PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO TRT7.GP Nº 106, DE 16 DE JULHO DE 2018 (*)

~~Aprova a revisão da Norma Complementar de Gestão de Riscos de Segurança da Informação e Comunicações.~~

~~**O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO**, no uso de suas atribuições legais e regimentais,~~

~~**CONSIDERANDO** as boas práticas de Governança de TI que visam agarantir a disponibilidade e integridade de sistemas, aplicativos, dados e de documentos digitais do TRT da 7ª Região;~~

~~**CONSIDERANDO** a necessidade de implementar e melhorar os mecanismos de controle da gestão de risco de segurança da informação,~~

~~**RESOLVE:**~~

~~**Art. 1º** Aprovar a revisão "2" da Norma Complementar nº 04/POSIC, que dispõe sobre a gestão de riscos de segurança da informação e comunicações, na forma do anexo, para observância e aplicação em todo o Regional.~~

~~**Art. 2º** Fica revogado o Ato nº 230/2013.~~

~~**Art. 3º** Este ato entra em vigor na data de sua publicação.~~

~~**PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.**~~
~~Fortaleza, 16 de julho de 2018.~~
~~**PLAUTO CARNEIRO PORTO**~~
~~Presidente do Tribunal~~

(*) Revogado pelo Ato TRT7.GP Nº 111/2022, disponibilizado no Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 3490, 09 de junho de 2022. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 1.

(*) Anexo alterado pelo ATO TRT7.GP N° 42/2020 disponibilizado no Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2945, 31 mar. 2020. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 1.

Tribunal Regional do Trabalho da 7ª Região Secretaria de Tecnologia da Informação e Comunicação	Número da Norma Complementar	Revisão
	04/NC/POSIC	3
	Gestão de Riscos de Segurança da Informação	

REGINA LDO GARCIA DUPIM

JOAREZ DALLA GO

ORIGEM
NÚCLEO DE APOIO À GESTÃO DE TIC E SEGURANÇA DA INFORMAÇÃO - NGTIC
CAMPO DE APLICAÇÃO
Esta Norma Complementar se aplica ao âmbito do Tribunal Regional do Trabalho da 7ª Região.
SUMÁRIO
1. Objetivo **2.** Fundamento legal da Norma Complementar **3.** Conceitos e Definições **4.** Princípios **5.** Diretrizes **6.** Gestão de Risco em Segurança da Informação **7.** Procedimentos **8.** Responsabilidades **9.** Vigência e Revisão Anexo A Anexo B Anexo C Anexo D Anexo E
INFORMAÇÕES ADICIONAIS
Não há

APROVAÇÃO

1. OBJETIVO

1.1. Estabelecer as diretrizes da Gestão de Riscos relacionada ao ambiente tecnológico no âmbito deste Tribunal e definir o Processo de Gestão de Riscos de Segurança da Informação do Tribunal Regional do Trabalho da 7ª Região.

2. FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

2.1. **Decreto nº 3.505**, de 13 de junho de 2000, que "*Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal*";

2.2. Art. 10**,** da **Resolução nº 211**, de 15 de dezembro de 2015, do Conselho Nacional de Justiça, estabelece que "A estrutura organizacional, o quadro permanente de servidores, a gestão de ativos e os processos de gestão de trabalho da área de TIC de cada órgão, deverão estar adequados às melhores práticas preconizadas pelos padrões nacionais e internacionais para as atividades consideradas como estratégicas*";*

2.3. **Instrução Normativa GSI/PR nº 01,** do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que "*disciplina a Gestão de Segurança da Informação na Administração Pública Federal, direta e indireta, e dá outras providências*";

2.4. **Norma Complementar 04/IN01/DSIC/GSIPR,** do Gabinete de Segurança Institucional, de 14 de agosto de 2009, Gestão de Riscos de Segurança da Informação e Comunicação – GRSIC, que "*estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicação – GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF*";

2.5. **Norma ABNT NBR ISO/IEC 27002:2005,** que trata de Código de Pratica para a gestão da Segurança da Informação;

2.6. **Norma ABNT NBR ISO/IEC 27005:2011,** que trata de Gestão de riscos de segurança da Informação;

2.7. **Norma ABNT ISO Guia 73,** Gestão de riscos – Vocabulário;

2.8. **Norma ABNT NBR ISO 31000:2009,** Gestão de risco – Princípios e Diretrizes;

3. CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições, em adição aos definidos na Resolução TRT7 n. 278/2017:

3.1. **Ativos de Informação** – os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

3.2. **Comunicação do risco** – troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas.

3.3. **Estimativa de riscos** – processo utilizado para atribuir valores à probabilidade e consequências de um risco.

3.4. **Gestão de Riscos de Segurança da Informação (GRSI)** – conjunto de procedimentos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

3.5. **Gestores de Riscos** – São considerados gestores de riscos, em seus respectivos âmbitos e escopos de atuação, os Diretores, Secretários e Coordenadores responsáveis por (ou proprietários de) ativos de informação.

3.6. **Riscos de Segurança da Informação** – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

3.7. **Tratamento dos riscos** – processo e implementação de ações de Segurança da Informação para evitar, reduzir, reter ou transferir um risco.

4. PRINCÍPIOS

4.1. Os princípios a seguir devem ser atendidos em todos os níveis da organização do TRT da 7ª região para que a gestão de riscos seja eficaz. A Gestão de Riscos:

4.1.1. cria e protege valor;

4.1.2. é parte integrante de todos os processos organizacionais;

4.1.3. é parte da tomada de decisões;

4.1.4. aborda explicitamente a incerteza;

4.1.5. é sistemática, estruturada e oportuna;

4.1.6. baseia-se nas melhores informações disponíveis;

4.1.7. Está alinhada ao contexto e ao perfil de risco da instituição;

4.1.8. considera fatores humanos e culturais;

4.1.9. é transparente e inclusiva;

4.1.10. é dinâmica, iterativa e capaz de reagir a mudanças;

4.1.11. facilita a melhoria continua da organização.

4.2. O Processo de Gestão de Risco em Segurança da Informação (PGRSI) é contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação no âmbito do TRT da 7ª Região.

4.3. O PGRSI está alinhado ao modelo denominado PDCA (*Plan-Do-Check-Act*), conforme a ISO 27001 de modo a fomentar a melhoria contínua da Gestão de Risco.

4.4. A escolha da metodologia PDCA levou em consideração a simplicidade do modelo e adequação à necessidade da Gestão de Risco em melhorar continuamente.

4.5. A GRSI produzirá subsídios para suportar o Sistema de Gestão de Segurança da Informação (SGSI) e a Gestão de Continuidade de Negócios do TRT da 7ª Região.

4.6. A GRSI é abordada de forma sistemática, com o objetivo de manter os riscos em níveis aceitáveis.

5. DIRETRIZES

5.1. A Gestão de Riscos deve considerar as definições do Planejamento Estratégico Institucional e do Planejamento Estratégico de TI e estar alinhada à Política de Segurança da Informação deste Tribunal.

5.2. Os riscos devem ser analisados e avaliados em função de sua relevância para os principais processos de negócio deste Tribunal e devem ser tratados de forma a assegurar respostas efetivas.

5.3. O processo de Gestão de Riscos de Segurança da Informação visa identificar e implementar as medidas de proteção necessárias para tratar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.

5.4. A gestão e comunicação dos riscos dos serviços essenciais devem ser realizadas de forma prioritária e alinhadas a esta norma.

5.5. Os graus de probabilidade a serem considerados na análise de riscos são: muito baixo, baixo, médio, alto e muito alto

5.6. Os níveis de risco a serem considerados são: baixo, médio, alto e extremo.

5.7. As ações de tratamento de riscos terão os seguintes objetivos:

5.7.1. evitar o risco: não iniciando ou descontinuando a atividade que dá origem ao risco;

5.7.2. reduzir o risco: implantando controles que diminuam a probabilidade de ocorrência do risco ou suas consequências;

5.7.3. reter o risco: assumindo o risco, por escolha consciente e justificada;

5.7.4. transferir o risco: transferindo ou compartilhando o risco com outra parte interessada.

5.8. As ações de tratamento de que trata o item anterior são:

5.8.1. ações de implantação imediata: quando a avaliação de riscos realizada indicar risco extremo. Postergação de medidas só com autorização do Comitê Gestor de Segurança da Informação.

5.8.2. ações de implantação de curto prazo (em até seis meses): quando a avaliação de riscos realizada indicar risco alto. Postergação de medidas só com autorização do Comitê Gestor de Segurança da Informação.

5.8.3. ações de implantação de médio prazo (em até dois anos): quando a avaliação de riscos indicar risco médio. Geralmente nenhuma medida especial é necessária, exceto manter controles e respostas para manter o risco nesse nível.

5.8.4. ações de implantação não ocorrerão em avaliações de risco que indiquem riscos baixos, tendo em vista que são admitidos como riscos aceitáveis.

6. GESTÃO DE RISCO EM SEGURANÇA DA INFORMAÇÃO

6.1. A implantação do processo de Gestão de Riscos de Segurança da Informação busca identificar as necessidades deste Tribunal em relação aos requisitos de Segurança da Informação de TI, além de integrá-lo ao Sistema de Gestão de Segurança da Informação.

6.2. Níveis de Risco considera duas variáveis:

6.2.1. Probabilidade: estima a probabilidade de que ocorra um evento.

6.2.2. Severidade: impacto na organização caso ocorra o risco previsto.

6.3. Devem ser considerados na identificação do nível de risco e na priorização do tratamento, no mínimo, os seguintes critérios de avaliação:

6.3.1. o valor estratégico do processo.

6.3.2. a criticidade dos ativos

6.3.3. o histórico de ocorrência de eventos de segurança.

6.3.4. o valor do ativo para o processo.

6.3.5. a probabilidade de ocorrências.

6.4. Não obstante possam ser estabelecidos limites diferentes para partes específicas do escopo da Gestão de Riscos, os riscos classificados como "Baixo" são aceitos pela Presidência do TRT da 7ª Região.

6.4.1. A aceitação do risco, neste caso, não significa negligenciá-lo, mas reconhecer sua existência e acompanhá-lo, a fim de evitar a evolução do nível do risco ou o desencadeamento de outros riscos.

6.5. Os riscos não priorizados para tratamento serão geridos de acordo com as necessidades levantadas pelas partes interessadas, pelas regulamentações e legislações vigentes e pela análise custo/benefício.

6.6. O Núcleo de Apoio à Gestão de TIC e Segurança da Informação (NGTIC), em conjunto com a Secretaria de Tecnologia da Informação e Comunicação e o Comitê Gestor de Segurança da Informação, são os responsáveis por gerenciar e coordenar as atividades inerentes ao processo de Gestão de Riscos de Segurança da Informação, no âmbito do TRT da 7ª Região.

6.7. Cabe ao Comitê Gestor de Segurança da Informação aprovar formalmente os seguintes documentos: lista de prioridades, o documento de aceitação de riscos e o plano de tratamento de riscos.

7. PROCEDIMENTOS

O Processo de Gestão de Riscos de Segurança da Informação será abordado de forma sistemática, com o objetivo de manter os riscos em níveis aceitáveis. Esse processo é apresentado no **Anexo A** desta Norma.

8. RESPONSABILIDADES

8.1. Cabe à Presidência:

8.1.1. Analisar as deliberações do Comitê de Segurança da Informação sobre Gestão de Riscos de Segurança da Informação e decidir sobre possíveis providências.

8.1.2. Aprovar as Diretrizes Gerais e o Plano de Gestão de Risco de Segurança da Informação, observada, dentre outras, a respectiva Política de Segurança Institucional.

8.1.3. Formalizar a aceitação dos riscos baixos, médios, altos e extremos.

8.2. Cabe ao Comitê Gestor de Segurança da Informação:

8.2.1. Deliberar sobre as principais diretrizes e temas relacionados à Gestão de Riscos.

8.2.2. Monitorar e avaliar periodicamente a estrutura de Gestão de Riscos e o sistema de controles internos, assim como propor melhorias consideradas necessárias.

8.2.3. Atuar como instância consultiva da Administração do Tribunal nas questões relativas a riscos.

8.2.4. Aprovar formalmente a Metodologia de Gestão de Riscos e suas futuras revisões.

8.2.5. Aprovar os critérios de riscos do TRT (graus de impacto, graus de probabilidade e classificações de riscos).

8.2.6. Estabelecer e revisar o contexto do PGRSI para efeito do ciclo PDCA (Plan, Do, Check, Act).

8.2.7. Aprovar o documento "Processo de Gerenciamento de Riscos de Segurança da Informação", inclusive a metodologia de gerenciamento adotada e revisões futuras.

8.2.8. Monitorar e analisar periodicamente a implementação do Plano de Gestão de Riscos de Segurança da Informação juntamente com os Gestores de Risco.

8.3. Cabe ao Núcleo de Apoio à Gestão de TIC e Segurança da Informação:

8.3.1. Gerir e executar o Processo de Gestão de Riscos no TRT junto aos gestores dos riscos.

8.3.2. Acompanhar a execução dos planos de ação.

8.3.3. Disseminar cultura voltada para identificação e tratamento de riscos.

8.3.4. Desenvolver, testar e implementar a metodologia para mensuração e gestão dos riscos.

8.3.5. Consolidar as ocorrências e os riscos informados pelos gestores por meio de relatórios periódicos direcionados à Administração do Tribunal Regional do Trabalho da 7ª Região.

8.3.6. Subsidiar o Comitê Gestor de Segurança da Informação com informações pertinentes à estrutura de gestão de riscos de segurança da informação.

8.3.7. Fornecer consultoria interna em Gestão de Riscos.

8.3.8. Gerenciar as atividades com elaboração sistemática de relatórios para a Secretaria de TI, cujo conteúdo constará a análise quanto à aceitação dos resultados obtidos, e consequente proposição de ajustes e de medidas preventivas e proativas à Presidência.

8.4. Cabe aos Gestores de Risco:

8.4.1. Monitorar e gerenciar os Riscos de Segurança da Informação dos ativos sob sua responsabilidade, de forma a mantê-los em um nível de exposição aceitável.

8.4.2. Comunicar ao Setor de Segurança da Informação os ativos e Riscos de Segurança da Informação, sejam eles novos, modificados ou não identificados anteriormente.

8.4.3. Definir, juntamente com Chefe de Segurança da Informação, os planos de ação e controles necessários para o tratamento dos riscos.

8.4.4. Assegurar a implementação das ações e dos controles definidos para tratamento dos riscos de ativos sob sua responsabilidade.

8.4.5. Os gestores de riscos deverão, no âmbito de suas unidades, designar servidores responsáveis por contribuir nas atividades de identificação, avaliação e tratamento dos riscos inerentes aos ativos de informação e por implementar os planos de ação definidos para tratamento dos riscos.

8.5. Cabe à Secretaria de Tecnologia da Informação e Comunicação:

8.5.1. No âmbito de suas atribuições, é responsável pela coordenação da Gestão de Riscos de Segurança da Informação no TRT.

9. VIGÊNCIA E REVISÃO

9.1. Esta norma deverá ser revisada e atualizada periodicamente, no máximo, a cada três anos.

9.2. Esta Norma Complementar entra em vigor na data de sua publicação.

ANEXO A

PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Índice

1. INTRODUÇÃO....13
2. PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO....14
2.1. Definir o contexto....16
2.1.1. Escala de probabilidades....16
2.1.2. Escala de impactos....16
2.1.3. Matriz "Probabilidade x Impacto" e Níveis de risco....16
2.1.4. Escala para avaliação de controles....16
2.2. Analisar e Avaliar os riscos....17
2.2.1. Identificar os riscos....18
2.2.1.2. Identificar as ameaças e suas fontes....19
2.2.1.3. Identificar as ações de Segurança da Informação já adotadas (controles existentes e planejados)....19
2.2.1.4. Identificar as vulnerabilidades existentes nos ativos....19
2.2.1.5. Identificar as consequências, caso os riscos se concretizem....19
2.2.2. Analisar os riscos....20
2.2.2.1. Avaliar as consequências....20
2.2.2.2. Avaliar a probabilidade dos incidentes....21
2.2.2.3. Estimar o nível do risco....21
2.2.3. Avaliar os riscos....21
2.3. Tratar os riscos....22
2.3.1. Reduzir o risco....23
2.3.2. Reter o risco....23
2.3.3. Evitar o risco....23
2.3.4. Transferir o risco....23
2.4. Aceitar os riscos....24
2.5. Implementar o Plano de Tratamento de Riscos....25
2.6. Monitorar os riscos....25
2.7. Analisar Criticamente os riscos....26
2.8. Melhorar o Processo de Gestão de Riscos de Segurança da Informação....27
2.9. Comunicação do Risco....27

1. INTRODUÇÃO

O constante tratamento de informações necessárias aos trabalhos no TRT da 7ª Região contém riscos inerentes e é preciso conhecê-los para decidir quais deles são aceitáveis e quais necessitam de controles especiais.

Desse modo, a Gestão de Riscos de Segurança da Informação, que é um dos processos do Sistema de Gestão de Segurança da Informação(SGSI), objetiva-se a dotar o Tribunal de ferramenta eficaz no intuito de minimizar os riscos das principais atividades desenvolvidas pela Secretaria de Tecnologia da Informação e Comunicação (SETIC) e, assim, dar maior segurança a todos que usam seus serviços (público interno e externo).

Segundo a norma ABNT NBR ISO/IEC 27005:2011, convém que a gestão de riscos de segurança da informação seja um processo contínuo que defina o contexto interno e externo, além de avaliar e tratar os riscos usando um plano de tratamento a fim de implementar as recomendações e decisões.

Algumas contribuições do Processo de Gestão de Riscos de Segurança da Informação:

- Identificação de riscos;
- Processo de avaliação de riscos em função das consequências ao Tribunal e da probabilidade de sua ocorrência;
- Comunicação e entendimento da probabilidade e das consequências destes riscos;
- Estabelecimento da ordem prioritária para tratamento do risco;
- Priorização das ações para reduzir a ocorrência dos riscos;
- Envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e mantidas informadas sobre a situação da gestão de riscos;
- Eficácia do monitoramento do tratamento do risco;
- Monitoramento e a análise crítica periódica dos riscos e do processo de gestão de riscos;
- Coleta de informações de forma a melhorar a abordagem da gestão de riscos;

- Treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los.

2. PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O Processo de Gestão de Riscos de Segurança da Informação do TRT da 7ª Região está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2011, ANBT NBR ISO/IEC 31000:2009, Norma Complementar 04/IN01/DSIC/GSIPR, Manual de Auditoria Operacional do TCU, Política de Gestão de Riscos aprovada pelo Tribunal Superior do Trabalho (Ato 131/2015 TST.ASGE.SEGP.GP, publicado no DEJT em 13/3/2015) e consiste nas seguintes etapas:

- Definir o contexto;
- Analisar e avaliar os riscos;
- Tratar os riscos;
- Aceitar os riscos;
- Implementar o Plano de Tratamento de Riscos;
- Monitorar os riscos;
- Analisar criticamente os riscos;
- Melhorar o Processo de Gestão de Riscos de Seguração da Informação.

Tribunal Regional do Trabalho da 7ª Região Secretaria de Tecnologia da Informação e Comunicação	Número da Norma Complementar	Revisão
	04/NC/SETIC	3
	Gestão de Riscos de Segurança da Informação	

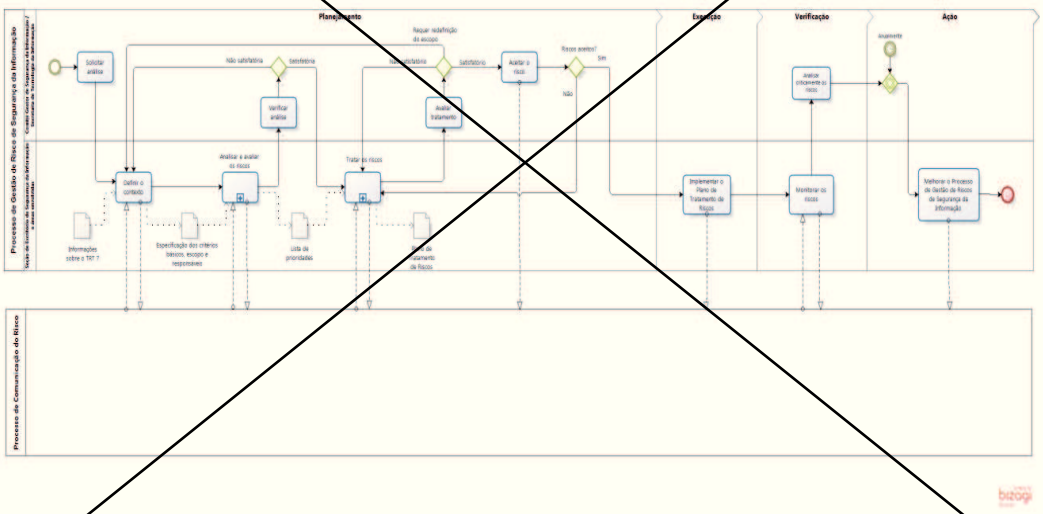


Figura 1: Processo de Gestão de Riscos de Segurança da Informação do TRT da 7ª Região.

2.1. Definir o contexto

O processo é iniciado com a solicitação de análise por parte do Comitê Gestor de Segurança da Informação ou da Secretaria de Tecnologia da Informação. Essa análise pode ser, por exemplo, de um requisito de conformidade ou de um ambiente.

Feito isto, a etapa de definição do contexto define os parâmetros internos e externos, critérios básicos necessários para a GRSI, escopo e limites, visando estruturar o Plano de Gestão de Riscos de Segurança da Informação.

A definição dos critérios básicos dependerá das características do Tribunal e das restrições a que está sujeito. Entre esses, podem ser citados:

2.1.1. Escala de probabilidades

Define como a probabilidade será medida. Essa escala é apresentada no **Anexo B** desta norma;

2.1.2. Escala de impactos

Define a natureza e o tipo de consequências, e como serão medidas nas diversas áreas de objetivo impactadas. Essa escala é apresentada no **Anexo C** desta norma;

2.1.3. Matriz "Probabilidade x Impacto" e Níveis de risco

Define como o nível de risco deve ser determinado. Essa matriz é apresentada no **Anexo D** desta norma;

2.1.4. Escala para avaliação de controles

Define critérios objetivos para análise dos controles implementados e para cálculo do risco residual. Essa escala é apresentada no **Anexo E** desta norma.

O escopo de aplicação da Gestão de Riscos de Segurança da Informação pode abranger o TRT da 7ª Região como um todo, um segmento, um processo, um sistema,

um recurso ou um ativo de informação. É recomendado que sejam considerados prioritariamente os principais serviços que suportam os processos de negócio do TRT da 7ª Região.

Definir o contexto	
Objetivo:	Definir o escopo e os limites que limitarão a execução do Processo de Gestão de Riscos de Segurança da Informação.
Responsável:	NGTIC e Áreas envolvidas.
Entrada:	Todas as informações sobre a organização relevantes para a definição do contexto.
Ação:	- Definir critérios de avaliação, impacto e aceitação de riscos; - Definir escopo e limites; - Estabelecer responsabilidades para a manutenção do processo.
Saída:	Especificação do contexto: critérios básicos e definição de escopo, limites e responsáveis pelo processo.

2.2. Analisar e Avaliar os riscos

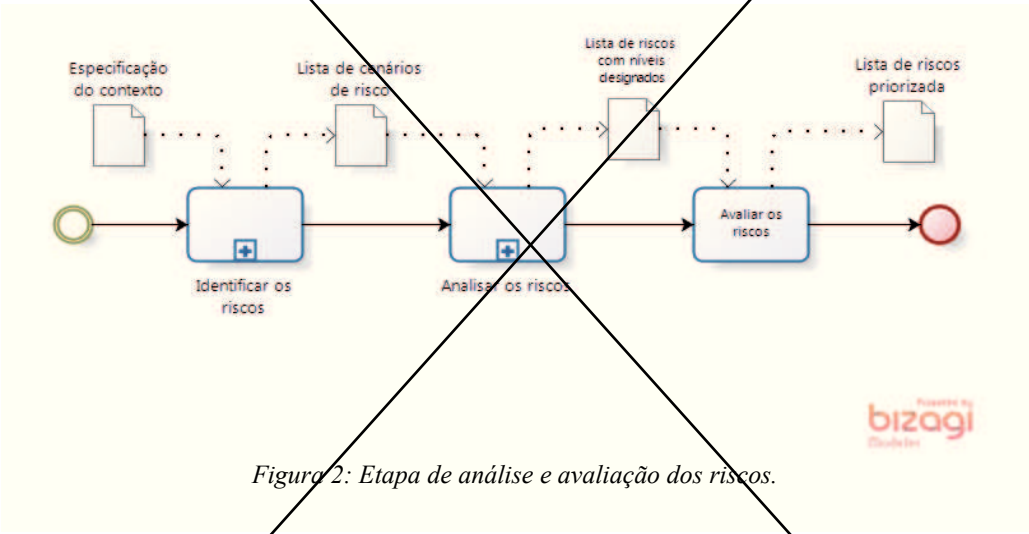


Figura 2: Etapa de análise e avaliação dos riscos.

Essa etapa determina o valor dos ativos de informação e identifica as ameaças e vulnerabilidades que podem existir, além de identificar os controles que já existem e seus efeitos nos riscos detectados. Também determina as consequências de possíveis concretizações dos riscos para, em seguida, estimar os níveis de riscos de modo que eles sejam avaliados e priorizados.

O subprocesso de Analisar e Avaliar os riscos consiste nas seguintes atividades:

2.2.1. Identificar os riscos

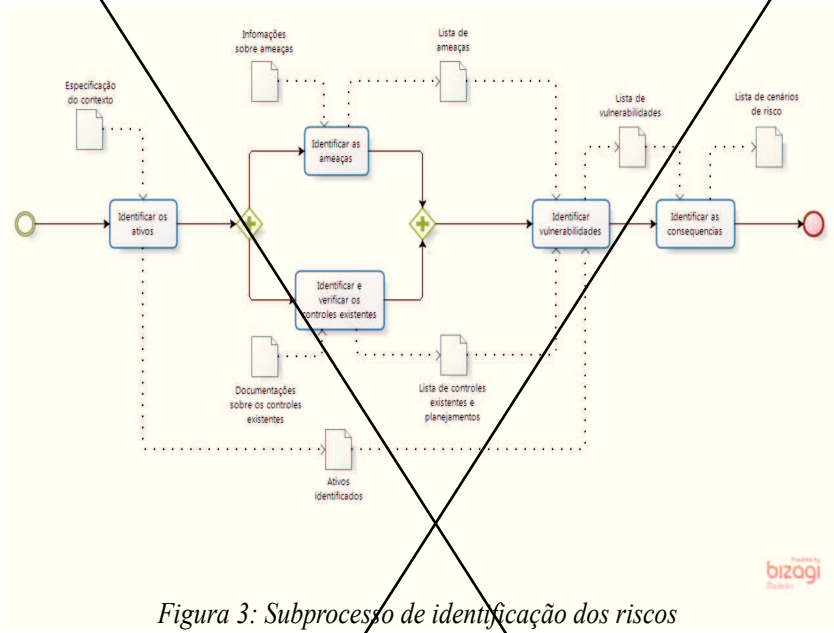


Figura 3: Subprocesso de identificação dos riscos

Esse subprocesso determina os eventos que podem causar perda potencial e determina como, onde e por que a perda pode acontecer. A identificação dos riscos é formada pelas seguintes atividades:

2.2.1.1. Identificar os ativos e seus respectivos responsáveis dentro do escopo estabelecido

O nível de detalhe dessa etapa influenciará na quantidade geral de informações reunidas durante o subprocesso de Análise e Avaliação dos Riscos.

2.2.1.2. Identificar as ameaças e suas fontes

É necessário cautela ao usar catálogos de ameaças, pois estas estão sempre mudando de acordo com o ambiente ou sistemas de informações.

2.2.1.3. Identificar as ações de Segurança da Informação já adotadas (controles existentes e planejados)

Essa etapa é importante para evitar custos e trabalho desnecessários, tais como duplicação de controles.

2.2.1.4. Identificar as vulnerabilidades existentes nos ativos

Mesmos as vulnerabilidades que não tem uma ameaça correspondente devem ser identificadas e monitoradas, no caso de haver mudanças.

2.2.1.5. Identificar as consequências, caso os riscos se concretizem

O impacto dessas falhas de segurança é determinado considerando os critérios de impacto definidos durante a etapa de definições do contexto.

Identificar os riscos	
Objetivo:	Definir eventos que possam causar perda potencial e deixar claro como, onde e por que a perda pode acontecer.
Responsável:	NGTIC e áreas envolvidas.
Entrada:	Especificações do contexto, tais como: escopo e limites para o processo de avaliação de riscos a ser executado; lista de componentes com responsáveis.
Ação:	- Identificar os ativos dentro do escopo estabelecido; - Identificar as ameaças e suas fontes; - Identificar os controles existentes e os planejados; - Identificar as vulnerabilidades que podem ser exploradas por ameaças; para comprometer os ativos ou a organização; - Identificar as consequências que a perda de confiabilidade, de integridade e de disponibilidade podem ter sobre os ativos.
Saída:	Lista de cenários de incidentes com suas consequências associadas aos ativos e processos do negócio.

2.2.2. Analisar os riscos

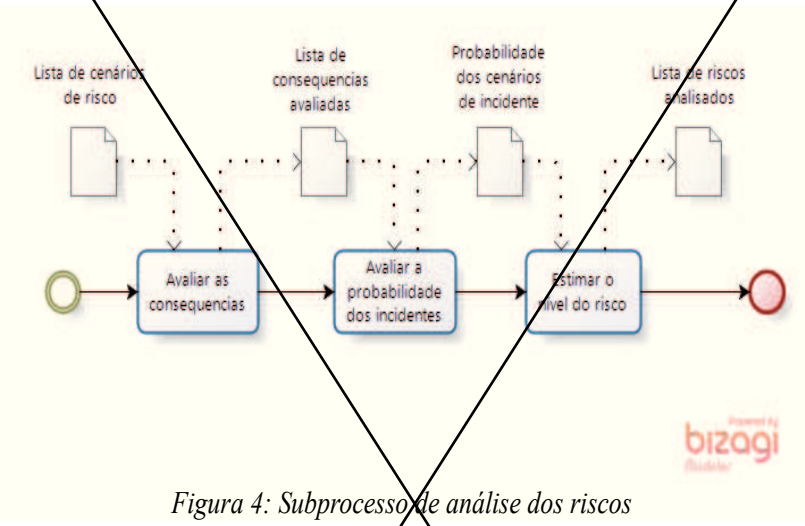


Figura 4: Subprocesso de análise dos riscos

Esse subprocesso descreve a magnitude das consequências potenciais e a probabilidade delas ocorrerem. A análise dos riscos pode ser qualitativa (exemplo: pequena, média e grande) ou quantitativa (valores numéricos), formada pelas seguintes etapas:

2.2.2.1. Avaliar as consequências

Podem ser expressas em função dos critérios monetários, técnicos ou humanos de impacto ou de outro critério relevante para o Tribunal.

2.2.2.2. Avaliar a probabilidade dos incidentes

Esta avaliação leva em conta a frequência da ocorrência das ameaças e a facilidade com que as vulnerabilidades podem ser exploradas.

2.2.2.3. Estimar o nível do risco

O risco estimado é uma combinação da probabilidade de um cenário de incidentes e suas consequências.

Analisar os riscos	
Objetivo:	Atribuir valores aos ativos, ameaças, vulnerabilidades e consequências a fim de ordenar os riscos por prioridade, permitindo tratá-los de acordo com sua urgência e criticidade.
Responsável:	NGTIC e áreas envolvidas.
Entrada:	Lista de cenários de incidentes identificados como relevantes, identificação das ameaças, vulnerabilidades, ativos afetados e consequências para os ativos e processos de negócio.
Ação:	- Avaliar o impacto que pode ser causado por possíveis incidentes relacionados à segurança da informação; - Avaliar a probabilidade dos cenários de incidentes; - Estimar os níveis de riscos para todos os cenários de incidentes considerados relevantes.
Saída:	Lista de riscos com níveis de valores definidos.

2.2.3. Avaliar os riscos

Essa atividade compara os níveis de riscos, priorizando-os de acordo com os critérios de avaliação e aceitação decididos na etapa de definições do contexto, além de requisitos contratuais, legais e regulatórios.

Ao final, é realizada uma atividade de verificação pelo Comitê Gestor de Segurança da Informação. Se a avaliação dos riscos for considerada insatisfatória, os trabalhos retornam para a fase de Definir o contexto para um maior aprofundamento. Caso seja considerada satisfatória, o trabalho segue para a fase de Tratar os riscos.

Avaliar os riscos	
Objetivo:	Priorizar os riscos de acordo com os níveis de riscos, com os critérios de avaliação e aceitação e com requisitos contratuais, legais e regulatórios.
Responsável:	NGTIC e áreas envolvidas.
Entrada:	Lista de riscos com níveis de valores designados e critérios para avaliação

	de riscos.
Ação:	- Comparar o nível dos riscos com os critérios de avaliação de riscos e com os critérios para a aceitação do risco.
Saída:	Lista de riscos priorizada, de acordo com os critérios de avaliação, em relação aos cenários de incidentes que podem levar a esses riscos.

2.3. Tratar os riscos

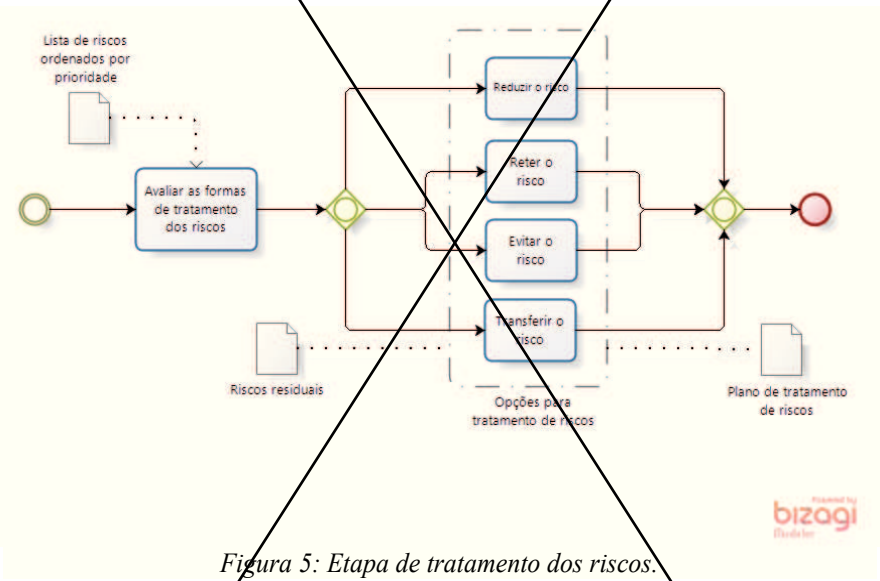


Figura 5: Etapa de tratamento dos riscos.

Essa etapa determina as formas de tratamento dos riscos, selecionadas com base no resultado do processo de avaliação de riscos; no custo esperado para implantação e nos benefícios previstos; nas restrições organizacionais, técnicas e estruturais e nos requisitos legais, considerando quatro opções que não são mutuamente exclusivas e podem ser combinadas, a fim de reduzir as consequências adversas ao mínimo possível:

2.3.1. Reduzir o risco

Implementa um ou mais tipos de proteção para minimizar o risco, tais como: correção, eliminação, prevenção, minimização do impacto, dissuasão, detecção, recuperação, monitoramento e conscientização.

2.3.2. Reter o risco

Não implementa controles adicionais (aceitar o ônus do risco) desde que este atenda aos critérios de aceitação.

2.3.3. Evitar o risco

Evitar que a atividade ou condição que dá origem ao risco seja evitada completamente, seja através de eliminação de uma determinada atividade (planejada ou existente), seja através de mudanças nas condições em que a operação da atividade ocorra.

2.3.4. Transferir o risco

Compartilha o risco com entidades externas, tais como seguros ou parceiros subcontratados, que possam gerenciá-lo de forma mais eficaz, dependendo da avaliação de riscos.

Tratar os riscos	
Objetivo:	Selecionar os controles para modificar, reter, evitar ou compartilhar os riscos e definir o Plano de Tratamento de riscos.
Responsável:	NGTIC e áreas envolvidas.
Entrada:	Lista de riscos priorizada, de acordo com os critérios de avaliação, em relação aos cenários de incidentes que podem levar a esses riscos.
Ação:	- Para cada risco, selecionar a forma de tratamento de acordo com as seguintes opções: – Reduzir o risco – Reter o risco

	– Evitar o risco – Transferir o risco
Saída:	Plano de Tratamento de Riscos e riscos residuais.

2.4. Aceitar os riscos

Análise crítica por parte do Comitê Gestor de Segurança da Informação, afim de aprovar, se for o caso, o plano de tratamento de riscos e os riscos residuais resultantes ou submetê-lo à nova avaliação.

As atitudes perante os riscos (condições associadas à aprovação ou não) devem ser registradas, além da responsabilidade pela decisão.

Aceitar os riscos	
Objetivo:	Aprovar o Plano de Tratamento de Riscos e os riscos residuais resultantes ou submetê-los à nova avaliação.
Responsável:	Comitê Gestor de Segurança da Informação / Secretaria de Tecnologia da Informação
Entrada:	Plano de Tratamento de Riscos e riscos residuais.
Ação:	- Aceitar ou recusar formalmente o Plano de Tratamento de Riscos e os riscos residuais resultantes.
Saída:	Lista de ricos aceitos e recusados com justificativa para aqueles que não satisfazem os critérios definidos.

2.5. Implementar o Plano de Tratamento de Riscos

Executa as ações de Segurança da Informação incluídas no Plano de Tratamento de Riscos aprovado.

Implementar o Plano de Tratamento de Riscos

Objetivo:	Executar e implementar as ações contidas no Plano aprovado após a aceitação dos riscos.
Responsável:	NGTIC e áreas envolvidas.
Entrada:	Plano de Tratamento de Riscos e riscos residuais.
Ação:	- Executar o Plano de Tratamento de Riscos.
Saída:	Lista de riscos gerenciados com controles associados.

2.6. Monitorar os riscos

Manter o Processo de Gestão de Riscos de Segurança da Informação alinhado às diretrizes gerais estabelecidas e às necessidades do TRT da 7ª Região, além de detectar possíveis falhas nos resultados, monitorar continuamente os riscos e as ações de Segurança da Informação, a fim de verificar regularmente, no mínimo, as mudanças:

- nos critérios de avaliação e aceitação dos riscos;
- no ambiente;
- nos ativos de informação;
- nas ações de Segurança da Informação – SIC;
- nos fatores do risco (ameaça, vulnerabilidade, probabilidade e impacto).

Monitorar os riscos	
Objetivo:	Monitorar os riscos levantados e detectar possíveis falhas nos resultados, nos controles implementados e na eficácia da GRSI.
Responsável:	NGTIC e áreas envolvidas.
Entrada:	Lista de ricos gerenciados com controles associados.

Ação:	- Monitorar os riscos; - Monitorar o processo de GRSI.
Saída:	Lista de riscos monitorados.

2.7. Analisar Criticamente os riscos

Verifica a eficácia do processo de Gestão de Riscos de Segurança da Informação e avalia, separadamente e/ou em conjunto, se riscos pequenos e aceitáveis não foram ampliados precisando, assim, serem tratados ou se ocorreu alguma mudança significativa que afete a organização.

Analisar criticamente os riscos	
Objetivo:	Avaliar, periodicamente ou em resposta a um fato específico, indicadores, resultados e mudanças no contexto.
Responsável:	Comitê Gestor de Segurança da Informação.
Entrada:	Informações sobre os riscos gerenciados, controles associados, indicadores e resultados.
Ação:	- Realizar reuniões periódicas do Comitê Gestor de Segurança da Informação para avaliar: – Eventos; – Resultados de indicadores; – Mudanças no contexto (interno e externo); – Resultados com a implantação dos controles; – Riscos emergentes que poderão surgir após o processo de análise crítica.
Saída:	Atas de reunião de análise crítica e lista de recomendações de melhoria do Processo de GRSI.

2.8. Melhorar o Processo de Gestão de Riscos de Segurança da Informação

Revisa o processo a cada três anos e, se for o caso, encaminha proposição ao Comitê Gestor de Segurança da Informação a fim de implementar as melhorias identificadas durante a fase de monitoramento e análise crítica, além de executar ações

corretivas ou preventivas aprovadas e garantir que as melhorias atinjam os objetivos pretendidos.

Melhorar o Processo de Gestão de Riscos de Segurança da Informação	
Objetivo:	Atingir resultados cada vez melhores no Processo de Gestão de Riscos de Segurança da Informação.
Responsável:	NGTIC e áreas envolvidas.
Entrada:	Informações gerais sobre o processo de GRSI.
Ação:	- Revisar o processo; - Encaminhar proposições; - Executar ações corretivas e preventivas.
Saída:	Proposições de melhorias no processo.

2.9. Comunicação do Risco

Mantém as instâncias superiores informadas a respeito de todas as fases do Processo de Gestão de Riscos de Segurança da Informação, tornando as informações disponíveis.

Esta etapa usa o Processo de Comunicação da Secretaria de Tecnologia da Informação vigente.

Anexo B – Escala de probabilidades

Escala de probabilidades

Exemplo Qualitativo

Descritor	Descrição	Nível
Muito Baixa	Evento extraordinário para os padrões conhecidos da gestão e operação do processo. Embora possa assumir dimensão estratégica para a manutenção do processo, não há histórico disponível de sua ocorrência...	1
Baixa	Evento casual, inesperado. Muito embora raro, há histórico conhecido de sua de ocorrência por parte dos principais gestores e operadores do processo...	2
Média	Evento esperado, que se reproduz com frequência reduzida, porém constante. Seu histórico de ocorrência é de conhecimento da maioria dos gestores e operadores do processo...	3
Alta	Evento usual, corriqueiro. Devido à sua ocorrência habitual ou conhecida em uma dezena ou mais de casos, aproximadamente, seu histórico é amplamente conhecido por parte de gestores e operadores do processo...	4
Muito Alta	Evento se reproduz muitas vezes, se repete seguidamente, de maneira assidua, numerosa e, não raro, de modo acelerado. Interfere de modo claro no ritmo das atividades, sendo evidente para os que conhecem o processo...	5

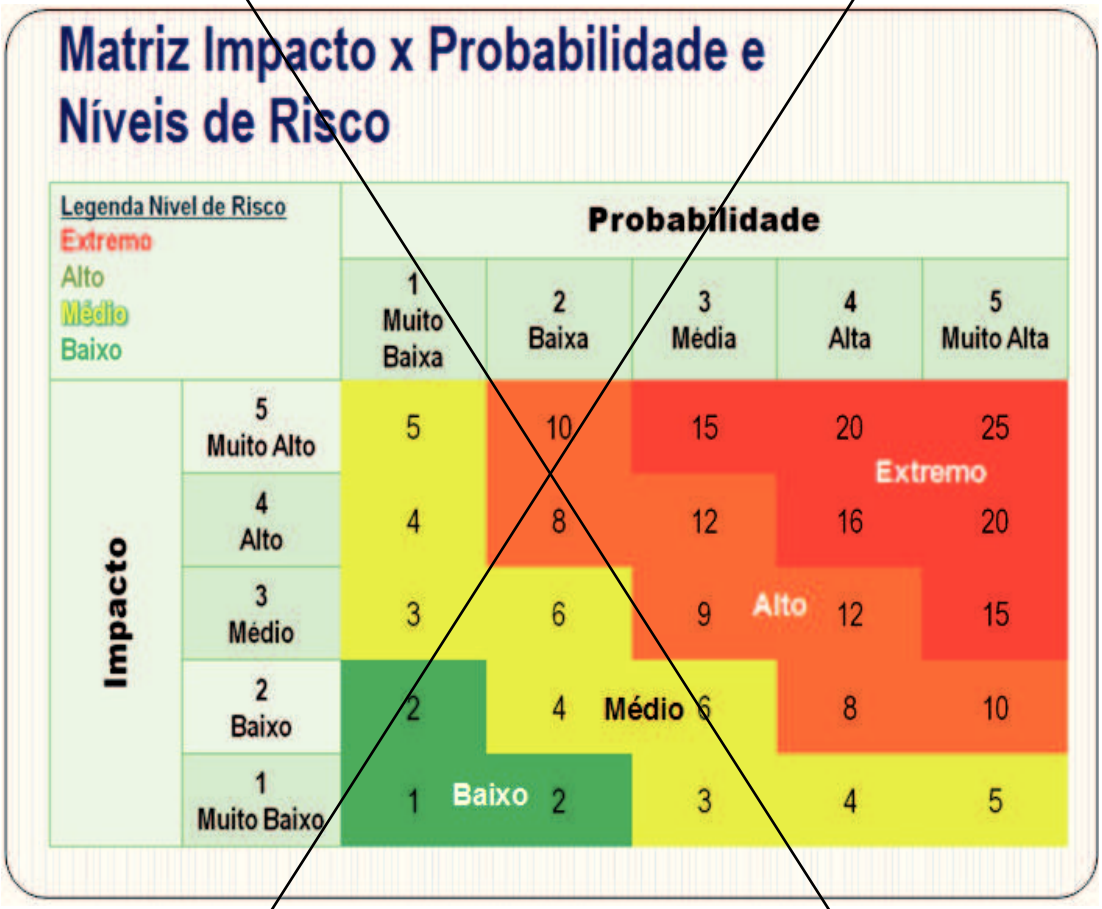
Anexo C – Escala de Impactos

Escala de Impactos

Exemplo qualitativo

Descritor	Descrição	Nível
Muito Baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, porém causando impactos mínimos nos objetivos de prazo, custo, qualidade, escopo, imagem ou relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interassadas (clientes internos/externos, beneficiários).	1
Baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, causando impactos pequenos nos objetivos...	2
Médio	Interrupção de operações ou atividades de processos, projetos ou programas, causando impactos significativos nos objetivos..., porém recuperáveis.	3
Alto	Interrupção de operações ou atividades de processos, projetos ou programas da organização, causando impactos de reversão muito difícil nos objetivos...	4
Muito Alto	Paralisação de operações ou atividades de processos, projetos ou programas da organização, causando impactos irreversíveis nos objetivos...	5

Anexo D – Matriz "Probabilidade x Impacto" e Níveis de risco



Anexo E – Escala para avaliação de Controles

Escala para avaliação de Controles

Situação do controle existente	Avaliação	Multiplicador do Risco Inerente
Ausência completa de controle.	1 - Inexistente	1,00
Controle depositado na esfera de conhecimento pessoal dos operadores do processo, em geral realizado de maneira manual.	2 - Fraco	0,80
Controle pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.	3 - Mediano	0,60
Controle normatizado e embora passível de aperfeiçoamento, está sustentada por ferramentas adequadas e mitiga o risco razoavelmente.	4 - Satisfatório	0,40
Controle mitiga o risco associado em todos os aspectos relevantes, podendo ser enquadrada num nível de "melhor prática".	5 - Forte	0,20