

SEGURIDAD OPERACIONAL 2026

Seguridad de Datos

En SurByte protegemos la información operacional de tus maquinarias, flotas y usuarios mediante controles de acceso, respaldos, monitoreo y buenas prácticas de seguridad tecnológica.

Contactar soporte

Descargar documento



Control de Acceso

Gestión de permisos por usuario, rol y responsabilidad.



Respaldos

Copias preventivas para continuidad operacional.



Monitoreo

Supervisión de actividad, accesos y comportamiento.



Aislamiento

Estructura multiempresa para separar clientes y datos.

1. Seguridad de la información

Nuestra política de seguridad se basa en la confidencialidad, integridad y disponibilidad de la información. Implementamos controles razonables para proteger los datos operacionales de cada cliente, incluyendo usuarios, maquinarias, flotas, mantenimientos, reportes, documentos y registros asociados al servicio.

2. Control de accesos y usuarios

SurByte utiliza un sistema de permisos basado en usuarios, roles y módulos. Los administradores pueden definir niveles de acceso para operadores, mantenedores, supervisores y gerencia, reduciendo la exposición innecesaria de información sensible.



Gestión responsable de credenciales

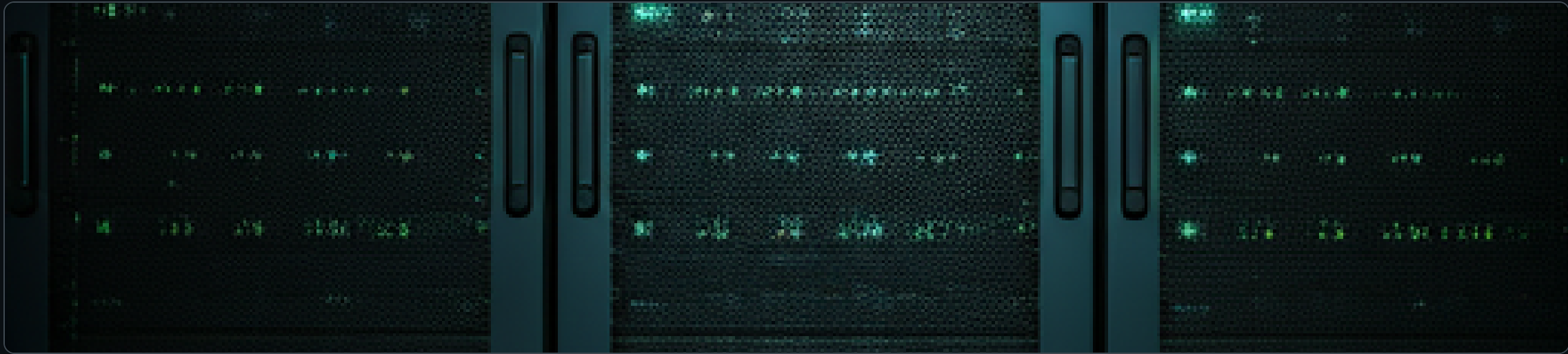
El cliente es responsable de mantener sus contraseñas seguras, administrar sus usuarios internos y solicitar la desactivación de accesos cuando corresponda.

3. Protección de datos operacionales

Los datos provenientes de GPS, telemetría, sensores, mantenimientos, costos, documentos y registros manuales se utilizan únicamente para operar la plataforma, entregar soporte, generar reportes y mejorar la continuidad del servicio. SurByte no vende ni comercializa datos de clientes.

4. Infraestructura y servidores

SurByte opera su infraestructura sobre servidores en **DigitalOcean**, aplicando medidas de seguridad como control de acceso, monitoreo, respaldos, separación lógica de clientes y buenas prácticas de administración de servidores para proteger la continuidad operacional.



5. Respaldos y recuperación

SurByte mantiene mecanismos de respaldo y recuperación orientados a disminuir riesgos de pérdida de información. Los respaldos permiten apoyar la continuidad operacional ante fallas técnicas, errores operativos o incidentes que requieran restauración de información.

6. Monitoreo y prevención

La plataforma cuenta con monitoreo técnico para revisar disponibilidad, comportamiento del servicio, accesos, errores y eventos relevantes. Estas medidas permiten detectar situaciones anómalas, aplicar acciones preventivas y mejorar la estabilidad del sistema.

7. Responsabilidad del cliente

La seguridad es una responsabilidad compartida. El cliente debe proteger sus credenciales, administrar correctamente los permisos de sus usuarios, mantener actualizada la información operativa y validar datos críticos antes de tomar decisiones relacionadas con seguridad, mantenimiento o gestión de activos.

8. Contacto de seguridad

Para reportar vulnerabilidades, solicitar revisión de accesos, consultar sobre tratamiento de datos o pedir soporte relacionado con seguridad, puedes comunicarte directamente con SurByte.



contacto@surbyte.cl



WhatsApp

Infraestructura protegida

Visualización de controles activos para continuidad operacional.



Control de Acceso

● OPERATIVO



Respaldos

● CONFIGURADOS



Monitoreo

● ACTIVO



Aislamiento Multiempresa

● APLICADO