PORTARIA TRT 18ª SGP/CSIN Nº 796/2024

PODER JUDICIÁRIO DA UNIÃO
TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO
SECRETARIA-GERAL DA PRESIDÊNCIA
COORDENADORIA DE SEGURANÇA DA INFORMAÇÃO

**** Texto compilado até as alterações promovidas pela Portaria GP/CSIN nº 2676/2024***

Institui o Processo de Gestão de Riscos de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 18ª Região.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO, no uso de suas atribuições legais e regimentais, tendo em vista o que consta do Processo Administrativo-Proad nº 23891/2023,

CONSIDERANDO a Resolução Administrativa TRT 18ª nº 145/2019, que institui a Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região;

CONSIDERANDO a Resolução Administrativa TRT 18ª nº 78/2019, que institui a Política de Gestão de Riscos do Tribunal Regional do Trabalho da 18ª Região;

CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Portaria CNJ nº 162/2021, que aprova Protocolos e Manuais criados pela ENSEC-PJ, em especial o anexo V, itens 11 a 21;

CONSIDERANDO a recomendação de auditoria do CSJT quanto à revisão do Processo de Gestão de Riscos de Segurança da Informação, que consta do Processo Administrativo-Sisdoc nº 10659/2022,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Portaria institui o processo de Gestão de Riscos de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 18ª Região.

§1º Aplica-se o disposto nesta Portaria aos ativos de informação sob gestão do Regional, nas seguintes ocasiões:

I - quando do estabelecimento ou da revisão de programa de segurança da informação e ou de Sistema de Gestão de Segurança da Informação do órgão;

II - anualmente, concomitantemente ao levantamento do grau de maturidade na adoção do “Manual para Proteção de Infraestruturas Críticas de TIC” do CNJ de que trata a Portaria TRT 18ª Região SGP/CSIN nº 3358/2022;

III - no suporte à gestão de incidentes de segurança da informação, gestão de continuidade de serviços essenciais de TIC, gestão de projetos e gestão de mudanças que envolvam ativos de informação.

§2º A gestão de riscos de segurança da informação em processos de trabalho, projetos e ações segue as orientações e determinações do respectivo processo e método estabelecidos em âmbito corporativo.

Art. 2º Para os fins desta Portaria, consideram-se as definições constantes do anexo VIII (Glossário) da Portaria CNJ nº 162/2021 e, no que couber, os Termos e Definições constantes no Anexo ao Plano de Gestão de Riscos do TRT da 18ª Região, Portaria TRT 18ª GP/SGGOVE nº 256/2022.

CAPÍTULO II
DO ALINHAMENTO

Art. 3º Este processo observa as diretrizes e os princípios estabelecidos na Política de Gestão de Riscos do TRT da 18ª Região e, no que couber, os princípios, diretrizes e objetivos sugeridos nos itens 12 a 14 do Anexo V à

Portaria CNJ nº 162/2021.

Art. 4º Para efeito de alinhamento com os regulamentos internos e externos sobre gestão de riscos e com a adoção dos manuais de referência do CNJ, conforme Portaria TRT 18ª Região SGP/CSIN nº 3358/2022, em especial com o Manual para Proteção de Infraestruturas Críticas de TIC, este Regional adapta e aplica o método e as ferramentas de apoio CIS - RAM para a gestão de riscos de segurança da informação em ativos.

CAPÍTULO III
DAS RESPONSABILIDADES

Art. 5º A unidade de gestão de segurança da informação gerencia este processo e fornece orientações acerca das atividades atribuídas aos gestores de riscos e demais envolvidos.

Art. 6º Os titulares das unidades responsáveis pelo ciclo de vida de ativos de informação são responsáveis pela gestão dos riscos associados a tais ativos.

Art. 7º Os membros de grupos gestores técnicos de ativos contribuem para as atividades de identificação, avaliação de riscos, proposição e implementação de planos de tratamento, comunicação de novos riscos e monitoramento de riscos já conhecidos.

CAPÍTULO IV
DO PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 8º O processo de gestão de riscos de segurança da informação em ativos do TRT da 18ª Região compreende as seguintes fases:

I - comunicação e consulta: consiste na manutenção de fluxo regular e constante de informações com as partes interessadas, durante todas as fases do processo de gestão de riscos;

II - estabelecimento do escopo, contexto e critérios: diz respeito à definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos (contexto) e ao estabelecimento do escopo e dos critérios de risco;

III - identificação de riscos: consiste na busca, reconhecimento e descrição de riscos, considerando-se:

a) os ativos e/ou classes de ativos incluídos no escopo de execução deste processo e suas respectivas vulnerabilidades;

b) as ameaças associadas às medidas de segurança recomendadas para a proteção de infraestruturas críticas de TIC, conforme anexo I da Portaria TRT 18ª Região SGP/CSIN nº 3358/2022;

IV - análise de riscos: refere-se à compreensão da natureza do risco e à determinação do respectivo nível de risco mediante a combinação da probabilidade (ou expectativa) de sua ocorrência e dos impactos possíveis;

V - avaliação de riscos: trata-se da comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional;

VI - tratamento dos riscos: consiste na seleção e implementação de opções para tratar riscos;

VII - monitoramento e análise crítica: trata-se do monitoramento e análise crítica em todas as fases do processo, a fim de assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo;

VIII - registro e relato: trata-se da documentação do processo de gestão de riscos de segurança da informação em ativos e de seus resultados e da apresentação de relatórios às partes interessadas, auxiliando as instâncias internas e externas de governança a cumprirem suas responsabilidades.

§1º O fluxo do presente processo de gestão de riscos de segurança da informação, em sua versão 1.1, e respectivos procedimentos são descritos no Anexo I a esta Portaria. (***Parágrafo alterado pela Portaria TRT 18ª GP/CSIN nº 2676/2024***)

§2º Eventuais conflitos de atuação decorrentes do processo de gestão de riscos de segurança da informação em ativos serão dirimidos pelo Subcomitê de Riscos.

CAPÍTULO V
DA DISPOSIÇÃO FINAL

Art.9º A presente Portaria substitui o conteúdo referenciado por outros atos normativos como documento “NO08 - Gestão de Riscos de Segurança da Informação”.

Art. 10. Esta Portaria entra em vigor na data de sua publicação, revogando-se a Portaria GP/SGGOVE nº 3895/2019.

Publique-se no Diário Eletrônico da Justiça do Trabalho.

(assinado eletronicamente)
GERALDO RODRIGES DO NASCIMENTO
Desembargador-Presidente
TRT da 18ª Região

Anexo I

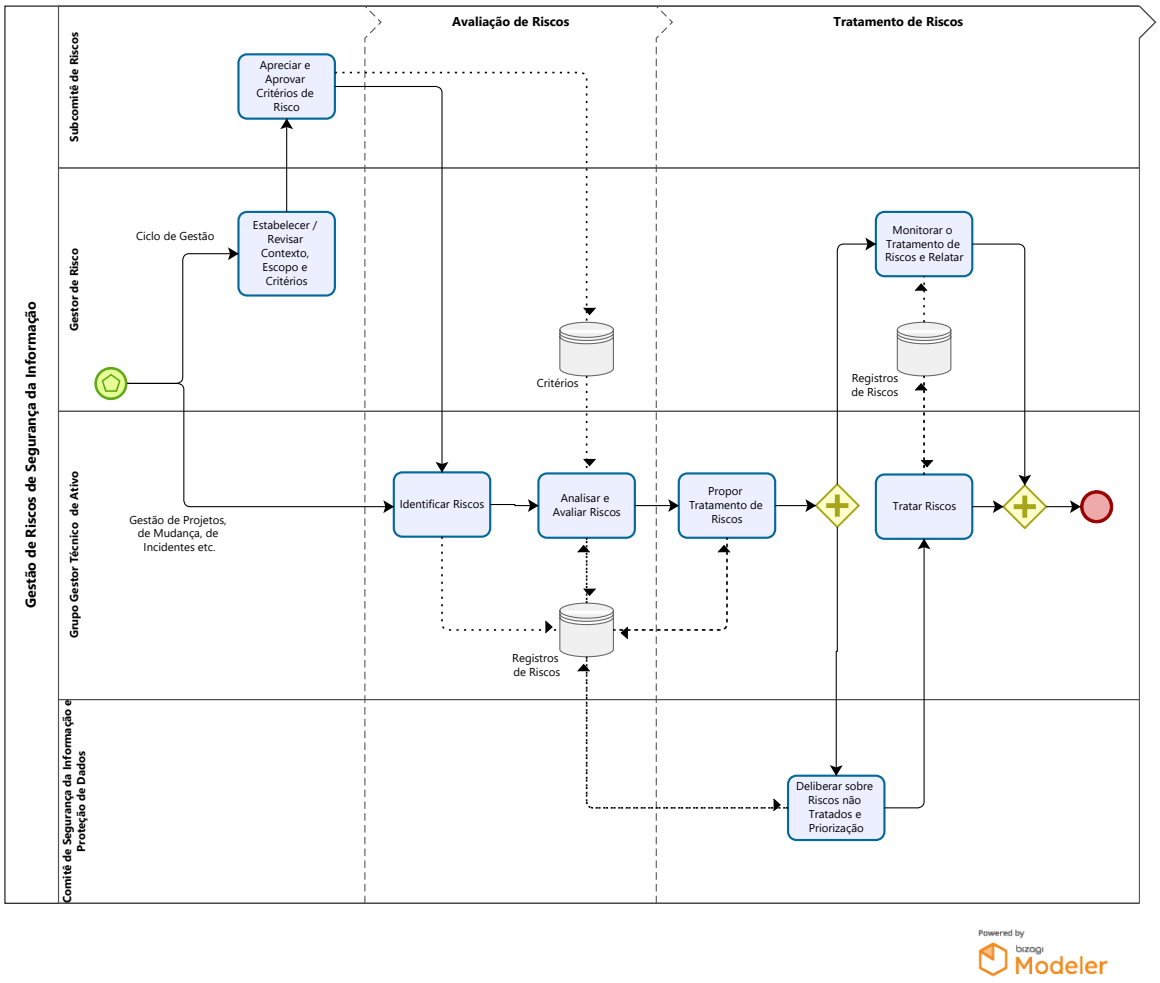
Fluxo do Processo de Gestão de Riscos de Segurança da Informação v1.1

Gestão de Riscos de Segurança da Informação - ver 1.1

Bizagi Modeler

Índice

1 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO



Processo Administrativo

23891/2023

Objetivo do Processo

Manter dentro do apetite a riscos definido pelo Subcomitê de Riscos os riscos de segurança da informação em ativos que possam ter impactos sobre a missão, objetivos operacionais e obrigações do TRT com terceiros, por meio de aplicação de Medidas de Segurança que trate adequadamente esses riscos.

Dono do Processo

Comitê de Segurança da Informação e Proteção de Dados

Gerente do Processo

Diretor da Coordenadoria de Segurança da Informação

Entradas

Informações para estabelecimento de contexto, escopo, critérios e apoio para gestão de riscos.

Saídas

Riscos de segurança da informação em ativos gerenciados.

Data da Revisão

30/08/2024

Obs:

Visando facilitar a leitura e entendimento do processo, as fases "comunicação e consulta", "monitoramento e análise crítica" e "registro e relato" não são explicitadas no presente fluxo.

· "Comunicação e Consulta" e "Registro e Relato" representam conjunto de atividades inerentes à execução do fluxo do processo e ao uso dos diversos recursos definidos dentro e fora do processo (normas diversas, ferramentas de colaboração, reuniões de comitês etc.);

· "Monitoramento e Análise Crítica" representa um conjunto de atividades inerentes às responsabilidades de gerentes de processos, a fim de assegurar e melhorar a qualidade e a eficácia da concepção, implementação e resultados do processo.

A seguinte pasta de trabalho, no ambiente Google Suite, contém subpastas com documentos do CIS RAM 2.1 e CIS RAM 2.2 originais em inglês e material traduzido em grande parte para o portugûes e adaptado para uso pelo TRT18:
https://drive.google.com/drive/folders/1PAfdD8Z1xxt56QXA7t2E2MXyjxqgLkpx?usp=sharing
Destacam-se:

· CIS_RAM_brochure_v2.1_2022 em Português.pdf

· CIS_RAM_v2.1__Core_Document__2022_08 em Português.pdf

· CIS_RAM_v2.2__IG2_Workbook_Guide - adaptado da v2.1.pdfl

· CIS_RAM_v2.2_for_IG2_Workbook - template TRT18 em Português

Versão:

1.1

Autor:

s161942

1.1 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

1.1.1 ELEMENTOS DO PROCESSO

1.1.1.1 ☐ Estabelecer / Revisar Contexto, Escopo e Critérios

Descrição

Diz respeito à definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos e ao estabelecimento do escopo e dos critérios de risco.

DO CONTEXTO

A definição de Contexto considera o conhecimento do ambientes interno e externo de ameaças ao TRT18, dos seus Planos Estratégicos e de Gestão e dos requisitos de segurança da informação das partes interessadas do órgão, dos regulamentos e dos convênios e contratos.

DO ESCOPO

· todos os ativos que integram as infraestruras críticas de TIC, quando o presente processo for iniciado para tratar um ciclo de gestão de riscos; tal escopo está determinado pela Portaria TRT da 18ª

SGP/CSIN nº 3358/2022, especialmente no que se refere à adoção do Manual para Proteção de Infraestruturas Críticas de TIC; ou

· ativos contidos no escopo de um processo demandade da gestão de riscos, como o processo de gestão de mudanças, de projetos, de incidentes etc.

DOS CRITÉRIOS

Para se calcular o nível de um risco identificado, e determinar se o mesmo precisa ou não de tratamento, faz-se necessário utilizar Critérios de Impacto, Critérios de Risco Inerente, Critérios de Expectativa ("probabilidade) e Critérios de Aceitação de Riscos.

O Gestores de Riscos, sob coordenação da unidade gestora de segurança da informação, devem:

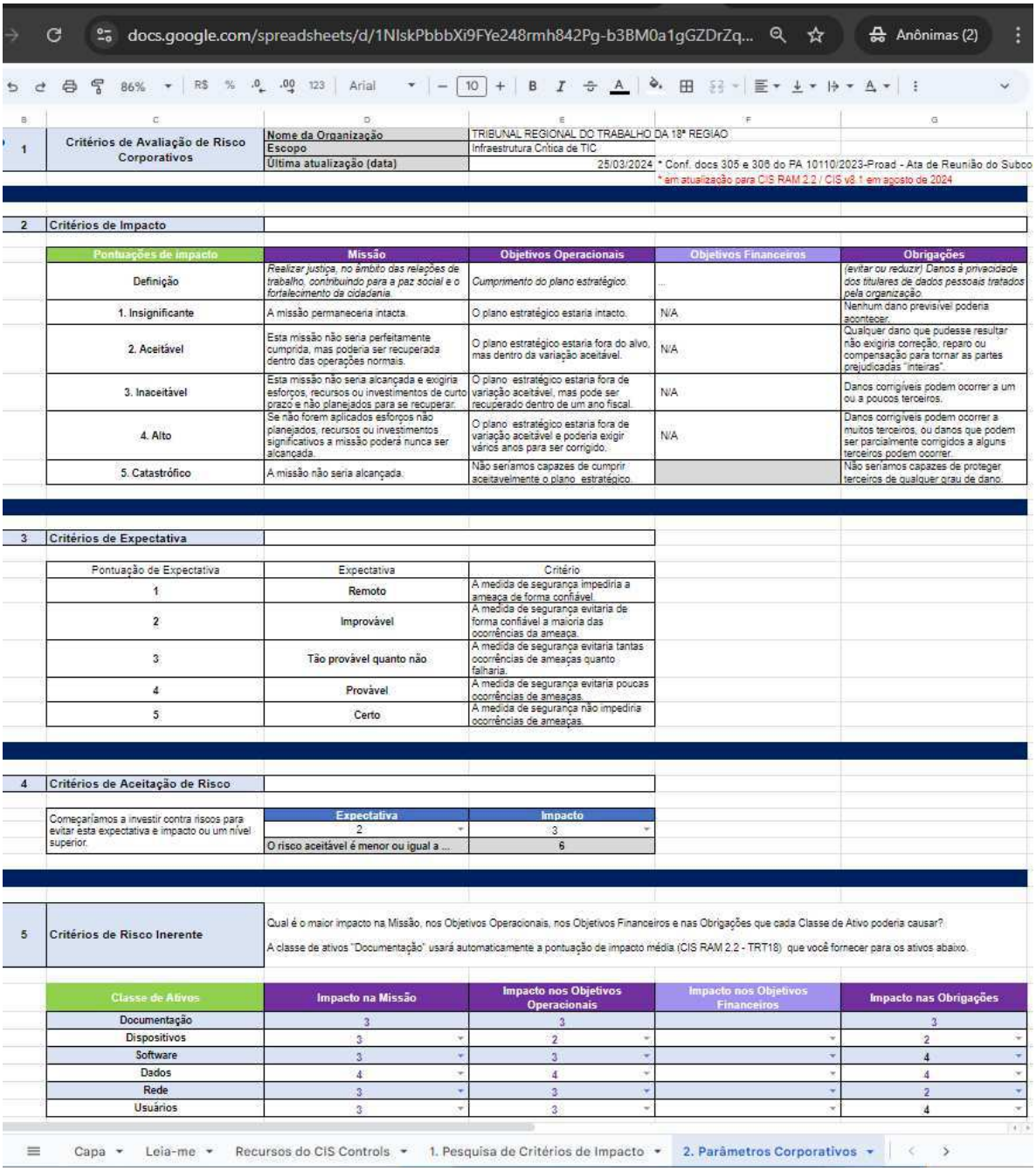
· seguir as instruções contidas nas seções "Pesquisa de Critérios de Impacto" e "Parâmetros Corporativos" do guia do Workbook CIS RAM v2.2 para IG2;

· estabelecer propostas de Critérios de Impacto, Critérios de Risco Inerente, Critérios de Expectativa e Critérios de Aceitação de Riscos; e

· submeter as propostas para deliberação pelo Subcomitê de Riscos.

O template Workbook CIS RAM v2.2 para IG2 contém em suas diversas abas os valores de critérios padrão.

Portanto, lembrar de ajustar o template caso sejam estabelecidos e aprovados critérios diversos do padrão.



docs.google.com/spreadsheets/d/1NIskPbbbXi9FYe248rmh842Pg-b3BM0a1gGZDrZq...

Anônimas (2)

1	Critérios de Avaliação de Risco Corporativos	Nome da Organização	TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIAO
		Escopo	Infraestrutura Crítica de TIC
		Última atualização (data)	25/03/2024 * Conf. docs 305 e 306 do PA 10110/2023-Proad - Ata de Reunião do Subco
			* em atualização para CIS RAM 2.2 / CIS v8.1 em agosto de 2024

2 Critérios de Impacto

Pontuações de Impacto	Missão	Objetivos Operacionais	Objetivos Financeiros	Obrigações
Definição	*Realizar justiça, no âmbito das relações de trabalho, contribuindo para a paz social e o fortalecimento da cidadania.*	*Cumprimento do plano estratégico.*	...	*(evitar ou reduzir) Danos à privacidade dos titulares de dados pessoais tratados pela organização.*
1. Insignificante	A missão permaneceria intacta.	O plano estratégico estaria intacto.	N/A	Nenhum dano previsível poderia acontecer.
2. Aceitável	Esta missão não seria perfeitamente cumprida, mas poderia ser recuperada dentro das operações normais.	O plano estratégico estaria fora do alvo, mas dentro da variação aceitável.	N/A	Qualquer dano que pudesse resultar não exigiria correção, reparo ou compensação para tornar as partes prejudicadas "inteiras".
3. Inaceitável	Esta missão não seria alcançada e exigiria esforços, recursos ou investimentos de curto prazo e não planejados para se recuperar.	O plano estratégico estaria fora de variação aceitável, mas pode ser recuperado dentro de um ano fiscal.	N/A	Danos corrigíveis podem ocorrer a um ou a poucos terceiros.
4. Alto	Se não forem aplicados esforços não planejados, recursos ou investimentos significativos a missão poderá nunca ser alcançada.	O plano estratégico estaria fora de variação aceitável e poderia exigir vários anos para ser corrigido.	N/A	Danos corrigíveis podem ocorrer a muitos terceiros, ou danos que podem ser parcialmente corrigidos a alguns terceiros podem ocorrer.
5. Catastrófico	A missão não seria alcançada.	Não seríamos capazes de cumprir aceitavelmente o plano estratégico.		Não seríamos capazes de proteger terceiros de qualquer grau de dano.

3 Critérios de Expectativa

Pontuação de Expectativa	Expectativa	Critério
1	Remoto	A medida de segurança impediria a ameaça de forma confiável.
2	Improvável	A medida de segurança evitaria de forma confiável a maioria das ocorrências da ameaça.
3	Tão provável quanto não	A medida de segurança evitaria tantas ocorrências de ameaças quanto falharia.
4	Provável	A medida de segurança evitaria poucas ocorrências de ameaças.
5	Certo	A medida de segurança não impediria ocorrências de ameaças.

4 Critérios de Aceitação de Risco

	Expectativa	Impacto
Começaríamos a investir contra riscos para evitar esta expectativa e impacto ou um nível superior.	2	3
	O risco aceitável é menor ou igual a ...	6

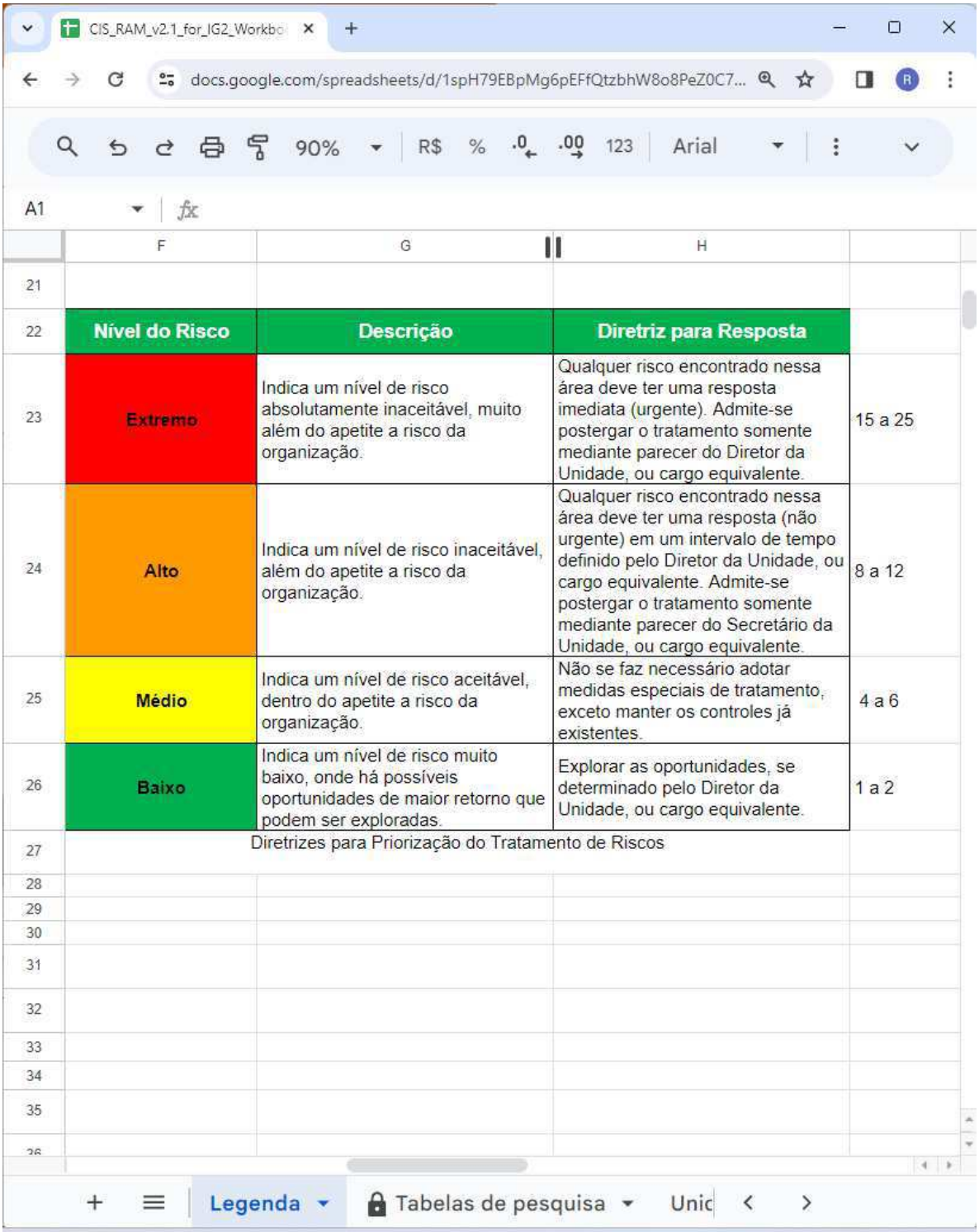
5 Critérios de Risco Inerente

Qual é o maior impacto na Missão, nos Objetivos Operacionais, nos Objetivos Financeiros e nas Obrigações que cada Classe de Ativo poderia causar?

A classe de ativos "Documentação" usará automaticamente a pontuação de impacto média (CIS RAM 2.2 - TRT18) que você fornecer para os ativos abaixo.

Classe de Ativos	Impacto na Missão	Impacto nos Objetivos Operacionais	Impacto nos Objetivos Financeiros	Impacto nas Obrigações
Documentação	3	3		3
Dispositivos	3	2		2
Software	3	3		4
Dados	4	4		4
Rede	3	3		2
Usuários	3	3		4

Capa | Leia-me | Recursos do CIS Controls | 1. Pesquisa de Critérios de Impacto | 2. Parâmetros Corporativos



Nível do Risco	Descrição	Diretriz para Resposta	
Extremo	Indica um nível de risco absolutamente inaceitável, muito além do apetite a risco da organização.	Qualquer risco encontrado nessa área deve ter uma resposta imediata (urgente). Admite-se postergar o tratamento somente mediante parecer do Diretor da Unidade, ou cargo equivalente.	15 a 25
Alto	Indica um nível de risco inaceitável, além do apetite a risco da organização.	Qualquer risco encontrado nessa área deve ter uma resposta (não urgente) em um intervalo de tempo definido pelo Diretor da Unidade, ou cargo equivalente. Admite-se postergar o tratamento somente mediante parecer do Secretário da Unidade, ou cargo equivalente.	8 a 12
Médio	Indica um nível de risco aceitável, dentro do apetite a risco da organização.	Não se faz necessário adotar medidas especiais de tratamento, exceto manter os controles já existentes.	4 a 6
Baixo	Indica um nível de risco muito baixo, onde há possíveis oportunidades de maior retorno que podem ser exploradas.	Explorar as oportunidades, se determinado pelo Diretor da Unidade, ou cargo equivalente.	1 a 2

Diretrizes para Priorização do Tratamento de Riscos

1.1.1.2 ☐Apreciar e Aprovar Critérios de Risco

Descrição

Consiste em apreciar, ajustar, se necessário for, e aprovar as propostas de Critérios de Impacto, Critérios de Risco Inerente, Critérios de Expectativa e Critérios de Aceitação de Risco.

Para alinhamento entre o Processo de Gestão de Riscos corporativo com o de Segurança da Informação em ativos, sugere-se usar no processo de Gestão de Riscos de Segurança da Informação em ativos:

· a mesma quantidade de escalas de Critérios de Impacto e de Critérios de Expectativa (probabilidade) definidas para o processo de Gestão de Riscos corporativo; e

· as mesmas Diretrizes para Aceitação de Riscos definidas para o processo de Gestão de Riscos corporativo.

1.1.1.3 ☐Identificar Riscos

Descrição

Consiste na busca, reconhecimento e descrição de riscos.

Cada Medida de Segurança CIS representa implicitamente um risco à Classe de Ativos a que é associada (rede, pessoas, dados, software, dispositivos e documentação).

Infere-se daí e da Portaria TRT18 SGP/CSIN nº 3358/2022 que o TRT da 18ª Região inicia seu ciclo de gestão com 130 riscos identificados automaticamente, o que corresponde ao total de Medidas de Segurança do grupo de Implementação 2 do CIS - IG2.

No entanto, considera-se as mesmas 130 Medidas de Segurança como base de pesquisa para identificação de riscos quando o escopo do processo não sobrecai sobre todas as infraestruturas críticas de TIC.

Como exemplo, um determinado ativo envolvido num processo de mudança, e que foi identificado como da Classe de Ativos "rede", possui 17 Medidas de Segurança associadas ao IG2. Ou seja, só esse ativo permite identificar 17 novos riscos de segurança da informação para posterior análise/avaliação e possível tratamento.

1.1.1.4 ☐Analisar e Avaliar Riscos

Descrição

Análise de Riscos: refere-se à compreensão da natureza do risco e à determinação do respectivo nível de risco mediante a combinação da probabilidade (ou expectativa) de sua ocorrência e dos impactos possíveis.

Avaliação de Riscos: trata-se da comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional.

Os membros do Grupo Gestor Técnico de Ativo (analisador/avaliador de risco) devem seguir as instruções da seção "Registro de Riscos: Análise de riscos" do guia Workbook CIS RAM v2.2 para IG2.

A partir do fornecimento da informação sobre a Pontuação de Maturidade de cada Medida de Segurança é possivel obter de modo automático a Pontuação de Risco, o respectivo Nível de Risco e a indicação se a medida é ou não aplicada de forma aceitável e razoável.

1.1.1.5 ☐Propor Tratamento de Riscos

Descrição

Consiste na seleção de opções para tratar riscos.

Os membros do Grupo Gestor Técnico de Ativo (analisador/avaliador de risco) devem seguir as instruções da seção "Registro de Riscos: Tratamento de riscos" do guia Workbook CIS RAM v2.2 para IG2.

Em suma, consiste em diferenciar os riscos que serão aceitos dos que serão tratados.

Para esses últimos, documentar qual implementação que se pretende realizar, em que prazo e qual Pontuação de Maturidade a alcançar após o tratamento do risco.

O próprio Workbook em sua aba "Controles dos Registros de Riscos v8.1" indicará sobre a aceitabilidade/razoabilidade do tratamento proposto.

1.1.1.6 ☐Deliberar sobre Riscos não Tratados e Priorização

Descrição

Consiste em tomar ciência dos riscos identificados e avaliados, da sugestão por aceitar ou mitigar riscos e das propostas de ações e de cronogramas para tratamento.

Espera-se que o Comitê de Segurança da Informação e Proteção de Dados delibere sobre a proposta de tratamento de Riscos, ajustando as questões de priorização e de aceite que enteder pertinentes.

1.1.1.7 ☐Tratar Riscos

Descrição

Consiste na implementação de opções aprovadas e priorizadas para tratar riscos.

Após deliberação pelo Comité de Segurança da Informação e Proteção de Dados, os membros do Grupo Técnico Gestor de Ativo devem registrar as ações planejadas de tratamento na ferramenta de gestão de projetos Redmine para pemitir o controle e acompanhamento das implementações.

Tais registros de ações plajenadas devem estar associados ao respectivo ciclo de gestão, se for o caso.

1.1.1.8 ☐Monitorar o Tratamento de Riscos e Relatar

Descrição

Refere-se ao acompanhamento e controle do andamento das ações de tratamento e do reporte do status ao Comitê de Segurança da Informação e Proteção de Dados.

Sugere-se destacar os atrasos, respectivas justificativas e possíveis implicações.