

AGROSER · RUT 76.333.148-2

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Código POL-SI-001

Versión 01

Aprobada por el Representante Legal

Vigente desde el 30 de septiembre de 2025

DOCUMENTO CORPORATIVO · POL-SI-001

Política de Seguridad de la Información y Ciberseguridad

Reglas con que AGROSER protege la confidencialidad, la integridad y la disponibilidad de su información, de los datos personales que trata y de sus sistemas. Cada control declara si está vigente o comprometido con plazo, y ninguna norma citada supone certificación.

Código POL-SI-001 | Versión 01 | Aprobada por el Representante Legal | Vigente desde el 30 de septiembre de 2025 | Sin certificación ISO/IEC 27001 ni ISO 22301 | AGROSER · RUT 76.333.148-2

1 Declaración de la alta dirección
2 Objetivo y alcance
3 Marco de referencia
4 Principios y riesgo RC-12
5 Roles y responsabilidades
6 Clasificación y accesos
7 Equipos, redes y respaldos
8 Continuidad y recuperación
9 Protección de datos personales
10 Gestión de incidentes
11 Terceros, capacitación y sanciones
12 Indicadores
13 Vigencia, revisión y aprobación

1 Declaración de la alta dirección

> **La información de nuestros clientes, trabajadores y operaciones es un activo que cuidamos con el mismo rigor con que cuidamos la seguridad en faena.** Cada persona de AGROSER es responsable de protegerla, y la empresa lo es de darle las reglas, las herramientas y la capacitación para hacerlo.
>
> Sergio E. Vallejos Godoy · Representante Legal · AGROSER

Dice qué exigimos y, en la misma página, en qué estado está cada exigencia al 30 de septiembre de 2025: lo que opera se declara vigente; lo que no, es un compromiso con responsable, fecha y código de acción del Plan de Acción (PAC-GR-001). **No presentamos como operativo ningún control cuya evidencia no podamos exhibir.** Forma un solo cuerpo con PUB-SI-001 y PLN-CIB-001.

2 Objetivo y alcance

Establecer los principios, las responsabilidades y las reglas con que AGROSER protege la confidencialidad, la integridad y la disponibilidad de su información, de los datos personales que trata y de sus sistemas, frente a amenazas internas y externas, incluidos los ciberataques.

Aplica a toda la información de la empresa, en cualquier formato —digital, papel o verbal—, a los equipos, sistemas, redes y servicios en la nube que utiliza, y a la administración, a los trabajadores cualquiera sea su tipo de contrato y a las **empresas de servicios** y proveedores que accedan a ellos, en oficinas, faenas o de forma remota.

Decimos **«empresa de servicios»** donde la legislación laboral habla de «contratista» o «subcontratista»: es el mismo sujeto. Conservamos la palabra legal solo en una cita normativa o contractual, como el certificado F30-1, según la convención de COD-EC-001.

3 Marco de referencia

Sin certificación en seguridad de la información ni en continuidad del negocio

AGROSER no cuenta con certificación ISO/IEC 27001 ni ISO 22301, ni tiene un proceso de certificación en curso en ninguna de las dos. Ambas, igual que ISO/IEC 27002, se usan **únicamente como marco de referencia**: **citar una norma no significa conformidad ni certificación**, y ninguna afirmación de este documento debe leerse así. AGROSER no tiene ninguna certificación de sistemas de gestión.

Norma o ley	Para qué la usamos	Condición
ISO/IEC 27001 y 27002	Sistema de gestión y controles	Referencia. Sin certificación ni proceso en curso
ISO 22301	Continuidad: impacto, RTO y RPO	Referencia. Sin certificación ni proceso en curso
NIST CSF 2.0 y SP 800-61	Las seis funciones de la gestión y el manejo de incidentes	Referencia. Sin certificación ni proceso en curso
Ley N° 19.628	Vida privada y datos personales	Vigente y exigible hoy
Ley N° 21.719	Nueva ley de datos personales	Publicada el 13-12-2024. **Rige desde el 1 de diciembre de 2026**
Ley N° 21.663	Ley Marco de Ciberseguridad	Vigente. Obliga a servicios esenciales y operadores de importancia vital

Norma o ley	Para qué la usamos	Condición
Ley N° 21.459	Delitos informáticos	Vigente y exigible hoy

Se suman los requisitos de seguridad de nuestros clientes, exigibles por contrato, y POL-GR-001. · AGROSER **no ha sido calificada** por la Agencia Nacional de Ciberseguridad como operador de importancia vital ni prestador de servicios esenciales: las obligaciones sustantivas de la Ley N° 21.663 **no le son exigibles hoy**. · **Antes del 01-12-2026**, Administración y Recursos Humanos adecuarán a la Ley N° 21.719 el registro de tratamientos, sus bases de licitud y el procedimiento de brechas.

4 Principios y riesgo RC-12

- **Confidencialidad, integridad y disponibilidad.** Solo la conoce quien está autorizado, es exacta, se modifica de forma trazable y está accesible dentro de los tiempos del §8.
- **Mínimo privilegio y seguridad desde el diseño.** Cada persona accede solo a lo que requiere su función, y hay requisitos de seguridad al adquirir sistemas y al contratar servicios tecnológicos.
- **Riesgo, trazabilidad y mejora continua.** Los controles se priorizan según RC-12, las acciones relevantes quedan registradas y se aprende de incidentes, pruebas y auditorías de clientes.

RC-12 · Pérdida de información o ciberataque

Categoría	Prob. × impacto	Inherente	Controles clave	Eficacia	Residual	Dueño
Información	3 × 3	9, medio	Respaldos, control de accesos y capacitación	Parcialmente efectivo	6, medio	Administración

Es el **único riesgo de este ámbito en la matriz corporativa**. «Parcialmente efectivo» significa, según MET-GR-001, que el control existe con debilidades de diseño, frecuencia o evidencia y y su plan de mejora ya se ejecutó: **A-24** y **A-25**.

Las **ocho manifestaciones** de RC-12 se publican en PUB-SI-001 §4 con el prefijo **RSI-01 a RSI-08**: phishing, secuestro de información, cuentas comprometidas y fraude, indisponibilidad de sistemas, filtración de datos personales, pérdida o robo de equipos, riesgos de terceros y uso indebido de información interna. Se gestionan dentro del nivel residual 6, medio. Los riesgos corporativos se numeran **RC-01 a RC-13** y los de derechos humanos, **RH-01 a RH-18**.

5 Roles y responsabilidades

La **responsabilidad de la seguridad de la información está radicada en Administración**, con la supervisión del **Comité de Riesgos y Sostenibilidad**, según el acta de aprobación de esta política del **30 de septiembre de 2025**. Es una responsabilidad del área, no de un cargo a título individual.

> **Hecho posterior a la fecha de corte.** En **septiembre de 2026** AGROSER designó por escrito a **Benjamín Cruces** como Encargado de Seguridad de la Información. La responsabilidad del área de Administración que fija esta sección se mantiene; a partir de esa designación existe además un cargo individual que la coordina. El suplente aún no ha sido designado. Esta política informa la situación al 30 de septiembre de 2025, que es su fecha de corte.

Rol	Responsabilidades
Representante Legal	Aprobar la política, asignar recursos y recibir los incidentes críticos.

Rol	Responsabilidades
Comité de Riesgos y Sostenibilidad	Supervisar estos riesgos. Constituido el 30-09-2025 (A-28), **a esa fecha no había celebrado sesiones**; sesionará cada trimestre desde octubre de 2025. Primer reporte: 31-01-2026 (A-29).
Administración	Tiene radicada la responsabilidad de la seguridad de la información: coordina la política, gestiona accesos e incidentes, opera respaldos y antivirus, supervisa a las empresas de servicios tecnológicos y reporta al Comité. Responsable de A-24 y A-25.
Coordinador(a) de Gestión de Riesgos	Segunda línea y secretaría del Comité. Verifica la implantación y la evidencia de los controles el 31-01-2026 (A-29).
Jefaturas	Dueñas de la información de su área: la clasifican (§6), autorizan y revisan los accesos de su equipo y velan por el cumplimiento.
Trabajadores y usuarios	Cumplir la política, proteger sus credenciales, firmar el compromiso de uso aceptable y **reportar de inmediato** cualquier incidente o sospecha.
Empresas de servicios y proveedores	Cumplir las cláusulas de confidencialidad y seguridad de sus contratos. Las de servicios tecnológicos operan bajo supervisión de Administración, que responde por ellas ante el Comité.

El **Encargado de Prevención de Delitos** conduce los hechos que puedan constituir delito informático y prepara el informe previo a la denuncia al Ministerio Público. · En POL-GC-001 la función de Administración se llama **Administración y Finanzas**, nombre con que el PAC-GR-001 le asigna A-24 y A-25: es la misma unidad.

6 Clasificación y accesos

CLASIFICACIÓN DE LA INFORMACIÓN

- **Pública.** Sitio web, políticas publicadas y folletos: sin restricciones; solo la publica el área autorizada por el Representante Legal.
- **Uso interno.** Procedimientos, programas de trabajo y comunicaciones internas: solo para personal de AGROSER, salvo autorización de la jefatura dueña.
- **Confidencial.** Contratos, ofertas, información de clientes y financiera y planos de faenas: acceso por necesidad de saber, nunca en cuentas personales, destrucción segura.
- **Restringida.** Datos personales y de salud, remuneraciones, credenciales y denuncias: acceso mínimo y nominativo, cifrado o clave, con registro de accesos.

Lo no clasificado se trata como **Uso interno**. La información de clientes se rige además por sus propias políticas, que prevalecen cuando son más exigentes. El expediente de una denuncia es siempre **Restringido**: lo custodia la secretaría del Comité de Ética y Cumplimiento (GES-DEN-001).

CONTROL DE ACCESOS

Regla de acceso	Qué exige	Estado al 30-09-2025
Cuenta personal	Personal e intransferible; sin cuentas compartidas, salvo cuentas de servicio controladas.	Vigente
Altas, cambios y bajas	Las solicita la jefatura y se registran. Al término del contrato, los accesos se eliminan **el mismo día**.	Vigente
Mínimo privilegio	Permisos por necesidad de saber, revisados **cada semestre**.	Vigente
Doble factor	Obligatorio en correo, sistemas financieros y de remuneraciones, y acceso remoto.	Vigente
Cuentas de administrador y accesos de terceros	Las primeras, solo para administrar; los de empresas de servicios, temporales, nominativos y supervisados.	Vigente
Bloqueo de sesión	Automático tras 10 minutos de inactividad.	Vigente

Vigente: existe y podemos mostrar su evidencia. · **Comprometido:** no opera todavía; tiene acción, responsable y fecha en el PAC-GR-001. Taxonomía de PLN-CIB-001 §4, válida para todas las tablas de estado.

Contraseñas. Mínimo **12 caracteres** con letras, números y símbolos, sin datos personales; personal e intransferible, nunca reutilizada entre cuentas personales y de la empresa, guardada solo en un gestor autorizado; cambio inmediato ante sospecha de exposición; **bloqueo tras 5 intentos fallidos**.

Uso aceptable. No se reenvía información confidencial o restringida a cuentas personales, no se abren adjuntos sospechosos, no se instala software no autorizado ni se desactiva el antivirus; la información de la empresa vive en la nube corporativa, por mensajería solo circula la de uso interno, se conectan únicamente dispositivos entregados por la empresa y en redes sociales se comparten las publicaciones oficiales, nunca fotografías de faenas de clientes. **Inteligencia artificial:** a esta fecha **no existe todavía una lista de herramientas autorizadas**; hasta que el Representante Legal la apruebe, antes del 30-09-2026, ninguna herramienta recibe información confidencial, restringida ni datos personales. Los recursos pueden ser monitoreados con fines de seguridad, conforme a la ley, de forma impersonal y respetando la dignidad de los trabajadores.

7 Equipos, redes y respaldos

Control	Qué exige esta política	Estado al 30-09-2025
Antivirus y protección de equipos	Todos los equipos **deben contar** con antivirus o protección de endpoint activa y actualizada, desde una consola central.	Vigente
Gestión de actualizaciones	Sistemas y aplicaciones actualizados; las críticas, en un plazo máximo de 15 días.	Vigente
Cifrado y segmentación de red	Disco cifrado y bloqueo de pantalla en notebooks, respaldos confidenciales cifrados y Wi-Fi de visitas separada de la red corporativa.	Vigente
Equipos en faena y baja de equipos	Protección contra pérdida, robo y daño, con aviso inmediato para bloquear accesos; borrado seguro antes de eliminar o reutilizar.	Vigente
Respaldos 3-2-1	Tres copias, en dos medios distintos y una fuera de las oficinas o en la nube, protegida contra modificación.	Vigente
Pruebas de restauración	Prueba trimestral documentada con fecha, participantes, resultado y tiempo de recuperación.	Vigente

Retención: **12 meses** para contabilidad, remuneraciones y facturación; **5 años** para documentos de faenas, contratos y registros de seguridad y salud; **30 días** para los equipos sincronizados con la nube. Se revisará con los tiempos del §8 el 30-09-2026.

8 Continuidad y recuperación

Siete servicios críticos, con su prioridad, su tiempo máximo de recuperación (RTO) y su pérdida máxima de datos tolerable (RPO), en horas. Es la tabla de PLN-CIB-001 §2 y prevalece sobre agrupaciones anteriores.

Servicio crítico	Prioridad	RTO / RPO
Correo electrónico y comunicaciones	1	24 h / 24 h
Remuneraciones y cotizaciones	1	48 h / 24 h
Facturación y cobranza	1	48 h / 24 h
Canal de Denuncias	2	48 h / 24 h
Registros de faena, seguridad y control de personal	2	72 h / 24 h
Contabilidad y compras	2	72 h / 24 h
Sitio web institucional	3	120 h / 168 h

El orden de recuperación

Se recupera **primero el correo**, no las remuneraciones: tiene el RTO más exigente, 24 horas frente a 48, y sin correo no se coordina la recuperación de lo demás.

1. Correo y comunicaciones, 24 h · **2.** remuneraciones, facturación y Canal de Denuncias, 48 h · **3.** registros de faena y seguridad, contabilidad y compras, 72 h · **4.** sitio web, 120 h.

Mientras el Canal de Denuncias esté caído, las denuncias se reciben en **contacto@agroserspa.cl** y en el **+569 9501 4156**, con los plazos de acuse de GES-DEN-001.

Sin sistemas, la operación sigue en modo manual: registros en papel, emisión de documentos tributarios desde el portal del Servicio de Impuestos Internos y conexión móvil de respaldo (PLN-CIB-001 §7). **Los RTO y RPO son preliminares:** no provienen de un análisis de impacto documentado — no hay fecha, método, participantes ni criterios que podamos exhibir— y **se validarán el 30-09-2026**.

9 Protección de datos personales

Los datos personales se tratan solo para **fines legítimos, informados y necesarios**, conforme a la **Ley Nº 19.628** y a la norma 4.6 del Código de Ética y Conducta. Los de salud, remuneraciones y denuncias son información **Restringida** (§6), y toda vulneración se gestiona como incidente (§10).

Derechos de los titulares, hoy. Conforme a la Ley Nº 19.628, pueden ejercer los derechos de **acceso, rectificación, eliminación y bloqueo** escribiendo a **contacto@agroserspa.cl** con el asunto **«Datos personales»**. AGROSER registra cada solicitud y responde por escrito **dentro de 5 días hábiles**, sin perjuicio de los plazos que fije la ley; el registro lo mantiene Administración y se informa al Comité cada trimestre.

Derechos que se incorporan el 1 de diciembre de 2026. Con la entrada en vigencia de la **Ley Nº 21.719** se sumarán los derechos de **oposición y portabilidad** y el deber de notificar las brechas a la Agencia de Protección de Datos Personales. Hasta esa fecha esos dos derechos **no son exigibles** y esta política no los ofrece: anunciarlos antes de tiempo sería ofrecer algo que la ley todavía no reconoce.

Datos sensibles: voluntarios, autodeclarados y agregados. Cuando AGROSER recoge datos de salud o discapacidad, lo hace sobre la base de una **declaración voluntaria de la persona**, que puede negarse sin consecuencia alguna, con la finalidad informada al recogerlos: salud ocupacional, Ley Nº 21.015 o adecuación del puesto. **Nunca se publican de forma individualizada:** todo reporte externo va en cifras agregadas (Ley Nº 19.628).

10 Gestión de incidentes

Todo trabajador informa de inmediato cualquier incidente o sospecha —phishing, pérdida de equipos, accesos no autorizados, virus, secuestro de información o filtración de datos—. **Reportar nunca es una falta;** callar una sospecha sí puede serlo.

1

Reportar y registrar

Aviso inmediato a Administración o a la jefatura, por contacto@agroserspa.cl con el asunto «Seguridad de la información» o por el +569 9501 4156. Registro el mismo día de la detección y, en los críticos, **clasificación de severidad dentro de 1 hora desde la detección**.

2

Contener y recuperar

Aislar equipos, bloquear cuentas y cambiar claves dentro del plazo que fija la severidad; eliminar la causa y restaurar desde respaldos verificados dentro del RTO del servicio (§8).

3

Notificar y aprender

Al Representante Legal de inmediato si es crítico, y a clientes, titulares y autoridades **dentro de los plazos legales aplicables**. Causa raíz y al menos una acción correctiva con responsable, fecha y estado, dentro de 10 días hábiles desde el cierre.

Severidad	Criterio	Plazo de contención
Crítica	Secuestro de información, filtración de datos restringidos o caída de un servicio crítico	4 horas
Alta	Cuenta comprometida, malware activo, pérdida de equipo con información confidencial	24 horas
Media	Malware contenido, phishing con clic sin entrega de credenciales	48 horas
Baja	Correo sospechoso reportado o amenaza bloqueada sin interacción	72 horas



Criterios y plazos son los de REP-SI-001 §3, para clasificar el incidente con el mismo rasero en los tres documentos. El registro lo administra **Administración** y se reporta al Comité cada trimestre. El reporte del período 01-10-2024 al 30-09-2025 **cerró sin eventos ni incidentes registrados**; el siguiente cubrirá del 01-10-2025 al 30-09-2026. Los delitos informáticos se denuncian a la Brigada del Cibercrimen o al Ministerio Público (Ley N° 21.459). **AGROSER no paga rescates.**

11 Terceros, capacitación y sanciones

- Las empresas de servicios y los proveedores con acceso firman **acuerdos de confidencialidad y cláusulas de seguridad**, vigentes; la evaluación anual está vigente, y los servicios en la nube y de soporte se evalúan **antes de contratarlos**.
- Nuestro personal cumple las políticas de seguridad del cliente cuyos sistemas utiliza, y los incidentes que lo afecten se le comunican dentro de los plazos de su contrato.
- **Seguridad física y documental:** acceso controlado a oficinas y archivos con información confidencial o restringida, escritorio y pantalla limpios, destrucción segura de documentos y retiro inmediato de las impresiones.

Capacitación	Dirigida a	Frecuencia	Estado al 30-09-2025
Inducción, con firma del compromiso de uso aceptable	Quien use recursos tecnológicos	Al ingreso	Vigente
Ciberseguridad, phishing, contraseñas y protección de datos	Personal administrativo, meta 100 %	Anual	Vigente
Simulación de phishing y alertas con buenas prácticas	Usuarios de correo y todo el personal	Semestral	**Comprometido** · primera simulación en marzo de 2026

El incumplimiento se sanciona según el Reglamento Interno de Orden, Higiene y Seguridad y la ley, sin perjuicio de las acciones de la **Ley N° 21.459**; en empresas de servicios y proveedores puede significar el término del contrato. Las conductas que además infrinjan el Código de Ética se tramitan por GES-DEN-001.

Compromiso de uso aceptable. Cada persona que usa recursos tecnológicos lo firma en la inducción, declarando que recibió y comprendió esta política y que se obliga a proteger la información, a no compartir sus contraseñas, a no almacenar información de la empresa en cuentas personales y a reportar de inmediato cualquier incidente. Por la empresa lo firma y lo custodia **Administración**, en la que está radicada esta responsabilidad; el formulario se mantiene como plantilla para rellenar a mano.

12 Indicadores

Los controles que miden estos indicadores **están vigentes**. La medición se consolida en el **reporte trimestral** que Administración presenta al Comité de Riesgos y Sostenibilidad, con la frecuencia que indica cada fila.

Indicador	Meta	Frecuencia
Incidentes críticos gestionados dentro de plazo, sobre los críticos del período	100 %	Trimestral

Indicador	Meta	Frecuencia
Clasificación de severidad dentro de 1 hora desde la detección, sobre los críticos	100 %	Trimestral
Servicios críticos recuperados dentro del RTO, sobre los afectados	100 %	Trimestral
Pruebas de restauración exitosas, sobre las programadas	100 %	Trimestral
Incidentes con informe de lecciones aprendidas en 10 días hábiles	100 %	Trimestral
Cuentas con doble factor, sobre las cuentas activas	100 %	Trimestral
Accesos eliminados el mismo día del término del contrato, sobre las bajas	100 %	Trimestral
Equipos con antivirus activo y actualizado, sobre el inventario	≥ 95 %	Trimestral
Revisión semestral de permisos realizada y documentada	100 %	Semestral
Usuarios que reportan la simulación de phishing, sobre los incluidos	≥ 70 %	Semestral
Personal administrativo capacitado en ciberseguridad en el año (A-25)	100 %	Anual

Mide **Administración**, salvo el informe de lecciones aprendidas, de la **Coordinación de Gestión de Riesgos**. La frecuencia es la de PLN-CIB-001 §9: el antivirus se mide **cada trimestre**, no cada mes, para que política y plan no rindan cuentas del mismo dato en fechas distintas. El alcance de la capacitación es el de A-25, **el personal administrativo**. **Si un período cierra sin incidentes, el porcentaje no existe y así se informará**, sin «0 %» ni «100 %» (GES-DEN-001 §6).

13 Vigencia, revisión y aprobación

Esta política rige desde el **30 de septiembre de 2025**, se publica en **agroserspa.cl** y se revisa al menos una vez al año. La **primera revisión vence el 30 de septiembre de 2026**: informará la verificación de controles del 31-01-2026, los RTO y RPO validados y el reporte de incidentes del período.

ACTA DE APROBACIÓN

En Baquedano 471, Nacimiento, el 30 de septiembre de 2025, la alta dirección de AGROSER, a través de su Administración y Representación Legal, aprueba esta política. Cada acuerdo lleva responsable, fecha y código de acción, y todos tratan el riesgo **RC-12**.

Acuerdo	Responsable	Fecha	Acción
Aprobar la política y publicarla en agroserspa.cl, comunicándola a trabajadores, clientes y empresas de servicios	Representante Legal	30-09-2025, cumplido	A-28
Radicar en Administración la responsabilidad de la seguridad de la información	Representante Legal	30-09-2025, cumplido	A-24
Implantar el respaldo automático verificado y el control de accesos con contraseñas personales y doble factor	Administración	30-09-2025, cumplido	A-24
Ejecutar las pruebas trimestrales de restauración, con registro del resultado	Administración	30-09-2025, cumplido	A-24
Hacer firmar el compromiso de uso aceptable y capacitar al 100 % del personal administrativo	Administración	30-09-2025, cumplido	A-25
Presentar al Comité de Riesgos y Sostenibilidad el primer reporte trimestral de seguridad de la información	Coordinador(a) de Gestión de Riesgos	31-01-2026	A-29



Sergio E. Vallejos Godoy

Representante Legal · AGROSER, RUT 76.333.148-2

Nacimiento, 30 de septiembre de 2025

Documento	Política de Seguridad de la Información y Ciberseguridad (POL-SI-001)
Versión	01, aprobada por la alta dirección a través del Representante Legal
Vigencia y revisión	Desde el 30 de septiembre de 2025; revisión anual, la primera el 30 de septiembre de 2026
Custodia	Administración, con copia controlada en la Coordinación de Gestión de Riesgos · alcance: riesgo RC-12 y sus manifestaciones RSI-01 a RSI-08
Certificaciones	Ninguna. ISO/IEC 27001, 27002 e ISO 22301 son solo marco de referencia, sin proceso en curso
Empresa	AGROSER, RUT 76.333.148-2 · Baquedano 471, Nacimiento, Región del Biobío, Chile · contacto@agroserspa.cl · +569 9501 4156 · agroserspa.cl