

## MANUAL INTERNO DE GESTÃO DE RISCOS

### *Programa de Gestão de Riscos (PGR)*

---

#### 1. INTRODUÇÃO

O presente Manual Interno de Gestão de Riscos estabelece as diretrizes e procedimentos para a identificação, avaliação, tratamento, monitoramento e comunicação de riscos na **R3S Soluções Tecnológicas**. Este programa visa proteger os ativos da empresa, garantir a continuidade das operações e salvaguardar a reputação, em conformidade com as melhores práticas de mercado e os requisitos regulatórios aplicáveis. A gestão de riscos é um pilar fundamental para a sustentabilidade e o sucesso da organização, integrando-se aos nossos sistemas de gestão certificados.

##### 1.1 Objetivo

O principal objetivo deste Programa de Gestão de Riscos (PGR) é assegurar a continuidade das operações críticas da **R3S Soluções Tecnológicas**, minimizando a probabilidade e o impacto de eventos adversos. Busca-se a redução de impactos negativos, a rápida recuperação de incidentes e a proteção dos ativos tangíveis e intangíveis da empresa. Este programa está alinhado com os princípios da **ISO 9001** (Gestão da Qualidade), **ISO 14001** (Gestão Ambiental) e **ISO 45001** (Saúde e Segurança Ocupacional), certificações obtidas em **28/10/2025**, cujos trâmites foram iniciados em abril de 2025. Adicionalmente, o PGR suporta a fase final de implantação da **ISO 27001** (Segurança da Informação) e a conformidade com a **Lei Geral de Proteção de Dados (LGPD)**, garantindo a resiliência e a segurança da informação.

##### 1.2 Escopo

O escopo deste Manual de Gestão de Riscos abrange todas as operações críticas da **R3S Soluções Tecnológicas**, incluindo, mas não se limitando a: infraestrutura de Tecnologia da Informação (TI), sistemas de controle de acesso físico e lógico, processos de suporte ao cliente, desenvolvimento e manutenção de software, e a entrega de todos os serviços essenciais que sustentam o negócio. Inclui a análise de riscos relacionados à segurança da informação, continuidade de negócios, conformidade regulatória e impactos operacionais em todas as áreas da empresa.

## 2. ESTRUTURA DO PROGRAMA DE GESTÃO DE RISCOS (PGR)

A estrutura do Programa de Gestão de Riscos da **R3S Soluções Tecnológicas** é composta por componentes interligados que garantem uma abordagem sistemática e proativa na gestão de incertezas. Cada elemento é projetado para identificar, analisar e responder eficazmente aos riscos que podem afetar os objetivos da organização.

### 2.1 Análise de Impacto no Negócio (BIA)

A Análise de Impacto no Negócio (BIA) é um processo fundamental para identificar e priorizar os processos críticos da empresa. Através da BIA, são avaliados os impactos financeiros, operacionais, reputacionais e legais de uma interrupção, determinando os Tempos Máximos de Interrupção Aceitáveis (RTO) e os Pontos de Recuperação Objetivos (RPO). Esta análise é crucial para direcionar os investimentos em mitigação e recuperação, alinhando-se aos requisitos da **ISO 27001** no que tange à continuidade dos negócios e à proteção de informações críticas.

### 2.2 Avaliação de Riscos

A avaliação de riscos envolve a identificação sistemática, análise e priorização de riscos potenciais. São considerados riscos de TI (falhas de hardware/software), riscos cibernéticos (ataques, vazamentos de dados), riscos operacionais (erros humanos, falhas de processo), riscos ambientais (desastres naturais, conformidade com **ISO 14001**), riscos ocupacionais (segurança dos colaboradores, conformidade com **ISO 45001**) e riscos relacionados à proteção de dados (conformidade com **LGPD** e **ISO 27001**). A avaliação considera a probabilidade de ocorrência e o impacto potencial de cada risco, utilizando uma matriz de risco padronizada.

### 2.3 Estratégias de Mitigação

As estratégias de mitigação são desenvolvidas para reduzir a probabilidade de ocorrência ou o impacto dos riscos identificados. Incluem a implementação de controles preventivos (segurança de rede, políticas de acesso), redundâncias (sistemas de backup, infraestrutura duplicada), e mecanismos de monitoramento contínuo (sistemas de alerta, auditorias internas). Estas estratégias são integradas aos nossos sistemas de gestão, garantindo que as ações de mitigação estejam em conformidade com os padrões da **ISO 9001** para qualidade e **ISO 27001** para segurança da informação.

### 2.4 Plano de Resposta a Riscos

O Plano de Resposta a Riscos detalha os procedimentos a serem seguidos em caso de materialização de um risco. Inclui a definição de equipes de resposta, protocolos de comunicação interna e externa, procedimentos de escalonamento e as ações imediatas para conter o incidente e minimizar seus efeitos. Este plano é testado regularmente para garantir sua

eficácia e a prontidão das equipes, sendo um componente vital para a continuidade dos negócios e a conformidade com a **ISO 27001**.

#### 2.5 Treinamento e Testes

A **R3S Soluções Tecnológicas** investe em treinamentos anuais obrigatórios para todos os colaboradores sobre gestão de riscos, segurança da informação e conformidade com as ISOs e LGPD. São realizadas simulações de cenários de risco (ex: ataques cibernéticos, falhas de sistema) e testes regulares dos controles de segurança e dos planos de resposta. Estes treinamentos e testes são essenciais para manter a equipe preparada e para validar a eficácia das estratégias de mitigação e resposta, conforme exigido pela **ISO 9001** e **ISO 27001**.

#### 2.6 Revisão e Atualização

O Programa de Gestão de Riscos é revisado e atualizado anualmente, ou sempre que houver mudanças significativas no ambiente de negócios, tecnologia ou regulamentação. Além disso, uma revisão pós-incidente é realizada para incorporar as lições aprendidas e aprimorar os planos e procedimentos. Este ciclo de melhoria contínua é um requisito fundamental da **ISO 9001** e **ISO 27001**, garantindo que o PGR permaneça relevante e eficaz.

### 3. PLANO DE GESTÃO DE RISCOS

O Plano de Gestão de Riscos detalha as atividades operacionais para a execução do Programa de Gestão de Riscos, estabelecendo as responsabilidades, procedimentos e ferramentas utilizadas para gerenciar os riscos de forma contínua e integrada.

#### 3.1 Objetivo

O objetivo do Plano de Gestão de Riscos é identificar proativamente, avaliar de forma consistente e tratar eficazmente os riscos que podem impactar os objetivos estratégicos e operacionais da **R3S Soluções Tecnológicas**, garantindo a conformidade com as políticas internas e os padrões das certificações **ISO**.

#### 3.2 Escopo

O escopo do Plano de Gestão de Riscos abrange todos os sistemas de TI, infraestrutura de rede, controle de acesso físico e lógico, processos de suporte, desenvolvimento de software e a infraestrutura física da **R3S Soluções Tecnológicas**, bem como a interação com fornecedores e parceiros que possam introduzir riscos relevantes.

#### 3.3 Papéis e Responsabilidades

- **Gerente de Riscos:** Responsável pela coordenação geral do PGR, pela metodologia e pela comunicação com a alta direção.

- **Equipe de TI:** Responsável pela identificação e tratamento de riscos tecnológicos e cibernéticos, e pela implementação de controles de segurança da informação (**ISO 27001**).
- **Equipe de Suporte ao Cliente:** Responsável pela identificação de riscos relacionados à satisfação do cliente e à qualidade do serviço (**ISO 9001**).
- **Comitê de Governança:** Responsável pela supervisão estratégica do PGR e pela aprovação de políticas.
- **Todos os Colaboradores:** Responsáveis por reportar riscos e incidentes em suas respectivas áreas.

### 3.4 Procedimentos

Os procedimentos a seguir descrevem as etapas para a gestão contínua dos riscos na **R3S Soluções Tecnológicas**.

#### 3.4.1 Identificação de Riscos

A identificação de riscos é um processo contínuo que utiliza diversas técnicas, como workshops de brainstorming, análise de incidentes passados, entrevistas com especialistas, análise de cenários e revisão de requisitos regulatórios (ex: **LGPD**). Os riscos são categorizados (tecnológicos, operacionais, financeiros, reputacionais, ambientais - **ISO 14001**, segurança ocupacional - **ISO 45001**) e registrados em um repositório centralizado.

#### 3.4.2 Avaliação e Priorização

Cada risco identificado é avaliado quanto à sua probabilidade de ocorrência e ao impacto potencial nos objetivos da empresa. Utiliza-se uma matriz de risco (probabilidade x impacto) para classificar os riscos em níveis (baixo, médio, alto, crítico) e priorizá-los. Esta avaliação é fundamental para alocar recursos de forma eficiente e focar nos riscos mais significativos, conforme a metodologia da **ISO 31000**.

#### 3.4.3 Tratamento de Riscos

Para cada risco priorizado, uma estratégia de tratamento é definida. As opções incluem: **Aceitar** (quando o custo da mitigação é maior que o impacto), **Evitar** (eliminar a atividade que gera o risco), **Transferir** (seguros, terceirização) ou **Mitigar** (implementar controles para reduzir probabilidade/impacto). Os planos de tratamento são detalhados com ações específicas, responsáveis e prazos, alinhados aos requisitos da **ISO 9001** para ações corretivas e preventivas.

#### 3.4.4 Monitoramento e Relatórios

Os riscos e os planos de tratamento são monitorados continuamente. Indicadores-chave de desempenho (KPIs) e indicadores-chave de risco (KRIs) são estabelecidos para acompanhar a evolução dos riscos e a eficácia dos controles. Relatórios periódicos são gerados para a alta

direção e o Comitê de Governança, detalhando o status dos riscos, incidentes ocorridos e as ações de melhoria contínua, suportando a revisão crítica da gestão exigida pelas **ISOs**.

### 3.5 Documentação

Toda a documentação relacionada à gestão de riscos é mantida de forma organizada e acessível. Isso inclui registros de identificação de riscos, análises de BIA, planos de tratamento, relatórios de incidentes, atas de reuniões do Comitê de Governança e lições aprendidas. A documentação é essencial para a rastreabilidade, auditoria e para a conformidade com os requisitos de documentação da **ISO 9001** e **ISO 27001**.

## 4. CRONOGRAMA DE IMPLEMENTAÇÃO

O cronograma a seguir detalha as fases de implementação e manutenção do Programa de Gestão de Riscos na **R3S Soluções Tecnológicas**, desde sua concepção até a operação contínua.

### Fase 1: Planejamento e Definição (Abril - Junho/2025)

- Definição da política de gestão de riscos e aprovação pela alta direção.
- Formação do Comitê de Gestão de Riscos.
- Definição da metodologia de BIA e avaliação de riscos.
- Alinhamento com os requisitos das ISOs 9001, 14001, 45001 e preparação para ISO 27001/LGPD.

### Fase 2: Análise e Desenvolvimento (maio/2025)

- Realização da Análise de Impacto no Negócio (BIA) para processos críticos.
- Identificação e avaliação inicial de riscos em todas as áreas.
- Desenvolvimento de estratégias de mitigação e planos de resposta.
- Criação do repositório de riscos e documentação inicial.

### Fase 3: Implementação e Treinamento (junho/2025)

- Implementação dos controles de mitigação e planos de resposta.
- Realização de treinamentos para colaboradores sobre gestão de riscos e segurança da informação.
- Início do monitoramento contínuo dos riscos e KPIs.
- Primeiras auditorias internas para verificar a conformidade com o PGR e as ISOs.

### Fase 4: Operação e Melhoria Contínua (A partir de agosto/2026)

- Operação plena do Programa de Gestão de Riscos.
- Revisões anuais do PGR e atualizações pós-incidentes.
- Realização de testes e simulações periódicas.
- Acompanhamento dos KPIs e KRIs, com relatórios regulares à alta direção.

- Busca pela certificação ISO 27001 e manutenção da conformidade LGPD.

## **5. DIAGRAMAS OPERACIONAIS**

Os diagramas a seguir ilustram os fluxos de trabalho dos principais processos do Programa de Gestão de Riscos, facilitando a compreensão e a execução das atividades.

### **5.1 Diagrama de Identificação de Riscos**

O fluxo de identificação de riscos inicia-se com a coleta de informações de diversas fontes (workshops, auditorias, feedback de colaboradores). As informações são analisadas para identificar potenciais eventos de risco, que são então registrados no sistema de gestão de riscos. Este processo é contínuo e iterativo, alimentando a base de dados de riscos da empresa.

### **5.2 Diagrama de Avaliação de Riscos**

Após a identificação, cada risco passa por uma avaliação de probabilidade e impacto. Os resultados são plotados em uma matriz de risco, que classifica o risco em níveis de prioridade. Riscos de alta prioridade são encaminhados para tratamento imediato, enquanto os de baixa prioridade são monitorados. Este fluxo garante que os recursos sejam focados nos riscos mais críticos.

### **5.3 Diagrama de Tratamento de Riscos**

Para riscos priorizados, o fluxo de tratamento envolve a seleção da estratégia mais adequada (aceitar, evitar, transferir ou mitigar). Um plano de ação detalhado é elaborado, com responsáveis e prazos. A implementação das ações é monitorada, e sua eficácia é verificada através de testes e auditorias. Este processo é fundamental para reduzir a exposição da empresa a ameaças.

### **5.4 Diagrama de Monitoramento e Relatórios de Riscos**

O fluxo de monitoramento envolve o acompanhamento contínuo dos riscos e dos controles implementados. KPIs e KRIs são coletados e analisados regularmente. Relatórios de status são gerados para diferentes níveis da organização, incluindo a alta direção, permitindo uma visão clara da postura de risco da empresa e suportando decisões estratégicas. Este ciclo se retroalimenta com novas identificações e avaliações de riscos.

---

## **DISPOSIÇÕES FINAIS**

Este Manual Interno de Gestão de Riscos entra em vigência na data de sua aprovação, em **20 de abril de 2025**. Ele será revisado anualmente, ou sempre que necessário, para garantir sua adequação e eficácia contínuas, refletindo as mudanças no ambiente de negócios, tecnologia e requisitos regulatórios. A adesão a este manual é obrigatória para todos os colaboradores da **R3S Soluções Tecnológicas**, e seu cumprimento é essencial para a proteção e o sucesso da organização.