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

SEGURANÇA DA INFORMAÇÃO - SI

Macroprocesso de Gestão de Segurança da Informação

Data: 16/12/2019

Versão 1.0

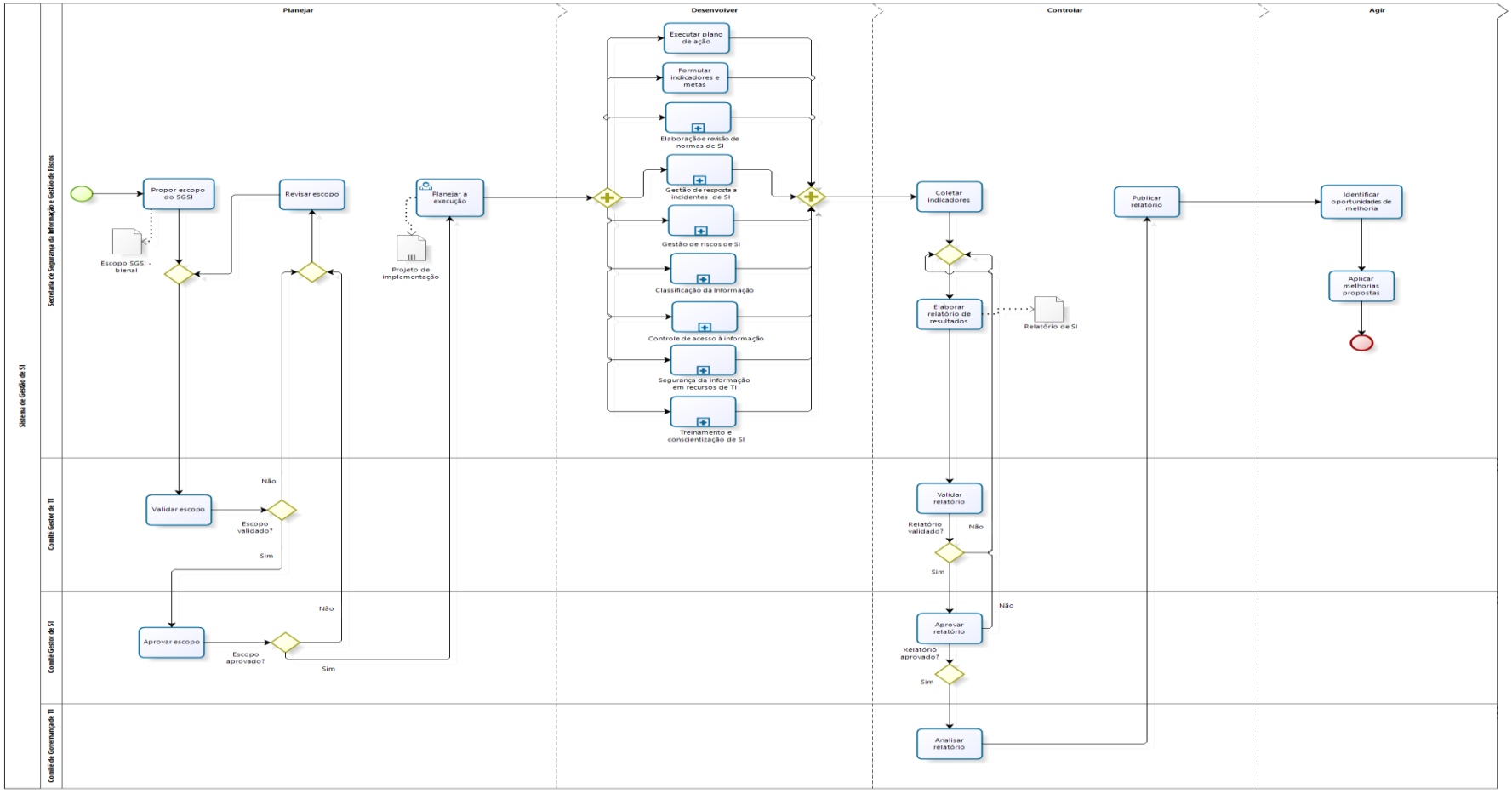
HISTÓRICO DE ALTERAÇÕES

DOCUMENTO		
Descrição	Documentação dos processos de segurança da informação	
Objetivo	Este documento descreve as atividades e procedimentos adotados para elaborar e revisar normas de segurança da informação no PJSC	
Responsável	**Nome/Matrícula** Luzmarina Rocesski – 25998	**Criado em** 16/12/2019
Setor Secretaria de Segurança da Informação e Gestão de Riscos – SSIGR		

VERSIONAMENTOS			
Versão	Data	Autor	Descrição
1.0	16/12/2019	Luzmarina Rocesski	Criação do Documento

SUMÁRIO

MACROPROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO



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.	Responsável pela análise dos indicadores de segurança da informação e pelos resultados obtidos no relatório de gestão, a fim de autorizar publicação.
Comitê Gestor de Segurança da Informação (CGSI)	Comitê multidisciplinar, vinculado ao CGovTI, formado por juiz auxiliar do Núcleo Administrativo e por servidores da área de tecnologia da informação.	Responsável pela aprovação das proposições e documentos produzidos no processo.
Comitê Gestor de Tecnologia da Informação (CGesTI)	Comitê vinculado ao CGovTI, formado por servidores de áreas multidisciplinares da Diretoria de Tecnologia da Informação.	Responsável pela validação do escopo do Sistema de Gestão de Segurança da Informação.
Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR)	Setor vinculado à DTI, responsável pela normatização e pela implementação da Política de Segurança da Informação e Gestão de Riscos, em conjunto com as demais áreas competentes.	Responsável pela gestão do processo e acompanhamento da execução das atividades relacionadas ao SGSI e validação das informações de controle e ações a serem tomadas.

CONTROLE DE EXECUÇÃO

Controle	Método de execução	Frequência
Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR)	Realizar coleta de indicadores para avaliar a implementação dos processos, os resultados obtidos e as oportunidades de melhoria. Elaborar relatório de gestão para análise pelas instâncias superiores.	Anual

FERRAMENTAS

SEI	Sistema Eletrônico de Informações.
Portal de TI	Portal onde são divulgados dados e informações relativos à área de tecnologia da informação.
Correio eletrônico	Serviço de envio e recebimento de mensagens eletrônicas, usualmente conhecido como e-mail.

DESCRIÇÃO DAS ATIVIDADES

Propor escopo do Sistema de Gestão de Segurança da Informação (SGSI)

Segundo a Política de Segurança da Informação do PJSC, o Sistema de Gestão de Segurança da Informação contempla os principais processos para garantir a segurança da informação, de acordo com as normas técnicas e boas práticas relacionadas ao tema. Dessa forma, a proposição do escopo compreende a definição das atividades a serem realizadas para a implementação do SGSI.

Objetivo: definir as atividades, os objetivos e os resultados esperados com a implementação do SGSI.

Responsável: Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas: Política de Segurança da Informação do PJSC (PSI/PJSC); diretrizes gerais do Conselho Nacional de Justiça para a implantação da gestão de segurança da informação no Poder Judiciário; Resolução n. 211, de 15 de dezembro de 2015, do Conselho Nacional de Justiça; e as normas técnicas da família NBR ISO/IEC 27001:2013, que estabelecem diretrizes para práticas de gestão e normas de segurança da informação, incluindo a seleção, a implementação e o gerenciamento de controles e riscos da segurança da informação.

Tarefas

- Definir o escopo com base na documentação de que trata as entradas do processo para o biênio seguinte.
- Documentar a proposta e enviar para validação do CGesTI.

Saídas: documento com o escopo do SGSI.

Validar escopo

Compreende a validação da proposta do escopo do SGSI, a devolução para ajustes, se for o caso, ou o encaminhamento para a aprovação do CGSI. A validação poderá ocorrer em reunião presencial, por e-mail ou em processo administrativo criado para esse fim.

Objetivos: realizar a análise da proposta e validá-la com base nas normas indicadas e no contexto organizacional de cada área envolvida nos processos do SGSI.

Responsável: Comitê Gestor de Tecnologia da Informação (CGesTI).

Entradas: documento com o escopo do SGSI.

Tarefas:

- Validar documento com o escopo do SGSI: realizar análise e manifestar-se quanto à validação ou à necessidade de ajustes.
- Solicitar ajustes: devolver para a SSIGR com as sugestões de alteração.
- Encaminhar para aprovação do CGSI: se a proposta foi validada sem ajustes, enviar para aprovação.

Saídas: documento com o escopo do SGSI validado ou solicitação de ajustes no documento.

Aprovar escopo

Compreende a aprovação da proposta do escopo do SGSI, devolução para ajustes, se for o caso, ou encaminhamento para elaboração do projeto de implementação. A aprovação poderá ocorrer em reunião presencial, por e-mail ou em processo administrativo criado para esse fim.

Objetivo: realizar análise da proposta e formalizar aprovação do escopo do SGSI.

Responsável: Comitê Gestor de Segurança da Informação (CGSI).

Entradas: documento com o escopo do SGSI validado pelo CGesTI.

Tarefas:

- Analisar documento com o escopo do SGSI e manifestar-se quanto à aprovação ou necessidade de ajustes.
- Solicitar ajustes, se for o caso: devolver para a SSIGR com as sugestões de alteração.
- Encaminhar para a SSIGR executar projeto de implementação.

Saídas: documento com o escopo do SGSI aprovado ou solicitação de ajustes no documento.

Revisar escopo

Compreende a revisão da proposta apresentada, nos termos dos ajustes indicados pelo CGesTI ou pelo CGSI.

Objetivo: adequar a proposta com as alterações sugeridas pelo CGesTI e/ou pelo CGSI.

Responsável: Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas: solicitação de ajuste no escopo do SGSI.

Tarefas:

- Revisar documento: realizar a revisão do documento de acordo com a solicitação do CGesTI ou do CGSI.
- Formalizar revisão do documento: elaborar versão atualizada.
- Encaminhar ao CGesTI para validação.

Saídas: documento com o escopo do SGSI atualizado.

Planejar a execução

Segundo a Política de Segurança da Informação do PJSC, o Sistema de Gestão de Segurança da Informação contém os principais processos para garantir a segurança da informação, de acordo com as normas técnicas e boas práticas relacionadas ao tema. Dessa forma, a proposição do escopo compreende a definição das atividades a serem realizadas para a implementação do SGSI.

Objetivo: definir as atividades, os objetivos e os resultados esperados para a implementação do SGSI.

Responsável: Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas:

Política de Segurança da Informação do PJSC; diretrizes gerais do Conselho Nacional de Justiça para a implantação da gestão de segurança da informação no Poder Judiciário; Resolução n. 211, de 15 de dezembro de 2015, do Conselho Nacional de Justiça; e as normas técnicas da família NBR ISO/IEC 27001:2013, que estabelece diretrizes para práticas de gestão e normas de segurança da informação, incluindo a seleção, a implementação e o gerenciamento de controles e riscos da segurança da informação.

Tarefas:

- Definir o escopo com base na documentação que trata das entradas do processo para o biênio que segue.
- Documentar a proposta e enviar para validação do CGesTI.

Saídas: documento com o escopo do SGSI.

Executar plano de ação

O plano de ação é resultado do escopo do SGSI e deve conter atividades pontuais e necessárias para sua implantação, tais como contratações de serviços, aquisição de softwares, análise de riscos, cronograma físico-financeiro e de implantação, etc.

Objetivo: executar as ações planejadas para a implantação do Sistema de Gestão de Segurança da Informação.

Responsável:
Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas: escopo do SGSI.

Tarefas:

- Identificar as ações prioritárias.
- Estabelecer cronograma de execução.
- Distribuir tarefas.
- Executar ações.

Saídas: projeto de execução implantado.

Formular indicadores e metas

Com base no plano de ação oriundo do escopo do SGSI, iniciar estudos para a criação de indicadores e metas que contemplem os resultados esperados com a implantação do SGSI.

Objetivo: estabelecer metas e indicadores de desempenho de segurança da informação.

Responsável: Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas: escopo do SGSI.

Tarefas:

- Criar indicadores de desempenho para o SGSI.
- Estabelecer metas a serem alcançadas para o período.
- Elaborar documento e publicar.

Saídas: documento com o índice de gestão de segurança da informação.

Executar processo: elaboração e revisão de normas de SI

De acordo com esse subprocesso, as normas de segurança da informação devem ser revisadas pelo menos uma vez ao ano ou quando houver alterações significativas no ambiente tecnológico ou administrativo.

Objetivo: operacionalizar o processo de elaboração e revisão de normas de segurança da informação.

Responsáveis:

- Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).
- Comitê Gestor de Segurança da Informação (CGSI).
- Comitê de Governança de TI (CGovTI).
- Gabinete da Presidência.
- Diretoria-Geral Judiciária (DGJ).

Entradas: N/A.

Tarefas: conforme descrito no processo.

Saídas: N/A.

Executar processo: gestão de resposta a incidentes de SI

De acordo com a Política de Segurança da Informação do PJSC, esse processo visa tentar reduzir a um nível aceitável a interrupção causada por desastres ou falhas, principalmente nos ativos que suportam os processos críticos de informação do Tribunal.

Objetivo: operacionalizar o processo de gestão de resposta a incidentes de SI.

Responsáveis:

- Unidades da Diretoria de Tecnologia da Informação (DTI).
- Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETRI-SI).
- Comitê Gestor de Segurança da Informação (CGSI).
- Comitê de Governança de TI (CGovTI).

Entradas: N/A.

Tarefas: conforme descrito no processo.

Saídas: N/A.

Executar processo: gestão de riscos de SI

De acordo com a Política de Segurança da Informação do PJSC, esse processo visa minimizar os riscos associados à informação, apresentando as medidas de segurança necessárias e realizando a avaliação contínua por meio de análise sistemática e periódica.

Objetivo: operacionalizar o processo de gestão de riscos de SI.

Responsáveis:

- Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).
- Comitê Gestor de Segurança da Informação (CGSI).
- Comitê de Governança de TI (CGovTI).
- Outras áreas do PJSC.

Entradas: N/A.

Tarefas: conforme descrito no processo.

Saídas: N/A.

Executar processo: classificação da informação

De acordo com a Política de Segurança da Informação do PJSC, esse processo busca inventariar e classificar as informações de acordo com sua confidencialidade e associá-las a um proprietário da informação.

Objetivo: operacionalizar o processo de classificação da informação.

Responsáveis:

- Proprietário da informação.
- Unidades do PJSC.
- Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).
- Comitê Gestor de Segurança da Informação (CGSI).
- Comitê de Governança de TI (CGovTI).

Entradas: N/A.

Tarefas: conforme descrito no processo.

Saídas: N/A.

Executar processo: controle de acesso à informação

De acordo com a Política de Segurança da Informação do PJSC, o acesso (lógico e físico) à informação deve ser controlado e estar de acordo com as normas e os procedimentos definidos.

Objetivo: operacionalizar o processo de controle de acesso à informação.

Responsáveis:

- Proprietário da informação.
- Unidades do PJSC.
- Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).
- Comitê Gestor de Segurança da Informação (CGSI).
- Comitê Gestor de Tecnologia da Informação (CGesTI).
- Comitê de Governança de TI (CGovTI).

Entradas: N/A.

Tarefas: conforme descrito no processo.

Saídas: N/A.

Executar processo: segurança da informação em recursos de TI

De acordo com a Política de Segurança da Informação do PJSC, esse processo corresponde ao inventário e gestão dos ativos críticos de tecnologia da informação e da comunicação.

Objetivo: operacionalizar o processo de segurança da informação em recursos de TI.

Responsáveis:

- Unidades da DTI.
- Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).
- Comitê Gestor de Segurança da Informação (CGSI).
- Comitê Gestor de Tecnologia da Informação (CGesTI).
- Comitê de Governança de TI (CGovTI).

Entradas: N/A.

Tarefas: conforme descrito no processo.

Saídas: N/A.

Executar processo: conscientização e treinamento em SI

De acordo com a Política de Segurança da Informação do PJSC, esse processo visa promover a validação das evidências de cumprimento da PSI/PJSC e a definição de utilização e responsabilidade com o uso das informações.

Objetivo: operacionalizar o processo de conscientização e treinamento em SI.

Responsáveis:

- Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).
- Comitê Gestor de Segurança da Informação (CGSI).
- Outras áreas do PJSC.

Entradas: N/A.

Tarefas: conforme descrito no processo.

Saídas: N/A.

Coletar indicadores

Com base no documento do índice de gestão de segurança da informação, coletar os indicadores de cada processo anualmente, ou em período diverso se estabelecido no documento.

Objetivo: realizar a coleta dos indicadores de SI.

Responsável: Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas: documento com o índice de gestão de segurança da informação.

Tarefas:

- Realizar a coleta dos indicadores, conforme estabelecido.
- Publicar os indicadores coletados na página de segurança da informação.

Saídas: levantamento de indicadores.

Elaborar relatório de resultados

Com base no levantamento dos indicadores dos processos de segurança da informação, elaborar relatório contendo os resultados alcançados das ações realizadas até o momento.

Objetivo: apurar os resultados de segurança da informação em comparação com o que foi planejado e o que foi realizado.

Responsável: Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas: levantamento de indicadores.

Tarefas:
- Compilar informações.
- Executar análise comparativa entre o planejado e o realizado.
- Confeccionar relatório.
- Encaminhar ao CGesTI para validação.

Saídas: relatório do SGSI.

Validar relatório

Objetivo: validar o relatório de resultados elaborado pela SSIGR.

Responsável: Comitê Gestor de Tecnologia da Informação (CGesTI).

Entradas: relatório do SGSI.

Tarefas:
- Analisar o relatório.
- Manifestar validação ou sugestão de alteração.
- Encaminhar para aprovação do CGSI ou devolver à SSIGR para ajustes.

Saídas: relatório do SGSI validado.

Aprovar relatório

Objetivo: aprovar o relatório de resultados elaborado pela SSIGR.

Responsável: Comitê Gestor de Segurança da Informação (CGSI).

Entradas: relatório do SGSI validado pelo CGesTI.

Tarefas:

- Analisar o relatório.
- Manifestar aprovação ou sugestão de alteração.
- Encaminhar para análise do CGovTI ou devolver à SSIGR para ajustes.

Saídas: relatório do SGSI aprovado.

Analisar relatório

Objetivo: realizar análise crítica do SGSI executado para conhecer os resultados alcançados, verificar os pontos fortes e pontos de melhoria para implementação posterior.

Responsável: Comitê de Governança de Tecnologia da Informação (CGovTI).

Entradas: relatório do SGSI aprovado pelo CGSI.

Tarefas:
- Analisar o relatório.
- Manifestar ações de melhoria ou necessidade de mudança dentro do processo.
- Aprovar publicação do relatório.

Saídas: análise crítica e indicação de melhorias.

Publicar relatório

Objetivo: dar transparência e publicidade aos resultados do SGSI.

Responsável: Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas: versão final do relatório de resultados do SGSI.

Tarefas:
- Publicar o relatório na página de SI.
- Divulgar publicação.

Saídas: relatório publicado.

Desenvolver plano de ações de melhorias

Objetivo: operacionalizar as melhorias indicadas no relatório de resultados do

SGSI.

Responsável: Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas: versão final do relatório de resultados do SGSI e manifestação do CGovTI.

Tarefas:

- Analisar as melhorias indicadas pelo CGovTI e apontadas no relatório de resultados do SGSI.
- Elaborar plano de ação de melhorias.
- Formalizar documento.

Saídas: plano de ação de melhorias do SGSI.

Aplicar melhorias propostas

Objetivo: executar plano de ação de melhorias.

Responsável: Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas: plano de ação de melhorias do SGSI.

Tarefas:

- Implementar plano de ação de melhorias.
- Criar cronograma de execução.
- Controlar e acompanhar a execução do plano de ação de melhorias.

Saídas: N/A.