PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
de Santa Catarina
Diretoria-Geral Administrativa
Diretoria de Tecnologia da Informação

MACROPROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Data: 12/11/2020
Versão 1.0

HISTÓRICO DE ALTERAÇÕES

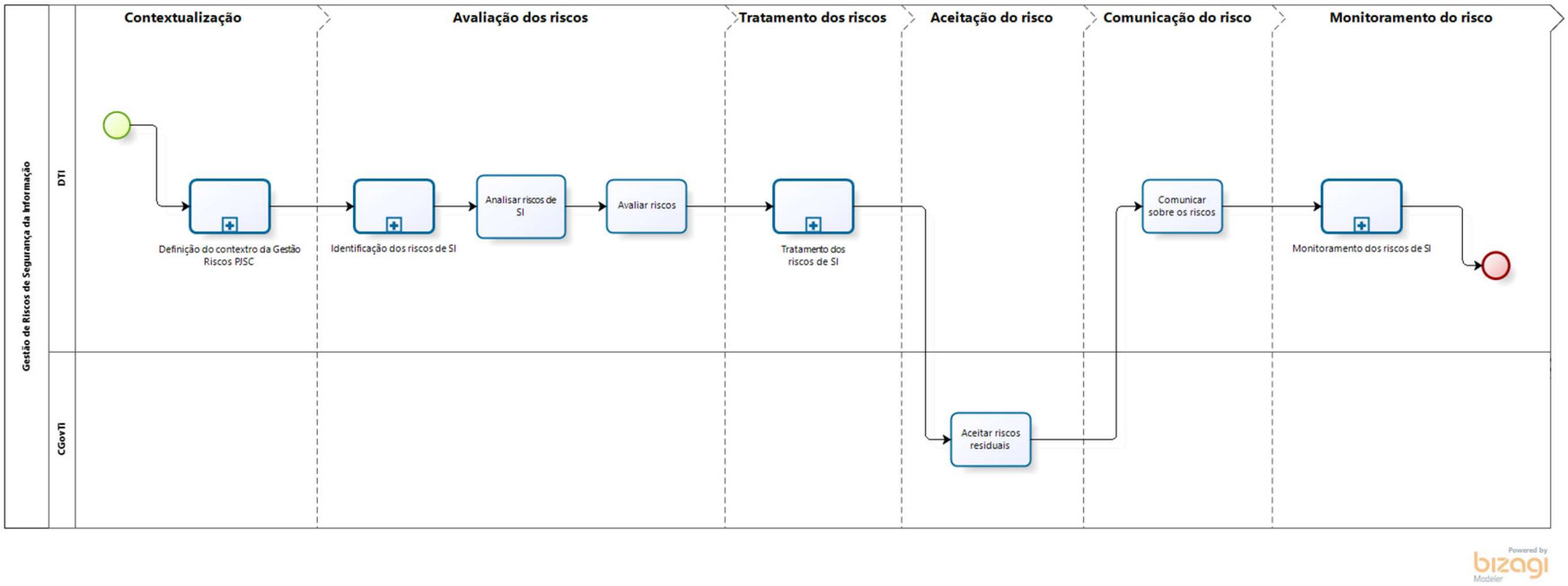
DOCUMENTO		
Descrição	Documentação dos processos de segurança da informação	
Objetivo	Este documento descreve os subprocessos e atividades componentes do Macroprocesso de Gestão de Riscos de Segurança da Informação do PJSC	
Setor	Secretaria de Segurança da Informação e Gestão de Riscos - SSIGR	
Responsável	**Nome/Matrícula** Rinaldo Feldmann - 2160	**Criado em** 20/10/2020

V E R S I O N A ME N TO S			
Versão	Data	Autor	Descrição
1.0	20/10/2020	Rinaldo Feldmann	Criação do Documento

SUMÁRIO

MACROPROCESSO DE GESTÃO DE RISCOS DE SI

Diagrama do Processo



PAPÉIS E RESPONSABILIDADES

Papéis		Responsabilidades
Comitê de Governança de Tecnologia da Informação (CGOVTI)	Comitê multidisciplinar formado por magistrados e servidores, vinculado à Presidência, de natureza deliberativa e de caráter permanente.	Analisar criticamente o plano de tratamento do risco e do processo de avaliação do risco residual e decidir pela sua aceitação ou não.
Diretoria de Tecnologia da Informação (DTI)	Tem como atribuições propor políticas, objetivos, estratégias, investimentos e prioridades de tecnologia da informação - TI e implementar ações que visem melhorar a gestão dos serviços e otimizar os recursos de TI, no âmbito do Poder Judiciário do Estado de Santa Catarina – PJSC.	Elaborar o desenho e detalhar os processos e atividades componentes do macroprocesso de gestão de riscos de SI, bem como elaborar a normatização correlata. Levantar informações relativas às etapas de contextualização, avaliação, tratamento, comunicação e monitoramento dos riscos de SI; Subsidiar o Comitê Gestor de Segurança da Informação com informações pertinentes ao tratamento dos riscos de SI.

CONTROLE DE EXECUÇÃO

Controle	Método de execução	Frequência
Divisões DTI	Realização de auditorias internas com o intuito de medir a efetividade dos processos componentes do macroprocesso de Gestão de riscos de TI e identificar oportunidades de melhorias	Anual
	Identificar novos riscos de TI e atualizar Plano de Tratamento de riscos	Mensal
CGOVTI	Avaliar efetividade do Plano de tratamento do risco	Anual
Secretaria da Segurança da Informação e Gestão de Riscos (SSIGR) **Divisões DTI**	Identificar oportunidade de melhorias no Plano de Comunicação de riscos	Anual
CGSI, Divisões DTI e SSIGR	Monitorar e analisar os fatores de risco;	Anual
	Monitorar, analisar e identificar oportunidades de melhorias no processo de gestão de riscos;	
	Identificar oportunidades de melhorias nos critérios de avaliação dos riscos.	

FERRAMENTAS

PDTI	Plano Diretor de TI
PETI-Indicadores	Planejamento Estratégico de TI – indicadores de desempenho do PETI
PSI/PJSC	Política de Segurança da Informação do PJSC
PTR	Plano de Tratamento do Risco
PCR	Plano de Comunicação de Riscos

DESCRIÇÃO DAS ATIVIDADES

CONTEXTUALIZAÇÃO

Definição do contexto da gestão de riscos do PJSC

Objetivo:

- Levantar informações para a definição do contexto da gestão de riscos de segurança da informação no PJSC.

Responsável:

- Divisões da DTI.

Entradas:

- Relação dos processos, serviços e ativos de TI.
- Planejamento estratégico institucional.
- Planejamento estratégico de TI.
- Política de Segurança da Informação.

Descrição das Atividades:

- Definir metodologia de gestão de riscos de TI.
- Definir escopo e limites do processo de gestão de riscos de SI.
- Definir organização responsável pelo processo.
- Definir critérios de avaliação, de impacto e de aceitação dos riscos.

Saídas:

- Escopo e limites do processo de gestão de riscos de SI.
- Metodologia de gestão de riscos de SI.

AVALIAÇÃO DOS RISCOS

Objetivo geral:

- Comparar os resultados da análise de riscos com os critérios de avaliação definidos na metodologia de gestão de riscos de segurança da informação.

Identificação dos riscos de SI

Objetivo:

- Mapear e descrever os riscos de segurança da informação.

Responsável:

- Divisões da DTI.

Entradas:

- Escopo e limites do processo de gestão de riscos de SI.
- Metodologia de gestão de riscos de SI.

Descrição das Atividades:

- Identificar processos, serviços ou ativos críticos de TI.
- Identificar fontes de risco, eventos, causas e consequências.
- Analisar registros de incidentes.
- Identificar vulnerabilidades e ameaças.
- Identificar controles existentes.

Saídas:

- Lista dos processos, serviços ou ativos críticos de TI.
- Mapa de riscos.
- Lista de vulnerabilidades e ameaças.
- Lista de cenários de incidentes com suas consequências associadas aos processos, serviços ou ativos de TI.
- Lista dos controles existentes e planejados.

Analisar riscos de SI

Objetivo:

- Compreender a natureza do risco e determinar o nível do risco.

Responsável:

- Divisões da DTI.

Entradas:

- Metodologia de gestão de riscos utilizada.
- Mapa de riscos.
- Lista de cenários de incidentes identificados como relevantes, incluindo a identificação de ameaças, vulnerabilidades, processos/serviços/ativos afetados e suas consequências.
- Lista dos controles existentes e planejados.

Descrição das Atividades:

- Mensurar as probabilidades de ocorrências dos riscos, considerando os cenários de incidentes relevantes.
- Identificar e avaliar as consequências (impactos) dos riscos.
- Avaliar probabilidades dos incidentes.
- Determinar níveis dos riscos.

Saídas:

- Lista de consequências avaliadas referentes a um cenário de incidente, relacionadas aos ativos e critérios de impacto.
- Probabilidade dos cenários de incidentes.
- Lista de riscos com níveis de probabilidade e consequências.
- Matriz de riscos: probabilidade x impacto.

Avaliar riscos de SI

Objetivo:

- Comparar os riscos estimados com os critérios de avaliação de riscos definidos durante a definição do contexto.

Responsável:

- Divisões da DTI.

Entradas:

- Lista de riscos com níveis de valores designados (probabilidade e impacto).
- Matriz de riscos: probabilidade x impacto.
- Critérios para a avaliação de riscos.

Descrição das Atividades:

- Aplicar critérios de avaliação.

Saídas:

- Lista de riscos priorizada, de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos.

Tratamento dos riscos de SI

Objetivo:

- Definir o plano de tratamento do risco e determinar os riscos residuais.

Responsável:

- Divisões da DTI.
- Secretaria de Segurança da Informação e Gestão de Riscos.

Entradas:

- Resultados da avalição de riscos.
- Lista de riscos priorizada.

Descrição das Atividades:

- Avaliar resultado da análise do risco.
- Selecionar controles para modificar, reter, evitar ou compartilhar os riscos.
- Definir o plano de tratamento do risco.

Saídas:

- Plano de tratamento do risco.
- Descrição dos riscos residuais.

Aceitar riscos residuais

Objetivo:

- Aprovar o plano de tratamento de riscos e formalizar a aceitação dos riscos residuais.

Responsável:

- CGOVTI.

Entradas:

- Plano de tratamento do risco.
- Processo de avaliação do risco residual.

Descrição das Atividades:

- Analisar os planos propostos de tratamento do risco e os riscos residuais.
- Verificar se os critérios de aceitação do risco foram atendidos.
- Aprovar os planos de tratamento do risco e os riscos residuais, se for o caso, com registro das condições associadas a essa aprovação.

Saídas:

- Lista dos riscos aceitos e aprovação do plano de tratamento de riscos.

Comunicar sobre os riscos de SI

Objetivo:

- Compartilhar informações sobre o gerenciamento dos riscos com as partes interessadas.

Responsável:

- Divisões da DTI.
- Secretaria de Segurança da Informação e Gestão de Riscos.

Entradas:

- Processo de gestão de riscos de SI.

Descrição das Atividades:

- Elaborar plano de comunicação do risco.

Saídas:

- Entendimento sobre o processo de gestão de riscos de SI do PJSC e dos resultados obtidos.

Monitoramento dos riscos de SI

Objetivo:

- Identificar eventuais mudanças no contexto da organização e manter uma visão geral dos riscos.

Responsável:

- Divisões da DTI.
- Secretaria de Segurança da Informação e Gestão de Riscos.
- Comitê Gestor de Segurança da Informação – CGSI.
- CGOVTI.

Entradas:

- Informações sobre os riscos obtidas através das atividades de gestão de riscos.

Descrição das Atividades:

- Monitorar e analisar os fatores de risco.
- Monitorar, analisar e identificar oportunidades de melhorias no processo de gestão de riscos.
- Identificar oportunidades de melhorias nos critérios de avaliação dos riscos.

Saídas:

- Alinhamento contínuo da gestão de riscos com os objetivos de negócios da organização e com os critérios para a aceitação do risco.