

Política de Seguridad y Backups

SisLab Gestión

Política de Seguridad y Backups de SisLab Gestión Medidas reforzadas para información sanitaria. Documento complementario de los Términos y Condiciones (Versión 2.0), de la Política de Privacidad y del DPA. Alineada con las recomendaciones de la **AAIP (Resolución 47/2018, Anexo I)** y con la Ley 25.326.

1. Objeto

- 1.1. Esta Política describe el marco de seguridad de la información y de gestión de respaldos del Servicio **SisLab Gestión**, su alcance, las medidas adoptadas, las limitaciones y las **responsabilidades compartidas** entre el Prestador y el Cliente.
- 1.2. Las medidas aquí descriptas son razonables y proporcionadas a la naturaleza sensible de los datos, pero **no constituyen garantía de inviolabilidad ni de disponibilidad absoluta** (Términos, Secciones 13, 18, 19 y 24).

2. Principios

El Prestador adopta un enfoque de seguridad basado en: **confidencialidad, integridad y disponibilidad**; *defensa en profundidad*; **mínimo privilegio**; *seguridad por diseño y por defecto*; mejora continua; y proporcionalidad respecto del riesgo y de la sensibilidad de los datos de salud.

3. Control de acceso

- 3.1. **Acceso por usuario individual:** cada Usuario accede con Credenciales propias; no se promueven cuentas compartidas.
- 3.2. **Roles y permisos:** el Servicio implementa control de acceso basado en roles y permisos granulares (p. ej. recepción, técnico, bioquímico validador, administración), administrados por el Cliente, de modo que cada Usuario acceda únicamente a lo necesario para su función.
- 3.3. **Autenticación:** contraseñas sujetas a requisitos de complejidad y almacenamiento mediante funciones de *hashing*. Según el Plan y la configuración, el Servicio puede ofrecer **dobles factor de autenticación (2FA)**.
- 3.4. **Gestión de sesiones:** expiración de sesiones por inactividad, cierre de sesión y, según configuración, **bloqueo de la cuenta** tras reiterados intentos fallidos de acceso.
- 3.5. **Protección de Credenciales:** las contraseñas no se almacenan en texto plano; los tokens y secretos se gestionan de forma segura. El Cliente y sus Usuarios son responsables de la custodia de sus Credenciales.

4. Cifrado

- 4.1. **En tránsito:** las comunicaciones entre el navegador del Usuario y el Servicio se cifran mediante protocolos **TLS/HTTPS**.
- 4.2. **En reposo:** según la infraestructura y el proveedor de alojamiento, los datos y/o los respaldos pueden almacenarse cifrados. El detalle técnico vigente puede solicitarse a sosporte@sislab.com.ar.

5. Registros de auditoría y trazabilidad

5.1. El Servicio mantiene **registros de auditoría** que pueden comprender, según funcionalidad y Plan: inicio y cierre de sesión, validaciones, modificaciones de datos, impresiones, firmas, cambios de Resultados y exportaciones.

5.2. Los registros permiten reconstruir las operaciones relevantes, atribuirlos a un Usuario y constituyen prueba de las acciones realizadas en el Servicio.

6. Gestión de vulnerabilidades y entorno de desarrollo

6.1. El Prestador aplica buenas prácticas de desarrollo seguro, actualización de componentes y dependencias, y separación entre los **entornos de desarrollo/prueba y de producción**.

6.2. Se procura no utilizar datos reales de Pacientes en entornos de prueba; cuando ello no sea posible, se aplican medidas de minimización o disociación.

6.3. El Prestador atiende razonablemente los reportes de vulnerabilidades. Las pruebas de seguridad por parte del Cliente o de terceros requieren autorización previa y escrita del Prestador.

7. Respaldos (backups)

7.1. **Realización:** el Prestador realiza respaldos periódicos de los datos de producción como medida de precaución.

7.2. **Frecuencia:** los respaldos se efectúan con una periodicidad razonable definida por el Prestador según la infraestructura (orientativamente, respaldos diarios), pudiendo variar por razones técnicas. La frecuencia vigente puede informarse a requerimiento.

7.3. **Conservación y rotación:** los respaldos se conservan por un período acotado y se rotan/sobrescriben según su ciclo de vida; no constituyen un archivo histórico permanente.

7.4. **Recuperación:** ante una pérdida o corrupción de datos, el Prestador realizará **esfuerzos razonables** de recuperación a partir del último respaldo disponible. **No se garantiza la recuperación total ni parcial, ni la ausencia de pérdida de datos** generados entre el último respaldo y el incidente.

7.5. **Limitaciones:** los respaldos están sujetos a límites técnicos y de almacenamiento. La recuperación puede implicar la pérdida de los datos cargados con posterioridad al respaldo restaurado.

8. Responsabilidad compartida y respaldos del Cliente

8.1. La protección de la información es una **responsabilidad compartida**.

8.2. **Responsabilidad del Cliente:** mantener **copias de respaldo propias e independientes** de su información crítica; utilizar las funciones de **exportación** del Servicio con periodicidad adecuada; gestionar correctamente Usuarios, roles y permisos; custodiar las Credenciales; mantener actualizados y protegidos sus dispositivos y redes; y aplicar buenas prácticas internas de seguridad. El cumplimiento de los plazos legales de conservación documental corresponde al Cliente (Términos, Sección 20).

8.3. **Responsabilidad del Prestador:** adoptar las medidas razonables descriptas en esta Política y realizar los respaldos en los términos aquí previstos.

9. Gestión de incidentes de seguridad

- 9.1. El Prestador cuenta con un proceso para **detectar, contener, analizar y remediar** Incidentes de Seguridad.
- 9.2. **Notificación al Cliente:** ante un Incidente que afecte Datos del Cliente, el Prestador lo notificará **sin demora indebida**, informando la naturaleza del Incidente, los datos potencialmente afectados y las medidas adoptadas, en la medida en que dicha información esté disponible.
- 9.3. **Deberes del Cliente:** la evaluación del Incidente y las eventuales **notificaciones a los Pacientes y a la AAIP** corresponden al Cliente como Responsable del Tratamiento, con la colaboración razonable del Prestador (DPA).
- 9.4. El Cliente debe informar al Prestador, sin demora, todo Incidente, sospecha de compromiso, uso indebido o pérdida de Credenciales que detecte.

10. Continuidad y disponibilidad

- 10.1. El Prestador procura la continuidad del Servicio mediante infraestructura adecuada, pero **no garantiza un uptime del 100%** ni un SLA, salvo contratación expresa (Términos, Sección 18).
- 10.2. Las interrupciones programadas de mantenimiento se anunciarán, cuando sea posible, con antelación razonable.

11. Destrucción segura de la información

- 11.1. Al finalizar el Contrato y vencidos los plazos de conservación (Términos, Sección 20; DPA), los Datos se eliminan de los entornos productivos mediante procedimientos de **borrado seguro**, sin perjuicio de las copias en respaldos cifrados que se sobrescriben según su ciclo de rotación.

12. Personal y confidencialidad

- 12.1. El personal del Prestador con acceso a los datos está sujeto a **deberes de confidencialidad** y al secreto del art. 10 de la Ley 25.326, que subsisten tras el cese de la relación.
- 12.2. El acceso del personal a datos de Pacientes se limita a lo estrictamente necesario para operar, mantener y dar soporte al Servicio.

13. Revisión de esta Política

- 13.1. El Prestador podrá actualizar esta Política para reflejar mejoras técnicas o cambios normativos, notificando los cambios sustanciales por los medios previstos en los Términos. La versión vigente estará disponible en la plataforma.

14. Contacto

- **Seguridad e incidentes:** soporte@sislab.com.ar

Esta Política integra los Términos y Condiciones (Versión 2.0) y se complementa con la Política de Privacidad y el DPA.