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

SEGURANÇA DA INFORMAÇÃO - SI

Processo de treinamento e conscientização de segurança da informação

---

Data: 29/11/2019

Versão 1.0

HISTÓRICO DE ALTERAÇÕES

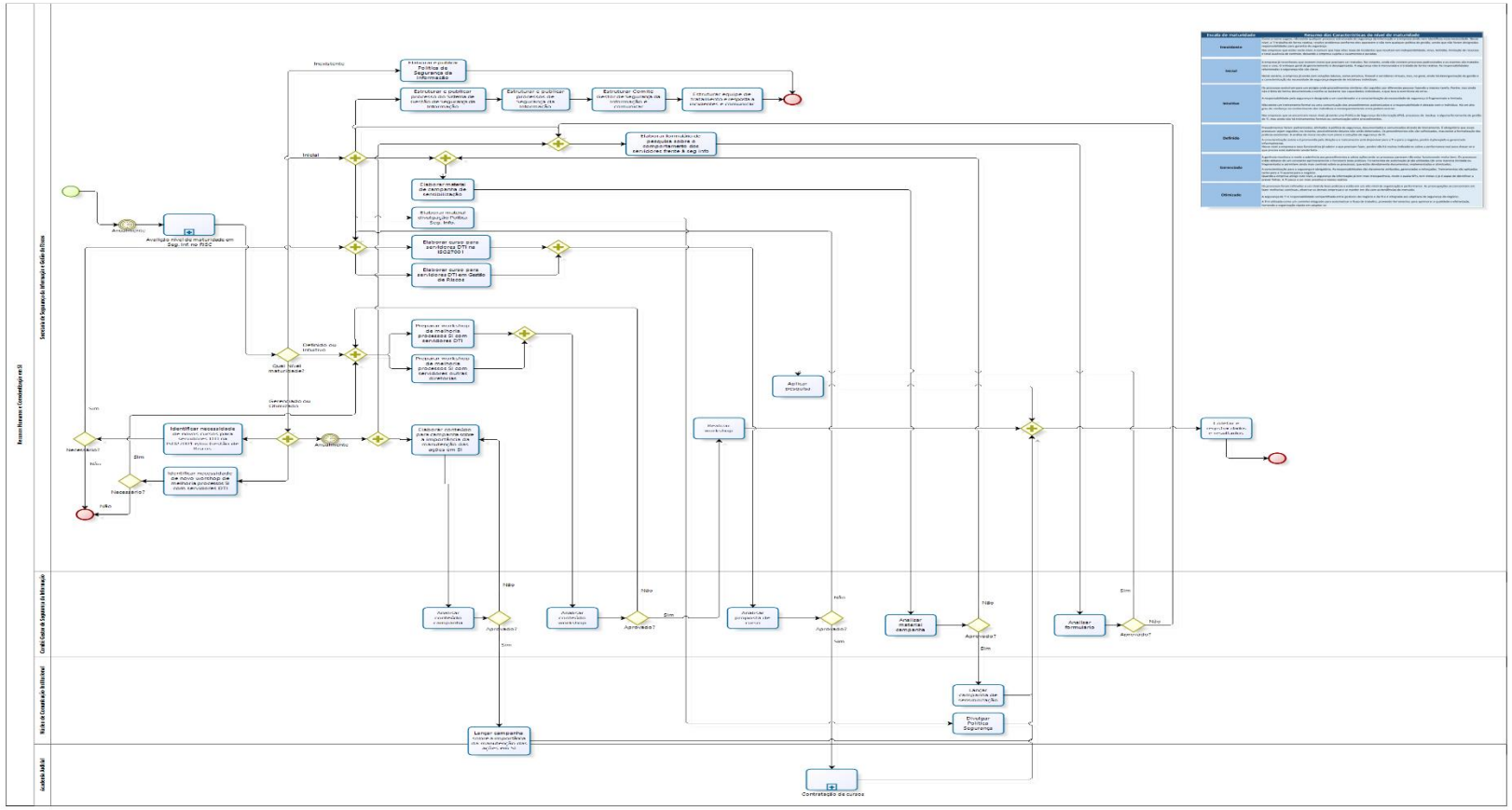
DOCUMENTO		
Descrição	Documentação dos processos de segurança da informação	
Objetivo	Este documento descreve as atividades e procedimentos adotados para conscientizar e capacitar os usuários de TI envolvidos direta ou indiretamente com os aspectos relacionados à segurança da informação no PJSC	
Responsável	**Nome/Matrícula** Rinaldo Feldmann – 2160	**Criado em** 29/11/2019
Setor Secretaria de Segurança da Informação e Gestão de Riscos - SSIGR		

VERSIONAMENTOS			
Versão	Data	Autor	Descrição
1.0	29/11/2019	Rinaldo Feldmann	Criação do Documento

SUMÁRIO

TREINAMENTO E CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Diagrama do Processo



PAPÉIS E RESPONSABILIDADES

Papéis		Responsabilidades
Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR)	Setor responsável pela normatização e atualização das normas de segurança da informação (SI), em conjunto com as demais áreas competentes.	Avaliar periodicamente o nível de maturidade do Poder Judiciário de Santa Catarina nos aspectos relacionados à segurança da informação.
		Identificar a necessidade de capacitação do corpo técnico da Diretoria de Tecnologia da Informação, bem como dos usuários de seus serviços, nos aspectos relacionados à segurança da informação.
		Formatar propostas de formulários, cursos, *workshops* e campanhas de sensibilização.
		Aplicar pesquisa de comportamento dos servidores quanto à segurança da informação.
		Realizar *workshops*.
		Registrar dados e resultados sobre pesquisas, campanhas, cursos e *workshops.*
Comitê Gestor de Segurança da Informação (CGSI)	Comitê multidisciplinar vinculado ao CGovTI, formado por juiz auxiliar do Núcleo Administrativo e servidores da área da tecnologia da informação.	Analisar propostas de formulários, cursos, *workshops* e campanhas de sensibilização.
Núcleo de Comunicação Institucional (NCI)	Setor responsável por supervisionar a comunicação institucional do PJSC, disseminando informações sobre assuntos de interesse público relacionados às ações e decisões do PJSC.	Lançar campanhas de sensibilização e conscientização sobre o tema segurança da informação.
		Divulgar política de segurança da informação.
Academia Judicial	Setor responsável por viabilizar a realização de cursos ao corpo técnico da Diretoria de Tecnologia da Informação, bem como a seus usuários, com temas relacionados à segurança da informação.	Contratar cursos.

CONTROLE DE EXECUÇÃO

Controle	Método de execução	Frequência
Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR)	Realização de pesquisa sobre o comportamento dos servidores diante da segurança da informação. Avaliação do nível de maturidade em SI do PJSC. Elaboração de plano de capacitação em SI. Revisão do processo.	Anual

FERRAMENTAS

SEI	Sistema Eletrônico de Informações.
Portal de TI	Portal onde são divulgados dados e informações relativos à área da tecnologia da informação.

DESCRIÇÃO DAS ATIVIDADES

Avaliar o nível de maturidade em segurança da informação no PJSC (ISO 27001)

Objetivo:

- Identificar o nível de maturidade do Poder Judiciário de Santa Catarina nos aspectos relacionados à segurança da informação, considerando o disposto na norma ISO 27001.

Responsável:

- Secretária de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas:

- Pesquisa de maturidade de segurança da informação com usuários do PJSC.

Descrição das atividades:

- Elaborar formulário de pesquisa a ser lançado aos usuários de TI do PJSC.
- Disponibilizar formulário no portal institucional.
- Comunicar usuários de TI do PJSC sobre o preenchimento do formulário.
- Compilar respostas e identificar nível de maturidade.
- Divulgar no portal institucional o nível de maturidade do PJSC.

Saídas:

- Número que caracteriza o nível de maturidade do PJSC em segurança da

informação.

Elaborar e publicar a Política de Segurança da Informação

Objetivo:
- Estruturar e divulgar a Política de Segurança da Informação do PJSC.

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

Entradas:
- Minuta de resolução.

Descrição das atividades:
- Elaborar minuta de resolução de SI do PJSC.
- Obter aprovação do CGSI e da Presidência.
- Publicar resolução.

Saídas:
- Formulários preenchidos.
- Resultado da pesquisa publicado no portal institucional.

Estruturar processo do Sistema de Segurança da Informação

Objetivo:
- Estruturar o processo referente ao Sistema de Segurança da Informação do PJSC.

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

Entradas:
- Normas ISO 27000.

Descrição das atividades:
- Estruturar processo.

Saídas:
- Processo estruturado.

Estruturar processos de segurança da informação

Objetivo:
- Estruturar processos componentes do Sistema de Segurança da Informação do PJSC.

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

Entradas:
- Normas ISO 27000.
- Processo do Sistema de SI do PJSC.

Descrição das atividades:
- Estruturar processos.

Saídas:

- Processos estruturados.

Estruturar Comitê Gestor de Segurança da Informação

Objetivo:
- Estruturar o Comitê Gestor de Segurança da Informação do PJSC, de acordo com o disposto no art. 21 da Resolução GP n. 15/2018.

Responsável:
- Gabinete do Diretor de TI.
- Comitê de Governança de Tecnologia da Informação – CGovTI.

Entradas:
- Resolução GP n. 15/2018.

Descrição das atividades:
- Identificar composição e competências do CGSI.
- Minutar portaria de funcionamento do CGSI.
- Publicar portaria.

Saídas:
- Portaria publicada.

Estruturar equipe de tratamento e resposta a incidentes

Objetivo:
- Analisar a efetividade das ações implementadas voltadas ao estabelecimento da cultura e ampliação do nível de maturidade da segurança da informação.

Responsável:
- Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).
- Gabinete do Diretor de TI.

Entradas:
- Resolução GP n. 15/2018.
- Normas ISO 27000.
- Processo do Sistema de SI do PJSC.

Descrição das atividades:
- Identificar composição e competências do CGSI.
- Estruturar processo de funcionamento da ETRI-SI.
- Minutar resolução de funcionamento da ETRI-SI.
- Obter aprovação do CGSI quando resolução e processo.
- Publicar portaria criando ETRI-SI.

Saídas:
- Portaria publicada.

Elaborar material de campanha de sensibilização

Objetivo:
- Promover sensibilização e incremento na conscientização dos usuários de TI do PJSC nos aspectos que envolvam segurança da informação,

visando incrementar o nível de maturidade do PJSC de inexistente para definido, bem como reduzir os incidentes de segurança da informação.

Responsável:

- Secretária de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas:

- Modelos de cartilhas e manuais de outros órgãos públicos e empresas privadas.

Descrição das atividades:

- Revisar as normas em vigor: verificar se há necessidade de alteração. A alteração da norma pode decorrer de uma melhoria no processo ou, ainda, de uma adequação ou acréscimo às diretrizes e procedimentos nela previstos. Se houver necessidade de alteração, elaborar proposta. Caso contrário, elaborar informação dando ciência da revisão e das conclusões que apontam para a manutenção do conteúdo.

Saídas:

- Cartilha de sensibilização.

Elaborar material divulgação da Política de Segurança da Informação

Objetivo:

- Disseminar o conhecimento dos usuários de TI do PJSC a respeito do disposto na Resolução TJ n. 15/2018, que instituiu a Política de Segurança da Informação no PJSC, visando dar os primeiros passos rumo à ampliação do nível de maturidade em segurança da informação de inexistente para definido.

Responsável:

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

Entradas:

- Resolução TJ n. 15/2018.

Descrição das atividades:

- Disponibilizar resolução do portal institucional do PJSC.
- Comunicar aos usuários de TI do PJSC sobre a disponibilização da resolução.

Saídas:

- Resolução TJ n. 15/2018 publicada no portal institucional.
- Comunicado aos usuários de TI do PJSC.

Elaborar curso para servidores da DTI na ISO 27001

Objetivo:

- Nivelar os servidores da DTI quanto às exigências impostas pela norma ISO 27001 nos aspectos relacionados à segurança da informação, visando ampliar o nível de maturidade em segurança da informação de inexistente para definido.

Responsável:

- Academia Judicial com o apoio da Secretária de Segurança da

Informação e Gestão de Riscos (SSIGR).

Entradas:

- Norma ISO 27001.
- Resolução TJ n. 15/2018.

Descrição das atividades:

- Formatar ementa do curso.
- Buscar empresa instrutora ou autônomo.
- Contratar empresa instrutora ou autônomo.

Saídas:

- Curso formatado.

Elaborar curso em Gestão de Riscos para servidores da DTI

Objetivo:

- Nivelar os servidores da DTI quanto à gestão de riscos relacionados à segurança da informação para ampliar o nível de maturidade em segurança da informação de inexistente para definido.

Responsável:

- Academia Judicial com o apoio da Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR).

Entradas:

- Norma ISO 27001.
- Resolução TJ n. 15/2018.

Descrição das atividades:

- Formatar ementa do curso.
- Buscar empresa instrutora ou autônomo.
- Contratar empresa instrutora ou autônomo.

Saídas:

- Curso contratado.

Preparar *workshop* de melhoria de processos em SI com servidores da DTI

Objetivo:

- Identificar oportunidades de melhorias nos processos componentes do Sistema de Gestão de Segurança da Informação do PJSC.

Responsável:

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

Entradas:

- Política de SI do PJSC.
- Processo do Sistema de Gestão de SI.
- Processo de treinamento e conscientização de SI.
- Processo de elaboração e revisão de normas.
- Critérios e lista de serviços críticos.
- Processo Gestão e respostas a incidentes.

- Processo Gestão de riscos de SI.
- Processo Controle de acesso à informação.
- Processo Classificação da informação.
- Processo Segurança em recursos de TI.
- Processo Gestão da continuidade de TI.

Descrição das atividades:

- Levantar indicadores e metas dos processos.
- Identificar metas não cumpridas.
- Estruturar *workshop* e convocar servidores da DTI.
- Apresentar processos com necessidade de melhorias.
- Colher dos participantes sugestões de melhorias dos processos.

Saídas:

- Sugestões de melhoria dos processos.
- Novos indicadores e metas.

Preparar *workshop* de melhoria processos de SI com servidores de outras diretorias

Objetivo:

- Identificar oportunidades de melhorias nos processos componentes do Sistema de Gestão de Segurança da Informação do PJSC.

Responsável:

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

Entradas:

- Política de SI do PJSC.
- Processo do Sistema de Gestão de SI.
- Critérios e lista de serviços críticos.

Descrição das atividades:

- Levantar indicadores e metas dos processos.
- Identificar metas não cumpridas.
- Estruturar *workshop* e convidar servidores de outras diretorias.
- Apresentar processos com necessidade de melhorias.
- Colher dos participantes sugestões de melhorias dos processos.

Saídas:

- Sugestões de melhoria dos processos.
- Novos indicadores e metas.

Identificar necessidade de novos cursos para os servidores da DTI na ISO 27001 e/ou em Gestão de Riscos

Objetivo:

- Identificar necessidade de novos cursos aos servidores da DTI para manter o alto nível de maturidade do PJSC em segurança da informação.

Responsável:

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

Entradas:

- Indicadores de todos os processos componentes do Sistema de Gestão de Segurança da Informação do PJSC.

Descrição das atividades:

- Identificar processos com metas não cumpridas.

Saídas:

- Lista de novos cursos aos servidores da DTI.

Identificar necessidade de novo *workshop* de melhoria nos processos de SI com servidores da DTI

Objetivo:

- Identificar necessidade de levantamento de oportunidades de melhorias nos processos componentes do Sistema de Gestão de Segurança da Informação do PJSC para manter o alto nível de maturidade do PJSC em segurança da informação.

Responsável:

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

Entradas:

- Indicadores de todos os processos componentes do Sistema de Gestão de Segurança da Informação do PJSC.

Descrição das atividades:

- Identificar processos com metas não cumpridas.

Saídas:

- Indicativo da necessidade ou não de novo *workshop*.

Elaborar conteúdo para campanha sobre a importância da manutenção das ações em SI

Objetivo:

- Manter o alto nível de maturidade do PJSC em segurança da informação.

Responsável:

- Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR) e Núcleo de Comunicação Institucional.

Entradas:

- Indicadores de todos os processos componentes do Sistema de Gestão de Segurança da Informação do PJSC.
- Oportunidades de melhorias levantadas nos *workshops* com servidores da DTI e das demais diretorias.

Descrição das atividades:

- Elaborar conteúdo para campanha.
- Lançar campanha.

Saídas:

- Portal atualizado.

Analisar conteúdo de campanha

Objetivo:
- Analisar e validar, com sugestões de melhorias, o material de campanha sobre a importância da manutenção das ações em segurança da informação.

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

Entradas:
- Proposta de campanha sobre a importância da manutenção das ações em segurança da informação.

Descrição das atividades:
- Encaminhar proposta de campanha ao CGSI.
- Implementar melhorias propostas e colher aprovação para lançamento da campanha.

Saídas:
- Proposta de campanha aprovada.

Analisar conteúdo de *workshop*

Objetivo:
- Analisar e validar, com sugestões de melhorias, o conteúdo proposto para a realização de *workshops* de melhoria dos processos de segurança da informação, a serem realizados com servidores da DTI e com servidores das demais diretorias.

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

Entradas:
- Propostas de *workshops*.

Descrição das atividades:
- Encaminhar propostas de *workshops* ao CGSI.
- Implementar melhorias propostas e colher aprovação para a realização dos *workshops*.

Saídas:
- Propostas de *workshops* aprovada.

Analisar proposta de curso

Objetivo:
- Analisar e validar, com sugestões de melhorias, o conteúdo proposto para a realização de cursos sobre as normas ISO da família 27000 e sobre Gestão de Riscos, a serem realizados com servidores da DTI.

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

Entradas:
- Propostas de cursos.

Descrição das atividades:

- Encaminhar proposta de cursos ao CGSI.
- Implementar melhorias propostas e colher aprovação para a realização dos cursos.

Saídas:

- Propostas de cursos aprovadas.

Analisar material de campanha

Objetivo:

- Analisar e validar, com sugestões de melhorias, o conteúdo proposto para a realização de campanha de sensibilização aos usuários de TI sobre a importância da segurança da informação.

Responsável:

- Comitê Gestor de Segurança da Informação (CGSI).

Entradas:

- Proposta de campanha.

Descrição das atividades:

- Encaminhar proposta de campanha ao CGSI.
- Implementar melhorias propostas e colher aprovação para a realização da campanha de sensibilização.

Saídas:

- Proposta de campanha aprovada.

Analisar formulário

Objetivo:

- Analisar e validar, com sugestões de melhorias, proposta de formulário de pesquisa sobre o comportamento dos usuários de TI ante a segurança da informação.

Responsável:

- Comitê Gestor de Segurança da Informação (CGSI).

Entradas:

- Proposta de formulário.

Descrição das atividades:

- Encaminhar proposta de formulário ao CGSI.
- Implementar melhorias propostas e colher aprovação para a elaboração de formulário.

Saídas:

- Proposta de formulário aprovada.

Lançar campanha sobre a importância da manutenção das ações de SI

Objetivo:

- Sensibilizar e cativar os usuários de TI quanto à importância da segurança da informação no dia a dia.

Responsável:
- Núcleo de Comunicação Institucional (NCI) e Academia Judicial.

Entradas:
- Proposta de campanha.

Descrição das atividades:
- Encaminhar proposta de campanha ao NCI.
- Alinhar modelo de campanha.
- Lançar campanha.

Saídas:
- Campanha lançada.

Lançar campanha de sensibilização

Objetivo:
- Sensibilizar os usuários de TI sobre o tema da segurança da informação.

Responsável:
- Núcleo de Comunicação Institucional (NCI).

Entradas:
- Proposta de campanha.

Descrição das atividades:
- Encaminhar proposta de campanha ao NCI.
- Alinhar modelo de campanha.
- Lançar campanha.

Saídas:
- Campanha lançada.

Divulgar Política de Segurança

Objetivo:
- Divulgar a todos os usuários de TI do PJSC a Política de Segurança da Informação do PJSC.

Responsável:
- Núcleo de Comunicação Institucional (NCI).

Entradas:
- Material de divulgação da política.

Descrição das atividades:
- Encaminhar material de divulgação ao NCI.
- Alinhar material de divulgação.
- Divulgar política.

Saídas:
- Política divulgada.

Realizar *workshops*

Objetivo:
- Realizar *workshops* voltados à melhoria dos processos de segurança da

informação do PJSC.

Responsável:

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

Entradas:

- Roteiros dos *workshops.*

Descrição das atividades:

- Encaminhar roteiro e conteúdo dos *workshops* ao CGSI.
- Obter aprovação do CGSI.
- Realizar *workshops* com servidores da DTI, inicialmente, e com servidores das demais diretorias.

Saídas:

- *Workshops* realizados.

Aplicar pesquisa

Objetivo:

- Verificar a cultura e hábitos dos servidores e magistrados quanto à segurança da informação.

Responsável:

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

Entradas:

- Formulário de pesquisa.

Descrição das atividades:

- Encaminhar proposta de formulário ao CGSI.
- Obter aprovação do CGSI.
- Aplicar pesquisa.

Saídas:

- Resultado da pesquisa divulgado.

Coletar e registrar dados e resultados

Objetivo:

- Manter registro das ações implementadas para a criação da cultura da segurança da informação e ampliação de seu nível de maturidade.

Responsável:

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

Entradas:

- Avaliação de reação dos cursos da ISO 27001 e em Gestão de Riscos.
- Avaliação de reação dos *workshops* de melhoria dos processos de SGSI.
- Resultado da pesquisa sobre o comportamento dos usuários de TI ante a segurança da informação.
- Resultado da campanha de sensibilização.
- Resultado da campanha de conscientização sobre a importância da manutenção das ações de segurança da informação.
- Resultado da divulgação da Política de Segurança da Informação.

Descrição das atividades:

- Coletar indicadores de desempenho dos processos componentes do SGSI, antes e após a implementação de cada ação.
- Registrar indicadores de desempenho de cada ação implementada, oportunidades de melhorias e os pontos positivos e negativos de cada ação implementada.

Saídas:

- Registro dos indicadores.
- Registro das oportunidades de melhorias.
- Registro dos pontos positivos e negativos de cada ação implementada.