ANEXO II - PORTARIA N° 185/2019 - PRES

TRIBUNAL REGIONAL ELEITORAL

DO RIO GRANDE DO NORTE

Gerenciamento de Incidentes de Segurança da Informação

VERSÃO 1.0

Natal/RN

Agosto/2019

CONTROLE DE VERSÕES

VERSÃO	Validado CPSI	RESPONSÁVEL
1.0	30.08.2019	Marcos Flávio Nascimento Maia

APRESENTAÇÃO

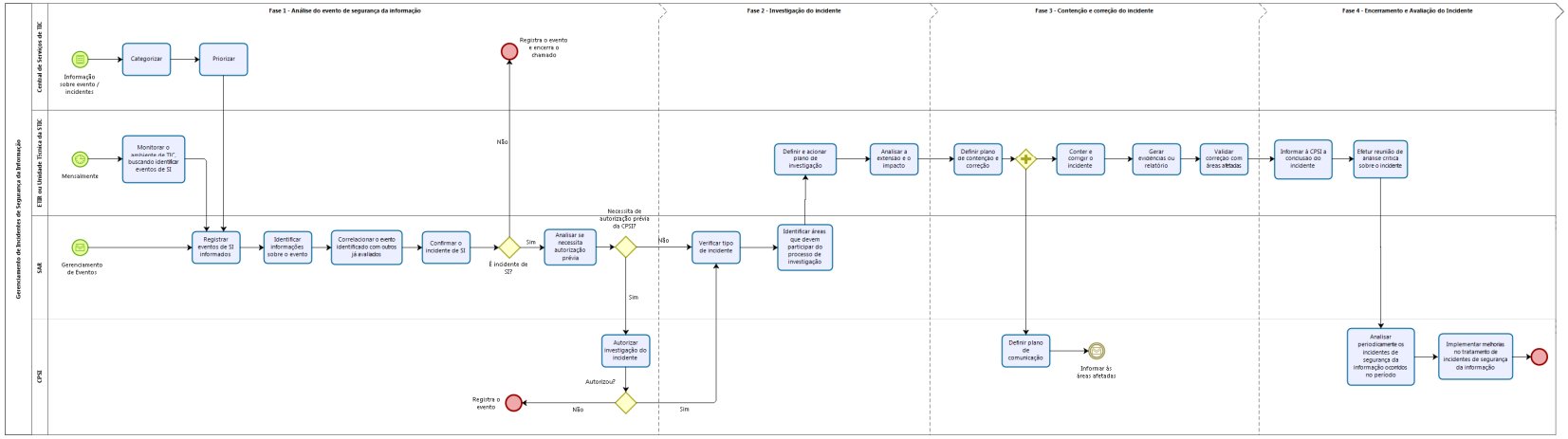
O objetivo deste manual é estabelecer responsabilidades e descrever as atividades para o Tratamento de Incidentes de Segurança da Informação no Tribunal Regional Eleitoral do Rio Grande do Norte, com o intuito de restaurar a operação normal dos serviços o mais rápido possível, minimizando os prejuízos à operação do negócio do TRE/RN e garantindo os níveis de serviço acordados.

As principais motivações para o estabelecimento do presente processo são o alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria, a necessidade de tratar os incidentes de segurança da informação com resposta rápida e eficiente, o correto direcionamento e dimensionamento de recursos tecnológicos e humanos para prover uma Gestão de Incidentes de Segurança da Informação com menor custo e maior qualidade, e a formalização de um processo sistemático para gerenciamento dos incidentes de segurança da informação, provendo insumos para minimizar e/ou evitar eventos futuros.

Além disso, nos casos em que for necessária uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, convém que sejam elaborados e respeitados procedimentos internos para a coleta e apresentação de evidências com propósito de iniciar a ação legal necessária (civil ou criminal).

Índice

1 GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO



1.1 MANUAL DO PROCESSO DE GERENCIAMENTO DE INCIDENTES DE SEGURANÇADA INFORMAÇÃO

1.1.1 FASE 1 - ANÁLISE DO EVENTO DE SEGURANÇA DA INFORMAÇÃO

1.1.1.1 Informação sobre evento / incidentes

Descrição

Registro de eventos, comunicação de suspeita ou ocorrência de incidente de SI, através de abertura de chamado no sistema Atendimento STIC

1.1.1.2 Categorizar

Descrição

A Central de Serviços deve ajusta a categoria adequada, caso necessário.

Executante: Central de Serviços

1.1.1.3 Priorizar

Descrição

Priorizar o incidente de segurança de acordo com os seguintes critérios:

Executante: Central de Serviços

1.1.1.4 Mensalmente

Descrição

Consoante a Portaria n.º¶ 423/2017-GP, art. 9º, mensalmente, a ETIR deverá apresentar à Comissão Permanente de Segurança da Informação (CPSI) relatórios estatísticos dos incidentes ocorridos no período.

1.1.1.5 Monitorar o ambiente de TIC, buscando identificar eventos de SI

Descrição

Consoante a Portaria n.º 423/2017-GP, art. 9º, mensalmente, a ETIR deverá apresentar à Comissão Permanente de Segurança da Informação (CPSI) relatórios estatísticos dos incidentes ocorridos no período, com os respectivos tratamentos adotados, com vistas à elaboração de estudos de melhoria dos mecanismos de segurança estabelecidos no Tribunal ou para fins de tomada de decisão estratégica relativa à Segurança da Informação junto à Administração.

Executante: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)

Referência: Portaria n.º 423/2017 - GP

1.1.1.6 Gerenciamento de Eventos

Descrição

Monitorar o ambiente de TIC, buscando identificar eventos de Segurança da Informação. O evento pode ser detectado por sistema de monitoramento ou demais mecanismos de defesa inatituídos, bem como, através de informação de origem externa.

Executante: Seção de Atendimento Remoto (SAR/CIT)

1.1.1.7 Registrar eventos de SI informados

Descrição

Registrar o incidente de segurança da informação para posterior análise e solução.

Executante: Seção de Atendimento Remoto (SAR/CIT)

1.1.1.8 Identificar informações sobre o evento

Descrição

Identifica o maior número de informações disponíveis sobre o evento,

tais como:

a) Nome e área do usuário notificador;

b) Dia e hora que o evento ocorreu;

c) Como foi detectado o incidente;

d) Tipo de incidente;

e) Quais operações estão indisponíveis;

f) Que sistemas foram afetados.

Executante: Seção de Atendimento Remoto (SAR/CIT)

1.1.1.9 Correlacionar o evento identificado com outros já avaliados

Descrição

Correlacionar o evento e as informações identificadas com outros eventos avaliados, visando identificar semelhanças e possíveis soluções.

Executante: Seção de Atendimento Remoto (SAR/CIT)

1.1.1.10 Confirmar o incidente de SI

Descrição

Verificar se, realmente, trata-se de incidente de segurança da informação e classificar conforme a tabela.

Executante: Seção de Atendimento Remoto (SAR/CIT)

1.1.1.11 Analisar se necessita autorização prévia

Descrição

Analisar se necessita autorização prévia da CPSI para prosseguir a investigação conforme incidentes já registrados e classificados.

Executante: Seção de Atendimento Remoto (SAR/CIT)

1.1.1.12 Autorizar investigação do incidente

Descrição

A CPSI deve reurnir-se, analisar o incidente relatado e autorizar ou não o presseguimento da investigação ou, se for o caso, solicitar informação adicionais para a análise.

Executante: Comissão Permanente de Segurança da Informação (CPSI)

1.1.1.13 Verificar tipo de incidente

Descrição

Verificar se trata-se de um incidente em Redes de Computadores, quando a investigação, contenção e correção será de responsabilidade da ETIR, ou se é um outro tipo de incidente de segurança da informação, quando deve ser acionada a Unidade Técnica da STIC responsável.

Executante: Seção de Atendimento Remoto (SAR/CIT)

1.1.1.14 Identificar áreas que devem participar do processo de investigação

Descrição

Identifica as áreas do TRE/RN e/ou entidades externas que devem atuar em conjunto com a ETIR ou Unidade Técnica responsável para contribuir com informações úteis durante a fase de investigação do incidente.

Executante: Seção de Atendimento Remoto (SAR/CIT)

1.1.1.15 Definir e acionar plano de investigação

Descrição

Definir e acionar o plano de investigação com as etapas necessárias para determinar as causas do incidente.

Executante: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) ou Unidade(s) Técnica(s) da STIC responsável

1.1.1.16 Analisar a extensão e o impacto

Descrição

Descrever e avaliar os reais impactos do incidente de Segurança da Informação e estima o tempo de resposta necessário para investigação, contenção e correção do incidente em questão.

Executante: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) ou Unidade(s) Técnica(s) da STIC responsável

1.1.1.17 Definir plano de contenção e correção

Descrição

Nesta etapa, definir o plano de contenção e correção do incidente, que descreve os métodos e técnicas que devem ser utilizados para impedir que o incidente se propague (contenção), corrigir a causa-raiz do incidente (correção) e tratar suas consequências.

Executante: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) ou Unidade(s) Técnica(s) da STIC responsável

1.1.1.18 Definir plano de comunicação

Descrição

Definir o plano de comunicação que descreve quais são as áreas/usuários participantes do processo de investigação, contenção e correção do incidente, que informações devem ser compartilhadas entre os participantes e envolvidos e quando devem ser comunicados.

Executante: Comissão Permanente de Segurança da Informação (CPSI)

1.1.1.19 Informar às áreas afetadas

Descrição

Comunicar incidente às áreas afetadas e envolvidas O plano de comunicação é acionado.

Executante: Comissão Permanente de Segurança da Informação (CPSI)

1.1.1.20 Conter e corrigir o incidente

Descrição

Executar o plano de contenção e correção implantando as ações necessárias para tratar o incidente de Segurança da Informação.

Se necessário, a Unidade Gestora de TIC deve apoiar a ETIR ou Unidade Técnica na execução das ações.

A ETIR ou a Unidade Técnica responsável deve manter as partes interessadas informadas sobre o andamento das atividades.

Executante: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) ou Unidade(s) Técnica(s) da STIC responsável

1.1.1.21 Gerar evidências ou relatório

Descrição

Coleta e preserva evidências (logs, cópias de tela, etc.) e outros registros referentes ao incidente que possam ser requisitados pela justiça para a resolução de ações civis e/ou criminais, ou por autoridades internas do TRE/RN.

Também deve manter evidências das ações e modificações efetuadas no ambiente que foram executadas para o tratamento do incidente.

Executante: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) ou Unidade(s) Técnica(s) da STIC responsável

1.1.1.22 Validar correção com áreas afetadas

Descrição

Validar as correções com as áreas afetadas e verifica se os componentes afetados retornaram à situação de normalidade.

Executante: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) ou Unidade(s) Técnica(s) da STIC responsável

1.1.1.23 ☐Informar à CPSI a conclusão do incidente

Descrição

Informar à Unidade Gestora de Segurança da Informação que o incidente está solucionado, destacando consequências tratadas e não tratadas.

Executante: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) ou Unidade(s) Técnica(s) da STIC responsável

1.1.1.24 ☐Efetur reunião de análise crítica sobre o incidente

Descrição

Após a conclusão do incidente de Segurança da Informação deve ser efetuada uma reunião de análise crítica onde as ações executadas durante o processo de tratamento são avaliadas, permitindo assim o registro de lições aprendidas e verificando a necessidade de revisão de procedimentos, processos, padrões, bem como a necessidade de ajustes ou contratação de novas ferramentas.

Devem participar dessa reunião, no mínimo, os membros da CPSI e os membros da ETIR. Outras partes interessadas que possam vir a contribuir para melhoria do processo podem, eventualmente, participar (ex.: autoridades policiais, corpo de bombeiros, consultores externos especialistas em Segurança da Informação, etc.).

Executante: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) ou Unidade(s) Técnica(s) da STIC responsável

1.1.1.25 ☐Analisar periodicamente os incidentes de segurança da informação ocorridos no período

Descrição

A CPSI deve analisar periodicamente os incidentes de Segurança da Informação ocorridos no período. O resultado desta análise é evidenciado através de um relatório, que apresenta:

· Os tipos de incidentes de segurança ocorridos;

· As áreas envolvidas;

· A recorrência de incidentes;

· As ações corretivas utilizadas para o tratamento dos incidentes;

· As ações preventivas utilizadas para evitar que incidentes voltem a ocorrer.

Executante: Comissão Permanente de Segurança da Informação (CPSI)

1.1.1.26 ❑Implementar melhorias no tratamento de incidentes de segurança da informação

Descrição

A CPSI deve promover a implementação das melhorias no tratamento de incidentes de Segurança da Informação.

Executante: Comissão Permanente de Segurança da Informação (CPSI)