Secretaria de TIC do TRT24

GESLAIN E PEREZ MAQUER TE

Processo Gerenciar Segurança da Informação

HISTÓRICO DO DOCUMENTO

	DATA	DESCRIÇÃO
01	29/07/2013	Mapeamento e desenho do processo
02	18/03/2015	Revisão do desenho e criação do documento de descrição do processo
03	24/08/2015	Revisão do desenho (Processo Gerenciar Aplicação de Boas Práticas)
04	27/10/2015	Alinhamento dos indicadores
05	09/08/2016	Revisão do gerente do processo, inclusão das atividades de controle e ANEXOS
06	20/09/2016	Inclusão do macroprocesso e alinhamento com processo COBIT APO13 (Gerenciar Segurança)
07	20/08/2018	Revisão do fluxo das atividades do processo
08	30/06/2022	Revisão do fluxo das atividades do processo, tarefas, ativos e do mapeamento dos riscos.

Secretaria de TIC do TRT da 24ª Região

Documento de Descrição de Processo de Trabalho

Processo Gerenciar Segurança da Informação

30/06/2022

EQUIPE DE DOCUMENTAÇÃO

	Nome	Cargo
01	João Carlos Ferreira Filho	Chefe da Divisão de Governança de TIC
02	Geslaine Perez Maquerte	Chefe da Divisão de Proteção de Dados e Segurança da Informação

Sumário

1 Objetivo

- Elaborar o documento relativo ao processo de Segurança da Informação do TRT24;
- Descrever as atividades de preparação, execução e avaliação de Segurança da Informação do TRT24;
- Orientar a execução das ações relativas a preservação da confidencialidade, integridade e disponibilidade da informação.

2 Abrangência

- **Secretaria** de Tecnologia da Informação e Comunicações do TRT24ª Região.

3 Definições

- **Macroprocesso:** é um agregado de processos ou atividades afins
- **Política de Segurança da Informação (PSI):** declaração das intenções e diretrizes da instituição relativas à segurança da informação
- **Política de Gestão de Riscos:** declaração da sistemática de análise/avaliação dos riscos de segurança da informação
- **Política de Controle de Acessos:** declaração da sistemática de acesso aos recursos de TI
- **Política de Gestão de Incidentes de Segurança:** declaração dos requisitos de notificação e tratamento de incidentes
- **Política de Gestão de Continuidade de Negócios:** declaração dos requisitos de continuidade de negócios
- **PROAD:** sistema de processo administrativo eletrônico

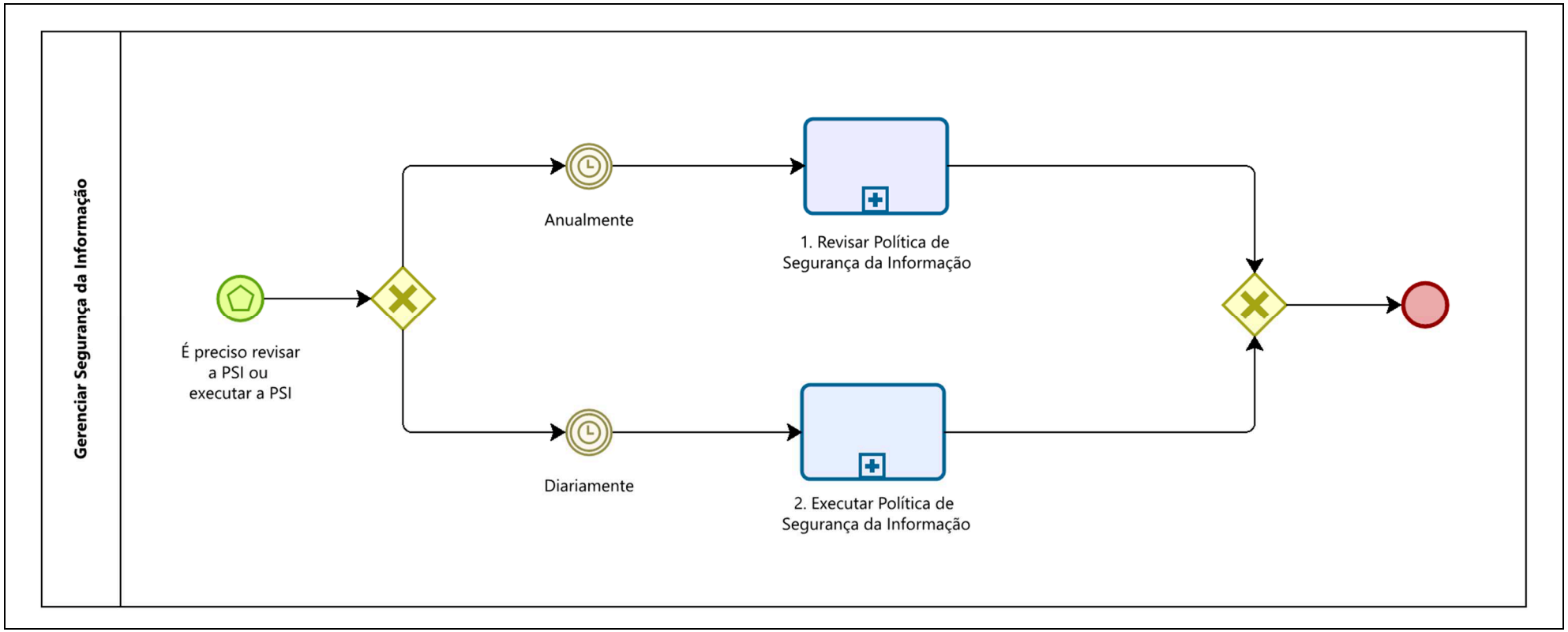
4 Processo Gerenciar Segurança da Informação

4.1 Papéis e Responsabilidades

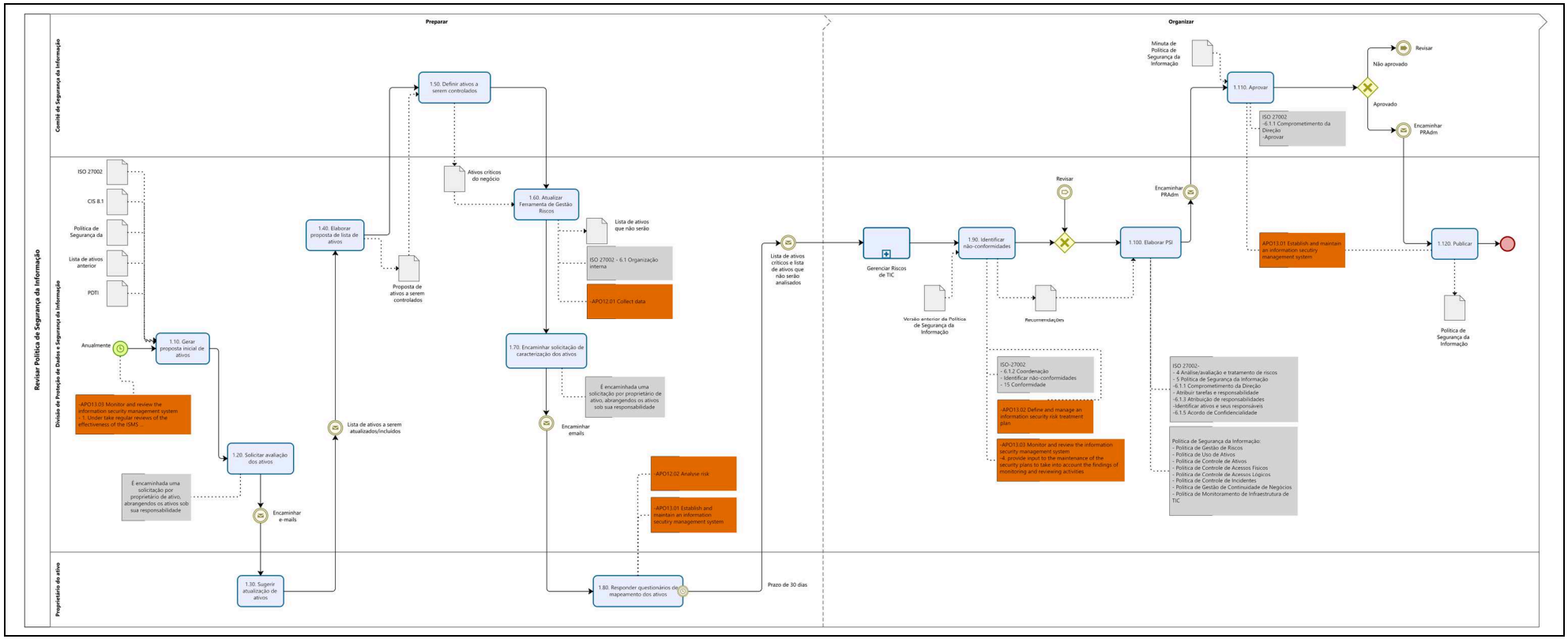
Papel	Responsabilidades	Responsável
Dono do Processo	• Buscar a qualidade e eficiência gerais do processo • Assegurar que todos os envolvidos na execução do processo sejam informados das mudanças e suporte efetuados	Diretor da SETIC
Gerente do Processo	• Buscar a eficiência e a efetividade do processo • Produzir informações gerenciais (indicadores) • Promover a execução das atividades do processo • Manter o desenho e indicadores do processo atualizados, garantindo que estejam adequados aos propósitos da organização	Chefe da Divisão de Proteção de Dados e Segurança da Informação
Comitê de Segurança da Informação	• Aprovar a Política de Segurança da Informação • Deliberar sobre eventuais providências a serem adotadas em função dos relatórios de segurança • Aprovar as atualizações do processo	Coordenador do Comitê de Segurança da Informação e Proteção de Dados
Divisão de Proteção de Dados e Segurança da Informação	• Elaborar/revisar as normas da Política de Segurança da Informação • Executar os planos táticos da PSI • Registrar os controles do processo • Elaborar relatórios de segurança	Chefe da Divisão de Proteção de Dados e Segurança da Informação
Proprietário do ativo	• Responder tempestivamente ao questionário de caracterização relativo aos ativos sob sua responsabilidade	Chefe da unidade responsável pelo ativo em análise

4.2 Fluxo do Processo

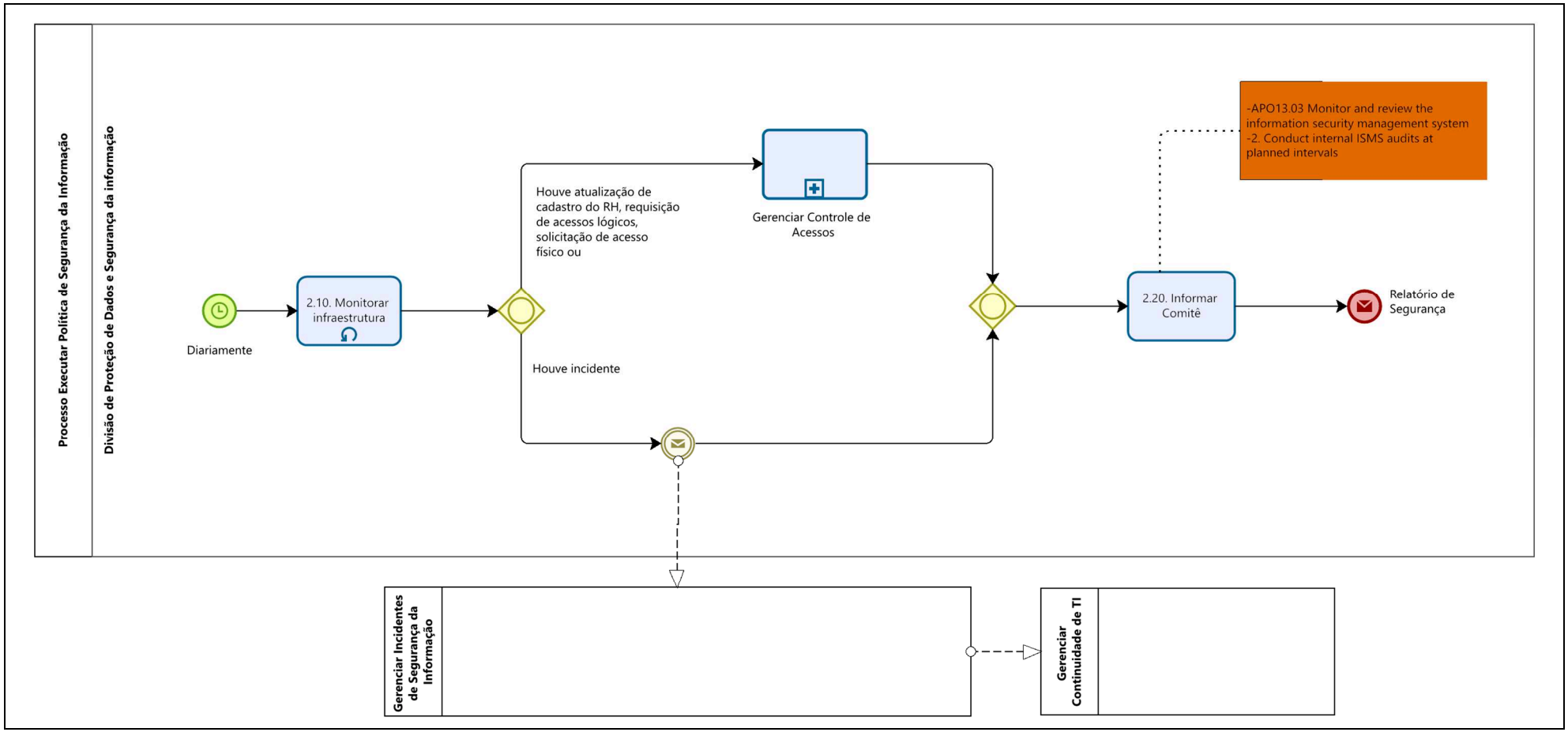
4.2.1 Fluxo macro



4.2.2 Fluxo Detalhado – Subprocesso Revisar Política de Segurança da Informação



4.2.3 Fluxo Detalhado – Subprocesso Executar Política de Segurança da Informação



4.3 Descrição do Processo

4.3.1 Descrição do subprocesso Revisar Política de Segurança da Informação

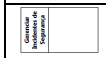
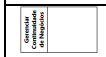
Id	Atividade	Responsável	Descrição
1.10	Gerar proposta inicial de ativos	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** ISO 27002, CIS 8.1, PSI, PDTI, Lista de Ativos Anterior
			Processamento: • Levantar, detalhar e estruturar os componentes de negócio, as ameaças, os agentes das ameaças, os perímetros e os ativos (Processos, Tecnologias, Ambientes, Pessoas e Fornecedores) que podem impactar os objetivos, missão e atividades-fim da Organização • Elaborar proposta de ativos a serem controlados, considerando a relação de ativos e processos críticos do negócio oriunda da Política de Segurança da Informação
			Saídas: Proposta de lista de ativos para atualização
1.20	Solicitar avaliação dos ativos	Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** lista de ativos críticos
			Processamento: • encaminhar a cada proprietário de ativo um e-mail com os ativos levantados da lista anterior, somados à PSI, PDTI e sugestões da Divisão de Proteção de Dados e Segurança da Informação para validação e sugestões de alterações, inclusões, ou exclusões
			Saídas: e-mails para os proprietários de ativos
1.30	Sugerir atualização dos ativos	Proprietário do Ativo	**Entradas:** e-mails de orientação
			Processamento: • Validar ativos, incluindo, alterando e excluindo quando necessário
			Saídas: Lista de ativos a serem atualizados/incluídos
1.40	Elaborar proposta de lista de ativos	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** PETI, ISO 27002, COBIT, PSI, CIS 8.1
			Processamento: • Elaborar proposta de ativos a serem controlados, considerando as sugestões recebidas dos proprietários de ativos
			Saídas: proposta de lista de ativos críticos
1.50			**Entradas:** proposta de lista de ativos a serem controlados

	Definir ativos a serem controlados	Comitê Segurança da Informação	**Processamento:** • Examinar proposta elaborada pela Divisão de Proteção de Dados e Segurança da Informação e manter, incluir ou excluir ativos. Para os ativos retidos, deverão ser definidas as suas relevâncias e criticidades para o Tribunal. **Saídas:** lista de ativos críticos
1.60	Atualizar Ferramenta de Gestão Riscos	Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** lista de ativos críticos **Processamento:** • Para cada elemento da lista de ativos, acessar a base da Ferramenta de Gestão Riscos e verificar se há definições para o ativo a ser avaliado dentro da metodologia utilizada • Atualizar/criar base para os ativos que serão analisados, considerando os recursos necessários (expertise, pessoal disponível, tempo...) e definir as características e o escopo do projeto de análise de risco, gerar questionários, bem como definir as pessoas que os responderão (proprietários ou respondentes) • Registrar os ativos não incluídos na base da **lista de ativos que não serão analisados** **Saídas:** questionários de avaliação do(s) ativo(s) e definição dos respondentes e lista de ativos que não serão analisados
1.70	Encaminhar solicitação de caracterização dos ativos	Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** lista de ativos críticos **Processamento:** • Encaminhar a cada proprietário de ativo um e-mail com as orientações para utilização da ferramenta e para preenchimento dos respectivos questionários de caracterização **Saídas:** e-mails para os proprietários de ativos
	Encaminhar e-mails		Encaminhar e-mail para todos os proprietários de ativos orientando como proceder para responder aos questionários
1.80	Responder questionários de mapeamento dos ativos	Proprietário do Ativo	**Entradas:** e-mails de orientação **Processamento:** • Responder aos questionários conforme orientações **Saídas:** Lista de ativos atualizada com as características dos ativos críticos
	Processo Gerenciar Riscos de TIC	Divisão de Proteção de Dados e Segurança da Informação	O processo **Gerenciar Riscos de TIC** será executado anualmente para avaliar os riscos dos ativos críticos do negócio

1.90	Identificar não-conformidades	Divisão de Proteção de Dados e Segurança da Informação	Entrada: Escopo, metas de segurança, normas e políticas pertinentes
			Processamento: • Avaliar as informações e controles de segurança gerados pela execução das políticas vigentes que integram a PSI • Identificar os eventos/ações/procedimentos não alinhados as políticas vigentes e que precisam ser regulamentados, conforme uma das seguintes possibilidades: o Incluir a regulamentação do tratamento do evento/ação/procedimento na política apropriada o Incluir a proibição do evento/ação/procedimento na política apropriada
			Saída: Recomendações para alinhamento das não-conformidades
1.100	Elaborar Política de Segurança da Informação	Divisão de Proteção de Dados e Segurança da Informação	Entrada: Versão anterior da PSI, recomendações da análise de não-conformidades, ISO27002, COBIT
			Processamento: • Definir as diretrizes, escopo e os limites em função das características do negócio • Alinhar as definições com a abordagem da instituição para a gestão da segurança • Definir e mapear o processo de trabalho relativo a segurança da informação • Definir os responsáveis e responsabilidades para cada um dos papéis previstos no processo de trabalho • Preparar e manter uma declaração de aplicabilidade que descreve o escopo da infraestrutura de segurança, processos e ativos críticos do negócio. • Definir a abordagem de comunicação da política
			Saída: minuta da revisão da PSI juntada no PROAD
	Encaminhar PROAD		Encaminhar o PROAD do Processo Gerenciar Segurança da Informação ao Comitê de Segurança da Informação, com despacho solicitando a aprovação da minuta da Política de Segurança da Informação
1.110	Aprovar	Comitê de Segurança da Informação	Entrada: PROAD (minuta de Política de Segurança da Informação)
			Processamento: • Fazer reunião para deliberação e aprovação • Juntar ao PROAD a ata da reunião
			Saída: ata de reunião juntada ao PROAD

	Encaminhar PROAD		Encaminhar o PROAD a SETIC
1.120	Publicar	Divisão de Proteção de Dados e Segurança da Informação	Entrada: Minuta aprovação da Política de Segurança da Informação
			Processamento: • Juntar a minuta ao PROAD do Processo Gerenciar Segurança da Informação • Disponibilizar despacho de encaminhamento do PROAD a DG solicitando a expedição de portaria de regulamentação • Enviar dados da portaria por chamado para Publicação da nova Portaria no site de Governança da SETIC
			Saída: Portaria da Política de Segurança da Informação publicada no site de governança da SETIC

4.3.2 Descrição do subprocesso Executar Política de Segurança da Informação

Id	Atividade	Responsável	Descrição
	Gerenciar Controle de Acessos	Divisão de Proteção de Dados e Segurança da Informação	O processo **Gerenciar Controle de Acessos s**erá executado quando houver necessidade de acesso físico aos ambientes de TIC ou acesso lógico aos ativos de TIC
	Gerenciar Incidentes de Segurança da Informação	Divisão de Proteção de Dados e Segurança da Informação	O processo **Gerenciar Incidentes de Segurança da Informação** será executado quando o monitoramento da infraestrutura detectar um incidente
	Gerenciar Continuidade de Negócios	Divisão de Proteção de Dados e Segurança da Informação	O processo **Gerenciar Continuidade de Negócios** será executado quando um incidente de segurança demandar procedimentos de continuidade
2.10	Monitorar infraestrutura	Divisão de Proteção de Dados e Segurança da Informação	Entrada: Controles do processo
			Processamento: • Monitorar alertas de segurança nos ativos de infraestrutura de TI com auxílio de ferramentas especializadas • Analisar e avaliar as providências pertinentes aos eventuais alertas retirados das ferramentas observadas
			Saída: incidente de segurança da informação
2.20	Informar Comitê de Segurança da Informação	Divisão de Proteção de Dados e Segurança da Informação	Entrada: incidente de segurança da informação
			Processamento: • Elaborar relatório contendo, no mínimo, as seguintes informações: o Descrição e detalhamento dos eventuais incidentes o Descrição dos tratamentos executados, assim como plano de ação preventiva para evitar novos eventos similares ocorram ou, se ocorrerem, se reduzam os danos. o Juntar o relatório ao PROAD do Processo de Segurança da Informação e despachar ao Comitê de Segurança
			Saída: PROAD encaminhado ao Comitê de Segurança da Informação

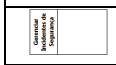
5 Tabela RACI

5.1 Subprocesso Revisar Política de Segurança da Informação

	Atividade	Comitê de Segurança da Informação	Divisão de Proteção de Dados e Segurança da Informação	Proprietários dos ativos
1.10	Gerar proposta inicial de ativos		R	
1.20	Solicitar avaliação dos ativos		R	C
1.30	Sugerir atualização de ativos		C	R
1.40	Elaborar proposta de lista de ativos	C	R	
1.50	Definir ativos a serem controlados	R	I	
1.60	Atualizar Ferramenta de Gestão Riscos		R	
1.70	Encaminhar solicitação de caracterização dos ativos		R	I
1.80	Responder questionários de mapeamento dos ativos		C	R
1.90	Identificar não-conformidades		R	C
1.100	Elaborar PSI	C	R	C
1.110	Aprovar	R	I	I
1.120	Publicar	I	R	I

Legenda: Responsável (R), Consultado (C), Informado (I)

5.2 Subprocesso Executar Política de Segurança da Informação

	Atividade	Comitê de Segurança da Informação	Divisão de Proteção de Dados e Segurança da Informação
	Gerenciar Controle de Acessos		R
	Gerenciar Monitoramento da Infraestrutura de TIC		R
	Gerenciar Incidentes de Segurança da Informação		R
	Gerenciar Continuidade de Negócios		R
2.10	Monitorar infraestrutura		R
2.20	Informar Comitê de Segurança da Informação	I	I

Legenda: Responsável (R), Consultado (C), Informado (I)

6 Indicadores do processo

6.1 Descrição dos indicadores

Nome do indicador	Índice de sucesso de indicadores de segurança
Origem	• APO13 (Gerenciar Segurança) • PAM outcome: APO13-03 • PAM base practices: AP013-BP3 ○ Enabling process Key management practice: APO13.03
Objetivo	Medir se as soluções de segurança são implementadas e executadas consistentemente em toda a organização
Meta	60%
Periodicidade	Trimestral
Forma de cálculo	Nº de indicadores dos processos de segurança na meta / nº de indicadores dos processos de segurança

Fonte	• Planilha do ANEXO I
	  ○ Nº de indicadores dos processos de segurança na meta: ver o valor da coluna “total de indicadores na meta
	  ○ Nº de indicadores dos processos de segurança: ver o valor da coluna “total de indicadores”

7 Divulgação dos resultados

Os resultados do processo serão demonstrados através dos indicadores de desempenho registrados no processo administrativo autuado com o fim específico de acompanhar as atividades desse processo de trabalho, bem como no site de governança da SETIC, menu Indicadores, item Indicadores Gerenciais, processo Gerenciar Segurança da Informação

8 ANEXO I – Índice de sucesso de indicadores de segurança

Data do registro	Nº de indicadores	Nº de indicadores na meta

Onde:

- **Para cada execução do processo:**
  - **Data do registro:** data de referência do registro
  - **Nº de indicadores de segurança**: ver a quantidade total de indicadores relativos aos processos de segurança previstos na PSI
  - **Nº de indicadores na meta:** ver a quantidade de indicadores dos processos previstos na PSI que estão na meta