



PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO MARANHÃO
DIRETORIA DE INFORMÁTICA E AUTOMAÇÃO

PROCESSO DE TRABALHO
GERENCIAR RISCOS EM SEGURANÇA DA INFORMAÇÃO

1. Objetivo

Suportar e reportar os riscos para a execução dos macrodesafios estratégicos do PETIC relacionados à governança e à gestão de recursos;

Identificar, controlar, registrar, reportar, auditar e verificar os riscos elencados na STIC;

Apresentar uma proposta de processos e artefatos a serem utilizados no gerenciamento de riscos de TIC;

Definição das etapas, papéis e responsabilidades, modelos e periodicidade para o plano de gerenciamento de riscos; e

Definição dos requisitos que devem constituir o plano de riscos.

2. Definições

PGR – Plano de Gestão de Risco

CGesTIC – Comitê Gestor de TIC

CGSI – Comitê Gestor de Segurança da Informação

3. Processo Gerenciar Riscos

3.1. Papéis e Responsabilidades

Papel	Responsabilidade	Responsável
Dono do processo	<ol style="list-style-type: none">Assegurar a efetividade do processo de Gerenciamento de riscos e controle interno.Registrar e monitorar a execução dos PGRCl's elaborados	Diretor de Informática e Automação
Identificador	<ol style="list-style-type: none">Registrar um risco	Qualquer pessoa que possa registrar e encaminhar o risco para o Gestor do risco
Gestor do risco	<ol style="list-style-type: none">Analisar o risco, colocar no plano de gerenciamento de riscos, definir o responsável pelo risco e a resposta a ele, além de manter o monitoramento periódico	Gestor do PGR específico
Responsável	<ol style="list-style-type: none">Realizar a execução do tratamento de risco	Pessoa elencado no formulário para executar a resposta definida ao risco
CGesTIC	<ol style="list-style-type: none">Registrar, analisar, aprovar o PGRCl, encaminhando-o para o Comitê competente.	Presidente do CGesTIC
CGSI	<ol style="list-style-type: none">Conhecer e analisar o PGRCl, segundo a competência do Comitê (segurança da informação)	Presidente do CGSI

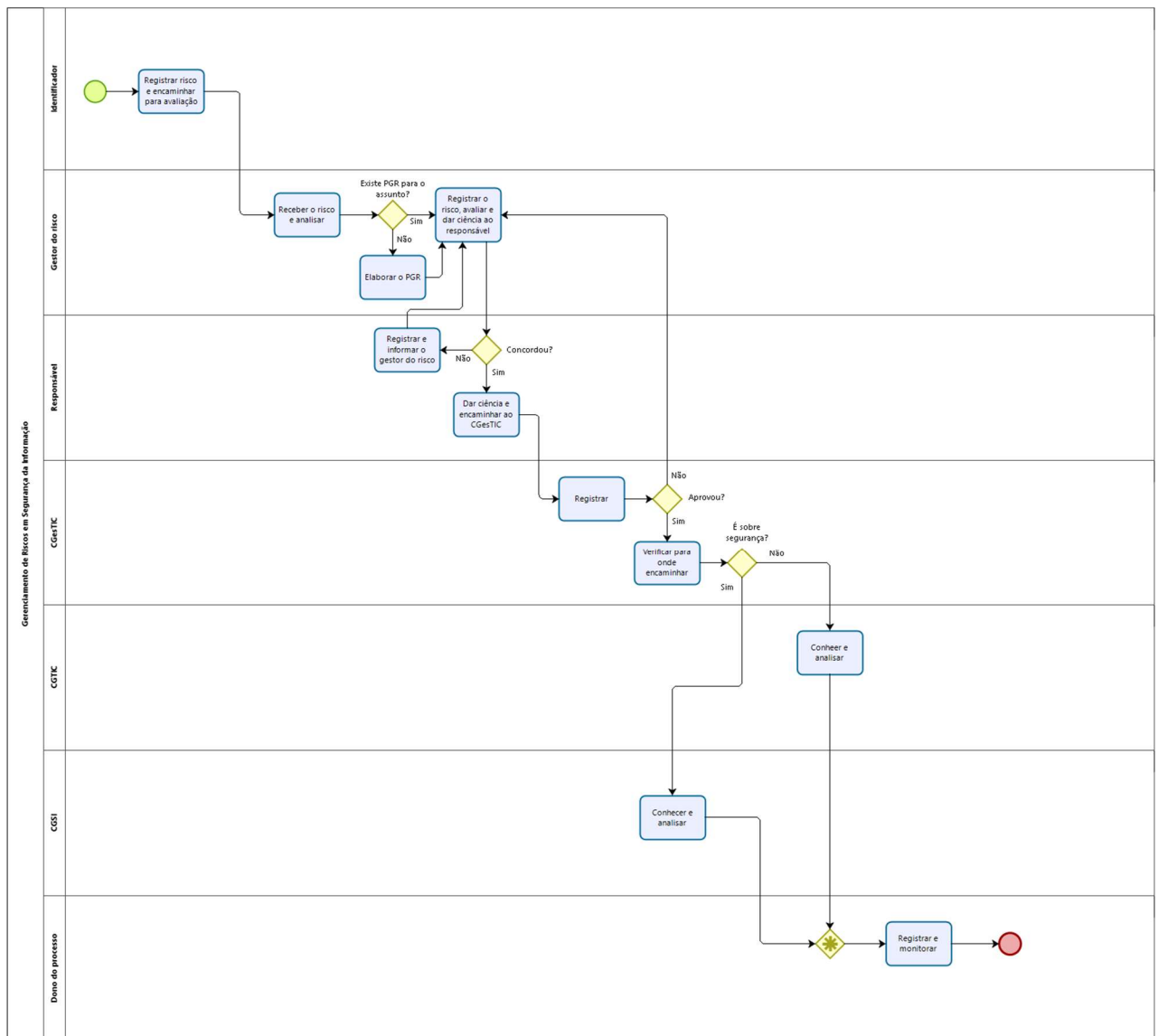


PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO MARANHÃO
DIRETORIA DE INFORMÁTICA E AUTOMAÇÃO

PROCESSO DE TRABALHO
GERENCIAR RISCOS EM SEGURANÇA DA INFORMAÇÃO

CGTIC	1. Conhecer e analisar o PGRCI, segundo a competência do Comitê (estratégia, investimentos e priorização das ações e projetos)	Presidente do CGTIC
-------	--	---------------------

3.2. Fluxo do Processo





PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO MARANHÃO
DIRETORIA DE INFORMÁTICA E AUTOMAÇÃO

PROCESSO DE TRABALHO
GERENCIAR RISCOS EM SEGURANÇA DA INFORMAÇÃO

3.3. Descrição do Processo

Atividade	Objetivo	Responsável	Entradas	Procedimentos	Saída
Registrar o risco e encaminhar para o avaliador	Registrar um possível risco a ser avaliado e tratado	Identificador	Risco possível	Registrar o risco possível no DIGIDOC	Risco possível registrado
Receber o risco e analisar	O responsável pelo plano de risco de uma unidade, processo, projeto ou segurança de TIC recebe o possível risco, analisando-o e o avaliando (qualitativamente e quantitativamente)	Gestor do risco	Risco possível registrado	Receber o possível risco, analisando-o e o avaliando (qualitativamente e quantitativamente)	Risco analisado
Elaborar o PGRCI	Caso não exista um plano de gerenciamento de riscos anterior, gerar um novo documento utilizando a metodologia e o processo definido por esse normativo	Gestor do risco	Risco analisado	Gerar um novo documento utilizando a metodologia e o processo definido por esse normativo	PGRCI
Registrar o risco no PGRCI, fazendo a avaliação e encaminhando para ciência ao responsável	Registrar o risco, sua avaliação, bem como a ação de resposta, se existir. Após isso, encaminhar ao gestor do risco para avaliação	Gestor do risco	PGRCI	Registrar o risco, sua avaliação, bem como a ação de resposta e encaminhar ao gestor do risco para avaliação	PGRCI
Dar ciência e encaminhar ao CGesTIC	O responsável conhecerá os riscos e respostas sob sua responsabilidade, dando ciência no documento e encaminhará o PGRCI ao CGesTIC	Responsável	PGRCI	Dar ciência no documento e encaminhará o PGRCI ao CGesTIC	PGRCI encaminhado



PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO MARANHÃO
DIRETORIA DE INFORMÁTICA E AUTOMAÇÃO

PROCESSO DE TRABALHO
GERENCIAR RISCOS EM SEGURANÇA DA INFORMAÇÃO

Atividade	Objetivo	Responsável	Entradas	Procedimentos	Saída
Registrar e informar o Gestor do risco	Registrar a concordância avaliação do risco e alteração no plano de gerenciamento de riscos e informar o Gestor do risco	Responsável	Risco	Registrar a concordância avaliação do risco e alteração no plano de gerenciamento de riscos e informar o Gestor do risco	Risco informado
Registrar	Registrar o plano, analisando as respostas elencadas e sua aplicação. Caso seja aprovado, encaminhar ao comitê competente. Caso não seja aprovado, volta ao item 4	Presidente do CGesTIC	Risco informado	Registrar o plano, analisando as respostas elencadas e sua aplicação. Caso seja aprovado, encaminhar ao comitê competente	Risco registrado
Verificar para onde encaminhar	Verificar qual comitê é competente para conhecer e analisar o PGRCI elaborado	Presidente do CGesTIC	Risco registrado	Verificar qual comitê é competente para conhecer e analisar o PGRCI elaborado	Risco encaminhado
Conhecer e analisar	O comitê competente conhecerá e analisará o PGRCI	Presidente do CGTIC ou do CGSI	Risco encaminhado	O comitê competente conhecerá e analisará o PGRCI	Risco aceito
Registrar e monitorar	O dono do processo registrará o PGRCI e monitorará a ocorrência dos riscos elencados	Dono do processo	Risco registrado	Registrar o PGRCI e monitorar a ocorrência dos riscos elencados	Risco monitorado



PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO MARANHÃO
DIRETORIA DE INFORMÁTICA E AUTOMAÇÃO

PROCESSO DE TRABALHO
GERENCIAR RISCOS EM SEGURANÇA DA INFORMAÇÃO

4. Matriz RACI

Atividade	Dono do processo	Identificador	Gestor do risco	Responsável	Presidente do CGTIC ou do CGSI
Registrar o risco e encaminhar para o avaliador		R			
Receber o risco e analisar			R		
Elaborar o PGRCI			R		
Registrar o risco no PGRCI, fazendo a avaliação e encaminhando para ciência ao responsável			R		
Dar ciência e encaminhar ao CGesTIC				R	
Registrar e informar o Gestor do risco				R	
Registrar					R
Verificar para onde encaminhar					R
Conhecer e analisar					R
Registrar e monitorar	R				

LEGENDA: (*Responsible* | *Accountable* | *Consulted* | *Informed* = R - Responsável | A - Prestador de Contas | C - Consultado | I - Informado)

5. Controles do Processo

Origem	
Descrição	
Periodicidade	
Meta	
Forma de cálculo	

6. Histórico de Revisão e Periodicidade



**PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO MARANHÃO
DIRETORIA DE INFORMÁTICA E AUTOMAÇÃO**

**PROCESSO DE TRABALHO
GERENCIAR RISCOS EM SEGURANÇA DA INFORMAÇÃO**

Descrição	Responsável	Data	Versão
Documentação do processo	Diretoria de Informática	15/03/2019	1.0