**1. Melhorias na Gestão de Acesso e Autenticação (Confidencialidade e Autenticidade):**

- **Implementação de Autenticação Multifator (MFA):** Para proteger o acesso de usuários autorizados (que atualizam dados críticos como `qtd_galinhas`), a MFA adicionaria uma camada de segurança robusta contra credenciais comprometidas.
- **Princípio do Mínimo Privilégio:** Refinar as restrições de acesso (atualmente genéricas como "usuários autorizados"). Detalhar quais papéis (ex: Gerente de Produção, Veterinário) têm permissão de escrita para cada dado crítico e quais têm apenas leitura.
- **Rotação e Complexidade de Senhas:** Detalhar a política de senhas (ex: complexidade mínima, rotação periódica forçada).

**2. Melhorias na Integridade e Trava de Segurança:**

- **Validação de Dados Biométricos Adicionais:** A Trava de Segurança (CT-07) se limita ao peso médio (`peso_medio < 5.0kg`). Seria útil implementar validações semelhantes para outros *inputs* críticos, como, por exemplo, limites razoáveis para `qtd_galinhas` (evitar erros de digitação de magnitude) ou limites biológicos para temperatura e umidade.
- **Integridade na Transmissão de Dados:** O documento foca na integridade do *input*. Para ambientes IoT, é crucial garantir a integridade dos dados durante a transmissão do hardware (sensores) para o software (Módulo de Gestão). Sugerir o uso de protocolos seguros (ex: TLS/SSL) e mecanismos de *checksum*.

**3. Melhorias na Disponibilidade e Resposta a Falhas:**

- **Redundância de Hardware:** Além do monitoramento (`status_sensor`), planejar a redundância para sensores críticos (ex: luminosidade, temperatura), garantindo que, em caso de falha de um, o sistema possa alternar automaticamente para um sensor de *backup*.
- **Plano de Continuidade de Negócios (BCP) e Recuperação de Desastres (DRP):** O sistema emite um Alerta de Falha. A melhoria seria detalhar o plano de ação (acionamento de equipes, procedimentos manuais de emergência) em caso de falhas críticas de hardware ou do próprio sistema de controle.

**4. Melhorias no Não Repúdio e Auditoria (Logs):**

- **Logs Detalhados de Acesso e Configuração:** Embora haja `log_racao_diaria`, seria benéfico expandir a auditoria para registrar *todas* as ações críticas de gestão: logins, tentativas de acesso negado, e *qualquer* alteração em configurações (ex: mudança nos horários de iluminação ou nas fórmulas de ração).
- **Proteção do Ambiente de Logs:** Garantir que os logs imutáveis (`log_racao_diaria`) sejam armazenados em um local seguro e segregado para evitar manipulação por um atacante que comprometa o sistema principal.

**5. Melhorias na Governança e Documentação:**

- **Matriz de Responsabilidade:** Criar uma matriz clara que defina quem é o proprietário (o responsável final) por cada dado crítico (ex: *qtd_galinhas*, *peso_medio*) e por cada Módulo do sistema.
- **Revisões Periódicas de Segurança:** Instituir um processo formal para revisões regulares (ex: anuais) das medidas de segurança e dos riscos operacionais.

**6. Identificação de Riscos (Conforme Ponto 6 da Diretriz)**
A tabela abaixo lista os riscos operacionais inerentes ao manejo manual e os riscos que o sistema monitora e mitiga, conforme o Ponto 6 da Diretriz (Identificar riscos).

## Tabela 1 — Riscos Identificados e Controles

| Categoria do Risco | Descrição do Risco | Mitigação (Controle) |
|---|---|---|
| Financeiro / Operacional | Inconsistência na operação humana (ligar/desligar luzes e liberar ração). | Automação via Módulo de Iluminação e Módulo de Nutrição. |
| Nutricional / Financeiro | Dosagem incorreta de ração, gerando desperdício financeiro e queda de produtividade. | O sistema calcula automaticamente a quantidade exata de ração, eliminando desperdícios. |
| Integridade de Dados (Input) | Entrada incorreta de dados biométricos (peso médio), comprometendo o cálculo de ração. | Trava de Segurança (CT-07) que bloqueia valores acima do limite biológico seguro (máx. 5,0 kg). |
| Disponibilidade (Hardware) | Falha no sensor de luminosidade ou outro hardware crítico. | Monitoramento em tempo real do *status_sensor*. |
| Acesso Indevido | Alteração indevida de dados críticos, como o número total de aves vivas. | Restrição de acesso: o dado **qtd_galinhas** só pode ser atualizado por usuários autorizados. |

## 2. Medidas de Segurança e Controles Implementados

O sistema adota mecanismos de segurança, rastreabilidade e governança, conforme as diretrizes do Ponto 6 (Propor medidas de segurança).

### Tabela 2 — Controles Implementados

| Medida de Controle | Módulo/Dado Envolvido | Detalhamento no Relatório |
|---|---|---|
| Registro de Logs (Auditoria) | Módulo de Gestão e Auditoria / **log_racao_diaria** | Geração de logs imutáveis e relatórios de consumo. O dado **log_racao_diaria** é imutável (read-only após gravação). |
| Política de Acesso | **qtd_galinhas** | Atualização permitida somente a usuários autorizados. |
| Trava de Segurança | **peso_medio** | O teste CT-07 valida o bloqueio automático de valores acima do limite biológico seguro. |
| Monitoramento e Alerta | **status_sensor** | O sistema emite alerta de falha em tempo real (< 2s), monitorando a saúde do hardware. |