CONSEMA & AUDITORES SpA

Política de Seguridad de la Información

Compromiso público con la seguridad de la información y la ciberseguridad

Documento público para publicación en sitio web

Código	CONSEMA-SI-PO-01
Versión	1.0
Fecha	Agosto de 2026
Clasificación	Público

1. Nuestro compromiso

En Consema & Auditores SpA reconocemos que la información constituye un activo fundamental para nuestra organización, nuestros clientes y las demás partes interesadas con las que nos relacionamos.

Por esta razón, asumimos el compromiso de proteger la información bajo nuestra responsabilidad mediante prácticas destinadas a preservar su confidencialidad, integridad y disponibilidad, así como la privacidad de los datos personales y la resiliencia de los servicios tecnológicos que soportan nuestras operaciones.

La seguridad de la información forma parte integral de nuestra forma de operar y de los servicios profesionales que prestamos.

2. Objetivo

Esta Política tiene como objetivo establecer públicamente los principios y compromisos generales de Consema & Auditores SpA respecto de la seguridad de la información y la ciberseguridad.

Nuestro enfoque busca proteger:

- Información perteneciente a nuestros clientes.
- Información corporativa.
- Datos personales.
- Información de proveedores y colaboradores.
- Credenciales y mecanismos de autenticación.
- Documentos y registros.
- Sistemas y servicios tecnológicos.
- Comunicaciones.
- Propiedad intelectual.
- Información contractual y comercial.
- Cualquier otro activo de información bajo nuestra responsabilidad.

3. Principios de seguridad

Confidencialidad

La información debe ser accesible únicamente para las personas, sistemas o entidades debidamente autorizadas.

Integridad

La información debe mantenerse exacta, completa y protegida frente a modificaciones no autorizadas o accidentales.

Disponibilidad

La información y los recursos tecnológicos necesarios deben estar disponibles para las personas autorizadas cuando sean requeridos.

Autenticidad

Procuramos implementar mecanismos que permitan verificar razonablemente la identidad de usuarios, sistemas y fuentes de información.

Trazabilidad

Las actividades relevantes realizadas sobre nuestros sistemas e información podrán ser registradas y monitoreadas conforme a criterios de seguridad, privacidad y necesidad operacional.

Resiliencia

Procuramos mantener capacidades orientadas a prevenir, resistir, responder y recuperarnos frente a eventos que puedan afectar nuestros sistemas, información y servicios.

4. Gestión basada en riesgos

Nuestro enfoque de seguridad se basa en la identificación y evaluación de los riesgos que puedan afectar la información y los sistemas tecnológicos.

Las medidas de protección se determinan considerando factores tales como:

- Criticidad de la información.
- Sensibilidad de los datos.
- Amenazas existentes.
- Vulnerabilidades.
- Probabilidad e impacto de posibles incidentes.
- Requisitos contractuales.
- Obligaciones legales y regulatorias.
- Necesidades de nuestros clientes.
- Evolución de las amenazas de ciberseguridad.

5. Protección de la información de clientes

La información recibida o generada durante la prestación de servicios profesionales es tratada de acuerdo con su naturaleza, criticidad y requisitos contractuales.

Consema & Auditores SpA mantiene como principios:

- Acceso basado en necesidad de conocimiento.
- Uso de la información exclusivamente para finalidades autorizadas.
- Protección frente a accesos no autorizados.
- Confidencialidad durante y después de la prestación de los servicios.
- Gestión controlada del intercambio de información.
- Protección de los documentos y evidencias entregados por los clientes.
- Eliminación o devolución de información cuando corresponda.
- Cumplimiento de acuerdos de confidencialidad y obligaciones contractuales.

6. Control de acceso

El acceso a información y sistemas se administra bajo criterios de autorización y necesidad operacional.

Consema & Auditores SpA promueve prácticas relacionadas con:

- Identificación individual de usuarios.
- Gestión de permisos.
- Principio de mínimo privilegio.

- Uso seguro de credenciales.
- Autenticación reforzada cuando resulte pertinente.
- Revisión periódica de accesos.
- Retiro o modificación de privilegios cuando cambien las funciones o termine una relación laboral, contractual o profesional.

7. Protección tecnológica

Implementamos y mantenemos medidas técnicas de seguridad de acuerdo con los riesgos identificados y las características de nuestros servicios.

Estas medidas pueden comprender mecanismos de:

- Protección de dispositivos.
- Seguridad de redes y comunicaciones.
- Gestión de identidades y accesos.
- Protección contra software malicioso.
- Gestión de vulnerabilidades.
- Actualización y mantenimiento de sistemas.
- Respaldo y recuperación de información.
- Registro y monitoreo de eventos.
- Protección de comunicaciones.
- Cifrado de información cuando resulte apropiado.
- Protección de servicios en la nube.
- Prevención y detección de accesos no autorizados.
- Por razones de seguridad, las configuraciones específicas de nuestra infraestructura y de los controles implementados no son divulgadas públicamente.

8. Seguridad en servicios en la nube y terceros

La utilización de proveedores tecnológicos y servicios en la nube es evaluada considerando criterios de seguridad, privacidad, continuidad y confiabilidad.

Cuando un tercero pueda acceder, almacenar o procesar información bajo nuestra responsabilidad, procuramos establecer requisitos contractuales y de seguridad acordes con la naturaleza y riesgo del servicio.

9. Gestión de vulnerabilidades

Consema & Auditores SpA mantiene un enfoque destinado a identificar y gestionar vulnerabilidades que pudieran afectar los sistemas y servicios tecnológicos utilizados por la organización.

Las acciones adoptadas se priorizan considerando el nivel de riesgo, criticidad del activo, exposición y potencial impacto para la organización o sus clientes.

10. Gestión de incidentes

Mantenemos mecanismos orientados a la identificación, evaluación, contención, respuesta, recuperación y aprendizaje frente a incidentes de seguridad de la información y ciberseguridad.

Cuando corresponda, los incidentes serán escalados internamente y comunicados a clientes, titulares de datos, proveedores, autoridades u otras partes interesadas de acuerdo con las obligaciones contractuales y legales aplicables.

11. Continuidad y recuperación

Consema & Auditores SpA promueve medidas orientadas a mantener la continuidad de sus operaciones y recuperar los servicios frente a eventos disruptivos.

Estas medidas se establecen considerando la criticidad de los procesos y recursos que soportan nuestros servicios.

12. Seguridad de las personas

Reconocemos que las personas constituyen un componente esencial de la seguridad de la información.

Por ello, promovemos:

- Cultura de seguridad.
- Concientización frente a amenazas de ciberseguridad.
- Manejo responsable de la información.
- Protección de credenciales.
- Identificación de intentos de fraude y phishing.
- Uso adecuado de recursos tecnológicos.
- Reporte oportuno de eventos e incidentes.

13. Trabajo remoto y movilidad

Cuando nuestros servicios sean prestados mediante modalidades remotas o híbridas, se aplicarán medidas destinadas a proteger la información y los recursos tecnológicos utilizados fuera de las instalaciones físicas de la organización.

14. Cumplimiento

Consema & Auditores SpA se compromete a identificar y cumplir los requisitos legales, regulatorios, contractuales y de otra naturaleza relacionados con la seguridad de la información, ciberseguridad, privacidad y protección de datos que resulten aplicables a sus operaciones.

Como parte de este compromiso se consideran, cuando corresponda:

- La legislación chilena en materia de protección de datos personales.
- La legislación chilena en materia de ciberseguridad.
- Obligaciones contractuales con clientes y proveedores.
- Requisitos de confidencialidad.
- Buenas prácticas y estándares internacionalmente reconocidos en materia de seguridad de la información, ciberseguridad, privacidad y continuidad.

15. Buenas prácticas y estándares

Consema & Auditores SpA considera como referencia para el desarrollo y mejora de sus prácticas de seguridad marcos y estándares reconocidos internacionalmente, incluyendo, según resulte pertinente,

principios establecidos en normas tales como ISO/IEC 27001, así como otros marcos de gestión de riesgos, ciberseguridad, privacidad y continuidad.

La utilización de estas referencias no implica necesariamente que todos los servicios, procesos o sistemas de Consema se encuentren certificados bajo dichos estándares.

16. Seguridad en nuestros servicios profesionales

Dada la naturaleza de nuestros servicios de consultoría, auditoría, cumplimiento, ciberseguridad, protección de datos y sistemas de gestión, procuramos integrar la seguridad de la información desde la planificación hasta el cierre de cada servicio.

Esto considera, entre otros aspectos:

- Definición de responsabilidades.
- Protección de documentación recibida.
- Control de accesos.
- Confidencialidad.
- Intercambio seguro de información.
- Gestión de evidencias.
- Protección de información sensible.
- Eliminación o devolución segura de información al término del servicio, cuando corresponda.

17. Responsabilidad compartida

La seguridad de la información requiere la participación activa de todas las partes involucradas.

Nuestros colaboradores, proveedores y terceros autorizados deben utilizar responsablemente los recursos de información a los que tengan acceso y respetar las obligaciones de seguridad y confidencialidad establecidas.

Asimismo, recomendamos a los usuarios de nuestros servicios proteger adecuadamente sus dispositivos, credenciales y medios de acceso.

18. Mejora continua

Consema & Auditores SpA revisa periódicamente sus prácticas de seguridad y procura adaptarlas considerando:

- Nuevas amenazas.
- Cambios tecnológicos.
- Vulnerabilidades.
- Resultados de evaluaciones y revisiones.
- Cambios regulatorios.
- Nuevos servicios.
- Lecciones aprendidas de incidentes.
- Evolución de las necesidades de nuestros clientes.

19. Reporte de vulnerabilidades o incidentes

Si una persona identifica una posible vulnerabilidad, incidente, exposición de información o situación que pudiera comprometer la seguridad de nuestros servicios o información, agradecemos que sea comunicada responsablemente a Consema & Auditores SpA.

Solicitamos que cualquier vulnerabilidad identificada sea comunicada de manera responsable y que no se realicen acciones que puedan afectar la disponibilidad, integridad o confidencialidad de nuestros sistemas o de información perteneciente a terceros.

Consema & Auditores SpA

Sitio web: www.consema.cl
Correo de seguridad: gustavo.cabrera@consema.cl
Chile

20. Revisión de la Política

Esta Política será revisada y actualizada cuando existan cambios relevantes en nuestras operaciones, tecnologías, riesgos, servicios o requisitos legales y regulatorios.

La versión vigente estará disponible en nuestro sitio web.

Aprobación del documento

La presente política ha sido aprobada por la autoridad competente de Consema & Auditores SpA y será revisada cuando existan cambios relevantes en la normativa, los servicios, la tecnología o los riesgos asociados.

Nombre	Gustavo R. Cabrera R
Cargo	Socio Director – Representante Legal
Firma	
Fecha	20/08/2026

Consema & Auditores SpA