# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA PLATAFORMA IRRICONTROL ONE

**Segurança da Informação e Defesa Cibernética**

## 1. OBJETIVO E ESCOPO

A **Plataforma IRRICONTROL ONE**, operada pela **IRRICONTROL CONTROLE INTELIGENTE DE IRRIGAÇÃO S.A.** ("**IRRICONTROL**"), é uma solução de alta criticidade tecnológica para a automação e telemetria de sistemas agrícolas em escala global. Esta Política de Segurança da Informação (PSI) estabelece os requisitos técnicos e operacionais específicos para a proteção de dados na Plataforma IRRICONTROL ONE, um serviço SaaS global de automação e telemetria.

### 1.1. Escopo de Aplicação

Esta PSI aplica-se integralmente a:

- Infraestrutura em nuvem (AWS, Azure, Google Cloud)
- Aplicações web e móveis da Plataforma
- Dispositivos IoT conectados (Nexus, SmartConnect, Irripump)
- Dados de clientes em 26 jurisdições

**Referência**: Para diretrizes corporativas genéricas de segurança, conscientização, treinamento e sanções, consulte a Política de Segurança da Informação Corporativa do Grupo Bauer do Brasil.

## 2. DIRETRIZES GERAIS E ALINHAMENTO COM NORMAS TÉCNICAS

Esta PSI é estruturada com base nas melhores práticas globais de segurança da informação, alinhando-se diretamente às diretrizes estabelecidas pelas normas técnicas internacionais **ABNT NBR ISO/IEC 27001** (Sistema de Gestão de Segurança da Informação - SGSI) e **ABNT NBR ISO/IEC 27002** (Controles de Segurança da Informação), bem como às legislações de cibersegurança e proteção de dados vigentes em cada jurisdição de operação.

## 3. REQUISITOS OBRIGATÓRIOS PARA CONTRATAÇÃO E AQUISIÇÃO DE SISTEMAS (TI/SI)

Em consonância com as melhores práticas de governança corporativa oriunda de seu grupo econômico, qualquer aquisição, locação, desenvolvimento interno ou contratação de sistemas, softwares, soluções computacionais e aplicativos (sejam internos ou de terceiros) que venham a se integrar ou dar suporte à Plataforma Irricontrol One deve, obrigatoriamente, cumprir os seguintes requisitos de segurança:

### 3.1. Usuário Administrador Gerenciado

Qualquer sistema contratado ou desenvolvido deve prever a definição obrigatória de um usuário administrador com acesso completo e irrestrito. Este acesso administrador deve ser gerenciado e controlado exclusivamente pela equipe interna de TI/SI da **IRRICONTROL**, sendo vedada a exclusividade de acesso por parte de terceiros ou fornecedores.

### 3.2. Aprovação e Testes Prévios

Nenhuma solução computacional ou software pode ser adquirido, locado ou negociado sem a aprovação prévia, formal e por escrito da equipe técnica de TI/SI da **IRRICONTROL**. A equipe técnica realizará testes de vulnerabilidade, análise de arquitetura de rede e verificação de conformidade com a LGPD, GDPR e demais legislações aplicáveis antes de emitir o parecer favorável.

### 3.3. Prova de Conceito (PoC) ou Prova de Valor (PoV) Obrigatória

Antes do fechamento de qualquer contrato de aquisição ou locação de novos sistemas ou ferramentas de terceiros, é obrigatória a realização de uma Prova de Conceito (PoC) ou Prova de Valor (PoV) sem custos para a **IRRICONTROL**. Esta etapa deve envolver ativamente as equipes técnicas de TI/SI e a área demandante da empresa, com o objetivo de validar:

- A viabilidade técnica de integração com a Plataforma Irricontrol One;
- O cumprimento de requisitos de segurança e criptografia de dados;
- A estabilidade e desempenho da solução em ambiente de testes homologado.
- A conformidade com requisitos de localização de dados em jurisdições que os exigem.

## 4. CONTROLES TÉCNICOS E OPERACIONAIS DE SEGURANÇA

A IRRICONTROL adota controles técnicos rigorosos para mitigar riscos de incidentes de segurança e vazamento de dados na Plataforma.

### 4.1. Controle de Acesso Lógico

- **Autenticação Multifator (MFA)**: Obrigatória para todos os administradores de sistema, desenvolvedores e colaboradores com acesso à infraestrutura de servidores da Plataforma;
- **Gestão de Privilégios**: Aplicação estrita do princípio do menor privilégio (*Need-to-Know*). Colaboradores têm acesso apenas às informações necessárias para o desempenho de suas funções;
- **Revogação de Acessos**: Desativação imediata de credenciais de acesso em caso de desligamento de colaboradores ou rescisão de contratos com prestadores de serviço.

### 4.2. Criptografia e Proteção de Dados

- **Dados em Trânsito:** Toda a comunicação entre os dispositivos de campo (IoT), os aplicativos dos Usuários e os servidores da Plataforma é protegida por criptografia utilizando protocolos de segurança de alto padrão (HTTPS, SSL/TLS);
- **Dados em Repouso:** Os dados pessoais, credenciais de acesso e informações críticas de operação armazenados nos bancos de dados em nuvem são protegidos por criptografia forte (AES-256).

### 4.3. Monitoramento, Logs e Auditoria



**Este documento é controlado pelo setor de segurança da informação. É reservado todos os direitos sobre este documento. A reprodução, uso ou entrega a terceiros sem autorização expressa da BAUER é proibida. Cópias deste documento serão consideradas "não controladas", salvo indicação contrária e poderão ser consideradas fruto de propriedade intelectual e o infrator sofrer todas as sanções e peso da legislação vigente.**

- **Geração de Logs:** A Plataforma registra logs detalhados de todas as atividades críticas, incluindo tentativas de login, alterações de privilégios, comandos enviados aos pivôs de irrigação e acessos a bancos de dados;
- **Centralização e Proteção de Logs:** Logs são centralizados em servidores específicos de auditoria e protegidos contra alterações ou exclusões (logs somente de gravação);
- **Análise de Vulnerabilidades:** Realização periódica de varreduras de segurança e testes de invasão (Pentests) na infraestrutura da Plataforma para identificar e corrigir vulnerabilidades de forma proativa.

## 5. INFRAESTRUTURA EM NUVEM E BACKUPS

A infraestrutura da Plataforma Irricontrol One é hospedada em provedores de nuvem de padrão internacional (como AWS, Azure ou Google Cloud), que oferecem alta resiliência e conformidade com normas globais de segurança (como SOC 2, ISO 27001).

### 5.1. Política de Backup e Recuperação de Desastres

- **Periodicidade**: Realização de cópias de segurança (backups) periódicas e automatizadas de todos os bancos de dados de operação e cadastro da Plataforma;
- **Armazenamento Seguro**: Backups são criptografados e armazenados em zonas geográficas distintas (redundância geográfica) para garantir a continuidade dos negócios em caso de desastres naturais ou falhas críticas de infraestrutura;
- **Testes de Restauração**: Realização de testes semestrais de restauração de backups para garantir a eficácia e rapidez do plano de recuperação de desastres (DRP).

## 6. GESTÃO DE INCIDENTES DE SEGURANÇA E RESPOSTA A VAZAMENTOS

Em conformidade com a LGPD e as normas ISO 27035, a **IRRICONTROL** mantém um plano estruturado de resposta a incidentes de segurança cibernética.

### 6.1. Fluxo de Resposta a Incidentes

1. **Identificação e Contenção**: Diante de qualquer suspeita ou confirmação de incidente (como invasão, vazamento de dados ou indisponibilidade crítica), a equipe técnica de TI/SI isolará imediatamente os sistemas afetados para conter a ameaça;
2. **Análise e Diagnóstico**: Investigação forense digital detalhada para identificar a origem da falha, a extensão dos dados afetados e as medidas de correção necessárias;
3. **Notificação de Incidentes**:
    - **Comunicação Urgente ao Cliente:** A **IRRICONTROL** notificará o Cliente de forma urgente e imediata sobre qualquer incidente ou suspeita de incidente envolvendo dados pessoais sob sua responsabilidade;
    - **Comunicação às Autoridades:** Se o incidente representar risco ou dano relevante aos titulares de dados, a IRRICONTROL auxiliará o Controlador (Cliente) a notificar a Agência



**Este documento é controlado pelo setor de segurança da informação. É reservado todos os direitos sobre este documento. A reprodução, uso ou entrega a terceiros sem autorização expressa da BAUER é proibida. Cópias deste documento serão consideradas "não controladas", salvo indicação contrária e poderão ser consideradas fruto de propriedade intelectual e o infrator sofrer todas as sanções e peso da legislação vigente.**

Nacional de Proteção de Dados (ANPD) no Brasil, as autoridades de proteção de dados equivalentes em outros países (como a CNIL na França ou a ICO no Reino Unido), e os titulares afetados no prazo legal regulamentar (72 horas no GDPR, 15 dias úteis no Brasil, conforme aplicável).

## 7. CONSCIENTIZAÇÃO E TREINAMENTO

A segurança da informação depende do comportamento humano. A **IRRICONTROL** realiza treinamentos semestrais obrigatórios de conscientização em segurança da informação, privacidade e LGPD para todos os seus colaboradores e prestadores de serviço.

## 8. SANÇÕES E PENALIDADES

O descumprimento das diretrizes e normas estabelecidas nesta PSI por parte de colaboradores ou prestadores de serviço da **IRRICONTROL** constituirá falta grave, sujeitando o infrator às medidas disciplinares cabíveis (advertência, suspensão, demissão por justa causa), além das sanções civis e criminais aplicáveis nos termos da legislação brasileira e das jurisdições onde a Plataforma opera.



**Este documento é controlado pelo setor de segurança da informação. É reservado todos os direitos sobre este documento. A reprodução, uso ou entrega a terceiros sem autorização expressa da BAUER é proibida. Cópias deste documento serão consideradas "não controladas", salvo indicação contrária e poderão ser consideradas fruto de propriedade intelectual e o infrator sofrer todas as sanções e peso da legislação vigente.**