



## CAS-CHILE<sup>®</sup> 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°: 18	Fecha de Modificación: 06-01-2024
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 página 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)
17	10-10-2023	Claudio Valdés	Actualización de objetivos específicos (punto 3.2), Roles y responsabilidades (punto 9) y Aspectos generales de la política de seguridad de la información respecto al incumplimiento de las políticas, (punto 5), incorporación del punto 6 Sistema de gestión de seguridad de la información, mecanismos de difusión (punto7),
18	06-01-2025	Claudio Valdés	Se actualiza: <ul style="list-style-type: none"> <li>• La misión de la organización.</li> <li>• Los principios en los que se basa la Seguridad de la Información de la organización</li> </ul>

			<ul style="list-style-type: none"><li>• concepto de seguridad de información</li><li>• Cambio de la estructura de los objetivos específicos: estratégicos, tácticos y operativos.</li><li>• Medios de difusión de la política.</li><li>• Políticas asociadas.</li><li>• Se vincula con matriz de roles y responsabilidades y instructivo para la emisión y respuesta de reportes de incidencia.</li></ul>
--	--	--	---

## 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 en la transformación digital del país, desarrollando sistemas computacionales de calidad, integrando y potenciando los talentos de nuestro equipo”**.

### 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<sup>1</sup> 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, 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 organizacional con los requisitos y estructura de la norma UNE – ISO/IEC 27001**, además del cumplimiento de la normativa chilena vigente aplicable al Sistema de Gestión de Seguridad de la Información.

---

<sup>1</sup> Tríada de la Seguridad de la Información

- **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.
- **Compromiso continuo con la mejora**, manteniendo y desarrollando 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:

##### **Estratégico**

- Mejorar 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.
- 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.

### Táctico

- Aumentar el compromiso y participación del personal de la organización en la seguridad de la información, así como en el cumplimiento de las políticas de seguridad.
- Mejorar el proceso de gestión de incidentes que permita garantizar la minimización del impacto en la confidencialidad, integridad y disponibilidad de la información, así como la mejora continua de las medidas de seguridad a través de la revisión y análisis post-incidente, con el fin de fortalecer la resiliencia organizacional.
- Mantener, desarrollar y/o actualizar los planes de Continuidad Operacional de todos los procesos críticos de la organización, con el fin de mejorar los tiempos objetivos de recuperación ante la presencia de incidentes que puedan o afecten 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.

### Operacional

- Mejorar la gestión de solicitudes formalizados a través de la plataforma ePulpo, enfocado en los procesos de formalización, seguimiento, tiempos de respuesta y comunicación.

**4. Alcance de la política de seguridad de la información:** 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
- Software as a Service
- Servicios Mesa de Ayuda

De acuerdo con lo anterior, se incluye en la Política de Seguridad de la Información de CAS-CHILE®, la aplicación para todos los niveles de la organización y partes interesadas: trabajadores, clientes, proveedores, 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.

- 4.1. **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 y data.
- 4.2. **Seguridad de la información:** es la preservación de la confidencialidad, integridad y disponibilidad de la información.

La seguridad de la información como vemos tiene por objetivo la protección de la confidencialidad, integridad y disponibilidad de los datos de los sistemas de información de cualquier amenaza y de cualquiera que tenga intenciones maliciosas.

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

- 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 según lo establecido en el procedimiento disciplinario del SGSI, el cual se basa con el Reglamento de Orden, Higiene y Seguridad en el Trabajo CAS-CHILE®.
- La Política General de la Seguridad de la Información es aprobada por la Alta Dirección de CAS-CHILE®, además se encuentra disponible para todas las partes interesadas según sea apropiado.
- La organización se reserva el derecho de 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 presente política 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 es difundida para todas las partes interesadas pertinentes al SGSI a través de los siguientes medios:
- Correos electrónicos, mediante documentos adjuntos
  - Página web de la empresa
  - Charlas presenciales y virtuales
  - Software del Sistema de Gestión de Seguridad de la Información (ePulpo)
- 8. Marco de control para el cumplimiento de requisitos de la seguridad de la información:** El Sistema de Gestión de la Seguridad de la Información de la organización está estructurado por bajo las siguientes políticas:
- Política General de Seguridad de la Información (AMSI-01)
  - Política de Seguridad de la Información en el Teletrabajo (AMSI-03)
  - Política de contraseña segura (AMSI -04)
  - Política de Dispositivos móviles (AMSI-05)
  - Política de Uso Aceptable de los Activos (AMSI-06)
  - Política de Escritorio y Pantalla Limpia (AMSI -07)
  - Política de Control de Accesos (AMSI-08)
  - Política de gestión de Vulnerabilidades (AMSI-09)
- 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. El detalle de los actores y sus respectivas responsabilidades dentro del SGSI se

encuentran detallados en la Matriz de Roles y Responsabilidades (MRR-01), así como en los respectivos contratos del personal.

**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 notificar el evento o incidente siguiendo lo establecido en el Instructivo para la emisión y respuesta de reportes de incidencia (ITS-02).

  
  
\_\_\_\_\_  
**Claudio Valdés Larrondo**  
**Gerente General**  
**CAS-CHILE<sup>®</sup>**