sistemas de gestión y planificación estratégica.

La misión de la organización es "contribuir al proceso de modernización e innovación de los organismos públicos, desarrollando e implementando soluciones informáticas integrales que mejoren la calidad de vida de los ciudadanos".

1. Declaración de la intención de la organización

CAS-CHILE S.A. de I., está consciente de la importancia que representa para su negocio mantener y asegurar la Integridad, Confidencialidad y Disponibilidad de los activos de información (Tríada de la Seguridad de la Información) tanto propios, como confiados por terceros y que son manejadas por la organización.

Por lo tanto, se compromete a Desarrollar, Implantar, Mantener y Mejorar continuamente su Sistema de Gestión de Seguridad de la Información (SGSI), bajo la normativa UNE – ISO/IEC 27001:2017, realizando todos sus esfuerzos para cumplir las metas y principios de seguridad que este estatuto contiene.

A su vez, la organización cumplirá con las obligaciones de seguridad que les son propias y que inciden en su estrategia de negocio, tales como requerimientos comerciales y legales vigentes, con el fin de proveer servicios con mayores niveles de seguridad y calidad.

2. Principios de la seguridad de la información

Los principios en los que se basa la Seguridad de la Información de la organización son:

- Compromiso y liderazgo de la alta dirección de CAS-CHILE S.A. de I. en las acciones de comunicación y motivación en el cumplimiento de la Política de Seguridad de la Información de todo el personal de la organización.

- Responsabilidad organizacional en el cumplimiento de las políticas, objetivos y procedimientos relacionados con la Seguridad de la Información para la mejora continua del sistema.

- Actualizaciones oportunas en toda la información documentada del SGSI, velando siempre por aprovechar todas las oportunidades de mejora.

- Mantener y desarrollar medidas de seguridad acordes a la realidad de la organización, analizando las necesidades y recursos en pro de la mejora continua del Sistema de Gestión de Seguridad de la Información.

3. Objetivos de la gestión de seguridad de la información

3.1 Objetivo general

Asegurar y proteger la Confidencialidad, Integridad y Disponibilidad de la información tanto propia como confiada por terceros y que son manejados por la Organización, además de resguardar adecuadamente todos los activos de información de la empresa.

3.2 Objetivos específicos

- Mejora en el nivel de madurez de los controles de seguridad de la información que se encuentran implementados en la empresa, de acuerdo con UNE – ISO/IEC 27001:2017 (de acuerdo con la revisión del análisis de riesgos: evaluación, valoración y mitigación de éstos).
- Monitoreo y análisis de las transacciones registradas en la aplicación web en modalidad de pago a fin de detectar y responder a eventos que puedan impactar en el rendimiento del sitio web de manera oportuna.
- Implementación de nuevos criterios para identificar los niveles de riesgo (Tolerancia y Capacidad del riesgo), apuntando a disminuir la escala del apetito de riesgo establecido en la empresa, así como la aplicación de los planes de acción.
- Aumentar el compromiso y participación del personal de la organización en la seguridad de la información.

- Detectar vulnerabilidades en el sistema a través de hacking ético y pentesting externo como complemento de la gestión de vulnerabilidades realizados internamente.
- Mayor presencia del SGSI en los clientes de CAS-CHILE S.A. de I., mejorando la comunicación efectiva frente a incidentes de seguridad y feedback para con el sistema.
- Implementar un equipo de respuesta ante incidentes para prevenir, gestionar y responder de manera efectiva y eficaz ante la presencia de incidentes de seguridad de la información.
- Mantener, desarrollar y/o actualizar los planes de Continuidad Operacional de todos los procesos críticos de la organización, de acuerdo con el análisis de impacto (BIA) y la evaluación de riesgos, así como el procedimiento de recuperación ante desastres.
- Mejorar tiempos objetivos para el análisis de impacto de los servicios críticos que se encuentran dentro del alcance del SGSI, ante la presencia de incidentes que afecten la seguridad de la información.
- Mejorar la resiliencia de los sistemas con enfoque a proteger y asegurar las operaciones propias de los servicios críticos de la organización para garantizar la seguridad de la información y mejora de los tiempos de recuperación frente a incidentes de seguridad y/o continuidad"

4. Alcance de la política de seguridad de la información:

4.1 Alcance general

El Alcance del Sistema de Gestión de Seguridad de la Información de CAS-CHILE® corresponde a los sistemas de información que dan soporte a los siguientes servicios:

- Servicio Comercio Electrónico (Vecino Digital y E-COM)
- Software as a Service (Cloud Computing y SLEP)
- Servicios Mesa de Ayuda

De acuerdo a lo anterior, se incluye en la Política de Seguridad de la Información de CAS-CHILE®, la aplicación para todos los niveles de la organización: usuarios (trabajadores y clientes), terceros (proveedores y contratistas), entes de control y entidades relacionadas que acceden, ya sea interna o externamente, a cualquier activo de información independientemente de su ubicación, que den soporte a los servicios definidos dentro del alcance del Sistema de Gestión de Seguridad de la Información.

4.2 Definición de los activos de información

CAS-CHILE S.A. de I, entiende como Activos de Información a todos aquellos elementos que hacen posible y sustentan los procesos del negocio, es decir:

- Hardware
- Software
- Infraestructura
- Redes
- Personas
- Data

4.3 Definición de seguridad de la información

La Seguridad de la Información se puede definir como un conjunto de reglas, planes, procedimientos, instructivos, políticas y acciones que permiten asegurar la información manteniendo la triada de la información, es decir: confiabilidad, integridad y disponibilidad de los activos de información según sea necesario para alcanzar los objetivos del negocio de la organización.

5. Aspectos generales de la política de seguridad de la información

- La política de seguridad de la información, así como también toda la información documentación del SGSI ha sido elaborado en base al cumplimiento de los requisitos y estructura de la norma UNE – ISO/IEC 27001:2017 además, del cumplimiento

de la normativa chilena vigente que aplique al Sistema de Gestión de Seguridad de la Información (UNE – ISO/IEC 27001:2017)

- El incumplimiento de cualquiera de las políticas de Seguridad de la Información establecidas por la organización, y de acuerdo con el análisis de causa y gravedad del impacto, será sancionado en base al Reglamento de Orden, Higiene y Seguridad en el Trabajo CAS-CHILE®, Capitulo XI "SANCIONES Y RECLAMOS" artículos 70 a 75 inclusive.

- La Política General de la Seguridad de la Información es aprobada por la Alta Dirección de CAS-CHILE®, igualmente en el caso de la información documentada contenida en el módulo de gestión documental del software del Sistema de Gestión de la Seguridad de la Información.

- La organización se reserva el derecho se realizar evaluaciones y controles a lo dispuesto en el Sistema de Gestión de la Seguridad de la Información, abogando siempre a la mejora continua en sus procesos y la eficiencia de resultados.

- La Alta Dirección se compromete a colaborar, cuando amerite o así se considere, en lo necesario para garantizar la Seguridad de la Información en la organización.

6. Evaluación y revisión

La Política General de Seguridad de la Información será revisada anualmente, enfocándose en los objetivos específicos correspondientes a dicho años. Igualmente, ante eventualidades o cuando la Alta Dirección lo estime conveniente, la presente política será analizada, evaluada y actualizada.

7. Mecanismos de difusión

La presente Política General de Seguridad de la Información es difundida a todo el personal de CAS-CHILE® a través de lo siguiente

- Software del Sistema de Gestión de Seguridad de la Información (ePulpo)
- Correos electrónicos, mediante documentos adjuntos

- Documentos impresos dispuestos en los ficheros de la empresa
- Murales de la empresa
- Charlas presenciales y virtuales

8. Marco de control de la seguridad de la información

8.1 Otras políticas y procedimientos

El Sistema de Gestión de la Seguridad de la Información de la organización está estructurado por lo siguiente:

- Política General de Seguridad de la Información
- Políticas específicas de acuerdo con los 14 dominios establecidos en el Anexo A de la norma UNE – ISO/IEC 27001:2017.
- Información documentada (documentación, procedimientos, formatos, instructivos, registros y manuales)

9. Responsabilidades en materia de seguridad de la información

La Política de Seguridad de la Información de la organización debe ser aplicada y respetada por cada integrante de CAS-CHILE®, cumpliendo cada control y procedimiento contenido en el SGSI.

A continuación, se detallan los principales actores del Sistema de Seguridad de la Información con sus respectivas responsabilidades:

- **Oficial de seguridad:** responsable de asegurarse que el Sistema de Seguridad de la Información (SGSI) es conforme con los requisitos de la norma UNE – ISO/IEC 27001:2017, así como de informar a la alta dirección sobre el comportamiento del SGSI.

- **Encargado de procesos SGSI:** responsable de desarrollar funciones relativas al Sistema de Seguridad de la Información (SGSI): gestión de procesos del sistema de gestión ISO 27001, verificación de procedimientos, monitoreo y control de indicadores establecidos en el SGSI, así como el cumplimiento de la planificación y

del plan formal de difusión, capacitación, y sensibilización de los trabajadores en torno a la seguridad de la información para el cumplimiento de esta Política.

- **Comité de seguridad de la información:** tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante el Gerente General, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones.
- **Unidad de auditoría interna:** o en su defecto quien sea propuesto por el Comité de seguridad de la información será responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente política.
- **Área de Comunicaciones:** responsable de apoyar la comunicación interna y externa, según corresponda, respecto a toda aquella información relevante sobre la Seguridad de la Información.
- **Área de Recursos Humanos:** el área de recursos humanos de la organización (RR.HH) debe preocuparse de mantener la actualización de los acuerdos de confidencialidad de todos los integrantes de la organización, así como mantener protocolos de ingresos y egresos de personal para la generación de accesos lógicos y físicos y entrega y devolución de activos de información.

10. Excepciones

Para la Política de Seguridad de la Información de la organización se presenta la excepción en los procesos relacionados con el desarrollo de software.

11. Actuación ante eventos e incidentes

Cada integrante de la organización que evidencie cualquier situación que considere un riesgo para la organización en materia de Seguridad de la Información, tiene la obligación

de formalizar el evento o incidente a través del software del Sistema de Gestión de la Seguridad de la Información o mediante correo electrónico. Desde esta herramienta de analizará y canalizará el reporte con el objetivo de dar soluciones y aplicar las respectivas acciones correctivas.

12. Referencias normativas

La Política de Seguridad de la Información de CAS-CHILE® y toda aquella información documentada contenida en el SGSI han sido elaborado en base a la norma UNE – ISO/IEC 27001:2017.

Claudio Valdés Larrondo
Gerente General
CAS-CHILE®