POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA PLATAFORMA IRRICONTROL ONE

Seguridad de la Información y Ciberdefensa

1. OBJETIVO Y ALCANCE

La **Plataforma IRRICONTROL ONE**, operada por **IRRICONTROL CONTROLE INTELIGENTE DE IRRIGAÇÃO S.A.** («**IRRICONTROL**»), es una solución de alta criticidad tecnológica para la automatización y la telemetría de sistemas agrícolas a escala mundial. La presente Política de Seguridad de la Información (PSI) establece los requisitos técnicos y operativos específicos para la protección de datos en la Plataforma IRRICONTROL ONE, un servicio SaaS global de automatización y telemetría.

1.1. Ámbito de aplicación

Esta PSI se aplica íntegramente a:

- Infraestructura en la nube (AWS, Azure, Google Cloud)
- Aplicaciones web y móviles de la Plataforma
- Dispositivos IoT conectados (Nexus, SmartConnect, Irripump)
- Datos de clientes en 26 jurisdicciones

Referencia: Para las directrices corporativas generales de seguridad, concienciación, formación y sanciones, consulte la Política de Seguridad de la Información Corporativa del Grupo Bauer do Brasil.

2. DIRECTRICES GENERALES Y ALINEACIÓN CON NORMAS TÉCNICAS

Esta PSI se estructura sobre las mejores prácticas mundiales de seguridad de la información y se alinea directamente con las directrices establecidas por las normas técnicas internacionales **ABNT NBR ISO/IEC 27001** (Sistema de Gestión de Seguridad de la Información – SGSI) e **ABNT NBR ISO/IEC 27002** (Controles de Seguridad de la Información), así como con la legislación de ciberseguridad y protección de datos vigente en cada jurisdicción de operación.

3. REQUISITOS OBLIGATORIOS PARA LA CONTRATACIÓN Y ADQUISICIÓN DE SISTEMAS (TI/SI)

En consonancia con las mejores prácticas de gobierno corporativo de su grupo económico, toda adquisición, arrendamiento, desarrollo interno o contratación de sistemas, software, soluciones informáticas y aplicaciones (internos o de terceros) que vayan a integrarse con la Plataforma Irricontrol One o darle soporte deberá cumplir obligatoriamente los siguientes requisitos de seguridad:

3.1. Usuario administrador gestionado

Todo sistema contratado o desarrollado deberá prever la definición obligatoria de un usuario administrador con acceso completo y sin restricciones. Este acceso de administrador deberá ser gestionado y controlado exclusivamente por el equipo interno de TI/SI de **IRRICONTROL**, quedando prohibida la exclusividad del acceso por parte de terceros o proveedores.

3.2. Aprobación y pruebas previas

Ninguna solución informática o software podrá adquirirse, arrendarse o negociarse sin la aprobación previa, formal y por escrito del equipo técnico de TI/SI de **IRRICONTROL**. El equipo técnico realizará pruebas de vulnerabilidad, análisis de la arquitectura de red y verificación del cumplimiento de la LGPD, el RGPD y demás legislación aplicable antes de emitir un dictamen favorable.

3.3. Prueba de Concepto (PoC) o Prueba de Valor (PoV) obligatoria

Antes de cerrar cualquier contrato de adquisición o arrendamiento de nuevos sistemas o herramientas de terceros, es obligatoria la realización de una Prueba de Concepto (PoC) o Prueba de Valor (PoV) sin coste para **IRRICONTROL**. Esta fase deberá implicar activamente a los equipos técnicos de TI/SI y al área solicitante de la empresa, con el objetivo de validar:

- La viabilidad técnica de la integración con la Plataforma Irricontrol One;
- El cumplimiento de los requisitos de seguridad y cifrado de datos;
- La estabilidad y el rendimiento de la solución en un entorno de pruebas homologado.
- El cumplimiento de los requisitos de localización de datos en las jurisdicciones que los exigen.

---

4. CONTROLES TÉCNICOS Y OPERATIVOS DE SEGURIDAD

IRRICONTROL adopta controles técnicos rigurosos para mitigar el riesgo de incidentes de seguridad y fugas de datos en la Plataforma.

4.1. Control de acceso lógico

- **Autenticación multifactor (MFA)**: Obligatoria para todos los administradores de sistemas, desarrolladores y empleados con acceso a la infraestructura de servidores de la Plataforma;
- **Gestión de privilegios**: Aplicación estricta del principio de mínimo privilegio (*Need-to-Know*). Los empleados solo tienen acceso a la información necesaria para el desempeño de sus funciones;
- **Revocación de accesos**: Desactivación inmediata de las credenciales de acceso en caso de baja de empleados o de resolución de contratos con proveedores de servicios.

4.2. Cifrado y protección de datos

- **Datos en tránsito:** Toda la comunicación entre los dispositivos de campo (IoT), las aplicaciones de los Usuarios y los servidores de la Plataforma está protegida mediante cifrado con protocolos de seguridad de alto nivel (HTTPS, SSL/TLS);
- **Datos en reposo:** Los datos personales, las credenciales de acceso y la información operativa crítica almacenados en las bases de datos en la nube están protegidos mediante cifrado robusto (AES-256).

4.3. Supervisión, registros y auditoría

Este documento está controlado por el área de seguridad de la información. Se reservan todos los derechos sobre este documento. Queda prohibida su reproducción, uso o entrega a terceros sin la autorización expresa de BAUER. Las copias de este documento se considerarán «no controladas», salvo indicación en contrario, y podrán considerarse fruto de la propiedad intelectual, quedando el infractor sujeto a todas las sanciones y al peso de la legislación vigente.

- **Generación de registros:** La Plataforma registra logs detallados de todas las actividades críticas, incluidos los intentos de inicio de sesión, los cambios de privilegios, los comandos enviados a los pívots de riego y los accesos a las bases de datos;
- **Centralización y protección de registros:** Los logs se centralizan en servidores de auditoría específicos y están protegidos frente a alteraciones o eliminaciones (logs de solo escritura);
- **Análisis de vulnerabilidades:** Realización periódica de análisis de seguridad y pruebas de intrusión (pentests) en la infraestructura de la Plataforma para identificar y corregir vulnerabilidades de forma proactiva.

---

5. INFRAESTRUCTURA EN LA NUBE Y COPIAS DE SEGURIDAD

La infraestructura de la Plataforma Irricontrol One está alojada en proveedores de servicios en la nube de nivel internacional (como AWS, Azure o Google Cloud), que ofrecen una alta resiliencia y el cumplimiento de normas mundiales de seguridad (como SOC 2 e ISO 27001).

5.1. Política de copias de seguridad y recuperación ante desastres

- **Periodicidad**: Realización de copias de seguridad (backups) periódicas y automatizadas de todas las bases de datos de operación y registro de la Plataforma;
- **Almacenamiento seguro**: Las copias de seguridad se cifran y se almacenan en zonas geográficas distintas (redundancia geográfica) para garantizar la continuidad del negocio en caso de catástrofes naturales o fallos críticos de infraestructura;
- **Pruebas de restauración**: Realización de pruebas semestrales de restauración de copias de seguridad para garantizar la eficacia y rapidez del plan de recuperación ante desastres (DRP).

---

6. GESTIÓN DE INCIDENTES DE SEGURIDAD Y RESPUESTA A FUGAS DE DATOS

De conformidad con la LGPD y las normas ISO 27035, **IRRICONTROL** mantiene un plan estructurado de respuesta a incidentes de ciberseguridad.

6.1. Flujo de respuesta a incidentes

1. **Identificación y contención**: Ante cualquier sospecha o confirmación de incidente (como una intrusión, una fuga de datos o una indisponibilidad crítica), el equipo técnico de TI/SI aislará inmediatamente los sistemas afectados para contener la amenaza;
2. **Análisis y diagnóstico**: Investigación forense digital detallada para identificar el origen del fallo, el alcance de los datos afectados y las medidas correctivas necesarias;
3. **Notificación de incidentes**:
    - **Comunicación urgente al Cliente: IRRICONTROL** notificará al Cliente de forma urgente e inmediata cualquier incidente o sospecha de incidente que afecte a datos personales bajo su responsabilidad;
    - **Comunicación a las autoridades:** Si el incidente supone un riesgo o daño relevante para los interesados, IRRICONTROL ayudará al Responsable (Cliente) a notificar a la Autoridad

Este documento está controlado por el área de seguridad de la información. Se reservan todos los derechos sobre este documento. Queda prohibida su reproducción, uso o entrega a terceros sin la autorización expresa de BAUER. Las copias de este documento se considerarán «no controladas», salvo indicación en contrario, y podrán considerarse fruto de la propiedad intelectual, quedando el infractor sujeto a todas las sanciones y al peso de la legislación vigente.

Nacional de Protección de Datos (ANPD) de Brasil, a las autoridades de protección de datos equivalentes de otros países (como la CNIL en Francia o la ICO en el Reino Unido) y a los interesados afectados dentro del plazo legal reglamentario (72 horas conforme al RGPD y 15 días hábiles en Brasil, según corresponda).

7. CONCIENCIACIÓN Y FORMACIÓN

La seguridad de la información depende del comportamiento humano. **IRRICONTROL** imparte formaciones semestrales obligatorias de concienciación en seguridad de la información, privacidad y LGPD a todos sus empleados y proveedores de servicios.

8. SANCIONES Y PENALIZACIONES

El incumplimiento de las directrices y normas establecidas en esta PSI por parte de empleados o proveedores de servicios de **IRRICONTROL** constituirá falta grave y someterá al infractor a las medidas disciplinarias que correspondan (amonestación, suspensión, despido disciplinario), además de las sanciones civiles y penales aplicables conforme a la legislación brasileña y a la de las jurisdicciones en las que opera la Plataforma.

Este documento está controlado por el área de seguridad de la información. Se reservan todos los derechos sobre este documento. Queda prohibida su reproducción, uso o entrega a terceros sin la autorización expresa de BAUER. Las copias de este documento se considerarán «no controladas», salvo indicación en contrario, y podrán considerarse fruto de la propiedad intelectual, quedando el infractor sujeto a todas las sanciones y al peso de la legislación vigente.