MANUAL DE PROCESSO DE TRABALHO 10

IDENTIFICAÇÃO DO PROCESSO

PROCESSO DE GERENCIAMENTO DE NORMAS DE SEGURANÇA CIBERNÉTICA		
OBJETIVO	Gerenciar o ciclo de elaboração e alteração do conjunto de normas de segurança cibernética no âmbito do Tribunal Regional Eleitoral de Sergipe.	
MANUAL	**NÚMERO**	10
	NOME	NORMAS DE SEGURANÇA CIBERNÉTICA
	VERSÃO	3

VISÃO SISTÊMICA

PROCESSO DE GERENCIAMENTO DE NORMAS DE SEGURANÇA CIBERNÉTICA	
ENTRADA(S)	Requisitos de negócios e segurança cibernética
FORNECEDOR(ES)	Unidades solicitantes Processo de Gerenciamento de Mudanças
SAÍDA(S)	Normativos de segurança cibernética
CLIENTE(S)	Unidades do TRE-SE Entidades parceiras Fornecedores
REGULAÇÃO	Política de Segurança da Informação da Justiça Eleitoral - Resolução TSE 23.644/21 (PSI) Família de normas ISO 27000
RECURSO(S)	SEI Editor de Textos

CADEIA DE VALOR

POSIÇÃO DO PROCESSO NA CADEIA DE VALOR	
MACROPROCESSO DE APOIO	Os macroprocessos de apoio garantem o suporte adequado aos processos finalísticos
MACROPROCESSO 13	Gestão de Tecnologia e Segurança Cibernética
PROCESSO 13.4	Gerir Segurança Cibernética
SUBPROCESSO 13.4.3	Gerenciamento de normas de segurança cibernética

GESTOR DO PROCESSO

GESTOR DO PROCESSO	
UNIDADE	A Assessoria Técnica de Segurança Cibernética da STI (ASSEC/STI) é a unidade responsável pela gestão do processo, cabendo-lhe seu acompanhamento, controle e melhoria. Esta unidade também receberá as dúvidas e sugestões acerca do processo para análise e providências necessárias.

PARTICIPANTE(S) DO PROCESSO

PARTICIPANTE(S)	
STI	Secretaria de Tecnologia da Informação e Comunicação. Unidade responsável por avaliar a viabilidade da elaboração de norma de segurança cibernética.
ASSEC	Assessoria Técnica de Segurança Cibernética. Unidade responsável por elaborar ou realizar alterações nas normas de segurança cibernética existentes.
CGSI	Comitê Gestor de Segurança da Informação. Grupo responsável pela análise crítica das normas de segurança cibernética.
DIRETORIA-GERAL	Autoridade responsável pela aprovação, em última instância, da norma de segurança.

TERMOS E DEFINIÇÕES

TERMO	DEFINIÇÃO
NORMA TÉCNICA	Documento aprovado por uma instituição reconhecida, que prevê, para um uso comum e repetitivo, regras, diretrizes ou características para os produtos ou processos e métodos de produção conexos, e cuja observância não é obrigatória. Também pode incluir prescrições em matéria de terminologia, símbolos, embalagem, marcação ou etiquetagem aplicáveis a um produto, processo ou método de produção, ou tratar exclusivamente delas (ex: ABNT NBR ISO 27002/2013).
REGRAS DE NEGÓCIO	Diretiva específica, acionável e testável que está sob o controle de uma organização e que apoia uma política do negócio.
RISCO	Combinação da probabilidade de ocorrência de um evento e sua consequência.

DOCUMENTO(S) DO PROCESSO

DOCUMENTO	NOME	ONDE É ENCONTRADO OU UNIDADE RESPONSÁVEL
D1	Solicitação de Criação de Norma de Segurança Cibernética	SEI

<table>
<tr><th>EVENTO DE RISCO</th><th>AÇÃO</th><th>ATIVIDADE LIGADA AO RISCO</th></tr>
<tr><td colspan="2" rowspan="2">1. Normas desatualizadas frente às ameaças atuais</td><td>- Instituir um ciclo formal de revisão periódica de normas
- Vincular a atualização normativa ao processo de gestão de riscos
- Adotar frameworks e padrões de referência atualizados
- Criar um comitê multidisciplinar de revisão normativa
- Monitorar continuamente o cenário de ameaças
- Prever mecanismos de flexibilização normativa controlada
- Integrar lições aprendidas de incidentes e exercícios
- Capacitar gestores e responsáveis normativos
- Estabelecer indicadores de maturidade normativa</td><td rowspan="3">2. Levantar requisitos</td></tr>
<tr><td>Nível de Risco: Alto
Resposta: Mitigar
Controle: Melhorar controle existente</td><td>Unidade/Servidor responsável:
STI-ASSEC /Selmo Pereira de Almeida</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">2. Distanciamento entre norma e prática operacional</td><td>- Integrar as áreas normativas e operacionais
- Alinhar as normas à análise de riscos - Traduzirr as normas em</td><td>2. Levantar requisitos</td></tr>
</table>

<table>
<tr><th colspan="2">EVENTO DE RISCO</th><th>AÇÃO</th><th>ATIVIDADE LIGADA AO RISCO</th></tr>
<tr><td colspan="2"></td><td>procedimentos operacionais claros
- Capacitação contínua e comunicação efetiva
- Monitoramento, auditorias e testes periódicos
- Retroalimentação por lições aprendidas.</td><td rowspan="3"></td></tr>
<tr><td>Nível de Risco:
Alto</td><td>Resposta:
Mitigar</td><td rowspan="2">Unidade/Servidor responsável:
STI / José Carvalho Peixoto</td></tr>
<tr><td colspan="2">Controle: Melhorar controle existente</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2">3. Excesso ou sobreposição de normativos</td><td>- Inventariar e mapear todos os normativos vigentes
- Consolidar e harmonizar normas
- Adotar uma arquitetura normativa hierarquizada
- Alinhar os normativos a frameworks de referência
- Estabelecer governança centralizada do ciclo normativo
- Vincular a produção normativa à gestão de riscos</td><td rowspan="3">2. Levantar requisitos</td></tr>
<tr><td>Nível de Risco:
Moderado</td><td>Resposta:
Mitigar</td><td rowspan="2">Unidade/Servidor responsável:
DG / Rubens Maciel Lisboa Filho</td></tr>
<tr><td colspan="2">Controle: Melhorar controle existente</td></tr>
</table>

INDICADOR(ES) DE DESEMPENHO

INDICADOR 1: ÍNDICE DE FORMALIZAÇÃO DE NORMAS DE SEGURANÇA	
TIPO	Eficácia
O QUE MEDE	O quantitativo de normas de segurança formalizadas em determinado período.
PARA QUE MEDIR	Evidencia o comprometimento da alta administração do TRE-SE com a segurança cibernética, mediante a expedição de diretrizes regulamentando o assunto.
QUEM MEDE	STI / ASSEC
QUANDO MEDIR	Anualmente
ONDE MEDIR	Plano de ação do PDTI
COMO MEDIR	Quantidade de normas de segurança cibernética a serem formalizadas (NSF) dividido pelo total de normas planejadas para formalização (TNPF), multiplicado por cem. (NSF / NPF) * 100 O TNPF deve constar do plano de ações, anexo do PDTI, do ano respectivo. Considera-se formalizada/institucionalizada a norma aprovada pela alta administração do Tribunal (Diretor-Geral ou Presidente).
META	Formalizar, pelo menos, 50% das normas de segurança planejadas para o ano.

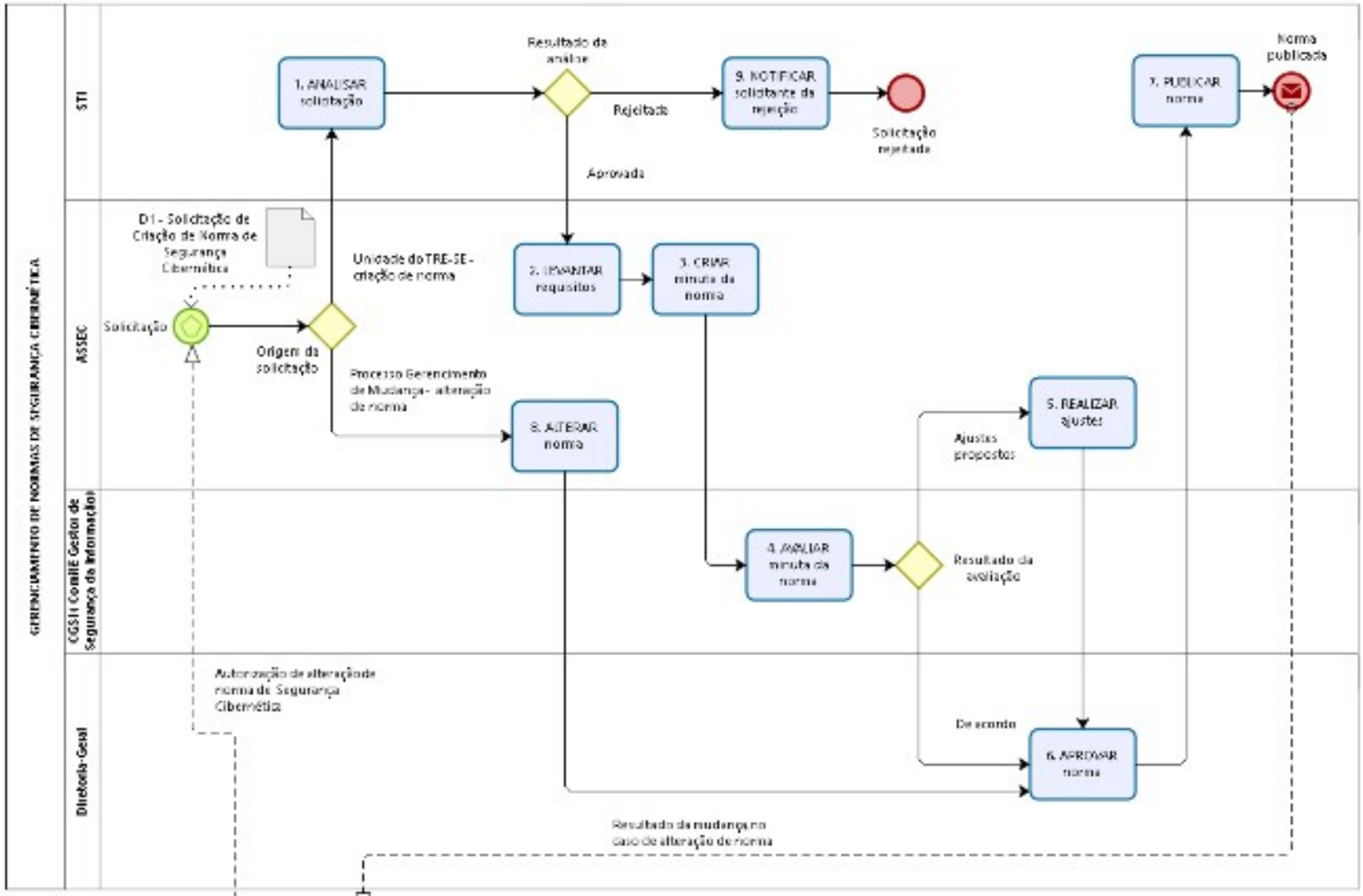
AUTORES DO MANUAL

MANUAL ELABORADO POR	
UNIDADES	ASSEC-STI – Assessoria Técnica de Segurança Cibernética
	SEORG - Seção de Otimização de Processos Organizacionais

SOBRE A VERSÃO

VERSÃO	RESUMO DAS ALTERAÇÕES	RESPONSÁVEL
1	Versão inicial.	Autores do manual
2	Revisão do mapeamento do processo e alteração do manual para o novo modelo padrão elaborado pela SEORG.	SEORG
3	Revisão para atualização e modificação do responsável	ASSEC

GERENCIAMENTO DE NORMAS DE SEGURANÇA CIBERNÉTICA



PROCESSOS/ENTIDADES RELACIONADOS

GERENCIAMENTO DE MUDANÇAS
DESCRIÇÃO
Processo responsável por controlar o Ciclo de Vida de todas as Mudanças. O principal objetivo do Gerenciamento de Mudança é permitir que as mudanças no ambiente sejam feitas com a mínima interrupção dos serviços de TI.

Solicitação
Descrição
Qualquer unidade do Tribunal pode solicitar a criação de norma que regule algum aspecto da segurança cibernética. As solicitações para alteração de norma são procedentes do processo Gerenciamento de Mudanças.

D1 - Solicitação de Criação de Norma de Segurança Cibernética
DESCRIÇÃO
D1 - Solicitação de Criação de Norma de Segurança Cibernética
Onde é encontrado ou unidade responsável: ASSEC

1. ANALISAR solicitação
DESCRIÇÃO
A STI analisará a oportunidade e conveniência de criação da norma, bem como seu impacto nos ambientes de negócio e de TI.

EXECUTANTE
STI

☐ **2. LEVANTAR requisitos**

DESCRIÇÃO

- Identificar normas técnicas, procedimentos, contratos e legislação pertinente;
- Identificar existência de possíveis conflitos entre normas;
- Identificar regras de negócio mediante entrevistas com partes interessadas ou envio de questionários;
- Identificar riscos envolvidos e as consequências da implantação da norma no ambiente de TIC;
- Considerar, durante o levantamento de requisitos, ameaças à segurança cibernética, atuais e futuras;
- Classificar e priorizar requisitos;
- Registrar lista de requisitos.

EXECUTANTE

ASSEC

☐ **3. CRIAR minuta da norma**

DESCRIÇÃO

- Elaborar versão inicial da norma de segurança;
- Disponibilizar minuta para avaliação do Comitê Gestor de Segurança da Informação.

EXECUTANTE

ASSEC

☐ **4. AVALIAR minuta da norma**

DESCRIÇÃO

- Avaliar todos os aspectos da minuta de norma, sobretudo os impactos nas áreas de negócio;
- Propor alterações, caso necessário.

EXECUTANTE

Comitê Gestor de Segurança da Informação - CGSI

5. REALIZAR ajustes

DESCRIÇÃO

- Realizar ajustes na norma de acordo com as instruções do CGSI.
- Submeter norma para aprovação.

EXECUTANTE

ASSEC

6. APROVAR norma

DESCRIÇÃO

Aprovar normativo e assiná-lo.

EXECUTANTE

Diretoria-Geral

7. PUBLICAR norma

DESCRIÇÃO

- Publicar normativo no Diário da Justiça Eletrônico (DJE) e nos sítios do Tribunal;
- Enviar comunicado a todos os servidores e partes externas relevantes.

EXECUTANTE

STI

8. ALTERAR norma

DESCRIÇÃO

Ao receber uma autorização de mudança, proveniente do processo de Gerenciamento de Mudanças, a ASSEC deve:

- Realizar as alterações aprovadas;
- Submeter norma alterada para aprovação superior.

EXECUTANTE

ASSEC

☐ **9. NOTIFICAR solicitante da rejeição**

DESCRIÇÃO

Caso a solicitação seja rejeitada, informar a decisão à unidade solicitante.

EXECUTANTE

STI