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

SEGURANÇA DA INFORMAÇÃO – SI

Gestão de resposta a incidentes em segurança da informação

Data: 11/12/2019

Versão 1.0

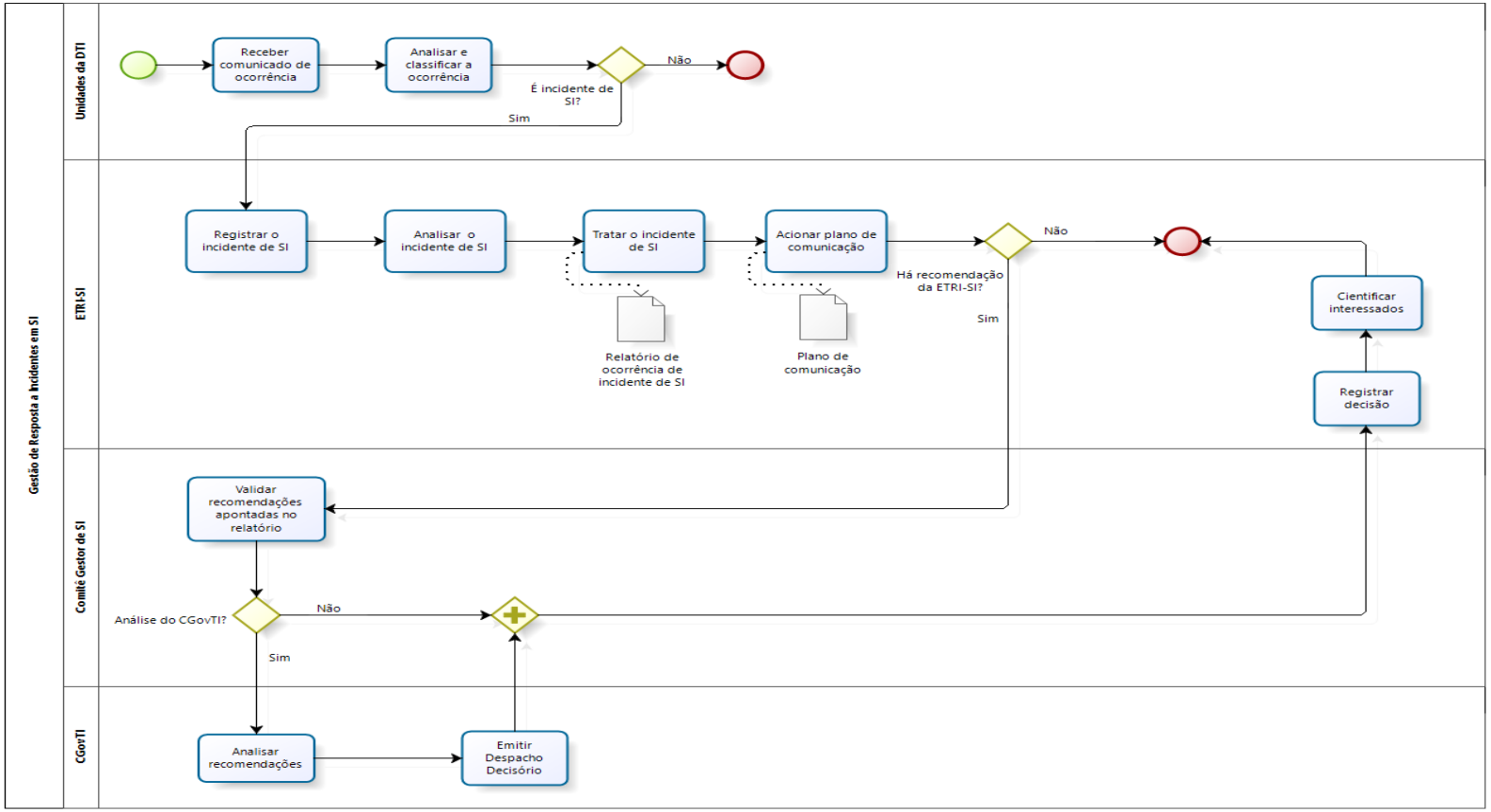
HISTÓRICO DE ALTERAÇÕES

DOCUMENTO		
Descrição	Documentação dos processos de segurança da informação	
Objetivo	Este documento descreve as atividades e procedimentos adotados para gerir a resposta a incidentes em segurança da informação no PJSC	
Responsável	**Nome/Matrícula** Rinaldo Feldmann – 2160	**Criado em** 11/12/2019
Setor Secretaria de Segurança da Informação e Gestão de Riscos – SSIGR		

V E R S I O N A ME N TO S			
Versão	Data	Autor	Descrição
1.0	11/12/2019	Rinaldo Feldmann	Criação do Documento

Sumário

PROCESSO DE GESTÃO DE RESPOSTA A INCIDENTES DE SI



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 dos 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 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 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
Equipe de Resposta a Incidentes em SI (ETRI-SI)	Elaborar relatório de incidentes no período.	Mensal
	Verificar se as recomendações emitidas pela ETRI-SI foram implementadas e se estão sendo cumpridas	Semestral
Secretaria de Segurança da Informação e Gestão de Riscos (SSIGR)	Realizar revisão do processo em conjunto com a ETRI-SI, visando identificar oportunidades de melhoria.	Semestral
	Estabelecer indicadores para medição da efetividade do processo.	Anual
	Identificar tendência dos indicadores por tipo de incidente.	Trimestral

FERRAMENTAS

Planilhas eletrônicas	Planilhas eletrônicas mantidas pelas áreas técnicas da DTI, em que serão registrados todos os incidentes em SI.
Correio eletrônico	Serviço de envio e recebimento de mensagens eletrônicas, também conhecido como e-mail, em que serão reportados à Equipe de Resposta a Incidentes em SI (ETRI-SI) os incidentes em SI.

DESCRIÇÃO DAS ATIVIDADES

Receber comunicado de ocorrência

Objetivo:

Fazer com que a ETRI-SI tome ciência de algum incidente em SI, reportado prioritariamente pelas chefias, ou, excepcionalmente, pelos subordinados.

Responsável:

Unidades técnicas da DTI.

Entradas:

E-mail, telefonema ou mensagem no Pandion, Skype ou WhatsApp informando um problema ou incidente.

Tarefas:

Receber comunicado de problema ou incidente dos usuários.

Saídas:

Registro do comunicado de problema ou incidente.

Analisar e classificar a ocorrência

Objetivo:

Verificar se problema ou incidente reportado pelo usuário é um incidente de SI. Em caso afirmativo, compartilhar incidente com ETRI-SI.

Responsável:

Unidades técnicas da DTI.

Entradas:

Problema ou incidente reportado pelo usuário.

Tarefas:

- Analisar problema ou incidente.
- Verificar se o problema ou incidente afeta a segurança da informação.

- Em caso afirmativo, comunicar problema ou incidente à ETRI-SI.

Saídas:
Problema ou incidente classificado.

Registrar incidente de SI

Objetivo:
Realizar o registro do incidente de SI visando controles futuros e geração de indicadores.
Responsável:
Equipe de Resposta a Incidentes em SI (ETRI-SI).
Entradas:
E-mail encaminhado por unidade técnica da DTI.
Tarefas:
Realizar o registro do incidente de SI em planilha eletrônica.
Saídas:
Novo registro em planilha eletrônica.

Analisar o incidente de SI

Objetivo:
Analisar a complexidade e o impacto do incidente de SI recebido.
Responsável:
Equipe de Resposta a Incidentes em SI (ETRI-SI).
Entradas:

- E-mail encaminhado por unidade técnica da DTI.
- Planilha eletrônica com o registro do incidente.

Tarefas:

- Analisar o tipo de incidente.
- Identificar se o incidente já havia ocorrido no passado e quais as soluções implementadas anteriormente.
- Avaliar o impacto do incidente.
- Alimentar planilha eletrônica sobre os achados do incidente.

Saídas:
Planilha eletrônica atualizada.

Tratar incidente de SI

Objetivo:
Identificar soluções para o incidente.
Responsável:
Equipe de Resposta a Incidentes em SI (ETRI-SI)
Entradas:

Planilha eletrônica atualizada.

Tarefas:

- Identificar o público afetado pelo incidente.
- Identificar a origem do incidente.
- Identificar as vulnerabilidades da infraestrutura e dos sistemas da DTI.
- Identificar o(s) responsável(eis) pela resolução do incidente.
- Resolver o incidente.
- Elaborar relatório detalhado envolvendo o incidente de SI.
- Incluir no relatório possíveis recomendações quanto ao incidente.

Saídas:

- Planilha eletrônica atualizada com histórico e solução do incidente.
- Relatório sobre o incidente, incluindo recomendações se necessário.

Acionar plano de comunicação

Objetivo:

Executar as ações necessárias voltadas à comunicação das partes envolvidas e interessadas sobre o incidente de segurança da informação em curso.

Responsável:

Equipe de Resposta a Incidentes em SI (ETRI-SI)

Entradas:

- Planilha eletrônica atualizada com histórico e solução do incidente.
- Plano de comunicação.

Tarefas:

- Analisar plano de comunicação.
- Identificar pessoas e setores a serem comunicados sobre a ocorrência do incidente de SI.

Saídas:

Pessoas e setores comunicados.

Validar recomendações apontadas no relatório

Objetivo:

Analisar sobre possibilidade de validação das recomendações apontadas pela ETRI-SI e quanto à necessidade de análise pelo CGovTI.

Responsável:

Comitê Gestor de Segurança da Informação (CGSI).

Entradas:

- Relatório de ocorrência do incidente.
- Plano de comunicação.

Tarefas:

- Analisar relatório de ocorrência do incidente.
- Analisar e validar recomendações da ETRI-SI se necessário.
- Analisar quanto à submissão do relatório ao CGovTI.

Saídas:

Indicativo quanto à validação ou não do relatório.

Analisar recomendações

Objetivo:

Analisar recomendações emitidas pela ETRI-SI.

Responsável:

Comitê de Governança de TI (CGovTI).

Entradas:

- Relatório de ocorrência do incidente.
- Plano de comunicação.

Tarefas:

- Analisar relatório de ocorrência do incidente e plano de comunicação.
- Analisar e validar recomendações da ETRI-SI.

Saídas:

Relatório analisado.

Emitir despacho decisório

Objetivo:

Emitir decisão quanto às recomendações da ETRI-SI sobre o incidente de SI em curso.

Responsável:

Comitê de Governança de TI (CGovTI).

Entradas:

- Resultado da análise do relatório de ocorrência do incidente.

Tarefas:

- Emitir despacho com decisão quanto às recomendações da ETRI-SI.

Saídas:

Despacho decisório.

Registrar decisão

Objetivo:

Registrar resultado da análise do CGSI e do CGovTI quanto a recomendações direcionadas ao incidente de SI em curso.

Responsável:

Equipe de Resposta a Incidentes em SI (ETRI-SI).

Entradas:

- Resultado da análise do CGSI.
- Recomendações do CGSI.
- Despacho decisório do CGovTI.

Tarefas:

- Atualizar planilha eletrônica com o resultado da análise e recomendações do CGSI e com a decisão do CGovTI envolvendo o incidente.

Saídas:

Planilha atualizada.

Cientificar interessados

Objetivo:

- Cientificar as pessoas e os setores envolvidos e interessados sobre a ocorrência do incidente, bem como quanto ao resultado da análise e recomendações do CGSI e decisão do CGovTI envolvendo o incidente.

Responsável:

Equipe de Resposta a Incidentes em SI (ETRI-SI).

Entradas:

- Resultado da análise do CGSI.
- Recomendações do CGSI.
- Despacho decisório do CGovTI.

Tarefas:

- Analisar plano de comunicação.
- Identificar pessoas e setores a serem cientificados sobre a ocorrência do incidente de SI.
- Encaminhar resultado da análise e recomendações do CGSI e despacho decisório do CGovTI.

Saídas:

Pessoas e setores cientificados.