MANUAL DE PROCESSO DE TRABALHO 29

IDENTIFICAÇÃO

PROCESSO DE GERENCIAMENTO DE VULNERABILIDADES DE SEGURANÇA DA INFORMAÇÃO		
OBJETIVO	Identificar, classificar e tratar as vulnerabilidades de segurança da informação no âmbito do TRE-SE.	
MANUAL	**NÚMERO**	29
	NOME	VULNERABILIDADES DE SI
	VERSÃO	2

VISÃO SISTÊMICA

PROCESSO DE GERENCIAMENTO DE VULNERABILIDADES DE SEGURANÇA DA INFORMAÇÃO	
ENTRADA(S)	Riscos de vulnerabilidades de segurança nos ativos de informação em operação
FORNECEDOR(ES)	Seção de Segurança da Informação (SESIN) e unidades técnicas responsáveis pelos ativos de informação
SAÍDA(S)	Ambiente computacional seguro
CLIENTE(S)	Usuários de TIC
REGULAÇÃO	Resolução TRE-SE 10/2019 Portaria TRE-SE 275/2018 Portaria TRE-SE 278/2018
RECURSO(S)	Framework com solução de varredura e gerenciamento de vulnerabilidades

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 11	Gestão da Informação
PROCESSO 11.7	Segurança da Informação
SUBPROCESSO 11.7.5	Gerenciamento de Vulnerabilidades de Segurança da Informação

GESTOR DO PROCESSO

GESTOR DO PROCESSO	
UNIDADE	A Seção de Segurança da Informação (SESIN) 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.

GESTOR DE SEGURANÇA DA INFORMAÇÃO

GESTOR DE SEGURANÇA DA INFORMAÇÃO	
UNIDADE	A Seção de Segurança da Informação (SESIN) responde, atualmente, pela gestão de segurança da informação no âmbito do TRE-SE, sendo responsável por propor diretrizes para a manutenção da confidencialidade, autenticidade, disponibilidade e integridade das informações institucionais.

GESTOR DE RISCOS

GESTOR DE RISCOS	
UNIDADE	Cabe à Seção de Segurança da Informação (SESIN) a análise dos riscos associados às vulnerabilidades dos ativos de informação em operação no TRE-SE, de acordo com a metodologia de gestão de riscos vigente na Instituição.

PARTICIPANTE(S) DO PROCESSO

PARTICIPANTE(S)	
ETIR	Equipe Técnica de Resposta a Incidentes de Redes Computacionais
SESIN	Seção de Segurança da Informação
RESPONSÁVEL PELO ATIVO	Unidade técnica identificada, oficialmente, como responsável pelo ativo de informação.

TERMOS E DEFINIÇÕES

TERMO	DEFINIÇÃO
ATIVO DE INFORMAÇÃO	Toda informação ou dado gerado, adquirido, utilizado ou custodiado pela Justiça Eleitoral, assim como qualquer equipamento, software ou recurso utilizado para seu processamento ou armazenamento.
AMEAÇA	Uma ocorrência potencialmente negativa.
VULNERABILIDADES	Fragilidades de um ativo ou grupo de ativos que podem ser exploradas por uma ou mais ameaças.
RISCO	Potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização.

INDICADOR(ES) DE DESEMPENHO

INDICADOR 1: ÍNDICE DE VULNERABILIDADES DE SEGURANÇA CONHECIDAS E TRATADAS	
TIPO	Eficácia
O QUE MEDE	O quantitativo de vulnerabilidades de segurança conhecidas e tratadas
PARA QUE MEDIR	Permite monitorar se as vulnerabilidades de segurança conhecidas estão documentadas, com tratamento adequado
QUEM MEDE	Seção de Segurança da Informação (SESIN)
QUANDO MEDIR	Trimestralmente
ONDE MEDIR	SEI
COMO MEDIR	Quantidade de vulnerabilidades tratadas (QVT) dividida pelo total de vulnerabilidades conhecidas (TVC), multiplicado por cem. (QVT / TVC) * 100
META	100% das vulnerabilidades conhecidas e tratadas

TABELA RACI

Definição e distribuição de papéis e responsabilidades que integram o Processo de Gerenciamento de Vulnerabilidades de Segurança da Informação.

R – **Responsável**: quem deve executar a atividade;
A – **Autoridade**: quem deve responder pela atividade;
C – **Consultado**: quem deve ou pode ser consultado durante a execução da atividade;
I – **Informado**: quem deve receber a informação de que uma atividade foi executada.

Atividade	SESIN	ETIR	RESPONSÁVEL PELO ATIVO
1. Atualizar ativos	C/I	-	R/A
2. Monitorar fontes de vulnerabilidades	R/A	C	-
3. REALIZAR auditoria	R/A	C	I
4. ABRIR chamado	R/A	C/I	-
5. AVALIAR o ambiente	C	R/A	C
6. CLASSIFICAR vulnerabilidade	C/I	R/A	-
7. IDENTIFICAR responsável	R/A	-	C
8. NOTIFICAR responsável	R/A	-	I
9. ACOMPANHAR tratamento	R/A	-	C
10. REALIZAR tratamento	C/I	-	R/A
11. RESPONDER notificação	I	-	R/A

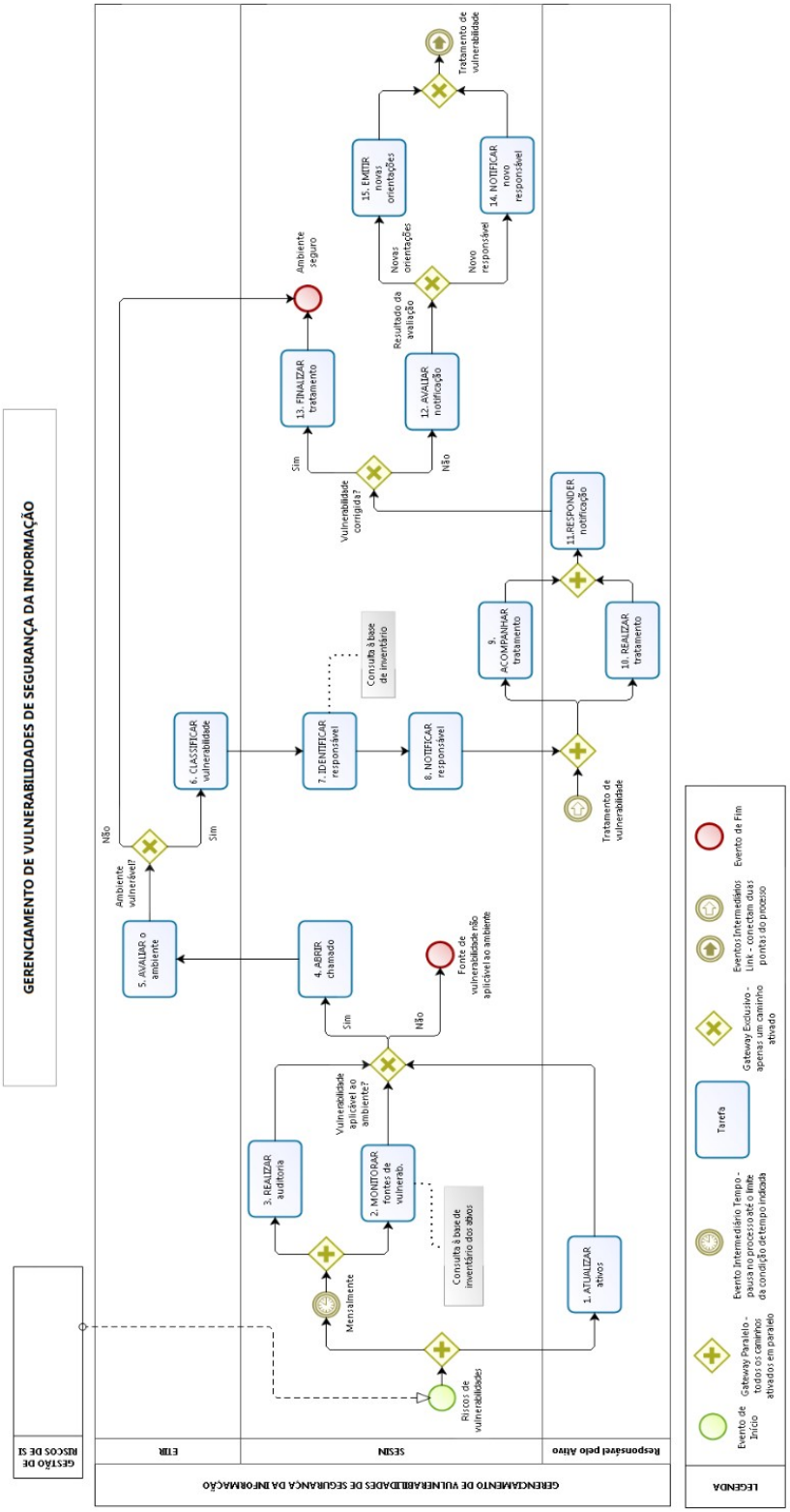
Atividade	SESIN	ETIR	RESPONSÁVEL PELO ATIVO
12. AVALIAR notificação	R/A	C	C
13. FINALIZAR tratamento	R/A	-	-
14. NOTIFICAR novo responsável	R/A	-	I
15. EMITIR novas orientações	R/A	C	I

AUTORES DO MANUAL

MANUAL ELABORADO POR	
UNIDADES	STI - Secretaria de Tecnologia da Informação
	SESIN - Seção de Segurança da Informação
	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


GERENCIAMENTO DE VULNERABILIDADES DE SEGURANÇA DA INFORMAÇÃO
GESTÃO DE RISCOS DE SI
ETIR
SESIN
Responsável pelo Ativo
Riscos de vulnerabilidades
Mensalmente
1. ATUALIZAR ativos
2. MONITORAR fontes de vulnerab.
3. REALIZAR auditoria
Consulta à base de inventário dos ativos
Vulnerabilidade aplicável ao ambiente?
Não
Sim
Fonte de vulnerabilidade não aplicável ao ambiente
4. ABRIR chamado
5. AVALIAR o ambiente
Ambiente vulnerável?
Não
Sim
6. CLASSIFICAR vulnerabilidade
7. IDENTIFICAR responsável
Consulta à base de inventário
8. NOTIFICAR responsável
Tratamento de vulnerabilidade
9. ACOMPANHAR tratamento
10. REALIZAR tratamento
11.RESPONDER notificação
Vulnerabilidade corrigida?
Sim
Não
13. FINALIZAR tratamento
Ambiente seguro
12. AVALIAR notificação
Resultado da avaliação
Novas orientações
Novo responsável
15. EMITIR novas orientações
14. NOTIFICAR novo responsável
Tratamento de vulnerabilidade
LEGENDA
Evento de Início
Gateway Paralelo - todos os caminhos ativados em paralelo
Evento Intermediário Tempo - pausa no processo até o limite da condição de tempo indicada
Tarefa
Gateway Exclusivo - apenas um caminho ativado
Eventos Intermediários Link - conectam duas pontas do processo
Evento de Fim

PROCESSOS/ENTIDADES RELACIONADOS

GESTÃO DE RISCOS
DESCRIÇÃO
Processo de análise dos riscos de segurança dos ativos de informação, de acordo com as normas de gestão de risco vigentes, realizado pelo Gestor de Segurança da Informação (SESIN).

1. ATUALIZAR ativos
DESCRIÇÃO
Devem ser implementadas ações preventivas, de acordo com as melhores práticas, para, no mínimo:
I. atualizar e manter atualizados os sistemas operacionais e aplicativos instalados em estações de trabalho e dispositivos móveis;
II. atualizar e manter atualizados os sistemas operacionais de servidores, sejam estes físicos ou virtuais;
III. atualizar e manter atualizados os servidores de aplicação (middleware);
IV. atualizar e manter atualizados os SGBDs (sistemas de gestão de bancos de dados);
V. atualizar e manter atualizada a infraestrutura de virtualização;
VI. atualizar e manter atualizados os sistemas e aplicações Web;
VII. atualizar e manter atualizados sistemas de IOT (Internet of Things ou "Internet das Coisas") e de comunicação;
VIII. testar novos sistemas de informação antes de sua entrada em produção;
IX. manter atualizado o inventário de ativos de informação.

EXECUTANTE
Responsável pelo Ativo

2. MONITORAR fontes de vulnerabilidades

DESCRIÇÃO

- Monitorar os sistemas listados no inventário de ativos da informação, visando detectar vulnerabilidades de segurança da informação.
- Comunicar-se com a ETIR (Equipe Técnica de Resposta a Incidentes de Redes Computacionais) e com as áreas da Secretaria de Tecnologia da Informação, responsáveis pelos ativos a fim de informar e obter informações acerca de vulnerabilidades existentes.
- Deverão ser acompanhados ao longo do tempo o surgimento de novas vulnerabilidades, o tempo de tratamento das vulnerabilidades descobertas e o nível de exposição dos principais ativos de informação.

Referência: Normas ISO 27001(A.12.6.1, A.12.6.2 e A.12.7.1) e ISO 27002(12.6)

EXECUTANTE

SESIN - Seção de Segurança da Informação

3. REALIZAR auditoria

DESCRIÇÃO

- Realizar auditoria nos sistemas com uma solução de varredura e gerenciamento de vulnerabilidades (ex: OpenVas), além de testes periódicos, visando detectar vulnerabilidades de segurança da informação.
- As atividades de varreduras e testes podem ser feitas de forma automatizada ou manual, de acordo com a disponibilidade e necessidade.

São tipos principais de varreduras:

I - Completa: é composta por testes para todas as vulnerabilidades conhecidas de aplicativos da Web, sistemas operacionais e redes, usando ferramentas manuais e automatizadas;

II - Rápida: é composta por testes das principais vulnerabilidades conhecidas, tipicamente realizada de forma automatizada.

Referência: Normas ISO 27001(A.12.6.1, A.12.6.2 e A.12.7.1) e ISO 27002(12.6).

EXECUTANTE

SESIN - Seção de Segurança da Informação

4. ABRIR chamado

DESCRIÇÃO

Abrir um chamado na Central de Serviços TI para ativar a ETIR com a finalidade de tratar a vulnerabilidade.

EXECUTANTE

SESIN - Seção de Segurança da Informação

5. AVALIAR o ambiente

DESCRIÇÃO

Consiste em efetuar uma análise detalhada da infraestrutura de segurança do ativo com base em requisitos do próprio TRE-SE ou em melhores práticas de mercado. Pode incluir: revisão da infraestrutura, revisão de processos, varredura da rede e testes de penetração.

EXECUTANTE

ETIR - Equipe Técnica de Resposta a Incidentes de Redes Computacionais

6. CLASSIFICAR vulnerabilidade

DESCRIÇÃO

- As vulnerabilidades encontradas nas varreduras e testes serão classificadas de acordo com o nível de criticidade, levando em conta o potencial de dano, a facilidade de exploração por ameaça, a importância do ativo para a atividade da Justiça Eleitoral e o nível de privacidade e sigilo das informações acessadas.
- As vulnerabilidades serão classificadas, no mínimo, através dos seguintes níveis: Alto, Médio e Baixo.

Parâmetros

Prioridade	Tempo Máximo para Solução (TMS)
1	Em até 8hs úteis
2	Em até 16hs úteis
3	Em até 5 dias úteis
4	Em até 10 dias úteis ou em data posterior específica ou programada

Riscos (Frequência x Impacto)		Impacto			
		I	II	III	IV
Frequência	E	3	4	5	5
	D	2	3	4	5
	C	1	2	3	4
	B	1	1	2	3
	A	1	1	1	2
Critério utilizado para **frequência**: *A* = Muito improvável *B* = Improvável *C* = Ocasional *D* = Provável *E* = Frequente		Critério utilizado para **impacto**: *I* = Desprezível *II* = Marginal *III* = Crítico *IV* = Catastrófico		Critério utilizado para **risco**: 1 = Desprezível (Determinar se ações corretivas são necessárias ou aceitar o risco) 2 = Menor 3 = Moderado (Controles adicionais devem ser avaliados com objetivo de obter-se uma redução dos riscos e implementados aqueles considerados praticáveis) 4 = Sério 5 = Crítico (Existe uma grande necessidade de executar medidas corretivas)	

Referência: Normas ISO 27001(A.12.6.1, A.12.6.2 e A.12.7.1) e ISO 27002(12.6).

EXECUTANTE

ETIR - Equipe Técnica de Resposta a Incidentes de Redes Computacionais

☐ 7. IDENTIFICAR responsável

DESCRIÇÃO

Consultar a base de inventário para identificação do responsável pelo ativo e obtenção do seu contato.

Referência: Normas ISO 27001(A.12.6.1, A.12.6.2 e A.12.7.1) e ISO 27002(12.6).

EXECUTANTE

SESIN - Seção de Segurança da Informação

☐ 8. NOTIFICAR responsável

DESCRIÇÃO

- Enviar e-mail para o responsável pelo ativo relatando o ocorrido, o tratamento necessário e a priorização definida para o atendimento.
- Estabelecer prazo para o tratamento.

Referência: Normas ISO 27001(A.12.6.1, A.12.6.2 e A.12.7.1) e ISO 27002(12.6).

EXECUTANTE

SESIN - Seção de Segurança da Informação

☐ 9. ACOMPANHAR tratamento

DESCRIÇÃO

Acompanhar o tratamento e prestar o suporte necessário ao responsável pelo ativo.

Referência: Normas ISO 27001(A.12.6.1, A.12.6.2 e A.12.7.1) e ISO 27002(12.6).

EXECUTANTE

SESIN - Seção de Segurança da Informação

10. REALIZAR tratamento

DESCRIÇÃO

- Corrigir as vulnerabilidades encontradas, em observância à priorização definida pela Seção de Segurança da Informação (SESIN).
- Atuar para diminuir a exposição ao risco a um nível aceitável, de acordo com o nível de criticidade do ativo.
- As vulnerabilidades de maior criticidade deverão ser tratadas no menor tempo possível.
- Os processos de correção de vulnerabilidades de criticidade alta ou média em ativos definidos como prioritários ao negócio devem ter suas atividades priorizadas em relação às demais atividades rotineiras das unidades técnicas.
- Implementar medidas para mitigar o risco referente às vulnerabilidades que não puderem ser corrigidas tempestivamente.
- O tratamento da vulnerabilidade é realizado com o suporte da SESIN.

Referência: Normas ISO 27001(A.12.6.1, A.12.6.2 e A.12.7.1) e ISO 27002(12.6).

EXECUTANTE

Responsável pelo Ativo

11.RESPONDER notificação

DESCRIÇÃO

- Responder à SESIN relatando o resultado do tratamento.
- No caso de impossibilidade de tratamento de alguma vulnerabilidade classificada como crítica, a SESIN e o Secretário de Tecnologia da Informação deverão ser imediatamente comunicados.

Referência: Normas ISO 27001(A.12.6.1, A.12.6.2 e A.12.7.1) e ISO 27002(12.6)

EXECUTANTE

Responsável pelo Ativo

12. AVALIAR notificação

DESCRIÇÃO

- Avaliar as considerações do responsável pelo ativo acerca do tratamento dispensado à determinada vulnerabilidade.
- No caso de vulnerabilidades críticas descobertas e que não puderem ser tratadas em tempo adequado, o Secretário de Tecnologia da Informação deve estar ciente para que possa comunicar o fato às áreas de negócio, ao encarregado pela proteção de dados pessoais e à Diretoria-Geral.

EXECUTANTE

SESIN - Seção de Segurança da Informação

13. FINALIZAR tratamento

DESCRIÇÃO

Finalizar o tratamento da vulnerabilidade, mantendo o histórico na base de conhecimento.

Referência: Normas ISO 27001(A.12.6.1, A.12.6.2 e A.12.7.1) e ISO 27002(12.6).

EXECUTANTE

SESIN - Seção de Segurança da Informação

14. NOTIFICAR novo responsável

DESCRIÇÃO

Enviar e-mail para um novo responsável pelo ativo identificado, relatando o ocorrido e o tratamento necessário.

Referência: Normas ISO 27001(A.12.6.1, A.12.6.2 e A.12.7.1) e ISO 27002(12.6).

EXECUTANTE

SESIN - Seção de Segurança da Informação

☐ **15. EMITIR novas orientações**

DESCRIÇÃO

Enviar e-mail para o responsável pelo ativo identificado relatando o ocorrido e apresentando novas alternativas de tratamento.

Referência: Normas ISO 27001(A.12.6.1, A.12.6.2 e A.12.7.1) e ISO 27002(12.6).

EXECUTANTE

SESIN - Seção de Segurança da Informação