guia de

GESTÃO DE RISCOS

Novembro/2025

GOVERNO DO ESTADO DO PARÁ
Controladoria-Geral do Estado do Pará

HELDER ZALUTH BARBALHO
Governador do Estado

HANA GHASSAN TUMA
Vice-Governadora

OZORIO ADOLFO JUVENIL GOES NUNES DE SOUZA
Controlador-Geral do Estado

ANA PAULA PANTOJA PINTO
Controladora-Geral Adjunta de Controle Interno

LUIZ HENRIQUE DE SOUZA REIMÃO
Controlador-Geral Adjunto de Gestão e Suporte

REALIZAÇÃO
CONTROLADORIA DE AUDITORIA INTERNA (C-AUDIN)
Amanda Carvalho Barbosa Campelo
Controladora de Auditoria Interna

ELABORAÇÃO
Adriana Cristina de Araújo Mendes
Auditora de Finanças e Controle

DIAGRAMAÇÃO
Adriana Cristina de Araújo Mendes
Auditora de Finanças e Controle

CONTROLADORIA-GERAL DO ESTADO (CGE)
Rua Municipalidade, 1655 Umarizal, CEP 66050-350 Belém - PA
(91) 3239-7650 E-mail: controladoria@cge.pa.gov.br
Site: https://cge.pa.gov.br Instagram: @cgepara

2025 - CONTROLADORIA-GERAL DO ESTADO DO PARÁ

CONTROLADORIA-GERAL DO ESTADO (CGE)
Rua Municipalidade, 1655. Umarizal, CEP 66050-350 - Belém-PA
(91) 3239 6476 / 6477 E-mail: controladoria@cge.pa.gov.br
Site: https://cge.pa.gob.br/ Instagram: @cgepara
Versão Eletrônica disponível em : https://cge.pa.gov.br

Elaboração: Adriana Cristina de Araújo Mendes
Revisão Técnica: Equipe Controladoria de Auditoria Interna
Capa e Ilustrações: Adriana Cristina de Araújo Mendes
Diagramação: Adriana Cristina de Araújo Mendes
Tiragem: 100

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil

Guia Estadual de Gestão de Riscos. 1ª edição - [Belém]
Controladoria-Geral do Estado do Pará, [2025] 48 páginas. Versão de bolso. ISBN 978-65-986928-1-0.

ISBN: 978-65-986928-1-0
CBL
9 786598 692810

Bem - Vindo !

A Controladoria-Geral do Estado do Pará (CGE-PA) tem a satisfação de apresentar este **Guia de Gestão de Riscos**, um instrumento fundamental para fortalecermos juntos a eficiência e a qualidade dos serviços públicos. Acreditamos que a participação ativa de cada um de vocês é essencial para gerenciarmos os desafios que podem impactar nosso trabalho e a entrega de valor à sociedade.

Este guia foi feito para VOCÊ!

Elaboramos este material com o objetivo de torná-lo acessível e útil a todos os servidores, independentemente da sua área de atuação ou nível hierárquico. Ao compreendermos e aplicarmos os conceitos aqui apresentados, estaremos contribuindo para um serviço público mais eficiente e confiável.

Acreditamos no seu engajamento para evoluirmos juntos nesta jornada!

GESTÃO DE RISCOS

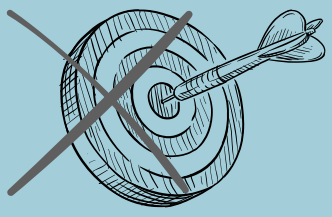
Prevenir é melhor que remediar, no nosso dia a dia no Pará !

Pense na Gestão de Riscos de forma simples: é como planejar uma viagem importante. Antes de sair, pensamos no que pode dar errado – um pneu furado, perda de um voo, uma chuva inesperada. Para cada "risco", pensamos em como nos preparar ou evitar o problema, seja levando um estepe, saindo com antecedência ou consultando a previsão do tempo. No nosso dia a dia no serviço público, a lógica é a mesma: identificar "o que pode dar errado" e nos prepararmos para garantir que os serviços à população não sejam prejudicados.

SUMÁRIO

O QUE SÃO RISCOS NO SERVIÇO PÚBLICO?

São eventos ou situações que podem acontecer e afetar negativamente a capacidade de alcançar os objetivos do nosso órgão ou entidade.



Pense neles como os "**imprevistos**" ou os "**problemas potenciais**" que podem surgir e atrapalhar o nosso trabalho. Eles podem ter diferentes origens e causar diversos tipos de impactos.

Existem também os "riscos positivos" - oportunidades que podem trazer benefícios - mas não vamos abordá-los aqui. Nosso foco é evitar problemas.

EXEMPLOS DE RISCOS

- Parada de sistemas atrasa serviços à população.
- Licitações lentas, análise demorada causam ineficiência e insatisfação.
- Descumprir leis gera multas e danos à imagem.
- Extravio de informação prejudica transparência e prestação de contas.
- Ausência de materiais, veículos ou orçamento limita o trabalho eficaz.
- Servidores sem as habilidades necessárias afeta a qualidade dos serviços.
- Greves, desastres naturais impedem a continuidade de serviços essenciais.
- Corrupção, fraude, assédio prejudicam a confiança pública e causam prejuízos.

O QUE A GESTÃO DE RISCOS TRAZ DE BOM?

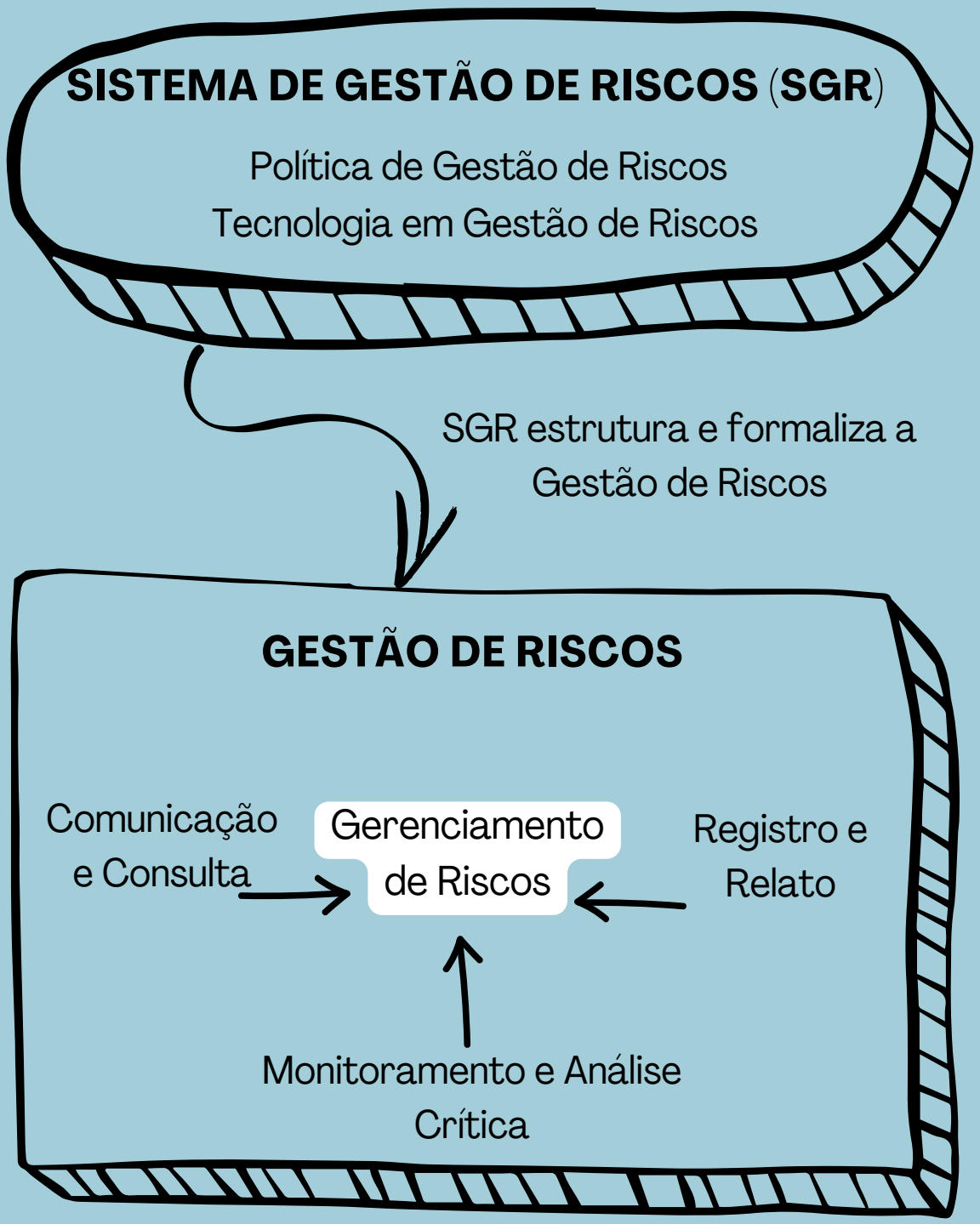
- Ajuda na **tomada de decisão** mais **segura**: Conhecer os riscos de aprovar um processo, implementar um projeto ou alocar recursos nos permite tomar decisões mais informadas e conscientes.
- Aumenta a chance de **atingir os objetivos,** evitando problemas e protegendo o patrimônio (recursos, bens, imagem).
- O trabalho fica mais **eficiente** e os recursos são usados melhor, com menos imprevistos e retrabalho.
- A organização fica **mais forte** para lidar com imprevistos e se recuperar.
- Melhora a **relação** com todos os interessados, mostrando que a organização se preocupa com os riscos.

ONDE A GESTÃO DE RISCOS SE APLICA?

Em tudo

A gestão de riscos serve para qualquer área ou atividade da organização, não importa o tamanho ou o que ela faz.

Exemplos: Projetos, processos, finanças, segurança da informação, meio ambiente, leis, etc.



SISTEMA DE GESTÃO DE RISCOS

Conjunto de instrumentos que estrutura e formaliza a Gestão de Riscos em toda a organização.

O SGR atua como a **base formal** que permite à organização planejar, executar, monitorar e melhorar continuamente suas atividades relacionadas a riscos. Ao promover uma **cultura** de riscos e otimizar **recursos** e **processos**, o SGR capacita a organização a operar de forma mais **segura**, **eficiente** e **resilient**e, garantindo que a consideração dos riscos seja parte integrante de suas operações.

GESTÃO DE RISCOS

Conjunto de ações estratégicas destinadas a dirigir e controlar uma organização em relação aos riscos, com o objetivo de criar e proteger valor em toda a sua estrutura.

Seu propósito fundamental é auxiliar a **tomada de decisões**, fornecendo acesso oportuno a informações precisas e relevantes sobre os riscos aos quais a organização está exposta. A Gestão de Riscos cria o **ambiente** para um Gerenciamento de Riscos eficaz.

GERENCIAMENTO DE RISCOS

Conjunto de atividades passo a passo que a organização aplica para lidar com riscos específicos no seu dia a dia, utilizando metodologias e técnicas para entender e responder a cada um individualmente.

É a implementação **operacional** da Gestão de Riscos.

POLÍTICA DE GESTÃO DE RISCOS

Estabelece os **princípios** e as **responsabilidades** para a Gestão de Riscos. Ela representa o compromisso da alta gestão em integrar a Gestão de Riscos em todos os níveis e atividades da organização, visando o alcance de seus objetivos estratégicos com maior segurança e resiliência.

Princípios

São as diretrizes essenciais que orientam a implementação de uma gestão de riscos eficaz e eficiente.

Integração: A gestão de riscos deve ser parte integrante de **todas** as atividades organizacionais.

Estruturação: Criar uma estrutura clara com **papéis**, **responsabilidades** e **processos** definidos.

Personalização: A abordagem da Gestão de Riscos precisa ser adaptada ao **contexto** específico da organização.

Inclusão: O envolvimento das **partes interessadas** e a consideração dos fatores humanos e culturais são cruciais.

Dinamicidade: A Gestão de Riscos deve ser **reativa** e **proativa** a mudanças, sendo um processo contínuo e interativo.

Melhores Informações: A tomada de decisão deve se basear nas melhores informações **disponíveis**.

Melhoria Contínua: O processo de gestão de riscos deve buscar constante **aprimoramento**, aprendendo com a experiência.

Responsabilidades

A Gestão de Riscos é uma responsabilidade compartilhada em toda a organização.

Alta Gestão: É responsável por aprovar a política, garantir a alocação de **recursos** necessários para a implementação e manutenção do SGR, e promover uma **cultura** de riscos positiva.

Área Responsável pela Gestão de Riscos: É responsável por desenvolver, implementar, manter e monitorar a Gestão de Riscos, fornecer **orientação** e **suporte** às demais áreas, e reportar à alta gestão sobre o desempenho da gestão de riscos.

Gestores de Área/Unidade: São responsáveis por identificar, analisar, avaliar e tratar os **riscos** em suas respectivas áreas, bem como por implementar e monitorar os **controles** definidos.

Todos os Servidores: São responsáveis por identificar e reportar potenciais riscos, cumprir os **procedimentos** de gestão de riscos e participar ativamente das iniciativas relacionadas à gestão de riscos.

TECNOLOGIA EM GESTÃO DE RISCOS

A implementação de ferramentas e soluções tecnológicas adequadas pode aprimorar significativamente a **eficiência**, a **precisão** e a **abrangência** das atividades de Gestão de Riscos, desde a identificação até o monitoramento e o relato. A seleção e implementação de tecnologias para a Gestão de Riscos devem ser baseadas nas necessidades específicas da organização, na complexidade de seus riscos, nos recursos disponíveis e nos objetivos estratégicos. É fundamental garantir a integração dessas tecnologias com os processos existentes e capacitar os usuários para sua utilização eficaz.

A integração da tecnologia no SGR visa:

Informação Unificada

Todos os dados de risco em um só lugar para fácil acesso e relatórios.

Processos Automáticos

Tarefas manuais automatizadas, liberando tempo para análise e decisão.

Análise Inteligente

Identificação de tendências e padrões para avaliar riscos com precisão.

Monitoramento Contínuo

Acompanhamento constante para detectar problemas cedo e prevenir eventos.

Relatórios Claros

Informações de risco personalizadas e atualizadas para todos.

Colaboração Facilitada

Compartilhamento fácil de informações entre as áreas envolvidas.

Decisões Embasadas em Dados

Informações confiáveis para escolhas mais seguras.

A CGE-PA já utiliza o sistema **SAEWeb**, desenvolvido pela Controladoria -Geral do Distrito Federal (CGDF), como ferramenta para a Gestão de Riscos.

5 PASSOS PARA GERENCIAR RISCOS

ESTABELECENDO ESCOPO, CONTEXTO E CRITÉRIOS

Construindo uma base sólida e um entendimento comum para o Gerenciamento de Riscos.

É a garantia que nossos esforços sejam focados, relevantes e alinhados com os objetivos do nosso órgão.

Escopo (o que vamos abranger?)

O escopo define os **limites** (fronteiras) do que será analisado. Precisamos decidir quais áreas, atividades, processos, ou projetos serão incluídos no processo de Gestão de Riscos. O escopo pode ser amplo (toda a organização) ou mais específico (um projeto em particular).

Ao definir o escopo, é importante considerar:

- Quais objetivos queremos proteger ou alcançar com a Gestão de Riscos nessa área específica?
- Quanto tempo, pessoal e orçamento temos para realizar a Gestão de Riscos nesse escopo?
- Quais são as expectativas dos cidadãos, de outros órgãos, da CGE em relação à Gestão de Riscos nessa área?

Contexto (cenário em que atuamos)

Compreender o **ambiente** interno e externo é crucial para **personalizar** o processo de gestão de riscos. A análise do contexto permite identificar como os riscos podem surgir e impactar a organização. Uma ferramenta útil para essa análise é a **Matriz SWOT**, que examina Forças (internas positivas), Fraquezas (internas negativas), Oportunidades (externas positivas) e Ameaças (externas negativas) que impactam a Gestão de Riscos.

Contexto Interno

- Como a organização lida com riscos normalmente?
- Como a organização está organizada? Quem faz o quê?
- Como as decisões são tomadas?
- Quais recursos (pessoas, dinheiro, tecnologia) a organização tem?
- Como a informação é gerenciada?

Contexto Externo

- Quais leis e regras a organização precisa seguir?
- Como está a economia? Quais são as tendências?
- Quais são os valores e costumes da sociedade?
- Quais novas tecnologias podem afetar a organização?

Critérios de Risco ("Regras do Jogo")

Os critérios de risco são as "regras do jogo" que usaremos para avaliar a importância dos riscos que identificarmos, levando em conta nosso contexto, objetivos e "**apetite a risco**" (o quanto de risco estamos dispostos a aceitar).

Ao definir os critérios de risco, precisamos considerar:

Escalas de probabilidade: O que consideramos "muito baixa", "baixa", "média", "alta", "muito alta" a chance de um risco acontecer?

Escalas de impacto: O que consideramos "muito baixo", "baixo", "médio", "alto", "muito alto" a gravidade das consequências se um risco acontecer ?

Níveis de Riscos: O que consideramos um risco, "baixo", "médio", "alto" ou “extremo”?

Apetite a Riscos: Que riscos podemos aceitar para alcançar nossos objetivos e quais precisam de ação urgente? Nossa tolerância a riscos varia dependendo da área, por exemplo em segurança pode ser quase zero.

Nossos Recursos: Quanto tempo, dinheiro e pessoal temos disponíveis para lidar com os riscos? Isso pode influenciar quais riscos podemos tratar primeiro e quais as melhores formas de fazê-lo.

Como os riscos serão priorizados: Quais fatores, além da probabilidade e do impacto, podem influenciar a prioridade de tratamento de um risco (ex: urgência, requisitos legais, preocupações das partes interessadas)?

IDENTIFICANDO RISCOS

Encontrando os Problemas Potenciais

Consiste em uma “investigação” para **reconhecer** e **descrever** potenciais eventos ou situações, de origem interna ou externa, que podem **afetar negativamente** (impedir, atrasar, prejudicar ou dificultar) o alcance dos **objetivos** organizacionais.

Nesta etapa proativa, busca-se antecipar possíveis falhas antes que ocorram.

O Que Procurar

Para facilitar essa "investigação", podemos olhar para os seguintes problemas no nosso trabalho e na organização:

- Computadores, internet e impressoras com defeito.
- Falta de cuidado com veículos.
- Instalações elétricas ruins.
- Falhas de segurança nos sistemas.
- Programas que não funcionam bem ou não se conversam.
- Perda de informações importantes.
- Muita burocracia e passos desnecessários.
- Falta de clareza e organização no trabalho.
- Falta de comunicação e conflitos entre as pessoas.
- Falta de gente que realmente entende de certas áreas importantes.
- Falta de regras para proteger informações.
- Falta de dinheiro ou demora para conseguir.
- Má administração de contratos e desperdício.
- Não conhecer ou não seguir leis e regras.

Como Encontrar os Riscos

Inicia-se com uma análise do contexto interno e externo da organização. Para enriquecer essa etapa, é fundamental consultar **especialistas** e integrar as perspectivas das diversas **partes interessada**s sobre o que pode representar um risco. A experiência prática e o conhecimento cotidiano da **equipe** são ativos valiosos e contribuem para o sucesso desta investigação detalhada.

Técnicas utilizadas

Brainstorming: Reuniões para gerar ideias e compartilhar experiências sobre problemas cotidianos, revelando riscos sob diferentes perspectivas.

Análise de Documentos: Revisão de planos, relatórios, processos, auditoria, reclamações e incidentes passados para identificar riscos recorrentes.

Entrevistas: Conversas com pessoas-chave para obter seus pontos de vista e percepções sobre riscos.

Análise de Cenários: Imaginar diferentes situações futuras e os riscos potenciais associados.

Diagramas de Causa e Efeito (**Espinha de Peixe ou Diagrama de Ishikawa**)**:** Ferramenta para entender as relações causais dos problemas e identificar suas raízes.

Análise SWOT: Avaliação das Forças, Fraquezas, Oportunidades e Ameaças para identificar riscos internos e externos.

Sintaxe para Identificação

Elementos, vulnerabilidades ou condições que possibilitam a ocorrência do evento de risco.

"Devido à [**CAUSA**], poderá ocorrer [**EVENTO DE RISCO**], o que levará a [**CONSEQUÊNCIA**], afetando [OBJETIVO]"

O que pode acontecer.

Resultados diretos ou indiretos do evento de risco nos objetivos organizacionais.

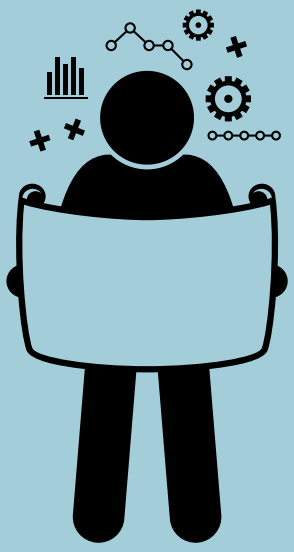
Considerações:

- Um evento pode ser causa de outro
- A identificação de causas e consequências dos riscos é crucial para embasar futuras decisões sobre as respostas aos riscos.
- Um evento de risco pode ter múltiplas causas e consequências, afetando diversos objetivos.
- É crucial envolver a equipe responsável pela execução dos processos na identificação dos riscos para criar responsabilidade e compromisso com o processo de gestão de riscos.

Produto da Identificação de Riscos

Matriz de Riscos (planilha) contendo:

- Evento de risco
- Causas
- Consequências
- Objetivo do processo impactado



ANALISANDO RISCOS

Entendendo a Gravidade dos Problemas

Depois de identificar os riscos, o próximo passo é entender quão sérios eles são. Este processo envolve examinar a **probabilidade** (chance de ocorrência) e o **impacto** (estrago da ocorrência). A combinação dessas duas dimensões permite mensurar o **nível de risco** e priorizar os que exigem maior atenção.

O Que Analisar

Probabilidade (Qual a chance do evento realmente se concretizar?)

Para determinar a probabilidade, considerar:

- Já tivemos esse problema antes? Se sim, qual a chance de repetir?
- Alguma coisa no nosso trabalho aumenta a chance desse risco acontecer? (Tipo um sistema antigo).
- Com que frequência esse tipo de problema acontece em outros lugares?
- Nossa experiência diz que esse risco é provável? Já vimos isso acontecer?

Escala de probabilidade

Peso	Classificação	Significado
1	Muito Baixa	Chance remota de ocorrência
2	Baixa	Pequena chance de ocorrência.
3	Média	Razoável chance de ocorrência
4	Alta	Grande chance de ocorrência
5	Muito Alta	Chance quase garantida de ocorrência

Impacto (Se o risco acontecer, qual a magnitude das consequências?)

Para melhor analisar e criar planos específicos, os impactos são categorizados em áreas relevantes da organização:

Operacional: Efeitos na continuidade e eficiência das atividades diárias, incluindo interrupção de trabalho, retrabalho e paralisação de serviços à população.

Financeiro: Perdas ou problemas com recursos financeiros.

Reputacional: Prejuízo à imagem da organização e abalo da confiança da população.

Legal (**Conformidade**)**:** Descumprimento de leis ou normas e de processos judiciais.

Integridade: Ameaças aos valores e princípios éticos da organização.

Estratégicos: Impacto nos objetivos principais da organização.

Cibernéticos: Ameaças a sistemas e dados digitais.

Pessoais: Falhas na proteção de informações pessoais.

Escala de Impacto

Peso	Classificação	Significado
1	Muito Baixo	Consequências insignificantes
2	Baixo	Consequências mínimas
3	Médio	Consequências com algum grau de prejuízo
4	Alto	Consequências significativas
5	Muito Alto	Consequências graves e duradouras

A determinação da probabilidade e o impacto devem ser fundamentados em **evidências**, como dados históricos e documentos, complementadas por **opiniões de especialistas** ou **análises estatísticas**.

Como Analisar

A probabilidade e o impacto são combinados para determinar o **Nível de Risco**. Uma ferramenta comum para fazer isso é a **Matriz de Probabilidade e Impacto** (Matriz de Calor), que mostra visualmente quais riscos são mais graves e precisam de atenção prioritária.

Determinação do Nível de Riscos: Do Inerente ao Residual

Determinação do Nível de Risco Inerente

Nível de Risco Inerente (NRI)

Representa a exposição de uma organização a um risco específico antes da implementação dos controles internos. Ele reflete a exposição inicial da organização aos riscos.

Análise dos Controles Internos existentes

Controles Internos

São os mecanismos (ações, políticas, práticas e procedimentos) estabelecidos em todos os níveis da organização para modificar o nível de risco.

Exemplos:

Checklists, atribuição de competências e limites de alçadas, capacitação e treinamento, manuais e padronização de procedimentos, monitoramento de indicadores de desempenho, revisão e aprovação de tarefas, segregação e rotação de funções, sistemas informatizados, proteção física e digital.

Determinação do Nível de Risco Residual

Nível de Risco Residual (NRR)

Representa o risco remanescente após a implementação e consideração da eficácia dos controles internos. Ele reflete a exposição real da organização aos riscos.

Determinação do Nível de Risco Inerente (NRI)

O Nível de Risco é calculado combinando os **pesos** de probabilidade e impacto.

NÍVEL DE RISCO = PROBABILIDADE x IMPACTO

Matriz de Probabilidade e Impacto

IMPACTO	PROBABILIDADE 1 Muito Baixa	2 Baixa	3 Média	4 Alta	5 Muito Alta
5 Muito Alto	5	10	15	20	25
4 Alto	4	8	12	16	20
3 Médio	3	6	9	12	15
2 Baixo	2	4	6	8	10
1 Muito Baixo	1	2	3	4	5

NR ≤ 04 : Risco Baixo **05 < NR ≤ 10 : Risco Médio**

11 < NR ≤ 16 : Risco Alto **NR > 17 : Risco Extremo**

Análise do Controle Interno existente

Este processo considera a interligação dos controles nos níveis operacional, tático e estratégico, e abrange as seguintes etapas:

- **Mapear** os **controles existentes** para cada risco através de entrevistas e questionários, considerando sua natureza (preventivo ou detectivo), capacidade de operação, alcance e as responsabilidades atribuídas.
- **Verificar** os seguintes **aspectos**:
  - Como o controle atua para prevenir ou detectar o risco.
  - Se o controle funciona conforme o esperado.
  - Como cada controle opera isoladamente e em conjunto com outros.
  - Identificar potenciais fragilidades (suscetibilidade a fraudes e erros).
  - Avaliar se o próprio controle introduz novos riscos.
  - Determinar se o controle é manual ou automatizado.
  - Verificar se há sobreposições (controles redundantes).

Nível de Confiança (**NC**)**:** reflete a avaliação da eficácia do controle em reduzir o risco, indicando a probabilidade de ele funcionar corretamente.

CLASSIFICAÇÃO	NC	SIGNIFICADO
Inexistente	0	Controle não existe ou não mitiga o risco
Fraco	0,1 - 0,3	Controle existe, mas com muitas falhas ou aplicação irregular, baixa confiança.
Mediano	0,4 - 0,6	Controle existe e opera de forma razoável, mas com algumas limitações ou inconsistências, confiança moderada.
Satisfatório	0,7 - 0,8	Controle bem desenhado e aplicado consistentemente, boa confiança.
Forte	0,9 - 0,95	Controle muito bem desenhado, aplicado de forma robusta e monitorado de perto, alta confiança.

NC nunca alcança 1 (100%), pois os controles fornecem apenas uma segurança razoável, e não absoluta, quanto ao cumprimento dos objetivos, devido as limitações inerentes (conluio, contorno ou falha humana).

Risco de Controle (RC): representa a probabilidade de os controles internos falharem em prevenir, detectar ou corrigir eventos adversos.

Ele é inversamente proporcional ao NC, calculado pela fórmula: **RC = 1 - NC**

Assim, quanto maior o Nível de Confiança nos controles, menor o Risco de Controle, e vice-versa. No entanto, como o NC nunca será 1 (100%) devido às limitações inerentes dos controles, o Risco de Controle nunca será zero.

Determinação do Nível de Risco Residual

A avaliação do Risco Residual é fundamental para determinar o risco a que a organização permanece exposta após a aplicação dos controles internos e orienta a necessidade de novas ações para mitigar ainda mais os riscos, se necessário.

O NRR pode ser calculado da seguinte forma: **NRR=NRI×RC**

Considerações:

- A análise pode variar em detalhamento e complexidade, dependendo do propósito, da disponibilidade de informações e dos recursos.
- Um risco pode exigir múltiplos controles e que um controle pode mitigar múltiplos riscos.
- A técnica **Bow Tie** pode ajudar na identificação dos controles existentes.

Produto da Análise de Riscos

Matriz de Riscos (planilha) atualizada com a análise de:

- Probabilidade
- Impacto
- Nível de Risco Inerente
- Controles Existentes
- Nível de Confiança dos Controles
- Nível de Risco Residual

AVALIANDO RISCOS

Decidindo o Que Fazer com os Problemas

Avaliar riscos significa **comparar** o **nível residual** de cada um com os **critérios** ("regras do jogo") que estabelecemos (lá no início, lembra?). O objetivo é determinar quais riscos ultrapassam o **apetite a riscos** (limites de tolerância), e portanto, necessitam de controle prioritário. É uma forma de "triagem" dos problemas para direcionar o foco e os recursos para os riscos mais críticos.

	CARACTERÍSTICAS	AÇÕES CORRELATAS
RISCO BAIXO	**Aceitável** e dentro da tolerância. Geralmente, os controles existentes são suficientes.	**Monitoramento:** Acompanhe periodicamente para garantir que as características não mudem. Não exige investimentos significativos em tratamento.
RISCO MÉDIO	**Tolerável**, mas exige atenção. Controles existentes podem não ser totalmente eficazes, ou o risco residual ainda é relevante.	**Revisão e Tratamento (opcional):** Avalie se ações de tratamento adicionais seriam benéficas e viáveis para reduzir o risco. **Monitoramento:** Acompanhe para prevenir agravamento.
RISCO ALTO	**Inaceitável** e ultrapassa a tolerância. Exige atenção imediata.	**Tratamento Prioritário:** Desenvolva e implemente planos de ação específicos e urgentes. Monitore a eficácia do tratamento.
RISCO EXTREMO	**Severamente inaceitável** e representa uma ameaça crítica. Pode paralisar operações e causar danos irreparáveis.	**Tratamento Imediato e Urgente:** Aloque todos os recursos necessários para mitigar ou eliminar o risco o mais rápido possível. Pode exigir a interrupção de atividades.

Opções de Tratamento

As opções de tratamento (aceitar, evitar, transferir e mitigar os riscos) não são mutuamente exclusivas.

ESTRATÉGIA	EXEMPLOS	QUANDO APLICÁVEL
ACEITAR Não tomar nenhuma ação específica para evitá-lo, transferi-lo ou mitigá-lo	Aceitar pequenos atrasos de fornecedores. Aceitar pequenas variações cambiais em compras online ocasionais	Risco residual baixo Não existem opções de tratamento viáveis ou econômicas
EVITAR Eliminar a fonte do risco Não iniciar ou interromper uma atividade	Desfazer-se de um ativo; Não iniciar um projeto de alto risco estratégico. Encerrar uma linha de produção com alto índice de acidentes	Outras respostas são ineficazes. Relação custo-benefício desfavorável. Capacidade de atuação limitada
TRANSFERIR Transferir ou compartilhar parte da sua responsabilidade ou consequências com terceiros	Contratar seguro. Terceirizar a segurança de um setor. Estabelecer parcerias com compartilhamento formal de riscos	Não apresenta boa relação custo-benefício para controles diretos. Organização tem domínio limitado sobre o risco ou atividade
MITIGAR Reduzir a probabilidade de ocorrência e/ou impacto a um nível aceitável.	Implementar controles internos rigorosos (treinamentos, planos de backup, manutenções preventivas, novas tecnologias, etc	Custo de implementar ações proporcional ao benefício esperado na redução do risco.

Decisão: Aceitar, evitar, compartilhar ou mitigar?

Ao confrontar o nível de risco residual com o apetite a risco estabelecido, a organização define se o risco será aceito ou tratado. A classificação do risco residual (baixo, médio, alto) orienta a priorização das ações. Além disso, a urgência ditada por prazos legais ou situações críticas é um fator crucial, exigindo intervenção imediata nos riscos que a demandam.

A seleção da opção de tratamento visa definir a resposta mais adequada a cada risco priorizado, considerando seu **nível**, o **contexto** organizacional e a relação **custo-benefício**. A decisão de tratamento busca um equilíbrio entre o custo da implementação e a redução esperada dos danos do risco. Evitaremos soluções que criem novos problemas ou custem mais do que o benefício de diminuir o risco, principalmente para eventos raros com grande impacto. A melhor estratégia reduz a gravidade dos riscos de forma eficiente e com um custo menor que os problemas que ela evita.

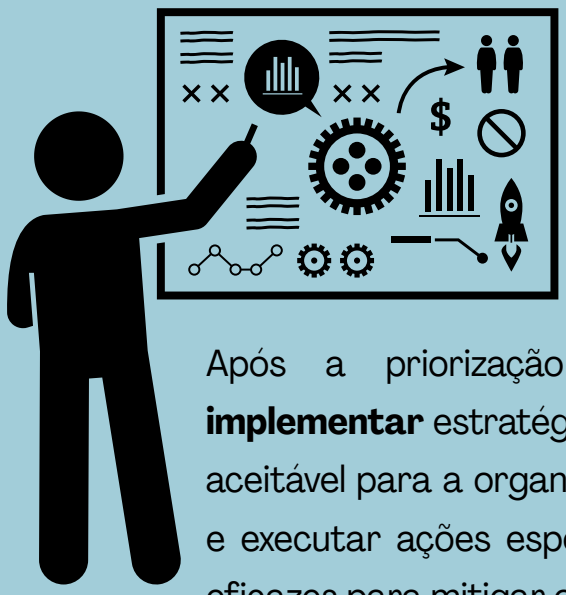
Considerações

- O impacto geralmente tem maior relevância que a probabilidade, devendo riscos de alto impacto ser priorizados.
- A decisão de aceitar um risco, mesmo que baixo ou médio, requer aprovação da alta gestão.
- A priorização ou não de medidas de tratamento para qualquer risco deve ser justificada pela unidade e aprovada pela alta estão.

Produto da Avaliação de Riscos

Matriz de Riscos (planilha) atualizada com:

- Avaliação do Nível de Risco Residual (comparação com critérios - apetite)
- Opção de tratamento aos Riscos



TRATANDO RISCOS

Agindo Contra os Problemas

Após a priorização dos riscos, o tratamento envolve **implementar** estratégias para modificar seu **nível** a um patamar aceitável para a organização. Este é o momento de agir: planejar e executar ações específicas, escolhendo as ferramentas mais eficazes para mitigar os problemas identificados.

Planos de Tratamento

Para cada risco que demanda intervenção, a organização deve desenvolver um **plano de ação**, considerando **custos**, **benefícios** e **recursos** disponíveis. A elaboração desse plano é crucial para implementar respostas eficazes aos riscos priorizados.

O plano detalha as ações específicas a serem tomadas, introduzindo novos controles ou ajustando os existentes. A prioridade inicial deve ser avaliar a possibilidade de **otimizar** ou **remover** controles existentes. Novas medidas devem ser propostas apenas se a redução do risco ainda for necessária e sua eficiência, eficácia e viabilidade econômica forem comprovadas.

A elaboração do plano deve priorizar a análise de **causas** e **efeitos** do risco, direcionando ações primárias para as causas e complementando com planos de contingência para mitigar os impactos inevitáveis ou insuficientemente prevenidos. Caso a prevenção completa não seja viável, o foco deve ser na mitigação dos efeitos.

Os controles definidos nos planos podem ser preventivos (atuando na causa) ou de atenuação/recuperação (minimizando consequências).

A identificação de medidas de tratamento pode ser auxiliada por modelos de situações semelhantes, literatura especializada e experiência da equipe.

Considerações

- A possibilidade de o tratamento se mostrar ineficaz, mesmo após implementação cuidadosa, demanda a **revisão** das opções estratégicas ou dos limites de exposição ao risco estabelecidos.
- Embora a Alta Gestão seja a responsável final pelo gerenciamento de riscos, a implementação e o monitoramento dos planos de tratamento são de responsabilidade das áreas **gerenciais** e **operacionais**, com designação de responsáveis por cada iniciativa.
- A justificativa para o tratamento deve considerar, responsabilidades e compromissos com as partes interessadas.
- Em iniciativas que envolvem múltiplos setores, a **validação conjunta** do plano é indispensável.

Produto do Tratamento de Riscos

Plano de Tratamento de Riscos contendo para cada risco priorizado:

- Opções de tratamento selecionadas (Mitigar, Evitar, Transferir, Aceitar)
- Ações específicas a serem implementadas
- Responsáveis pela implementação
- Prazos para implementação

COMUNICAÇÃO E CONSULTA

São processos **interdependentes** que permeiam todas as etapas do gerenciamento de riscos. Seu propósito principal é garantir que as partes interessadas compreendam os riscos, o embasamento das decisões e as justificativas para as ações necessárias. Simultaneamente, busca-se engajar essas partes por meio da coleta de feedback e informações que enriqueçam o estabelecimento do contexto e o processo decisório.

Objetivos

- Assegurar que as visões, percepções, necessidades, e preocupações das **partes interessadas** sejam identificadas, registradas e consideradas.
- Integrar diferentes **áreas de especialização** para cada etapa do processo.
- Fomentar o **envolvimento** de todos por meio da divulgação periódica do progresso das ações, assegurarando que os envolvidos compreendam seus **papéis** e **responsabilidades** na gestão de riscos.

Plano e Canais de Comunicação e Consulta

Visa garantir uma **troca de informações** em todas as direções hierárquicas, utilizando diversos canais para fortalecer o gerenciamento de riscos e disseminar a cultura correspondente.

Fluxos de Comunicação

Interna
- **Vertical:** Formal, respeitando a hierarquia (ascendente para reportar; descendente para diretrizes).
- **Horizontal:** Ágil e oportuna entre indivíduos ou equipes (ex: e-mails).

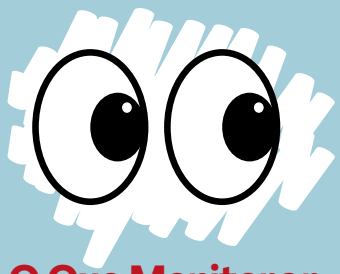
Externa Direcionada à sociedade, requer monitoramento para alinhar-se às expectativas da população.

A **confidencialidade**, a **integridade**, a **confiabilidade** e a **tempestividade** das informações devem ser observadas, garantindo a integração, a colaboração e o alinhamento entre as instâncias e partes interessadas.

MONITORAMENTO E ANÁLISE CRÍTICA

São atividades **interligadas**, essenciais para a adaptação e relevância da gestão de riscos em um ambiente organizacional dinâmico e sujeito a novas ameaças. Ao manter um **olhar atento** sobre o processo de gestão de riscos e os próprios riscos, a organização verifica a **eficácia** das ações, aprende com a **experiência** e implementa **ajustes** para garantir a preparação diante de incertezas.

Monitoramento: Acompanhamento Contínuo



Consiste na **observação** regular e sistemática do desempenho da gestão de riscos e da evolução dos próprios riscos.

O Que Monitorar

- Mudanças no contexto externo e interno da organização.
- Variações na probabilidade e impacto dos riscos existentes, surgimento de novos riscos e desaparecimento de riscos antigos.
- Implementação das ações e sua eficácia na redução dos riscos.
- Correta aplicação das etapas do gerenciamento de riscos, eficácia da comunicação e clareza das responsabilidades.
- Contribuição da gestão de riscos para o alcance dos objetivos organizacionais.

Como Monitorar

- Designar responsáveis para o acompanhamento e controle.
- Criar mecanismos para coleta, registro e análise de informações relevantes.
- Desenvolver e acompanhar indicadores (métricas) para avaliar o desempenho da gestão de riscos.
- Realizar reuniões periódicas para discutir riscos e o progresso dos planos.
- Acompanhar as atividades e a aplicação dos controles na prática.

Análise Crítica: Aprendizado

Consiste numa **avaliação** aprofundada e periódica da Gestão de Riscos, focada em aprender com a experiência e identificar oportunidades de melhoria.

O Que Analisar

- Resultados gerados pelo **acompanhamento** contínuo.
- Adequação do desenho e eficácia da operação dos **controles** implementados.
- Avaliação da eficácia das **ações** na mitigação dos riscos.
- **Experiências** passadas de sucessos e insucessos no tratamento de riscos.

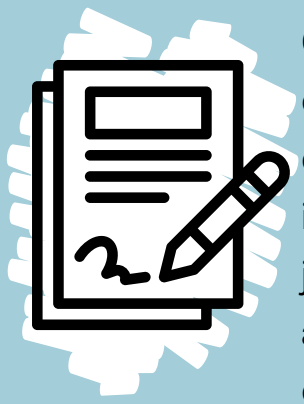
Como Analisar

- Designar **responsáveis** pela coordenação e execução da análise crítica.
- Identificar **pontos fortes** e **áreas** que necessitam de **aprimoramento.**
- Extrair **lições** de sucessos e insucessos.
- Buscar formas de aumentar a **eficácia** e a **eficiência** do processo de gestão de riscos.

Ações Decorrentes do Monitoramento e Análise Crítica

- Revisar e adaptar planos de ação, metas, prazos, responsabilidades e estratégias de tratamento com base em desvios identificados ou novas necessidades.
- Adotar medidas para corrigir desvios, otimizar processos e controles existentes.
- Implementar ou reforçar controles para mitigar riscos de forma mais eficaz.
- Incorporar novos riscos identificados ao processo de gestão, garantindo sua abrangência e atualização constante.

REGISTRO E RELATO



Consistem em documentar sistematicamente todas as etapas e resultados do gerenciamento de riscos, além de compartilhar informações relevantes com as partes interessadas. Essa prática estabelece um **histórico** claro da jornada da organização na gestão de riscos, facilitando o aprendizado, a tomada de decisões informadas e o engajamento de todos os envolvidos.

Propósito

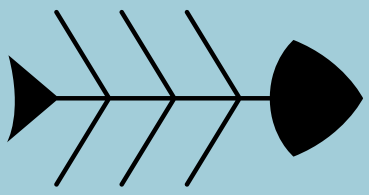
- Documentar ações e suas justificativas, fornecendo informações valiosas para análises futuras e melhorias contínuas.
- Demonstrar o comprometimento da organização com a gestão de riscos e atender a requisitos legais e regulatórios.
- Facilitar o diálogo e o compartilhamento de informações relevantes com as partes interessadas.
- Apoiar decisões estratégicas embasadas em dados históricos e tendências identificadas.
- Promover a transparência e o engajamento das partes interessadas.

Formas de Compartilhamento

- Relatórios formais (periódicos ou específicos).
- Apresentações (em reuniões ou eventos).
- Reuniões (equipes ou alta gestão).
- Comunicações por e-mail.
- Sistemas de informação dedicados à gestão de riscos.

FERRAMENTAS VISUAIS

O Diagrama de Causa e Efeito (Espinha de Peixe ou Ishikawa)

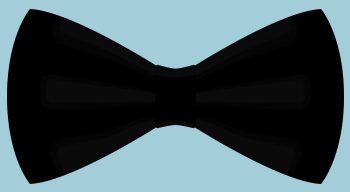


Visualiza as causas potenciais de um risco (efeito) e facilita entender as origens dos riscos para planejar ações mais eficazes. Ele ajuda a organizar as ideias e a visualizar as relações de causa e efeito de forma estruturada.

Como construir:

- Defina claramente o risco (cabeça do peixe).
- Identifique as principais categorias de causas (espinhas principais - ex: Pessoas, Processos, Tecnologia).
- Liste as possíveis causas em cada categoria (ramificações).
- Para cada causa, pergunte "por quê?" para encontrar causas mais profundas (ramificações menores).

Análise Bow Tie (gravata borboleta)



Mostra o caminho de um risco: suas causas, o risco em si e suas consequências, com as barreiras de prevenção (antes do risco) e mitigação (depois do risco). Ele ajuda a entender e controlar os riscos de forma clara e proativa. Avalia a eficácia dos controles. É a base para planos de ação (melhorar barreiras).

Como construir:

- Defina o risco central (o "nó").
- Liste as causas à esquerda.
- Liste as consequências à direita.
- Identifique controles para impedir as causas.
- Identifique controles para reduzir o impacto.

Exemplo Simplificado de Como Gerenciar Riscos

Para mostrar como funciona na prática o gerenciamento de riscos, vamos usar um exemplo fácil de entender. Assim, você poderá ver como aplicar cada etapa no seu trabalho.

Central de Serviços ao Cidadão (CSC)

É um órgão público estadual (hipotético) responsável por oferecer diversos serviços essenciais à população, incluindo agendamento de serviços, emissão de documentos, informações sobre programas sociais, atendimento ao público por telefone e internet, e comunicação interna entre seus setores.

Escopo

Infraestrutura de Tecnologia da Informação (TI) que suporta os serviços essenciais oferecidos. Isso inclui servidores, internet, programas que usamos, onde guardamos os arquivos e quem cuida disso.

Contexto

Contexto Interno

- Dependemos muito da TI para tudo: agendar, emitir documentos, falar com as pessoas e ter informações. Se a TI parar, o trabalho para.
- Temos equipamentos e sistemas de TI mais antigos e mais novos, alguns podem dar mais problema.
- Nossa equipe de TI é pequena e pode ter dificuldade para resolver problemas grandes e evitar que eles aconteçam.

Contexto Externo

- Existem muitos hackers atacando órgãos públicos com vírus ou golpes.
- Existem leis que nos obrigam a proteger os dados e garantir que os serviços não parem.

Critérios

Apetite a Riscos

NR ≤ 04 : **Risco Baixo** Aceitável	11 < NR ≤ 16 : **Risco Alto** Inaceitável
05 < NR ≤ 10 : **Risco Médio** Tolerável	NR > 17 : **Risco Extremo** Inaceitável

Escala de probabilidade

Peso	Classificação	Significado	Frequência Esperada
1	Muito Baixa	Chance remota de ocorrência	uma vez a cada > 5 anos
2	Baixa	Pequena chance de ocorrência	uma vez a cada 2-5 anos
3	Média	Razoável chance de ocorrência	uma vez por ano
4	Alta	Grande chance de ocorrência	mais de uma vez por ano
5	Muito Alta	Chance quase garantida de ocorrência	várias vezes ao ano

Escala de Impacto

Peso	Classificação	Significado	Impacto nos serviços
1	Muito Baixo	Consequências insignificantes	Quase não atrapalha o trabalho e os serviços
2	Baixo	Consequências mínimas	Atrapalha um pouco, mas dá para resolver rápido
3	Médio	Consequências com algum grau de prejuízo.	Atrapalha o trabalho e os serviços por um tempo, precisamos de mais esforço para resolver
4	Alto	Consequências significativas	Para quase tudo, prejudica muito as pessoas que precisam dos nossos serviços e nossa imagem fica ruim
5	Muito Alto	Consequências graves e duradouras	Para tudo por muito tempo, causa muitos problemas para as pessoas, podemos ter problemas legais e nossa imagem fica muito ruim

IDENTIFICANDO RISCOS

Diagrama de Causa e Efeito (Espinha de Peixe ou Ishikawa)

Neste diagrama, o objetivo principal do órgão (oferecer diversos serviços essenciais à população de forma eficiente e acessível) foi o ponto de partida para identificar as possíveis causas do risco.

IDENTIFICANDO RISCOS

A partir deste momento, vamos focar em três objetivos específicos que ajudam a alcançar o objetivo principal do órgão. Para cada um desses objetivos, escolhemos um risco principal.

EVENTO DE RISCO	CAUSAS	CONSEQUÊNCIAS	OBJETIVO VINCULADO
Indisponibilidade do sistema de agendamento online	Falha inesperada de um servidor principal	Impossibilidade dos cidadãos agendarem serviços pela internet	Facilitar o acesso aos serviços públicos
Perda de acesso ao banco de dados de informações dos cidadãos	Configuração incorreta realizada por um técnico	Impossibilidade de consultar dados cruciais para o atendimento e decisões	Fornecer informações precisas e suporte adequado aos cidadãos
Invasão não autorizada aos sistemas	Senhas Fracas ou Comprometidas Erros Humanos	Vazamento de dados sensíveis dos cidadãos Exposição de informações confidenciais do órgão	Proteger a privacidade e os dados dos usuários e a confidencialidade de informações do órgão

IDENTIFICANDO RISCOS

Para mostrar como identificamos um risco, usamos um dos exemplos da tabela anterior.
Veja a seguir a descrição completa:

Sintaxe para identificação

CAUSA

EVENTO DE RISCO ← Devido à **falha de um servidor principal**, poderá ocorrer a **indisponibilidade do sistema de agendamento online**, o que levará a **impossibilidade dos cidadãos agendarem serviços pela internet**, afetando o objetivo de **facilitar o acesso aos serviços públicos**. → CONSEQUÊNCIAS

OBJETIVO ESPECÍFICO

ANALISANDO RISCOS

Agora, para mostrar como a Análise Bow Tie (Gravata Borboleta) funciona na prática, usaremos como exemplo outro risco da nossa lista.

Análise Bow Tie (gravata borboleta)

4.1 ANALISANDO RISCOS

PROBABILIDADE x IMPACTO

EVENTO DE RISCO	PROBABILIDADE		IMPACTO		CATEGORIA DO IMPACTO/JUSTIFICATIVA	NÍVEL DE RISCO INERENTE
Indisponibilidade do sistema de agendamento online	Média	3	Médio	3	Agendar serviços fica impossível (**operacional**) e faz o órgão parecer ineficiente (**reputacional**)	9
Perda de acesso ao banco de dados de informações dos cidadãos	Baixa	2	Médio	3	Não conseguir acessar os dados para o trabalho para tudo (**operacional**), pode dar problemas com a lei (**legal**), faz a gente duvidar se os dados são confiáveis (**integridade**) e mostra que a gente não está cuidando bem dos dados pessoais	6
Invasão não autorizada aos sistemas	Alta	4	Muito Alto	5	Hackers atrapalham os sistemas (**operacional**), custam dinheiro (**financeiro**), queimam a imagem (**reputacional**), podem dar problemas na justiça (**legal**), bagunçam os dados (**integridade**), prejudicam nossos planos de segurança (**estratégico**) e colocam os dados das pessoas em risco (**cibernético, pessoal**)	20

ANALISANDO RISCOS

EVENTO DE RISCO	NÍVEL DE RISCO INERENTE	CONTROLE EXISTENTE			RISCO DE CONTROLE RC=1-NC	NÍVEL DE RISCO RESIDUAL NRR=NRI×RC
		DESCRIÇÃO	NÍVEL DE CONFIANÇA			
Indisponibilidade do sistema de agendamento online	9	Monitoramento manual e esporádico da disponibilidade do sistema	Fraco	0,2	0,8	7,2
Perda de acesso ao banco de dados de informações dos cidadãos	6	Backups regulares, mas controles de acesso e testes de restauração deficientes	Mediano	0,4	0,6	3,6
Invasão não autorizada aos sistemas	20	Antivírus instalado nas estações de trabalho, mas com atualizações irregulares	Fraco	0,2	0,8	16

AVALIANDO RISCOS

Comparação dos Níveis de Risco Residuais com a apetite a riscos hipotéticos do CSC.

Apetite a Riscos Hipotético da CSC

NR ≤ 04 : **Risco Baixo** Aceitável

05 < NR ≤ 10 : **Risco Médio** Tolerável

11 < NR ≤ 16 : **Risco Alto** Inaceitável

NR > 17 : **Risco Extremo** Inaceitável

EVENTO DE RISCO	NÍVEL DE RISCO RESIDUAL		OPÇÃO DE TRATAMENTO	
Indisponibilidade do sistema de agendamento online	7,2	Médio	Mitigar	Revisão e possível tratamento adicional
Perda de acesso ao banco de dados de informações dos cidadãos	3,6	Baixo	Aceitar	Monitoramento regular
Invasão não autorizada aos sistemas	16	Alto	Mitigar	Tratamento prioritário necessário

TRATANDO RISCOS

Plano de Tratamento (Plano de ação)

Risco Prioritário: **Invasão não autorizada aos sistemas**
Objetivo do Tratamento: Reduzir a probabilidade e o impacto do RISCO a um nível aceitável.

Prevenção (Redução da Probabilidade):

CAUSA	AÇÃO	RESPONSÁVEL	PRAZO
Senhas Fracas ou Comprometidas	Fortalecer as políticas de segurança de senhas (complexidade, troca periódica, não reutilização)	Setor de TI, Segurança da Informação	1 mês
Erros Humanos	Implementar um programa de treinamento em segurança da informação para todos os servidores	Setor de Recursos Humanos, Segurança da Informação, Comunicação	Programa inicial em 3 meses, campanhas trimestrais

Mitigação (Redução do Impacto)

CONSEQUÊNCIAS	AÇÃO	RESPONSÁVEL	PRAZO
Potencial vazamento de dados sensíveis dos cidadãos	implementar e executar o Plano de Resposta a Incidentes Cibernéticos, com foco nos procedimentos de contenção e avaliação de danos	Setor de TI, Segurança da Informação	Imediato
Exposição de informações confidenciais do órgão			

REFERÊNCIAS

BRASIL. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 31000: Gestão de Riscos: Diretrizes.** Rio de Janeiro, 2018. Disponível em: https://dintegcgcin.saude.gov.br/attachments/download/23/2018%20-%20Diretrizes%20-%20Gest%C3%A3o%20de%20Riscos_ABNT%20NBR%20ISO%2031000.pdf. Acesso em: 22 abr. 2025.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO). **Manual de Gestão de Riscos**. 2. ed. Brasília, DF: TCU, 2020. Disponível em: https://portal.tcu.gov.br/data/files/46/B3/C6/F4/97D647109EB62737F18818A8/Manual_gestao_riscos_TCU_2_edicao.pdf. Acesso em: 30 abr 2025.

DISTRITO FEDERAL. Controladoria-Geral do Distrito Federal. **Guia prático de Gerenciamento de Riscos Corporativos.** Brasília, DF: CGDF, [s.d.]. Disponível em: http://www.gestaoderiscos.cg.df.gov.br/. Acesso em: 29 abr. 2025.

PARÁ. Tribunal de Justiça do Estado do Pará. **Manual de Gestão de Riscos**. Belém: TJPA, 2024. Disponível em: https://www.tjpa.jus.br/CMSPortal/VisualizarArquivo?idArquivo=1523629. Acesso em: 24 abr. 2025.

PERNAMBUCO. Secretaria da Controladoria Geral do Estado de Pernambuco. **Cartilha de Estruturação e Implementação da Gestão de Riscos**. [S. l.]: SCGE-PE, 2022. Disponível em: https://conaci.org.br/noticias/scge-pe-lanca-guia-pratico-e-cartilha-sobre-gerenciamento-de-riscos/. Acesso em: 25 abr. 2025.

SÃO PAULO (Município). Controladoria Geral. **Manual de Gestão de Riscos da Controladoria Geral.** São Paulo: CGM, 2023. Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/Manual_Gestao_Riscos_versao01_2023_publicacao_03_01_2024.pdf. Acesso em: 23 abr. 2025.


CONTROLADORIA GERAL DO ESTADO DO PARÁ
GOVERNO DO
PARÁ
POR TODO O PARÁ