

Manual do Processo de Gerenciamento do Sistema de Gestão de Segurança da Informação

Assessoria de Segurança da Informação



Assessoria de Segurança da Informação	Responsável: ---
Versão: 1	Data de Emissão: 26/04/2024
Elaborado por: Luciano Correia Pereira Filho	Aprovado por: Luciano Correia Pereira Filho

1. OBJETIVO

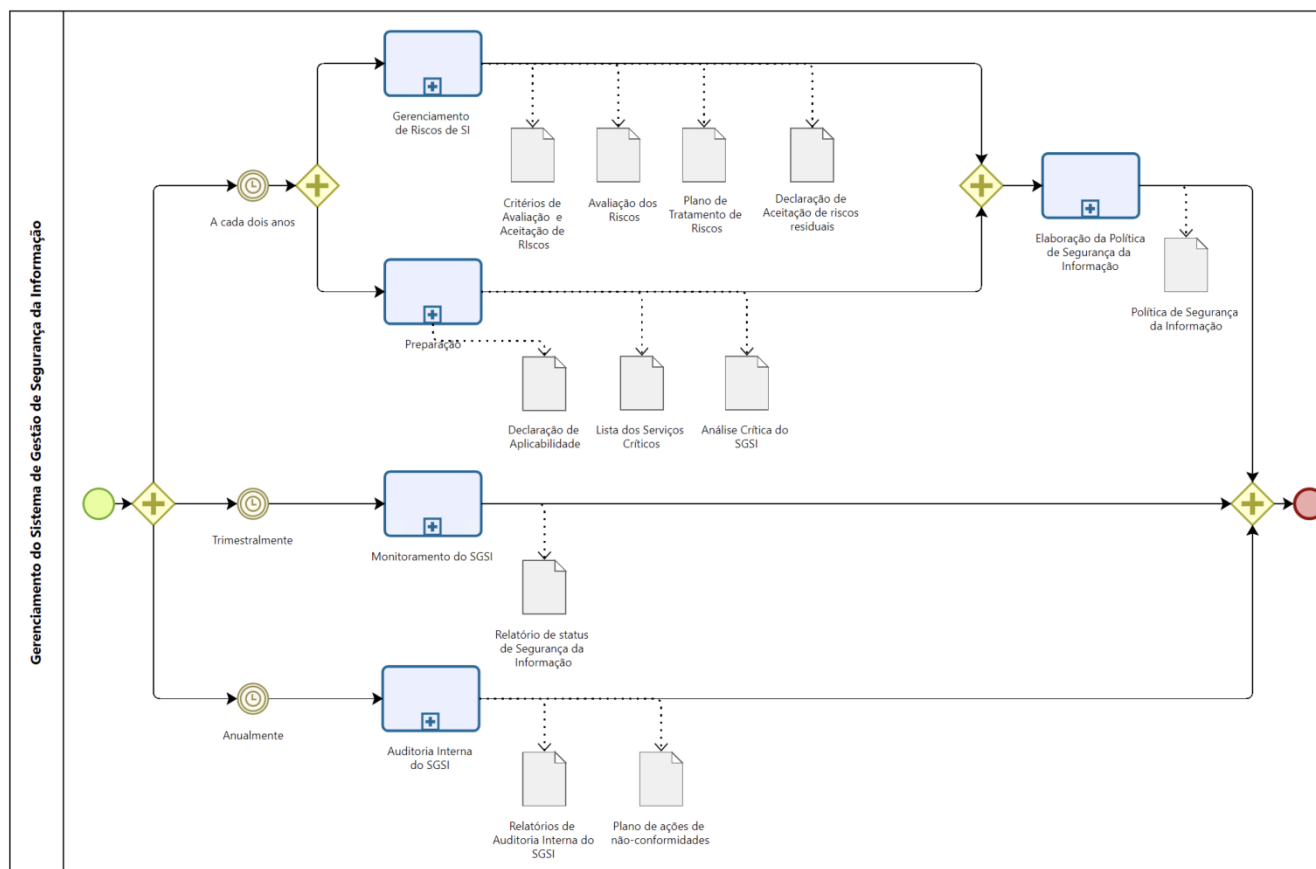
Definir o processo de gerenciamento do sistema de gestão de segurança da informação do Poder Judiciário de Mato Grosso do Sul.

2. DOCUMENTAÇÃO NORMATIVA DE REFERÊNCIA

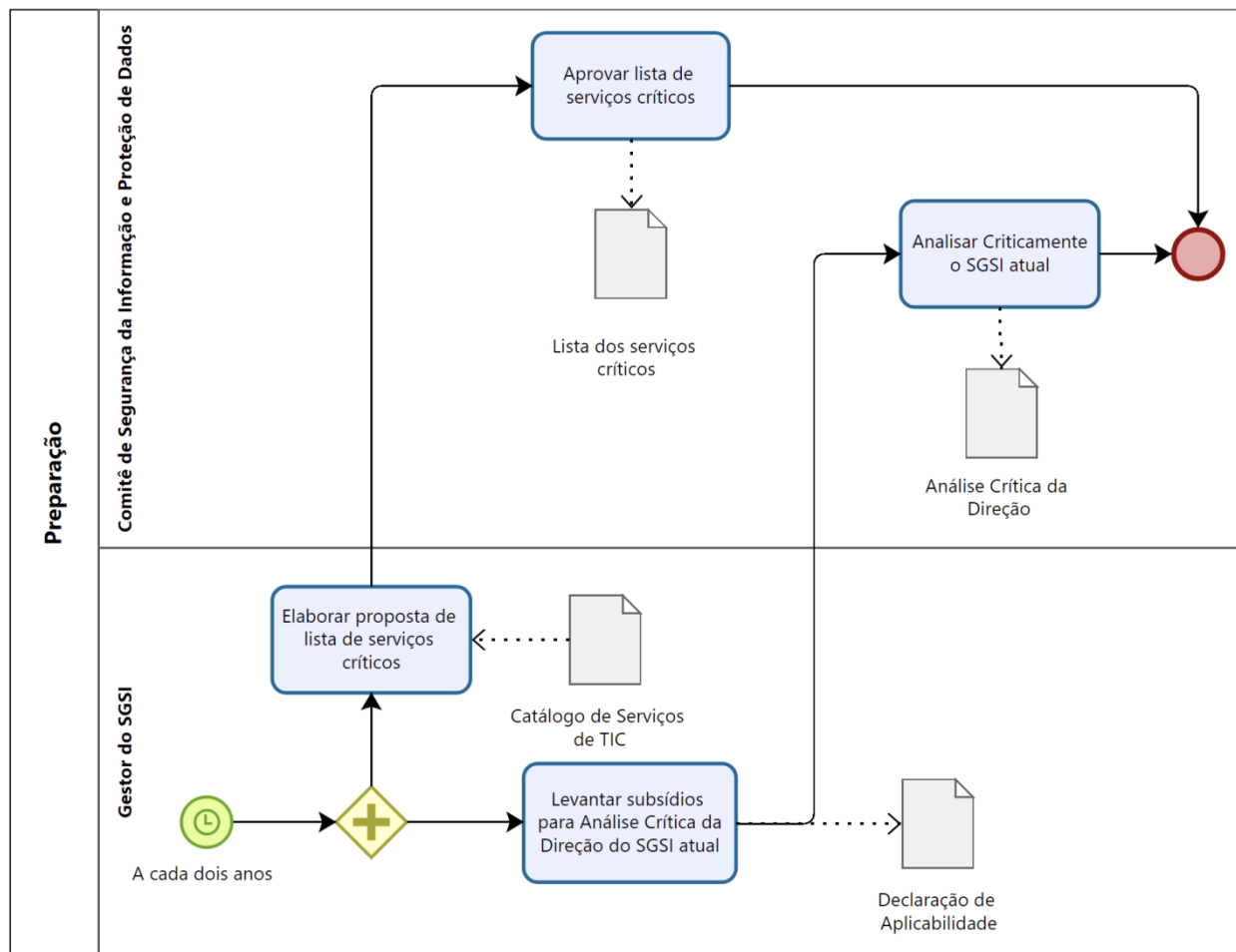
- São utilizadas como referências as normas ISO 27001:2022 e ISSO 27002:2022
- Resolução CNJ 396/2021 que institui a Estratégia Nacional de Segurança da Informação

3. DESENHO DO PROCESSO

3.1 Gerenciamento do Sistema de Gestão de Segurança da Informação

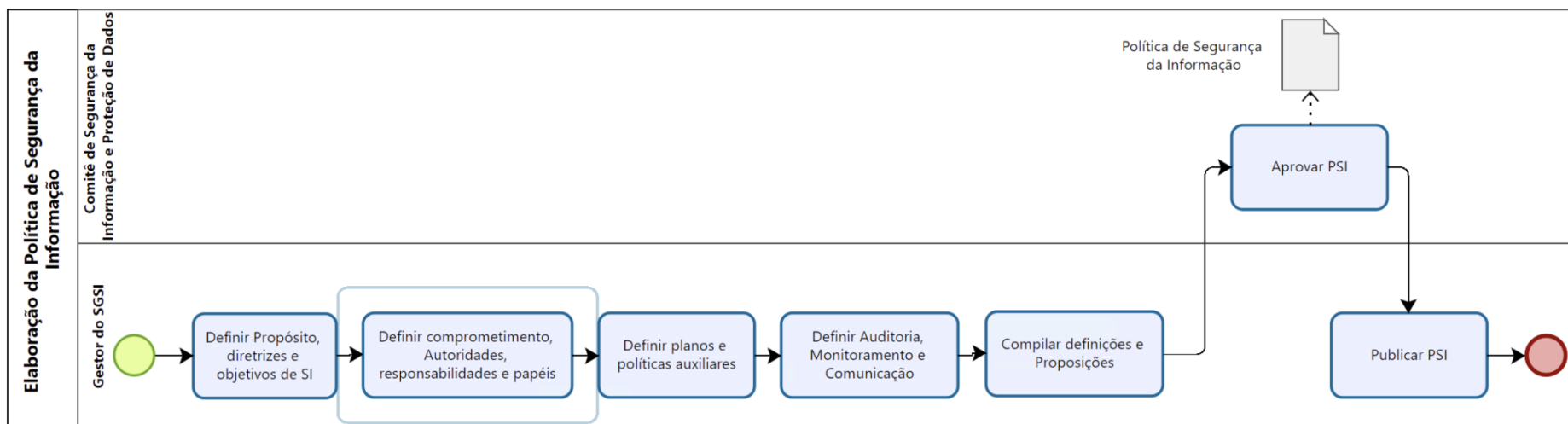


3.2 Subprocesso: Preparação



ATIVIDADE	RESPONSÁVEL	ENTRADAS	PROCEDIMENTOS	SAÍDAS
Elaborar proposta de lista de serviços críticos	Gestor do SGSI	Catálogo de Serviços de TIC	Levantar os serviços atualmente fornecidos e utilizando os critérios de impacto, disponibilidade e tipo da informação propor uma lista de serviços prioritizados que serão escopo do SGSI	Proposta da Lista de Serviços Críticos
Levantar subsídios para Análise Crítica da Direção do SGSI atual	Gestor do SGSI	Relatórios de Status de Segurança,	Levantar os pontos de não conformidades e ações corretivas, monitoramento e resultado das medições, resultados das auditorias, avaliação dos riscos, partes interessadas, oportunidades de melhoria, situações críticas anteriores e mudanças de questões internas ou externas relevantes para segurança da informação.	Informações compiladas e Declaração de Aplicabilidade atualizada
Aprovar lista de serviços críticos	Comitê de Segurança da Informação e Proteção de Dados	Proposta da Lista de Serviços Críticos	Analisar e deliberar sobre a proposta da lista de serviços críticos. Em caso de necessidade de ajuste, retornar para a atividade anterior.	Lista de Serviços Críticos aprovada
Analisar Criticamente o SGSI atual	Comitê de Segurança da Informação e Proteção de Dados	Informações compiladas	Analisar e deliberar sobre os pontos e funcionamento do SGSI.	Análise Crítica da Alta Direção

3.3 Subprocesso: Elaboração da Política de Segurança da Informação

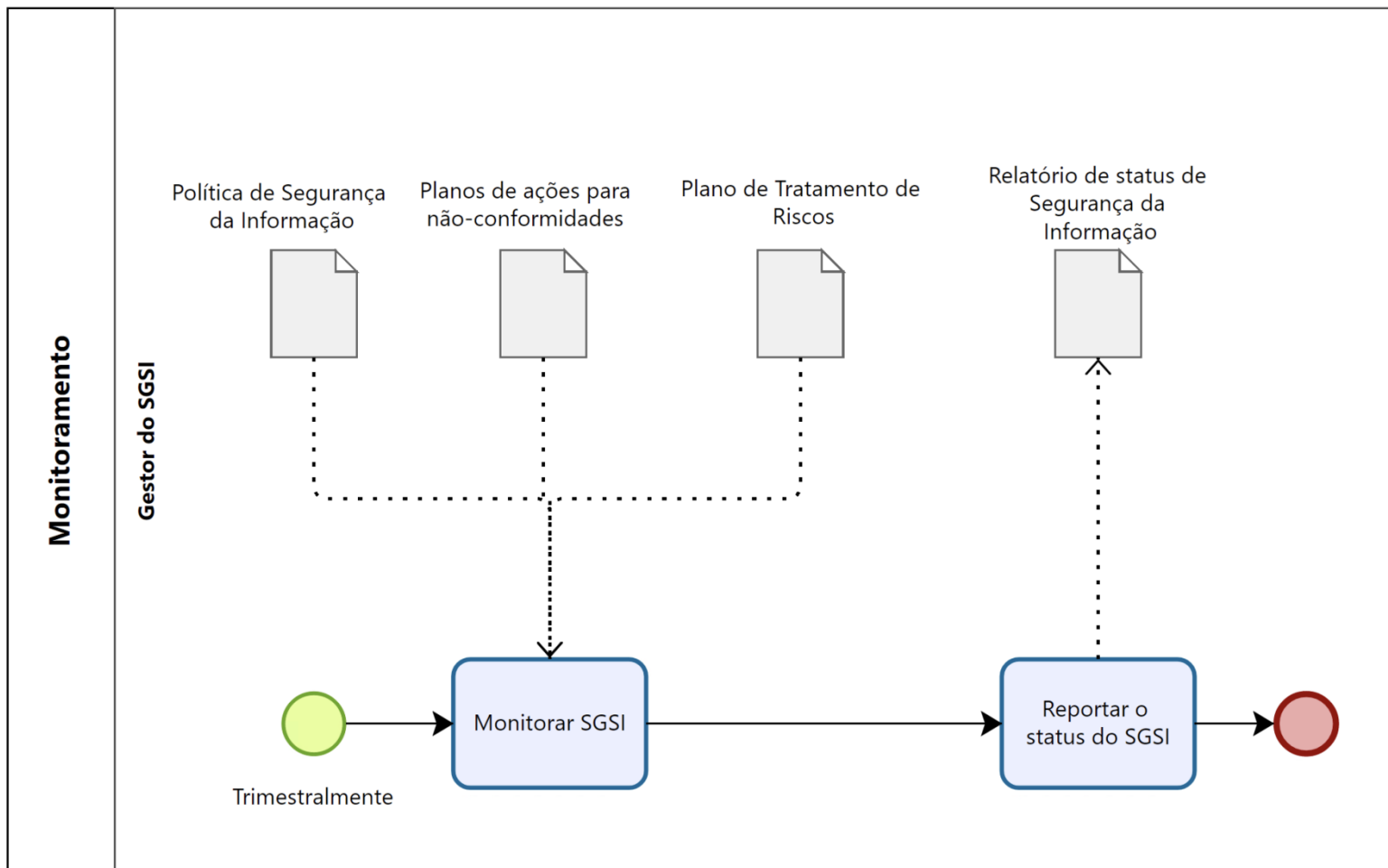


ATIVIDADE	RESPONSÁVEL	ENTRADAS	PROCEDIMENTOS	SAÍDAS
Definir Propósito, diretrizes e objetivos de SI	Gestor do SGSI	PSI atual, Relatórios de Status do SGSI,	Analisar e propor propósito, diretrizes e objetivos de SI para a nova versão da PSI	Proposta de propósito, diretrizes e objetivos de SI

		Normas sobre o tema, Planos do órgão.		
Definir comprometimento, autoridades, responsabilidades e papéis	Gestor do SGSI	PSI atual, Relatórios de Status do SGSI, Normas sobre o tema, Planos do órgão.	Analisar e propor comprometimento, autoridades, responsabilidades e papéis para a nova versão da PSI	Proposta de propósito, diretrizes e objetivos de SI
Definir planos e políticas auxiliares	Gestor do SGSI	PSI atual, Relatórios de Status do SGSI, Normas sobre o tema, Planos do órgão.	Analisar e propor planos e políticas auxiliares para nova versão da PSI	
Definir Auditoria, Monitoramento e Comunicação	Gestor do SGSI	PSI atual, Relatórios de Status do SGSI, Normas sobre o tema, Planos do órgão.	Analisar e propor funcionamento da auditoria, monitoramento e comunicação para a nova versão da PSI	
Compilar definições e proposições	Gestor do SGSI	Proposições feitas	Compilar as proposições feitas e harmonizá-las para a nova versão da PSI	Proposta de novo PSI

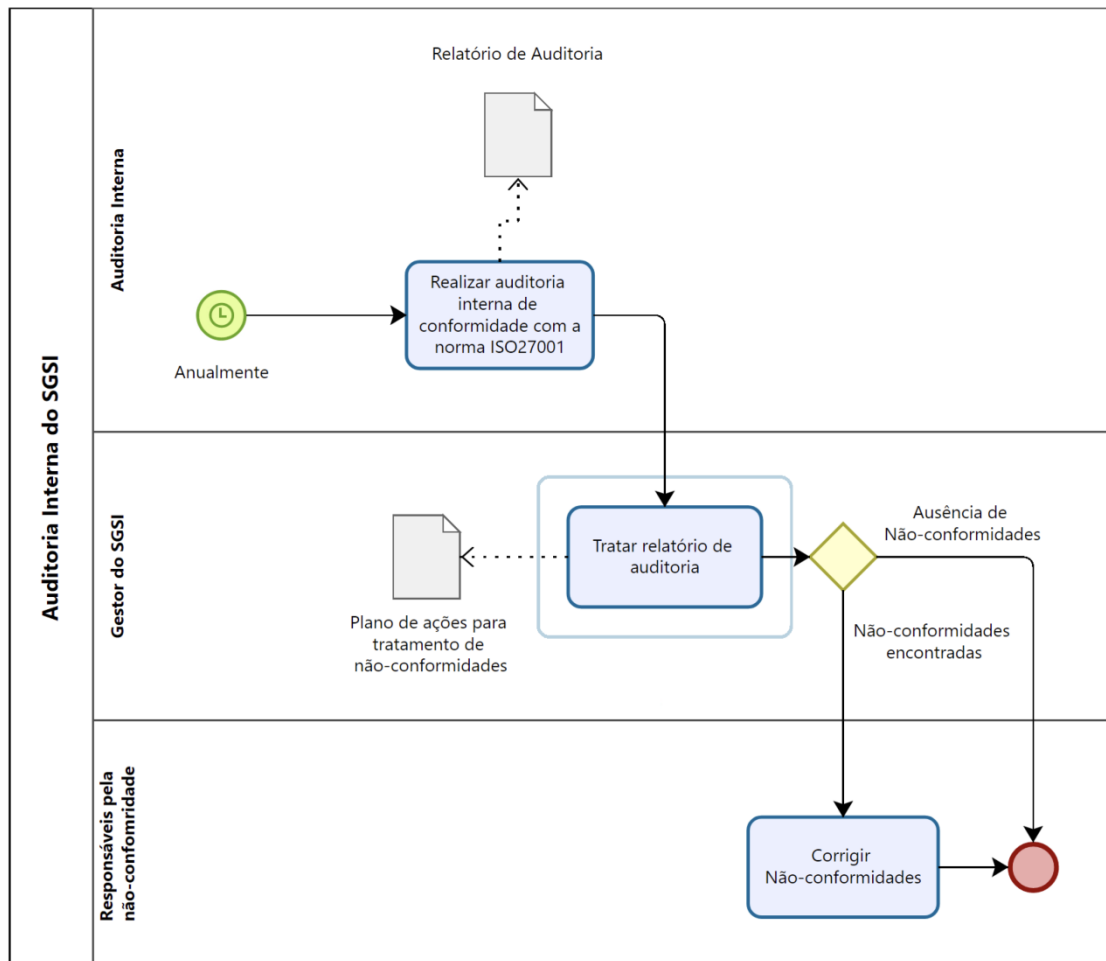
Aprovar PSI	Comitê de Segurança da Informação e Proteção de Dados	Proposta de novo PSI	Analisar e deliberar sobre a proposta da nova PSI. Em caso de necessidade de ajuste, retornar para a atividade anterior.	Nova PSI aprovada
Publicar PSI	Comitê de Segurança da Informação e Proteção de Dados	Nova PSI aprovada	Publicar no portal e comunicar o órgão sobre a nova PSI	Comunicação realizada

3.4 Subprocesso: Monitoramento do SGSI



ATIVIDADE	RESPONSÁVEL	ENTRADAS	PROCEDIMENTOS	SAÍDAS
Monitorar SGSI	Gestor do SGSI	PSI e normas complementares, Planos de ações de não-conformidades e plano de tratamento de riscos	Verificar e coletar os pontos de controles, indicadores e ações do sistema de gestão de segurança da informação	Status dos controles, indicadores e ações coletados
Reportar o status do SGSI	Gestor do SGSI	Status dos controles, indicadores e ações coletados	Criar relatório demonstrando a evolução e o status atual dos controles, indicadores e ações do SGSI.	Relatório de Status de Segurança da Informação

3.5 Subprocesso: Auditoria Interna do SGSI



ATIVIDADE	RESPONSÁVEL	ENTRADAS	PROCEDIMENTOS	SAÍDAS
Realizar auditoria interna de conformidade com a norma ISO 27001	Auditoria Interna	Evidências dos processos	Realizar auditoria interna de conformidade do sistema de gestão de segurança da informação	Relatório de Auditoria
Tratar relatório de auditoria	Gestor do SGSI	Relatório de Auditoria	Recepcionar o relatório de auditoria e planejar as ações de correção.	Plano de ações para tratamento de não-conformidades
Corrigir não-conformidades	Responsáveis pelos Riscos	Plano de ações para tratamento de não-conformidades	Executar as ações para correção de não-conformidades	Não-conformidades resolvidas