PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 8ª REGIÃO

PORTARIA PRESI Nº 1231, DE 23 DE NOVEMBRO DE 2017

Define o processo de gerenciamento de ativos e riscos de TIC.

A **DESEMBARGADORA VICE-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA OITAVA REGIÃO**, no uso de suas atribuições legais e regimentais,

CONSIDERANDO que constitui iniciativa estratégica da Justiça do Trabalho da 8ª Região estabelecer a gestão de riscos, com base no desenvolvimento de metodologia, capacitação e implantação da cultura do gerenciamento de riscos de modo a promover ações relativas ao tratamento de riscos inerentes às atividades institucionais;

CONSIDERANDO o que consta na Resolução nº 31, de 8 de junho de 2015, que instituiu a Política de Gestão de Riscos da Secretaria e dos Serviços Auxiliares do Tribunal Regional do Trabalho da 8ª Região;

CONSIDERANDO as ações previstas no Planejamento Estratégico de Tecnologia da Informação e Comunicação do Tribunal Regional do Trabalho da 8ª Região com a implantação dos controles da ISO 27001 aderentes à Política de Segurança da Informação do TRT da 8ª Região;

CONSIDERANDO a observância das recomendações do Código de Boas Práticas em Segurança da Informação publicado pelo Tribunal de Contas da União;

CONSIDERANDO a observância e a conformidade à norma ISO 27005:2011, que trata da gestão de riscos de segurança da informação;

CONSIDERANDO a Portaria PRESI nº 757 de 28 de julho de 2016 que estabelece a Política de Controle de Ativos de Tecnologia da Informação do Tribunal Regional do Trabalho da 8ª Região;

CONSIDERANDO a Portaria PRESI nº 1068/2015 de 13 de novembro de 2015 que estabelece a Política de Controle de Ativos de Tecnologia da Informação do Tribunal Regional do Trabalho da 8ª Região,

RESOLVE:

Art. 1º Fica aprovado, na forma do Anexo a esta Portaria, o processo de gerenciamento de ativos e riscos de TIC do Tribunal Regional do Trabalho da 8ª Região.

Art. 2º O Assistente de Segurança da Informação será o responsável por manter atualizado o processo previsto no art. 1º.

Parágrafo único. As versões atualizadas deverão ser publicadas em área específica do sítio do Tribunal, no endereço www.trt8.jus.br.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

Publique-se, dê-se ciência e cumpra-se.

SULAMIR PALMEIRA MONASSA DE ALMEIDA
Vice-Presidente,
no exercício da Presidência

Processo de Gerenciamento de Ativos e Riscos de TIC

Histórico de Alterações

Data	Versão	Descrição	Autor
24/11/17	1.0	Processo formal de gerenciamento de Ativos e Riscos de TIC	Thiago da Silva Gilla

Sumário

1. Objetivo

Atender às demandas de gestão de ativos e riscos de TI, determinando um processo formal, baseado no Manual de Gestão de Riscos do TRT8, Portaria PRESI nº 1068/2015 e na norma ABNT NBR ISO/IEC 27005:2011, que trata da gestão de riscos de segurança da informação.

2. Escopo

Este processo tem por orientação a portaria PRESI nº 757 de 28 de julho de 2016 que estabelece a Política de Controle de Ativos de Tecnologia da Informação do Tribunal Regional do Trabalho da 8ª Região. Desta forma, tem por escopo os ativos restritos àqueles para os quais se pretende gerenciar riscos.

3. Definições

Ameaça: ação de origem humana (intencional ou acidental) ou ambiental, que explora uma vulnerabilidade presente num ativo e provoca impactos na organização.

Ativo: qualquer recurso que possui valor para a organização e cujo risco precisa ser controlado e gerenciado. Pode ser uma operação, uma atividade, um projeto, um programa, um serviço, um processo ou mesmo um objetivo estratégico.

Controle: políticas, práticas, procedimentos, estruturas organizacionais, dispositivos de hardware e funções de software, que visam eliminar vulnerabilidades ou minimizar os impactos causados por incidentes.

Impacto: consequência sobre os ativos e negócios de uma organização, caso uma ameaça venha a se efetivar.

Incidente de segurança: materialização de uma ameaça. Um incidente de segurança provoca danos a um ou mais ativos, além de impactos ao negócio.

Probabilidade: possibilidade de concretização de uma ameaça.

Risco: é a combinação da probabilidade de que algum incidente ocorra e sua conseqüência.

Risco residual: é o nível de risco remanescente após a organização ter aplicado ações de controle do risco.

Vulnerabilidade: fragilidade de um ativo que pode ser explorada por uma ameaça.

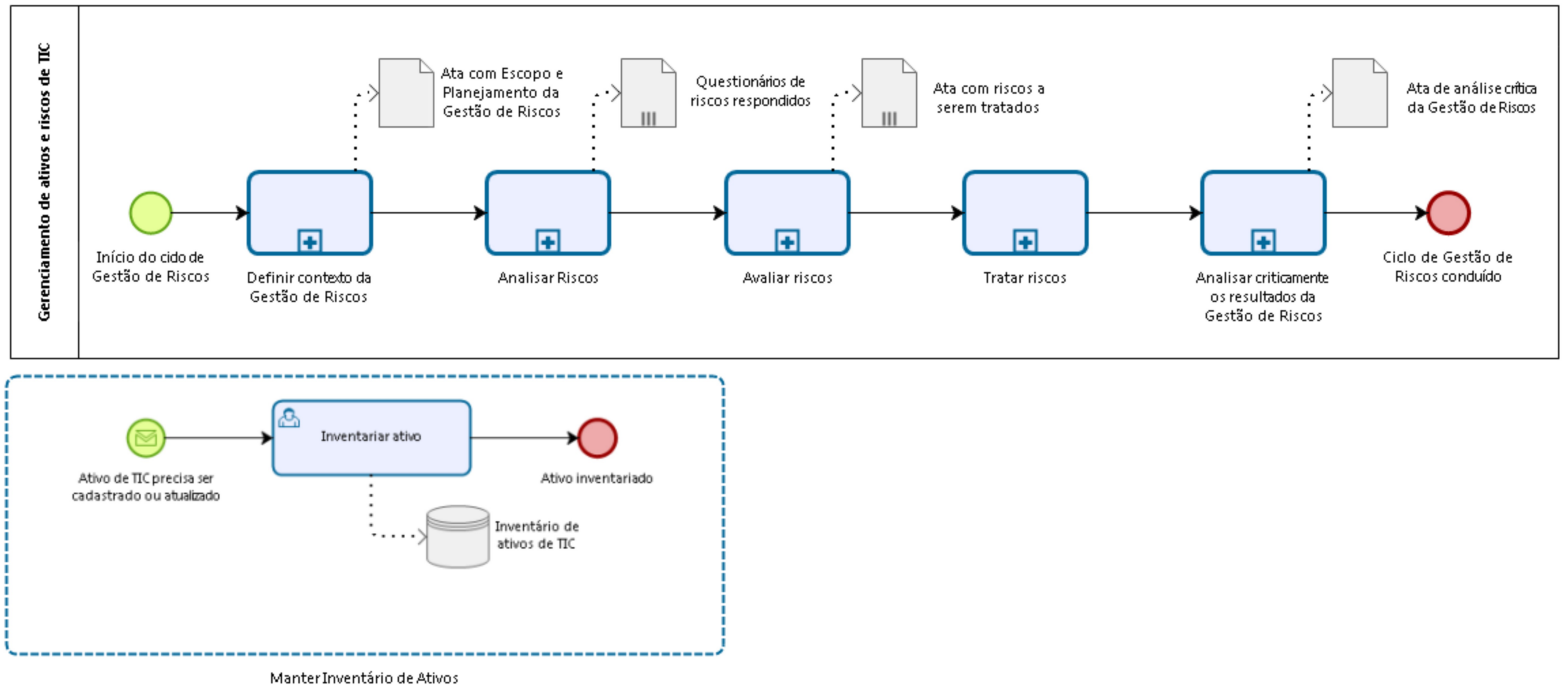
4. Papéis e responsabilidades

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; • Definir o escopo de cada ciclo de gestão de riscos de TIC;	Comitê Gestor de Segurança da Informação

	• Aprovar o Relatório de Análise de Riscos; • Aprovar as demandas do Plano de Tratamento de Riscos.	
Gerente do Processo	• Buscar a eficiência e a efetividade do processo; • Produzir informações gerenciais (indicadores gerenciais); • Promover a execução das atividades do processo; • Manter o desenho e indicadores do processo atualizados, garantindo que estejam adequados aos propósitos da organização.	Assistente de Segurança da Informação
Responsável pelo ativo	• Cadastrar os ativos, mantendo as informações sobre estes; • Cooperar com a avaliação dos riscos, apoiando o Gerente do processo sempre que solicitado; • Preencher os questionários de avaliação de riscos; • Aplicar os controles do tratamento de riscos para o ativo.	Servidor da SETIN designado como responsável pelo ativo

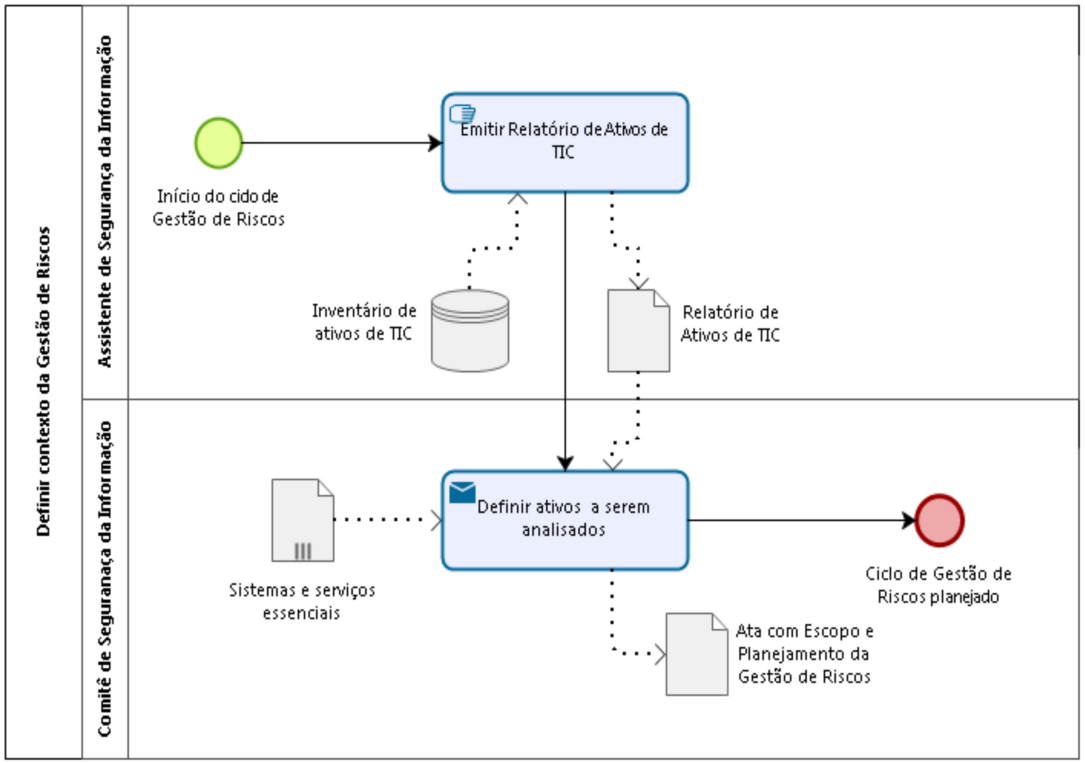
5. Fluxo do processo

Fluxo Geral

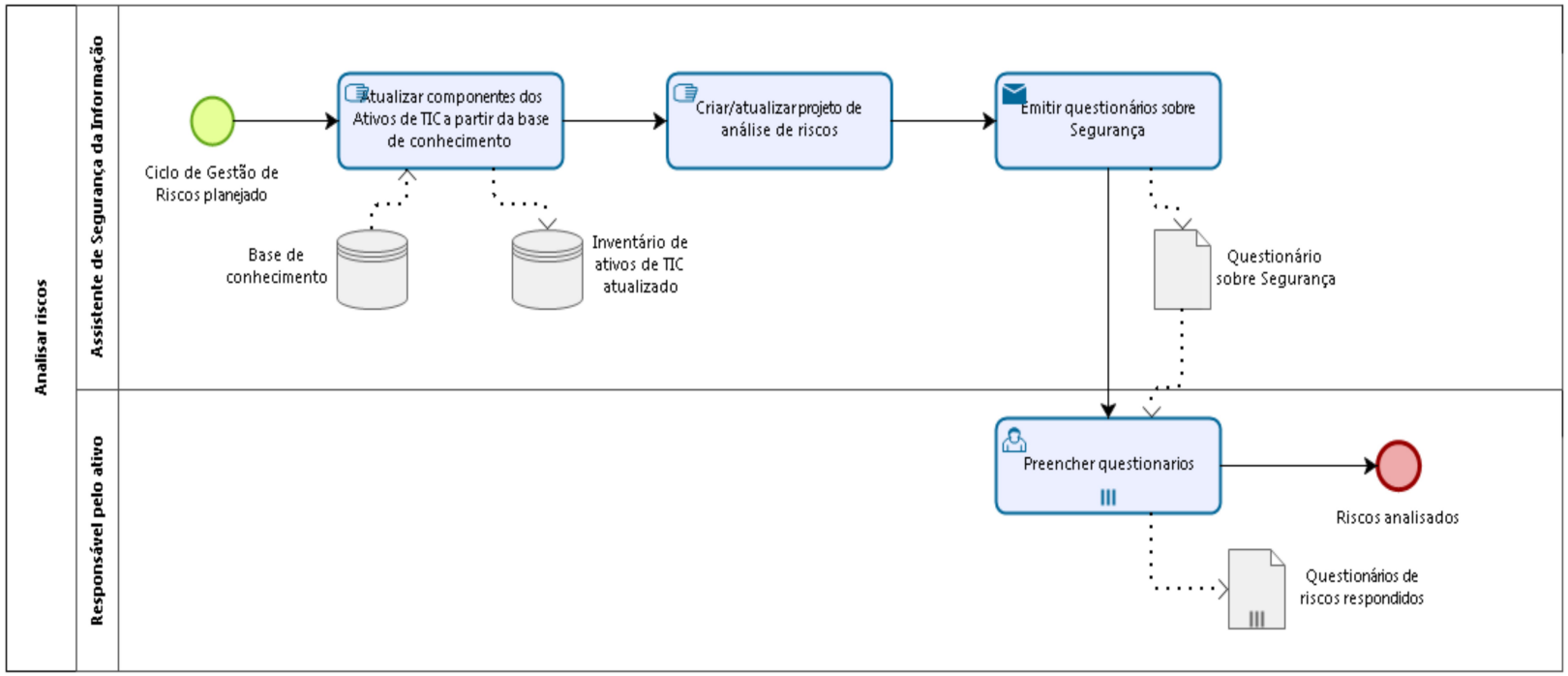


Manter inventário de Ativos

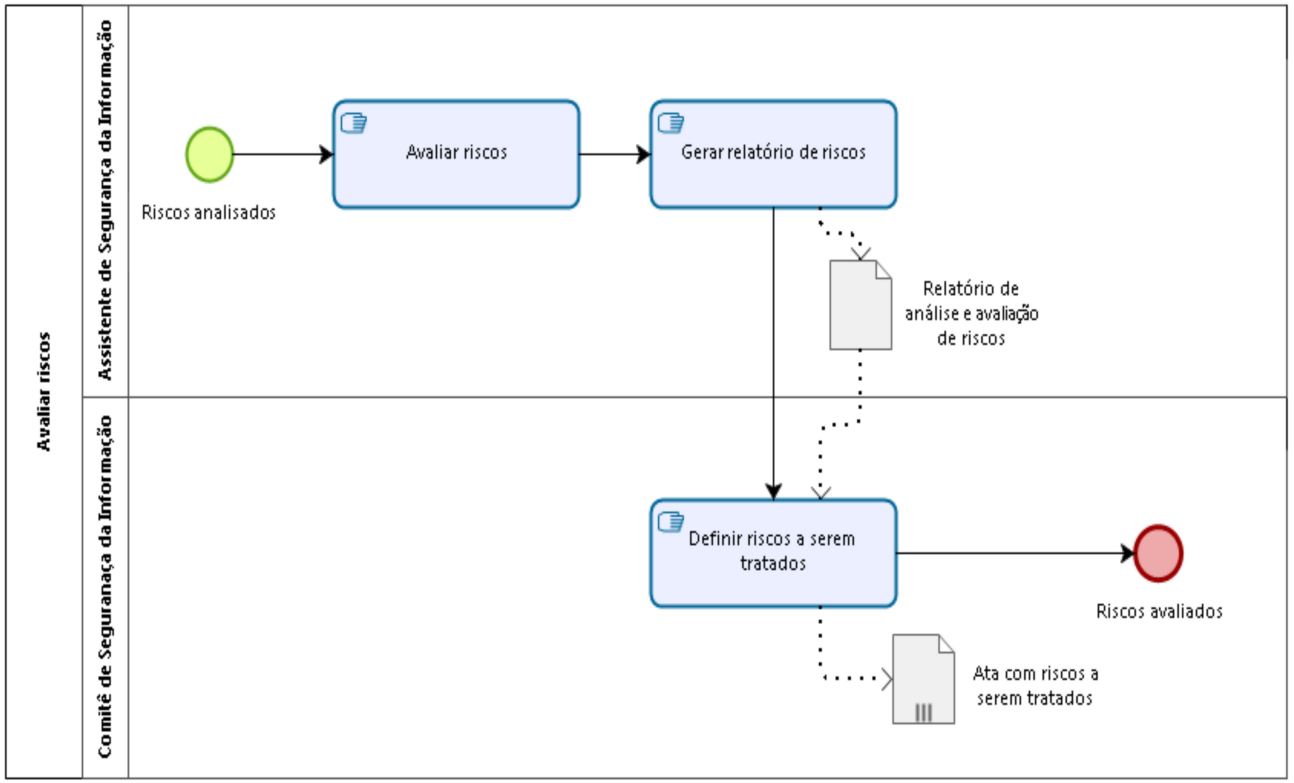
Definir Contexto da Gestão de Riscos



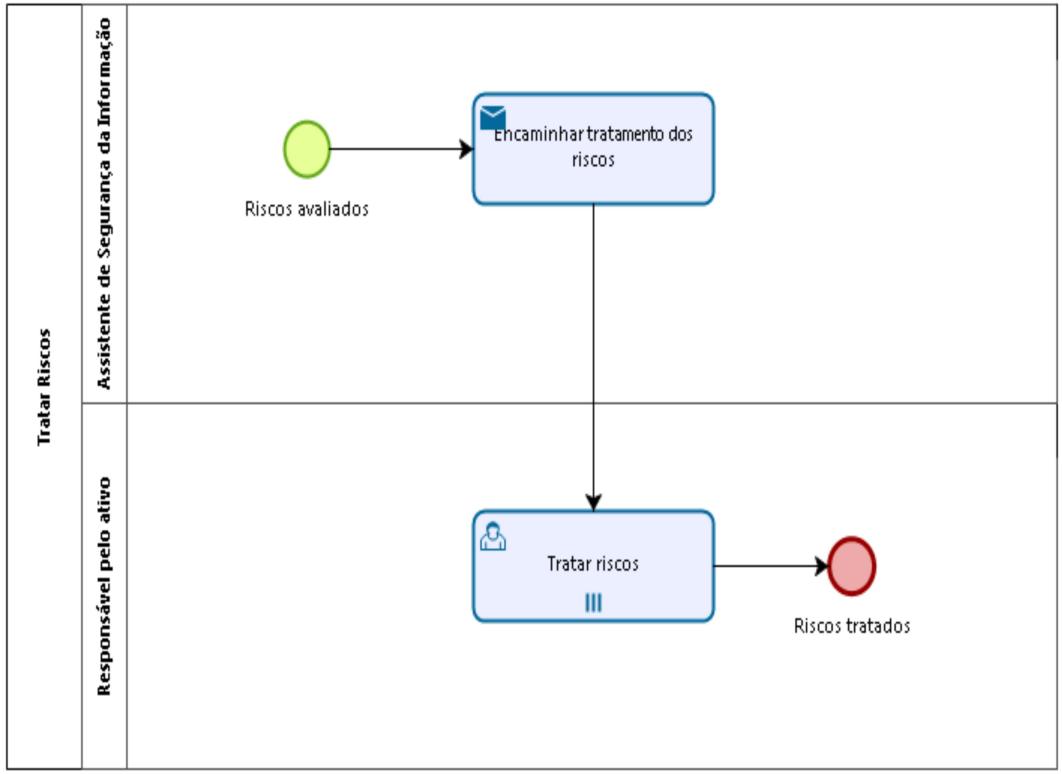
Analisar Riscos



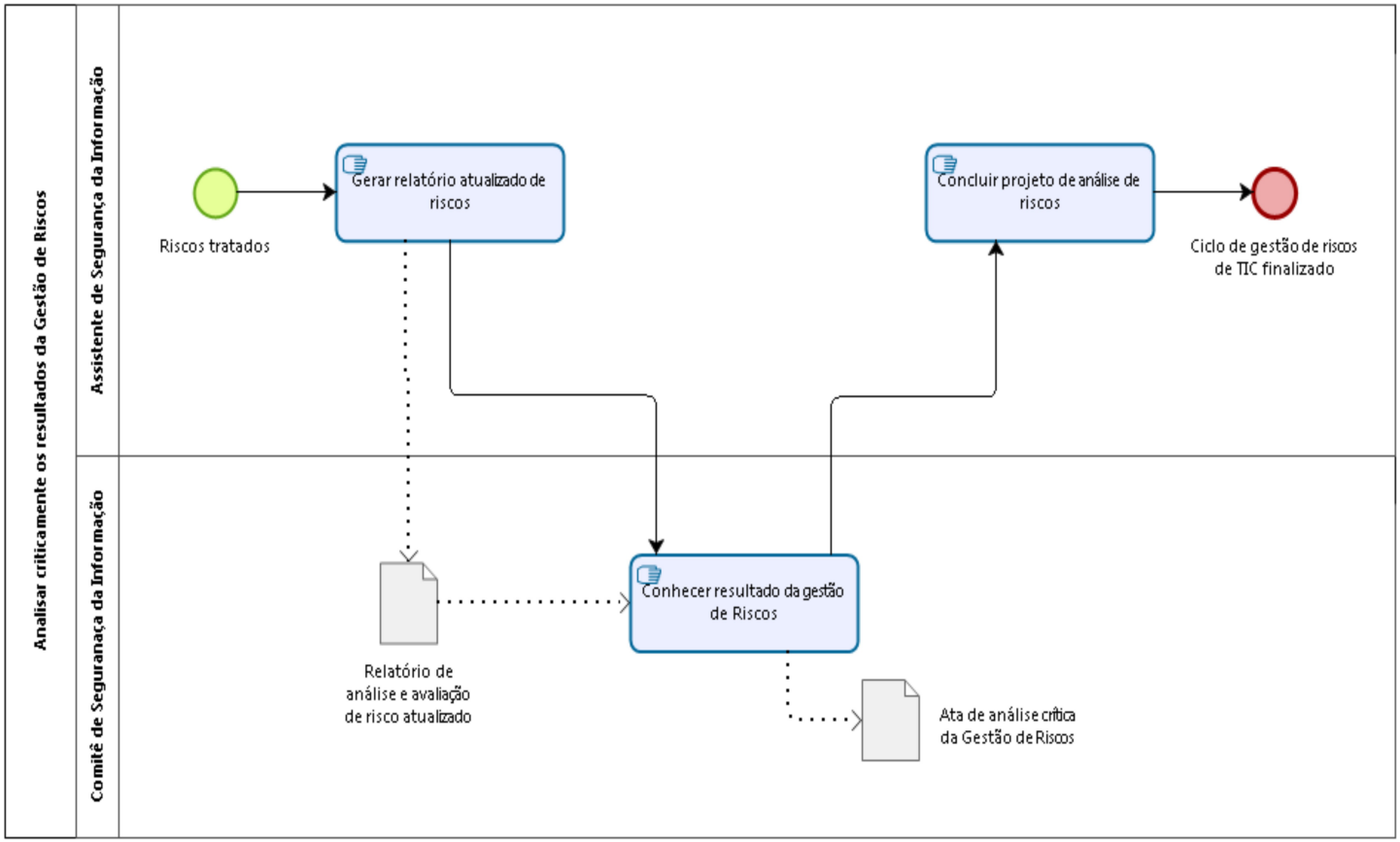
Avaliar Riscos



Tratar Riscos



Analisar criticamente os resultados da Gestão de Riscos



6. Descrição do processo de gerenciamento de ativos e riscos de TIC

Id	Atividade	Objetivo	Responsável	Descrição
1	Inventariar ativo.	Manter o cadastro dos ativos de TIC.	Responsável pelo ativo.	Entrada: compra de novo ativo ou atualização de informações sobre um ativo já existente.
				Processamento: cadastro/atualização do ativo.
				Saída: banco de dados de ativos.
2	Emitir relatório de ativos de TIC.	Subsidiar a gestão dos ativos de TIC.	Assistente de Segurança da Informação.	Entrada: Inventário de ativos de TIC.
				Processamento: configuração do relatório.
				Saída: relatório de ativos de TIC.
3	Definir ativos a serem analisados.	Definir o escopo do projeto de análise/avaliação de	Comitê Gestor de Segurança da	Entrada: lista de sistemas e serviços essenciais deTIC.
				Processamento: seleção dos sistemas e serviços que sofrerão

		riscos.	Informação.	análise e avaliação de riscos.
				Saída: ata com escopo e planejamento da Gestão de Riscos.
4	Atualizar componentes dos ativos a partir da base de conhecimento.	Determinar os componentes de configuração refletindo a realidade dos ativos.	Assistente de Segurança da Informação.	Entrada: ata com escopo e planejamento da Gestão de Riscos e banco de dados da base de conhecimento.
				Processamento: relacionar ativos que suportam os sistemas e serviços e cadastrar/atualizar os componentes de cada ativo.
				Saída: inventário de ativos de TIC atualizado.
5	Criar/Atualizar projeto de análise de riscos.	Criar projeto de análise de riscos, fazendo as parametrizações necessárias à avaliação requerida.	Assistente de Segurança da Informação.	Entrada: lista dos ativos que serão analisados.
				Processamento: Definir as características, o escopo do projeto e gerar questionários.
				Saída: questionários de análise dos ativos de TIC.
6	Emitir questionário sobre	Obter o nível de adoção	Assistente de	Entrada: lista dos ativos que serão analisados.

	Segurança	dos controles de segurança para cada ativo do projeto	Segurança da Informação.	Processamento: gerar questionário a partir da base de conhecimento do ativo.
				Saída: questionário sobre segurança.
7	Preencher questionários.	Avaliar a existência de controles de segurança e o nível de risco associado ao ativo.	Responsável pelo ativo.	Entrada: questionário sobre segurança.
				Processamento: analisar cada controle e verificar se o ativo está atendendo cada um deles.
				Saída: questionários de riscos respondidos.
8	Avaliar riscos.	Avaliar a existência de controles e o nível de risco associado ao ativo.	Assistente de Segurança da Informação.	Entrada: questionários de riscos respondidos.
				Processamento: avaliar os riscos baseado na metodologia de gestão de riscos do TRT8.
				Saída: classificação dos riscos de TIC.
9	Gerar relatório de riscos.	Subsidiar a decisão	Assistente de	Entrada: classificação dos riscos de TIC.

		sobre a priorização do tratamento dos riscos.	Segurança da Informação.	Processamento: emissão do relatório.
				Saída: relatório de análise/avaliação dos riscos.
10	Definir riscos a serem tratados.	Definir o escopo do tratamento dos riscos.	Comitê Gestor de Segurança da Informação.	Entrada: relatório de análise/avaliação dos riscos de TIC.
				Processamento: analisar a metodologia de gestão de riscos do TRT8, o planejamento estratégico institucional, os custos de tratamento e definir os riscos que serão tratados.
				Saída: ata com riscos a serem tratados.
11	Encaminhar tratamento dos riscos.	Distribuir aos responsáveis pelos ativos solicitação de tratamento dos ativos de TIC.	Assistente de Segurança da Informação.	Entrada: lista de riscos a serem tratados.
				Processamento: selecionar os riscos a serem tratados e solicitar o tratamento aos respectivos responsáveis pelos ativos.
				Saída: encaminhamento do tratamento dos riscos.
12	Tratar riscos.	Configurar os controles	Responsável pelo	Entrada: encaminhamento do tratamento dos riscos.

		determinados para os ativos de TIC.	ativo.	Processamento: configurar os controles para o tratamento dos ativos.
				Saída: ativos com controles configurados.
13	Gerar relatório atualizado de riscos.	Exibir o resultado da aplicação do ciclo de gestão de riscos de TIC.	Assistente de Segurança da Informação.	Entrada: ativos com controles configurados.
				Processamento: emissão de relatório.
				Saída: relatório atualizado de análise/avaliação de riscos.
14	Conhecer resultado da gestão de riscos.	Avaliar criticamente a gestão de riscos de TIC.	Comitê Gestor de Segurança da Informação.	Entrada: relatório atualizado de análise/avaliação de riscos.
				Processamento: analisar o tratamento dos riscos e se os riscos residuais são aceitáveis.
				Saída: ata de análise crítica da Gestão de Riscos.

15	Concluir Projeto de análise de riscos.	Encerrar o ciclo de gestão de riscos de TIC.	Assistente de Segurança da Informação.	Entrada: ata da reunião do Comitê Gestor de Segurança da Infrormação.
				Processamento: registro das sugestões e melhorias a serem realizadas no próximo ciclo.
				Saída: encerramento do projeto.