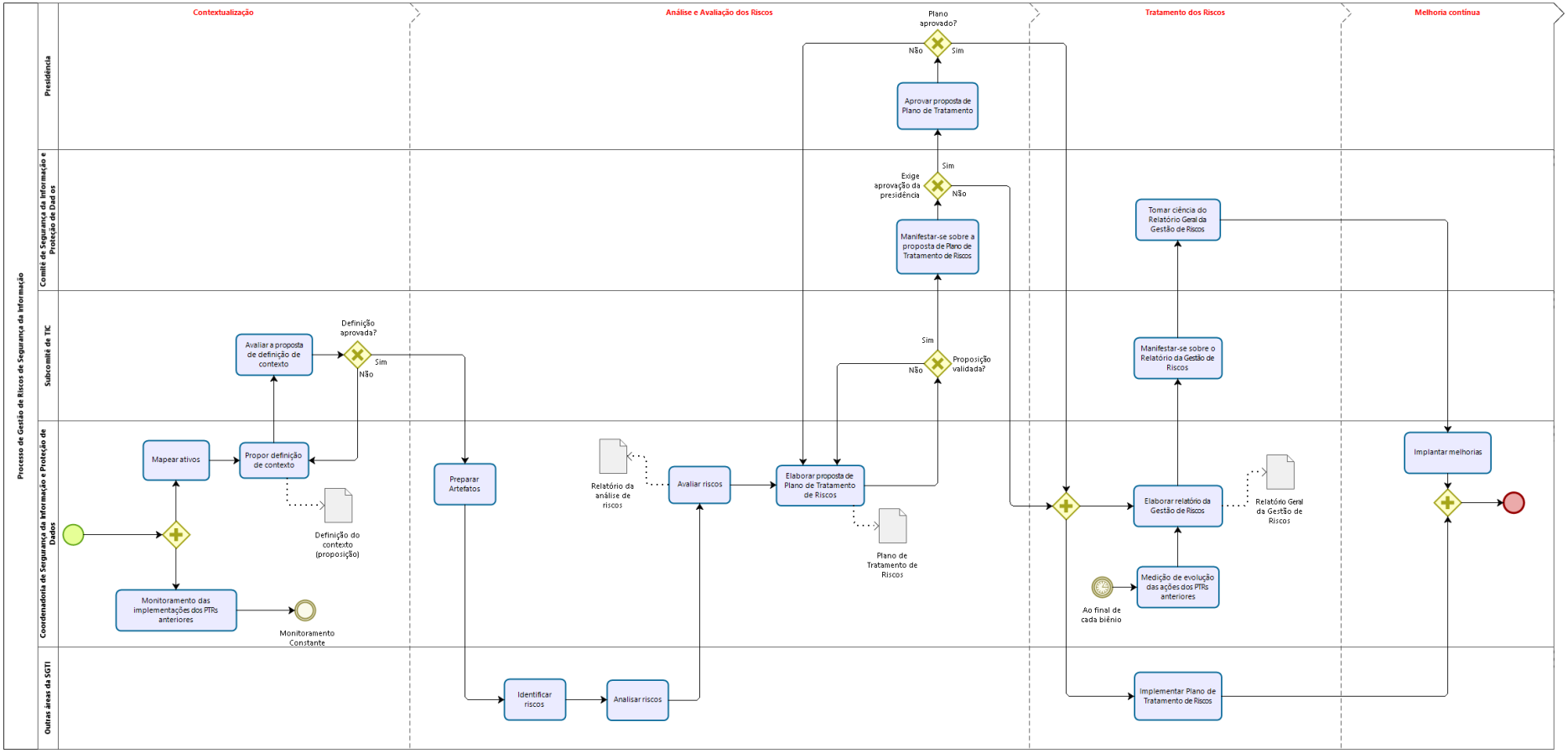
PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

DESENHO DO PROCESSO
DEFINIÇÕES
DESCRIÇÃO DAS TAREFAS

Versão set.2025

DESENHO DO PROCESSO



Processo de Gestão de Riscos de Segurança da Informação
CSIPD/SGTI/TRT4

CONTROLE DE VERSÕES

Versão e data	Alterações
set.2025	Versão de controle inicial

DEFINIÇÕES

Objetivo do Processo
Identificar, analisar e tratar riscos que possam comprometer a confidencialidade, integridade e disponibilidade das informações, fornecendo subsídios para decisões de segurança baseadas em risco e apoiando a melhoria contínua da proteção organizacional.

Responsável pelo Processo
Coordenadoria de Segurança da Informação e Proteção de Dados

Papéis e responsabilidades	
Coordenadoria de Segurança da Informação e Proteção de Dados (CSIPD)	Responsável pela gestão do processo e acompanhamento da execução das atividades relacionadas à gestão dos riscos de TIC.
Outras áreas da SGTI	Compreende as áreas que gerenciam os sistemas, serviços e infraestrutura de TIC, responsáveis pela implementação dos controles definidos no tratamento dos riscos
Subcomitê de TIC	Comitê interno da SGTI, responsável pela aprovação em primeiro nível de alguns documentos gerados no processo.
Comitê de Segurança da Informação e Proteção de Dados	Responsável pela avaliação das proposições e documentos produzidos no processo de gestão de risco, subsidiando a tomada de decisão pela Administração no que se refere à matéria em questão.
Presidência	Responsável pela aprovação ou rejeição final de documentos e proposições referentes ao Tratamento de Riscos e às propostas de melhoria do processo.

Termos/Artefatos
Planos de Tratamento de Riscos anteriores, Relatórios de análises anteriores, Relatórios de Incidentes de Segurança da Informação (RISI), planilhas de identificação e análise de riscos.

Ferramentas	
PROAD	Sistema de processo administrativo eletrônico
Suite SA	Ferramenta utilizada para apoio na Gestão de Riscos
Google Suite	Planilhas e documentos utilizados para apoio

Referências técnicas, legais e normativas que fundamentam o Processo	
Norma ABNT NBR ISO/IEC 27001:2022	**E**stabelece os requisitos para um Sistema de Gestão da Segurança da Informação
Norma ABNT NBR ISO/IEC 27002:2022	Fornece um conjunto de referências de controles de segurança da informação.
ABNT NBR 27005:2022	Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação

Indicador de benefício do processo		
Descrição do indicador	**Método de apuração / fórmula de cálculo**	**Frequência**
Ações Pendentes	= Somatório de ações de PTRs anteriores e do atual, não concluídas até o final do ciclo atual	Bianual, final do ciclo
Execução do Plano de Tratamento de Riscos (PTR)	= (ações realizadas ao longo do ciclo) / ((Ações Pendentes do ciclo anterior) + (ações propostas no PTR do ciclo atual))	Bianual, final do ciclo

Controle de execução do processo		
Controle	**Método de execução**	**Frequência**
Auditoria	Realizar uma reunião com as equipes executoras do processo, para avaliar a aderência, os benefícios gerados e oportunidades de melhoria do processo. Essa reunião deve identificar se o processo necessita de revisão.	Anual

DESCRIÇÃO DAS TAREFAS

Monitoramento das implementações dos PTRs anteriores		
Descrição	Realizar o acompanhamento das ações aprovadas em PTRs anteriores.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados Outras áreas da SGTI	
Considerações importantes	A CSIPD realiza o acompanhamento, porém a execução é de responsabilidade das áreas responsáveis pelas ações, indicadas no PTR.	
Entradas	PTRs anteriores	
Saídas	Acompanhamento das ações dos PTRs anteriores	
Atividades	**Acompanhar ações**	CSIPD, com apoio das áreas responsáveis pelas ações, acompanha o andamento das mesmas.
Ferramentas	Google Docs	

Propor definição de contexto		
Descrição	Compreende a proposição dos objetivos, escopo e limites da avaliação de riscos a ser realizada, com a identificação das partes interessadas e observados os critérios definidos no Anexo 6 da Política de Segurança da Informação. As exclusões do escopo também devem ser definidas e justificadas.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Considerações importantes	A proposta de definição de contexto é elaborada pela Coordenadoria de Segurança da Informação e Proteção de Dados, em conjunto com a Diretoria da Secretaria-Geral de Tecnologia e Inovação. O documento é encaminhado para avaliação do Subcomitê de TIC.	
Entradas	PETIC, SGSI anterior,mapeamento dos ativos de TIC dentre outros,	
Saídas	Definição do contexto (proposição)	
Atividades	**Definir contexto**	Identificar o propósito da avaliação de riscos a ser realizada. Esta definição guiará a definição do escopo (p. ex. suportar o SGSI, conformidade legal, requisitos de segurança para uma solução de TIC). Descrever o escopo (que pode abranger o Tribunal como um todo, um segmento, um processo, um sistema, ou um recurso), limites da avaliação de risco a ser realizada e listar as partes interessadas na análise de riscos.
	Formalizar a proposta	As definições preliminares deverão ser formalizadas conforme modelo utilizado pela Coordenadoria de Segurança da Informação e Proteção de

		Dados. Avaliar-se-á a abertura de processo administrativo específico para a aprovação dos documentos e resultados da análise de riscos.
	Encaminhar ao Subcomitê **de TIC**	CSIPD remete o documento para avaliação do Subcomitê de TIC, que poderá solicitar ajustes ou validá-lo.
Ferramentas	Google DOCS, PROAD	

Avaliar a proposta de definição de contexto		
Descrição	O Subcomitê de TIC avalia o contexto proposto para a análise de riscos a ser executada, podendo aprová-lo ou não. Em caso de não aprovação, devolve à CSIPD indicando os ajustes necessários.	
Papéis	Subcomitê de TIC	
Considerações importantes	A manifestação do Subcomitê de TIC deve ser formalizada dentro do PROAD respectivo.	
Entradas	Proposta de definição de contexto	
Saídas	Decisão aprovando a Definição de Contexto ou propondo correções/ajustes	
Atividades	**Avaliar a proposta**	Análise do contexto proposto, com base nas informações contidas no documento proposto pelo CSIPD.
	Aprovar a proposta	Aprova o documento.
	Solicitar ajustes	Reprova o documento, informando à CSIPD os ajustes indicados.
Ferramentas	Google Suite, PROAD	

Mapear ativos		
Descrição	Atividade que consiste em elencar os ativos de TIC que comporão o escopo da Gestão de Riscos.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Considerações importantes	O correto mapeamento dos ativos resulta em uma análise de riscos precisa.	
Entradas	Tabela/lista de ativos de outras áreas da SGTI, escopo da análise de riscos, , Oraculum, etc;	
Saídas	Mapeamento dos ativos	
Atividades	**Levantamento dos ativos**	Mapear os ativos da organização e seus responsáveis.
Ferramentas	Módulo de *Risk Manager* da Suíte SA, Oraculum, Google Docs	

Preparar Artefatos		
Descrição	Preparar o ambiente para a execução do processo de Gestão de Riscos.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Considerações importantes	N/A	
Entradas	Definição de contexto da Gestão de Riscos aprovada**,** Gestão de riscos anterior	
Saídas	Sistemas configurados para a realização da Gestão de Riscos	
Atividades	**Preparar sistemas**	CSIPD prepara os sistemas, planilhas e outros artefatos necessários para a Gestão de Riscos.
Ferramentas	Suite SA, Google Docs	

Identificar riscos		
Descrição	Atividade que consiste na identificação dos riscos relacionados aos ativos mapeados.	
Papéis	Outras áreas da SGTI Coordenadoria de Segurança da Informação e Proteção de Dados	
Considerações importantes	Poderão ser utilizados outros meios para identificar os riscos, tais como: resultados de análises de vulnerabilidades, entrevistas com gestores de ativos, etc. Cada área da SGTI atuará na identificação de riscos dos ativos (parte do escopo) de sua responsabilidade, com o apoio da CSIPD. Obs.: É importante seguir a Metodologia de Gestão de Riscos, elaborada para orientar a realização do processo de análise de riscos.	
Entradas	Definição de Escopo Aprovada Planilhas e ferramentas de trabalho	
Saídas	Riscos identificados	
Atividades	**Identificação inicial dos riscos**	CSIPD realiza processo de identificação preliminar de riscos associados a cada ativo.
	Identificação dos riscos	Cada área da SGTI recebe a relação preliminar dos riscos identificados para os ativos pelos quais é responsável, complementando com a identificação de novos riscos.
Ferramentas	Módulo de *Risk Manager* da Suíte SA e Google Docs	

Analisar riscos	
Descrição	Nesta atividade são estimados os valores de impacto e probabilidade para cada risco, além de possíveis controles já existentes.
Papéis	Outras áreas da SGTI Coordenadoria de Segurança da Informação e Proteção de Dados

Considerações importantes	Assim como a identificação dos riscos, a análise de risco é conduzida com o apoio da CSIPD. Cada área da SGTI realizará essa atividade para os riscos referentes aos ativos sob sua responsabilidade.	
Entradas	Riscos identificados	
Saídas	Riscos analisados (probabilidade e impactos inerentes determinados). Controles identificados, e com eficácia mensurada, para os riscos**.**	
Atividades	**Determinação da Probabilidade e Impacto**	As áreas da SGTI determinam (com base no histórico de ocorrência, nível de exposição dos ativos, vulnerabilidades conhecidas e etc) os níveis inerentes de probabilidade e de impacto para cada risco.
	Identificação dos controles	Áreas da SGTI realizam a identificação dos controles existentes para tratar os riscos identificados.
	Apuração da eficácia dos controles	As áreas da SGTI avaliam a eficácia dos controles identificados em relação aos riscos.
	Módulo de *Risk Manager* da Suíte SA e Google Docs	

Avaliar Riscos		
Descrição	Nesta etapa avaliam-se criticamente os riscos identificados e analisados, confrontando o nível de risco de cada um ao apetite de riscos do definido pelo Tribunal.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Considerações importantes	Riscos que ficarem acima do apetite estabelecido pela organização deverão ter avaliada a forma de tratamento, conforme metodologia.	
Entradas	Riscos analisados	
Saídas	Relatório de Avaliação de Riscos	
Atividades	**Verificação do nível de risco**	Avaliar o nível de risco associado a cada risco, identificando aqueles cujo nível ultrapassa o apetite definido pelo Tribunal, para elaboração de plano de tratamento.
	Identificar tratamento para os riscos	Para cada risco com nível acima do apetite definido, as áreas, com apoio da CSIPD, devem sugerir o tratamento recomendado ao risco, que pode ser: ● Aceitar: manter o risco como está, monitorando-o para que não atinja níveis maiores. Este tratamento exige a devida justificativa; ● Compartilhar: propor ações que permitam o compartilhamento do risco com outra organização (ex.: terceirização), diminuindo assim a probabilidade de ocorrência ou o impacto gerado;

		● Evitar: definir, quando possível, formas para evitar que o risco possa ocorrer ou os impactos gerados; ● Mitigar: propor ações que permitam mitigar as chances de ocorrência do risco ou o impacto gerado por ele.
	Elaborar relatório	Elaborar relatório de acordo com modelo utilizado pela CSIPD.
Ferramentas	Módulo de *Risk Manager* da Suíte SA e Google Docs	

Elaborar proposta Plano de Tratamento de Riscos		
Descrição	Atividade que compreende a elaboração de plano visando à definição das formas de tratamento dos riscos, da implantação de controles, dos responsáveis por sua implementação e do estabelecimento de prazos.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados Outras áreas da SGTI Subcomitê de TIC	
Considerações importantes	O Plano de Tratamento deve ser aprovado pela Administração, após validação pelo Subcomitê de TIC e pelo Comitê de Segurança da Informação e Proteção de Dados, pois poderá demandar investimento de recursos financeiros e reorganização de prioridades das equipes. Deverá ser encaminhado à Administração o expediente administrativo contendo todas as informações relacionadas à análise de risco em questão.	
Entradas	Relatórios de Avaliação de Riscos Relação dos riscos além do apetite determinado pelo Tribunal	
Saídas	Proposta de Plano de Tratamento de Riscos	
Atividades	**Elaborar PTR**	O Plano de Tratamento de Riscos (PTR) deverá conter tratamentos para TODOS os riscos além do apetite, informando, ao menos: ● Qual a forma de tratamento sugerida; ● Quem será responsável pelo tratamento; ● Quais as ações necessárias para realização do tratamento, detalhando: ○ Prazos necessários; ○ Áreas envolvidas; ○ Custos estimados, quando houver; ● Quando será o plano será implantado (Início e duração estimadas); ● Quem deve ser informado sobre o andamento das ações;
	Validação do PTR	O Subcomitê de TIC valida o plano proposto, considerando a necessidade de investimentos de recursos financeiros e humanos.

Ferramentas	Documentos e planilhas

Manifestar-se sobre a proposta de Plano de Tratamento de Riscos		
Descrição	Compete ao Comitê manifestar-se sobre o plano de ação proposto para tratamento dos riscos apontados durante a análise, indicando possíveis ajustes.	
Papéis	Comitê de Segurança da Informação e Proteção de Dados	
Considerações importantes	N/A	
Entradas	Proposta do Plano de Tratamento de Riscos	
Saídas	Manifestação sobre o plano com possíveis recomendações de ajustes	
Atividades	**Opinar sobre a proposição**	Manifestação sobre a proposta de plano, sugerindo à Presidência sua aprovação ou alterações que entender necessárias.
Ferramentas	PROAD ou e-mail	

Aprovar proposta de Plano de Tratamento de Riscos		
Descrição	Atividade que compreende a ciência sobre os resultados da análise e avaliação de riscos e a apreciação do Plano de Tratamento de Riscos (PTR) proposto.	
Papéis	Presidência do TRT	
Considerações importantes	Quando a implementação de controles representar a utilização de recursos financeiros, humanos e tecnológicos, além de impactar na execução de outros projetos estratégicos já planejados para o período, a proposta de PTR precisará ser apreciada e aprovada pela Presidência.	
Entradas	Proposta de PTR e considerações sobre o plano (feitas pelo Comitê de Segurança da Informação e Proteção de Dados).	
Saídas	Decisão aprovando a proposta de PTR ou determinando correções/ajustes.	
Atividades	**Avaliar a proposição encaminhada**	Analisar, considerando as manifestações do Comitê de Segurança da Informação e Proteção de Dados, os resultados da análise e avaliação de riscos realizada e o Plano de Tratamento de Riscos proposto, em especial no que diz respeito aos critérios de aceitação de riscos.
	Aprovar a proposta	Aprovado o PTR, inicia-se a implementação dos controles, conforme Plano apresentado.
	Solicitar ajustes	Não aprova o documento, mediante despacho, e devolve o expediente à SGTI para ajustes.
Ferramentas	PROAD	

Implementar Plano de Tratamento de Riscos

Descrição	Nessa atividade, as áreas da SGTI implementam os controles para tratar os riscos elencados, dentro do prazo definido no PTR.	
Papéis	Outras áreas da SGTI	
Considerações importantes	É importante que a implementação dos controles seja realizada de acordo com o Plano, dentro dos prazos e utilizando os recursos previstos.	
Entradas	Plano de Tratamento de Riscos	
Saídas	Controles implementados	
Atividades	**Delegar as atividades de implementação dos controles**	A implementação dos controles deverá ser delegada de acordo com as responsabilidades estabelecidas no Plano de Tratamento.
	Gerenciar implementação dos controles	Cada área deverá planejar e acompanhar a execução das ações, a fim de executá-las no prazo e forma ajustados.
Ferramentas	N/A	

Medição de evolução das ações dos PTRs anteriores		
Descrição	A CSIPD mede, a partir do monitoramento realizado das ações dos PTRs anteriores, o estágio de implementação de cada ação.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Considerações importantes	N/A?	
Entradas	Acompanhamento das ações dos PTRs anteriores	
Saídas	Medições de evolução para uso na confecção do Relatório Geral da Gestão de Riscos	
Atividades	**Medir ações**	Medir a evolução de cada ação dos PTRs anteriores. Obs.: uma vez que uma ação é encerrada e medida pela última vez, ela deixa de ser monitorada e medida.
Ferramentas	Google Docs, Suíte SA	

Elaborar relatório da gestão de riscos	
Descrição	Atividade que compreende a elaboração de relatório com as informações gerais da Gestão de Riscos e do Plano de Tratamento de Riscos proposto. O relatório tem a finalidade de, analisar criticamente o processo para posteriores melhorias, além de detalhar a Gestão de Riscos realizada.
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados
Considerações importantes	N/A?
Entradas	Definição de Contexto

	Relatório da análise de riscos Plano de Tratamento de Riscos	
Saídas	Relatório da Gestão de Riscos	
Atividades	**Elaborar relatório**	Redigir o documento com as informações
	Encaminhar para avaliação	Encaminhar relatório para manifestação do Subcomitê de TIC e, após, à ciência superior. O Subcomitê poderá devolver o relatório para ajustes.
Ferramentas	N/A	

Manifestar-se sobre o Relatório da Gestão de Riscos		
Descrição	O Subcomitê de TIC manifesta-se sobre o relatório elaborado pela CSIPD da Gestão de Riscos realizada ao longo do biênio	
Papéis	Subcomitê de TIC	
Considerações importantes	N/A?	
Entradas	Relatório da Gestão de Riscos	
Saídas	Relatório da Gestão de Riscos	
Atividades	**Manifestar-se sobre o relatório**	Manifestar-se sobre o relatório produzido, propondo ajustes quando necessário.
Ferramentas	PROAD, e-mail	

Tomar ciência do Relatório da Gestão de Riscos		
Descrição	O Comitê de Segurança da Informação e Proteção de Dados toma ciência do relatório apresentado	
Papéis	Comitê de Segurança da Informação e Proteção de Dados	
Considerações importantes	N/A?	
Entradas	Relatório da Gestão de Riscos	
Saídas	N/A?	
Atividades	**Tomar ciência do relatório**	Tomar ciência dos resultados apresentados e as propostas de melhorias
Ferramentas	PROAD, e-mail	

Implantar melhorias

Descrição	As melhorias propostas no Relatório da Gestão de Riscos são encaminhadas para implantação	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Considerações importantes	N/A	
Entradas	Relatório Geral da Gestão de Riscos	
Saídas	Implementação das melhorias	
Atividades	**Implementar melhorias**	Realizar ou planejar as ações aprovadas para o próximo ciclo.
Ferramentas	N/A	