Plano de Respostas aos Riscos

Projeto: Controlap

Data: 12/09/2025

Versão: 1.0.0

1. Introdução

Este documento detalha as estratégias e ações específicas planejadas para responder aos riscos identificados no projeto Controlap. O objetivo principal é implementar estratégias que possam aumentar as oportunidades (riscos positivos) e reduzir ou eliminar as ameaças (riscos negativos) que podem impactar o sucesso do projeto. A equipe de gerenciamento de riscos deve usar este plano e atualizá-lo continuamente conforme o progresso do projeto.

O gerenciamento de riscos é uma atividade dinâmica, e as respostas podem ser ajustadas conforme os riscos se materializam ou novas informações se tornam disponíveis. A eficácia de cada estratégia será monitorada constantemente, e o plano de resposta será ajustado conforme necessário para garantir a redução dos impactos negativos e o aproveitamento de oportunidades.

2. Tabela de Respostas aos Riscos

Esta tabela serve como o núcleo do plano de respostas aos riscos, detalhando as estratégias e as ações específicas para cada risco identificado no projeto.

ID do Risco	Descrição do Risco	Nível do Risco (Prioridade)	Estratégia de Resposta	Ações Específicas Planejadas	Responsável pela Ação	Prazo para Implementação	Status
TEC-001	Falha nos sensores de IoT, resultando em perda de controle de luzes, temperatura e estoque na loja.	**Extremo**	**Mitigar**	1. Realizar testes regulares de funcionalidade dos sensores. 2. Implementar redundância no sistema de sensores. 3. Garantir manutenção preventiva semestral.	Gerente de Projeto	20/10/2025	Não Iniciado
TEC-002	Interrupção na conectividade entre dispositivos IoT e sistema central	**Alto**	**Mitigar**	1. Verificar qualidade da conexão de internet na loja.	Líder Técnico	31/10/2025	Não Iniciado

ID do Risco	Descrição do Risco	Nível do Risco (Prioridade)	Estratégia de Resposta	Ações Específicas Planejadas	Responsável pela Ação	Prazo para Implementação	Status
	devido a falhas na rede de internet da loja. pode deixar o projeto			2. Implementar um sistema de backup de conexão (ex: rede móvel). 3. Realizar testes de conectividade regulares.			
TEC-003	Vazamento de dados sensíveis dos clientes através dos dispositivos IoT ou da infraestrutura de rede.	**Alto**	**Mitigar**	1. Implementar criptografia nos dados trocados entre sensores e o sistema central. 2. Realizar auditorias de segurança regularmente. 3. Treinar a equipe sobre boas práticas de segurança.	Arquiteto de Software	31/11/2025	Não Iniciado

ID do Risco	Descrição do Risco	Nível do Risco (Prioridade)	Estratégia de Resposta	Ações Específicas Planejadas	Responsável pela Ação	Prazo para Implementação	Status
GER-001	Atraso na entrega de componentes de hardware IoT (sensores, controladores de ar-condicionado, etc.) pelos fornecedores.	**Médio**	**Transferir**	1. Incluir cláusulas contratuais com prazos de entrega rigorosos. 2. Estabelecer contratos com fornecedores alternativos. 3. Garantir penalidades por atrasos.	Gerente de Infra	30/09/2025	Não Iniciado
GER-002	Falhas na integração entre o sistema IoT e o software de gerenciamento da loja (ex: PDV, controle de estoque).	**Alto**	**Mitigar**	1. Realizar testes de integração contínuos. 2. Criar planos de contingência para falhas temporárias de integração. 3. Documentar fluxos de dados e processos de integração.	Gerente de Projeto	Contínuo	Não Iniciado
EXT-001	Interrupções no fornecimento de energia elétrica, que afetam o funcionamento dos	**Médio**	**Mitigar**	1. Implementar sistemas de backup de energia (geradores ou UPS).	Líder Técnico	31/09/2025	Não Iniciado

ID do Risco	Descrição do Risco	Nível do Risco (Prioridade)	Estratégia de Resposta	Ações Específicas Planejadas	Responsável pela Ação	Prazo para Implementação	Status
	dispositivos IoT e da infraestrutura da loja.			2. Verificar com o fornecedor de energia as condições de estabilidade do fornecimento.			
GER-003	Falhas operacionais devido à falta de treinamento adequado da equipe da loja para utilizar o sistema IoT corretamente.	**Alto**	**Mitigar**	1. Criar um programa de treinamento contínuo para os funcionários. 2. Desenvolver materiais de apoio (manuais, vídeos). 3. Realizar testes de usabilidade do sistema com a equipe.	Gerente de RH	31/10/2025	Não iniciado
OPP-001	Aumento da eficiência operacional da loja, gerando uma redução significativa nos custos de energia e estoque.	**Alto**	**Explorar**	1. Analisar métricas de eficiência de energia e estoque. 2. Desenvolver um dashboard para monitoramento em tempo real de consumo e reposição.	Gerente de Operações	Contínuo	Não Iniciado

ID do Risco	Descrição do Risco	Nível do Risco (Prioridade)	Estratégia de Resposta	Ações Específicas Planejadas	Responsável pela Ação	Prazo para Implementação	Status
				3. Reforçar a comunicação com as franquias sobre as melhorias.			
OPP-002	Melhoria na experiência do cliente com o controle inteligente de temperatura e iluminação, aumentando o tempo de permanência na loja.	**Médio**	**Melhorar**	1. Realizar pesquisa com clientes sobre conforto na loja. 2. Ajustar a configuração dos dispositivos IoT para otimizar a experiência. 3. Monitorar indicadores de satisfação dos clientes.	Gerente de Marketing	20/10/2025	Não Iniciado
EXT-003	Falhas em fornecedores terceirizados de tecnologia ou serviços de rede, impactando a estabilidade do sistema IoT.	**Muito Alto**	**Transferir**	1. Rever os contratos com fornecedores, incluindo acordos de nível de serviço (SLAs). 2. Definir fornecedores alternativos com processos de contingência.	Gerente de TI	10/10/2025	Não Iniciado

3. Detalhamento das Estratégias de Resposta

3.1. Estratégias para Ameaças (Riscos Negativos)

- **Prevenir (Evitar):** Consiste em modificar o plano do projeto para eliminar completamente o risco identificado, evitando que ele aconteça. Essa abordagem é aplicada quando o risco apresenta grande potencial de impacto negativo e existe uma alternativa viável para o caminho original.
    - *Exemplo:* Substituir uma tecnologia experimental por uma solução já consolidada e familiar para a equipe.
- **Transferir:** Esta estratégia envolve delegar a responsabilidade da gestão do risco a uma terceira parte, como fornecedores, parceiros ou seguradoras. Embora o risco não desapareça, o impacto negativo é deslocado para outra entidade que possua maior capacidade de gerenciamento.
    - *Exemplo:* Contratar uma empresa especializada para a manutenção do sistema IoT ou adquirir seguro contra falhas tecnológicas.
- **Mitigar:** Objetiva reduzir a probabilidade de ocorrência do risco ou minimizar seu impacto, através da implementação de medidas preventivas e corretivas. Essa é a estratégia mais utilizada, pois torna os riscos mais controláveis e menos críticos.
    - *Exemplo:* Realizar testes adicionais nos sensores para detectar falhas antecipadamente e implementar redundância nos dispositivos.
- **Aceitar:** Quando o risco for pequeno, inevitável ou o custo de mitigação for superior ao benefício, opta-se por aceitar o risco. A aceitação pode ser:.
    - **Aceitação Ativa:** Alocar recursos ou reservas específicas para lidar com o risco caso ele ocorra.
    - **Aceitação Passiva:** Não realizar ações preventivas, assumindo as consequências caso o risco se materialize.
        - *Exemplo:* Considerar pequenas variações no custo de componentes como aceitáveis e reservar tempo extra no cronograma para eventuais atrasos.

3.2. Estratégias para Oportunidades (Riscos Positivos)

- **Explorar:** A estratégia consiste em garantir que a oportunidade seja plenamente realizada, dedicando esforços para que ela aconteça e gere valor máximo para o projeto.

    - *Exemplo:* Destinar os melhores recursos e talentos para concluir uma etapa antes do prazo, ampliando a eficiência.
- **Melhorar (ou Realçar):** Tem como objetivo aumentar a probabilidade de ocorrência da oportunidade ou maximizar seus impactos positivos.
    - *Exemplo:* Investir em treinamentos para a equipe usar uma nova ferramenta que pode acelerar processos.
- **Compartilhar:** Consiste em transferir a responsabilidade de aproveitar a oportunidade para um terceiro com mais capacidade ou expertise, formando parcerias estratégicas para potencializar resultados.
    - *Exemplo:* Firmar acordo com fornecedor especializado para explorar uma nova tecnologia integrada ao sistema IoT.
- **Aceitar:** A equipe decide não tomar ações ativas para provocar ou aumentar a chance da oportunidade, mas permanece vigilante para aproveitar os benefícios caso ela ocorra.
    - *Exemplo:* Aproveitar descontos pontuais de fornecedores, sem esforço extra para garanti-los.

4. Monitoramento e Revisão

O plano de respostas será revisado de forma sistemática a cada quinze dias, durante as reuniões regulares de acompanhamento do projeto. Nesta ocasião, serão avaliados o progresso das ações implementadas, o status dos riscos e a identificação de novos riscos emergentes.

O campo "Status" será atualizado continuamente, indicando o andamento das ações, com as categorias: *Não Iniciado*, *Em Andamento*, *Concluído* ou *Cancelado*.

Além disso, a revisão periódica permitirá que riscos previamente identificados sejam reavaliados conforme o projeto evolui, ajustando as estratégias conforme necessário. Esse processo garante que o gerenciamento de riscos seja dinâmico, adaptativo e alinhado às necessidades do projeto, promovendo maior segurança e probabilidade de sucesso.