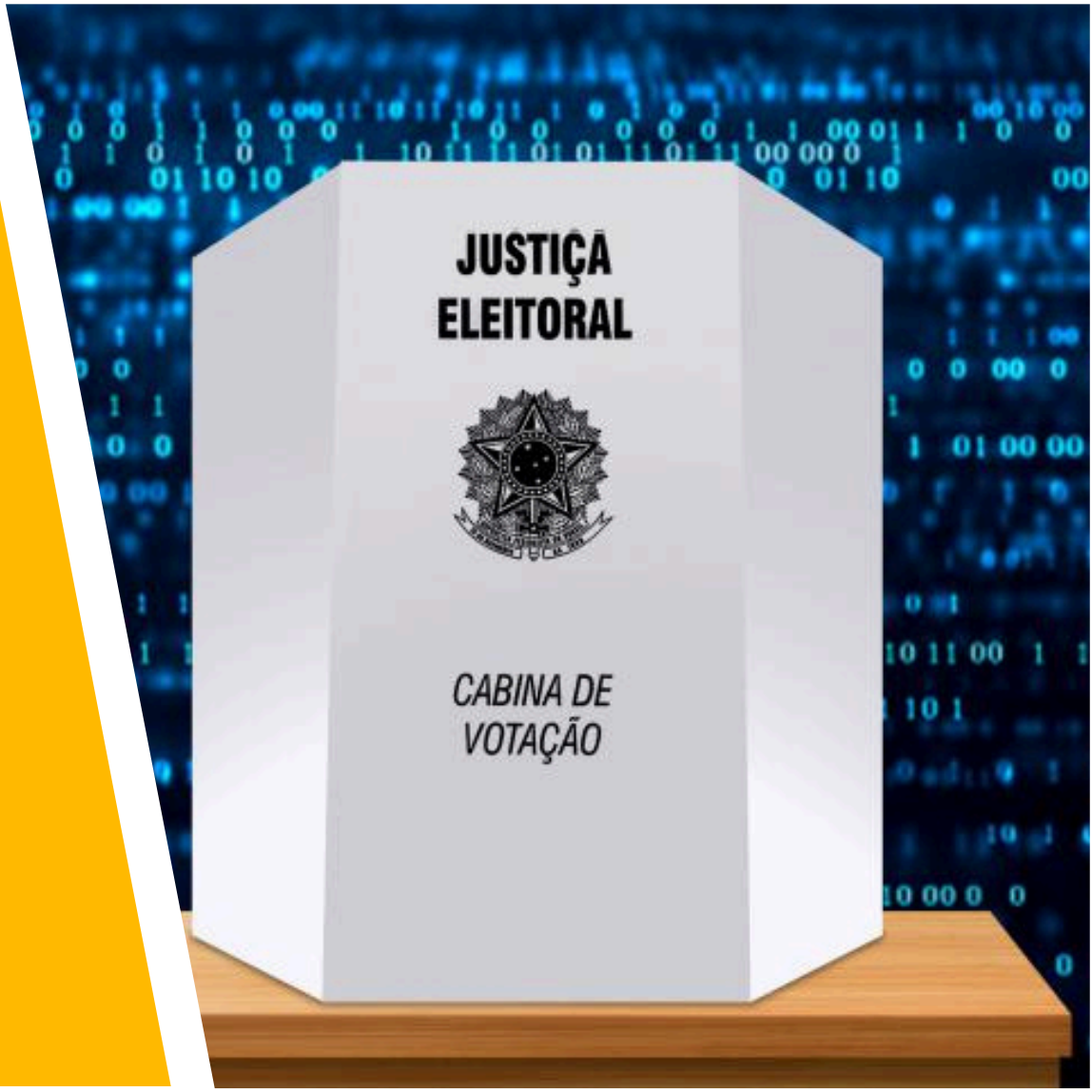
Plano de Ação

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E VIOLAÇÃO DE DADOS PESSOAIS

Tribunal Regional Eleitoral
de Sergipe

SEGURANÇA DA INFORMAÇÃO



PLANO DE AÇÃO

Tribunal Regional Eleitoral de Sergipe

ESTE PLANO DE AÇÃO DETALHA AS AÇÕES A SEREM EXECUTADAS EM CASO DE AMEAÇA OU EFETIVO ATAQUE À SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO TRIBUNAL REGIONAL ELEITORAL DE SERGIPE, INCLUSIVE ENVOLVENDO DADOS PESSOAIS.

Des. Diógenes Brreto
Presidente do TRE/SE - Representante do Controlador

Tribunal Regional Eleitoral de Sergipe

Presidente
Des. Diógenes Barreto

Vice-Presidente
Desa. Ana Bernadete Leite de Carvalho Andrade

Juízes-membros
Juiz Tiago José Brasileiro Franco
Juíza Dauquíria de Melo Ferreira
Juíza Brígida Declerk Fink
Juiz Breno Bergson Santos
Juiz Cristiano César Braga de Aragão Cabral

Procurador-Regional Eleitoral
Martha Carvalho Dias de Figueiredo

Diretor-Geral
Rubens Lisboa Maciel Filho

Sumário

1 Apresentação

O presente plano de ação apresenta medidas de enfrentamento a eventuais ataques à segurança da informação, em qualquer de suas modalidades: fisíca ou cibernética, inclusive envolvendo a violação de dados pessoais tratados no âmbito do Tribunal Regional Eleitoral de Sergipe.

2 Objetivos

- Planejar as ações a serem executadas em caso de incidente de segurança da informação e proteção de dados pessoais;
- Estabelecer roteiro de execução de ações no menor tempo possível;
- Definir modelo de comunicação entre as Unidades envolvidas no tratamento de incidente;
- Estabelecer procedimentos técnicos e estratégicos de resposta a incidente.

3 Escopos

Alinhados aos objetivos, o presente plano de ação conta com os seguintes escopos:

- Manter monitamento constante, por meio dos recursos tecnológicos e humanos disponíveis, a fim de identificar, no mais breve tempo possível, eventuais ameaças ou ataques efetivos;

- Tornar os envolvidos conhecedores das ações e estratégias a serem seguidas, ante ameaça ou efetiva constatação de ataque cibernético ou físico à segurança da informação, inclusive envolvendo violação de dados pessoais.

4 Período de Aplicação

Este plano de ação tem prazo de aplicação indeterminado, devendo ser revisado, no mínimo, a cada 3 (três) anos.

5 Justificativa

O Tribunal Regional Eleitoral de Sergipe (TRE/SE), seguindo a Política de Segurança da Informação aprovada pelo Tribunal Superior Eleitoral (TSE) por meio da Resolução TSE 23.644/2021, dotou-se de estrutura administrativa, tanto em aspectos técnicos quanto de governança, hábil a enfrentar incidentes relacionados à segurança da informação, inclusive os envolvendo violação de dados pessoais.

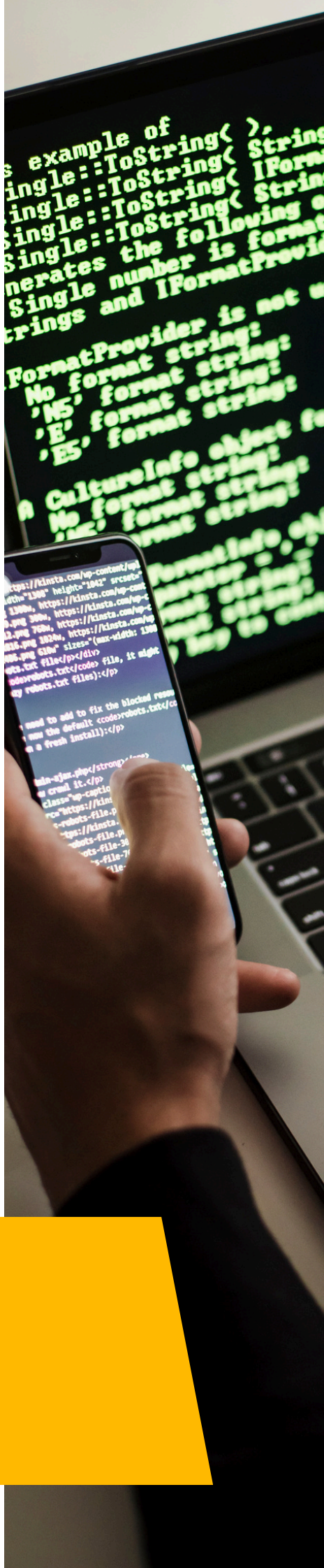
Vinculado diretamente à Diretoria-Geral, o Núcleo de Segurança da Informação e Proteção de Dados Pessoais (NSI) tem atribuições estratégicas em assuntos de segurança da informação e proteção de dados pessoais.

No âmbito da Secretaria da Informação e Tecnologia (STI), a Assessoria Técnica de Segurança Cibernética (ASSEC) tem função operacional de monitoramento de ameaças à segurança cibernética.

Como órgão deliberativo e consultivo, o TRE/SE dipõe do:

- Comitê Gestor de Segurança da Informação (CGSI), com atribuições voltadas a integrar as partes interessadas (stakeholders) ao tema da segurança da informação.

[...]



Segurança da informação e proteção de dados não se gerencia com achismos e opiniões, somente com dados e fatos concretos.

MAURÍCIO ROSA BARBOSA

5 Justificativa

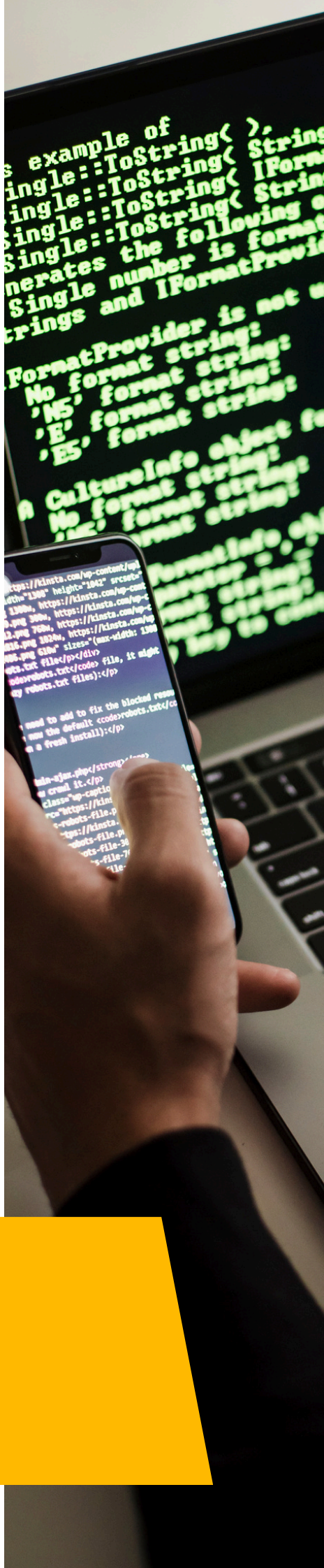
[...]

- Comitê Gestor de Tratamento e Proteção de Dados Pessoais (CGTPDP), com a finalidade de deliberar sobre assuntos relativos à proteção de dados pessoais.

Em momentos de crises, atuam três órgãos internos:

- a Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais (ETIR), para ações operacionais imediatas de enfrentamento a ataques cibernéticos;
- o Comitê Crises Cibernéticas (CCC), para tomada de decisões visando ao retorno à normalidade, no mais breve tempo;
- o Comitê Gestor de Crises (CGC), que atua em caráter deliberativo em ocasiões nas quais o negócio eleitoral seja afetado de forma sistêmica, paralisando as atividades do TRE/SE.

Portanto, este plano de ação agrega-se ao sistema implantado no Tribunal e corrobora a relevância, a seriedade e o compromisso institucional do TRE/SE com a segurança da informação e proteção de dados pessoais.

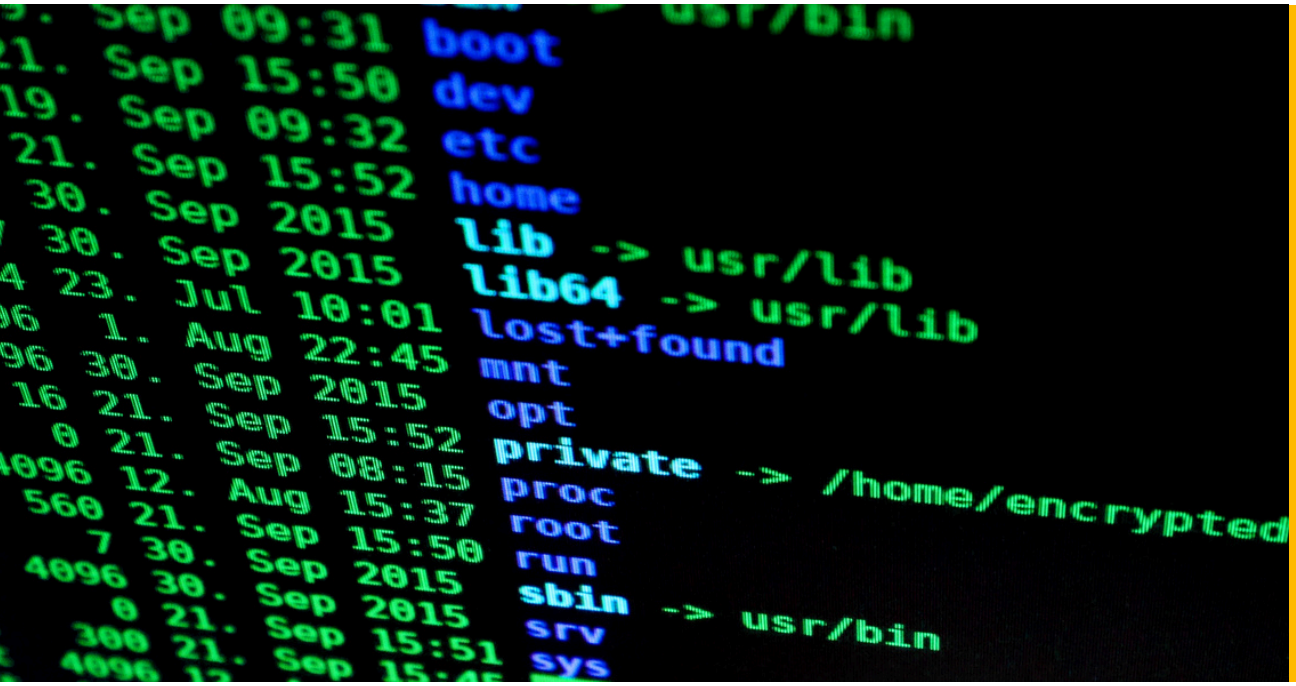


A tecnologia move o mundo.

STEVEN JOBS.

6 Premissas

- Em caso de incidente grave, assim considerado de acordo com conceito atribuído pelo ANEXO VIII da Portaria CNJ nº 162, de 10 de junho de 2022 (Glossário), o CCC deve ser convocado para se reunir imediatamente na "sala de situação";
- A partir da comunicação do incidente por um dos membros da ETIR ao Gestor de Segurança da Informação (para incidente estritamente de segurança da informação) e ao Encarregado (quando envolver violação a dados pessoais), estes serão os responsáveis por interagir com as demais unidades envolvidas e com os órgãos de controle,
- O Presidente do CCC é o responsável por comunicar o incidente ao representante do Controlador (Presidente do TRE/SE);
- O Núcleo de Inteligência e Segurança Institucionais (NIS) atuará nas situações em que o incidente comprometer a estrutura física do TRE/SE ou a integridade de seu corpo de pessoal;
- O representante do Controlador decidirá sobre a convocação do CGC e sobre o momento de comunicação do incidente à imprensa e à sociedade;
- A Assessoria de Comunicação (ASCOM) será a unidade responsável pela comunicação à imprensa e à sociedade;
- As providências relativas ao tratamento de incidente devem ser documentadas (vide Relatório de Incidente de Segurança da Informação - RISI, na seção de Anexos).



7 Restrições

- Os trabalhos técnicos da ETIR devem ser reservados, sem interferência de pessoas estranhas à equipe, a menos que tenham sido convocadas para colaborar no tratamento do incidente;
- As reuniões da ETIR e dos Comitês convocados para deliberar sobre questões de segurança da informação, inclusive envolvendo proteção de dados pessoais, dar-se-ão em ambiente restrito e suas decisões, até manifestação em contrário do Controlador, terão caráter sigiloso;
- A documentação produzida para tratamento do incidente deverá ser incluída em processo SEI classificado como “sigiloso”, no mínimo em grau “reservado”, conforme Política de Classificação da Informação do TRE/SE.

8 Atuação das Unidades Envolvidas

Unidade(s)	Atuação
Assessoria Técnica de Segurança Cibernética (ASSEC) Coordenadoria de Infraestrutura (COINF)	Monitoramento e identificação do incidente.
Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do TRE/SE	Tratamento do incidente identificado; Categorização dos incidentes; Acionamento dos protocolos de resposta aos incidentes.
Núcleo de Segurança da Informação e de Proteção de Dados (NSI)	Acompanhamento do plano de ação e tomada de providências administrativas para sua execução.
Gestor de Segurança da Informação (GSI)	Acompanhamento e integração entre os órgãos envolvidos na segurança da informação.
Encarregado	Acompanhamento e integração entre os órgãos internos envolvidos na proteção de dados pessoais e comunicação à Autoridade Nacional de Proteção de Dados e titulares afetadas(os).
Comitê Gestor de Segurança da Informação (CGSI)	Deliberação sobre questões relativas à aplicação deste Plano de Ação.
Comitê Gestor de Tratamento e Proteção de Dados Pessoais (CGTPDP)	Deliberação sobre questões relativas à aplicação deste Plano de Ação quando envolve violação de dados pessoais.

8 Atuação das Unidades Envolvidas

Órgão(s)	Atuação
Comitê de Crises Cibernéticas (CCC)	Deliberação sobre assuntos sensíveis relacionados a crises de segurança cibernética.
Comitê Gestor de Crises (CGC)	Deliberação sobre assuntos sensíveis relacionados à segurança da informação que afetem sistemicamente as atividades do negócio do TRE/SE.
Controlador (Presidência)	Decisão sobre as ações definidas pelos Comitês; Decisão sobre o momento de comunicação à imprensa e à sociedade.
Assessoria de Comunicação (ASCOM)	Comunicação do incidente e de seus efeitos à imprensa e à sociedade.
Núcleo de Inteligência e Segurança Institucionais (NIS)	Atuação nas situações em que o incidente comprometa a estrutura física do TRE/SE ou a integridade pessoal de seus (suas) agentes.

9 Detalhamento

A seguir, o detalhamento das ações que devem ser executadas em caso de ameaça ou efetivo ataque considerado relevante, também representado no Fluxograma presente na seção de Anexos

1

Identificação do incidente

Caracterizado o ataque relevante pela ASSEC, esta Assessoria deve convocar imediatamente as(os) membras(os) da ETIR.

2

Atuação da ETIR

A ETIR deve, *incontinenti*, voltar-se a mitigar os efeitos do ataque, registrando as constatações no Relatório de Incidente de Segurança da Informação - RISI, constante na seção de Anexos.

3

Comunicação ao GSI e ao Encarregado

Um dos membros da ETIR deve ser destacado para comunicar a ocorrência do incidente ao GSI e ao Encarregado (se constatar violação de dados pessoais), reportando as medidas iniciais adotadas. O GSI e o Encarregado conduzirão o cumprimento deste Plano de Ação.

4

Convocação do Comitê de Crises Cibernéticas

O GSI e o Encarregado, após interação direta com a ETIR e confirmando a gravidade do ataque sofrido, devem convocar reunião do Comitê de Crises Cibernéticas (CCC) (Portaria TRE 117/2022) e dos Comitês Gestores: de Segurança da Informação e de Proteção de Dados Pessoais, na pessoa de seus respectivos presidentes.

5

Cientificação do NSO

Nas situações em que o incidente de segurança da informação ameaçar ou atingir, integral ou parcialmente, a estrutura física do Tribunal ou for capaz de violar a integridade pessoal de suas (seus) agentes, o GSI cientificará o NIS, que tomará as medidas necessárias à cessação ou mitigação das consequências do ataque conforme suas atribuições regimentais.

9 Detalhamento

6

Comunicação do Comitê Gestor de Crises

Caso a ameaça ou o efetivo ataque impactar as atividades eleitorais de maneira ampla e irrestrita, provocando a paralisação dos trabalhos finalísticos do Tribunal, o GSI deve comunicar o incidente ao CGC, na pessoa de seu Presidente.

7

Convocação de servidoras e servidores

O GSI e o Encarregado, julgando necessário, poderão convocar servidora ou servidor do quadro efetivo para colaborar nos trabalhos de mitigação dos efeitos do ataque, ainda que não seja integrante de unidade da segurança da informação ou proteção de dados pessoais, estendendo-se à (ao) convocada(o) o dever de sigilo e confidencialidade a que estão sujeitos as (os) integrantes dos órgãos do Sistema de Segurança.

8

Comunicação ao Representante do Controlador

Apurada a gravidade do incidente, o Presidente do Comitê de Crises Cibernéticas (CCC) deve imediatamente comunicar o incidente ao representante do Controlador (Presidente do TRE/SE).

9

Convocação de profissionais especialistas

O Comitê de Crises Cibernéticas (CCC) deliberará, em situações excepcionais de extrema gravidade do ataque, convidar profissional externo especialista da área de segurança da informação e proteção de dados pessoais, a fim de colaborar nos trabalhos de identificação e mitigação dos efeitos do ataque sofrido.

10

Comunicação à ANPD e às(aos) titulares de dados pessoais

Em tendo havido violação de dados pessoais, o Encarregado deve comunicar o incidente à Autoridade de Proteção de Dados Pessoais (ANDP), no prazo de três dias úteis (Resolução CD/ANPD nº 15, de 24 de abril de 2024), por meio do canal oficial da ANPD - Comunicação de incidente de segurança - Peticionamento Eletrônico ANPD e às(aos) titulares de dados pessoais, por meio de comunicação compatível com o número de afetadas(os).

11

Divulgação do ataque à imprensa e sociedade

A divulgação do ataque à imprensa e à sociedade será realizada pela ASCOM, por ordem do Controlador.

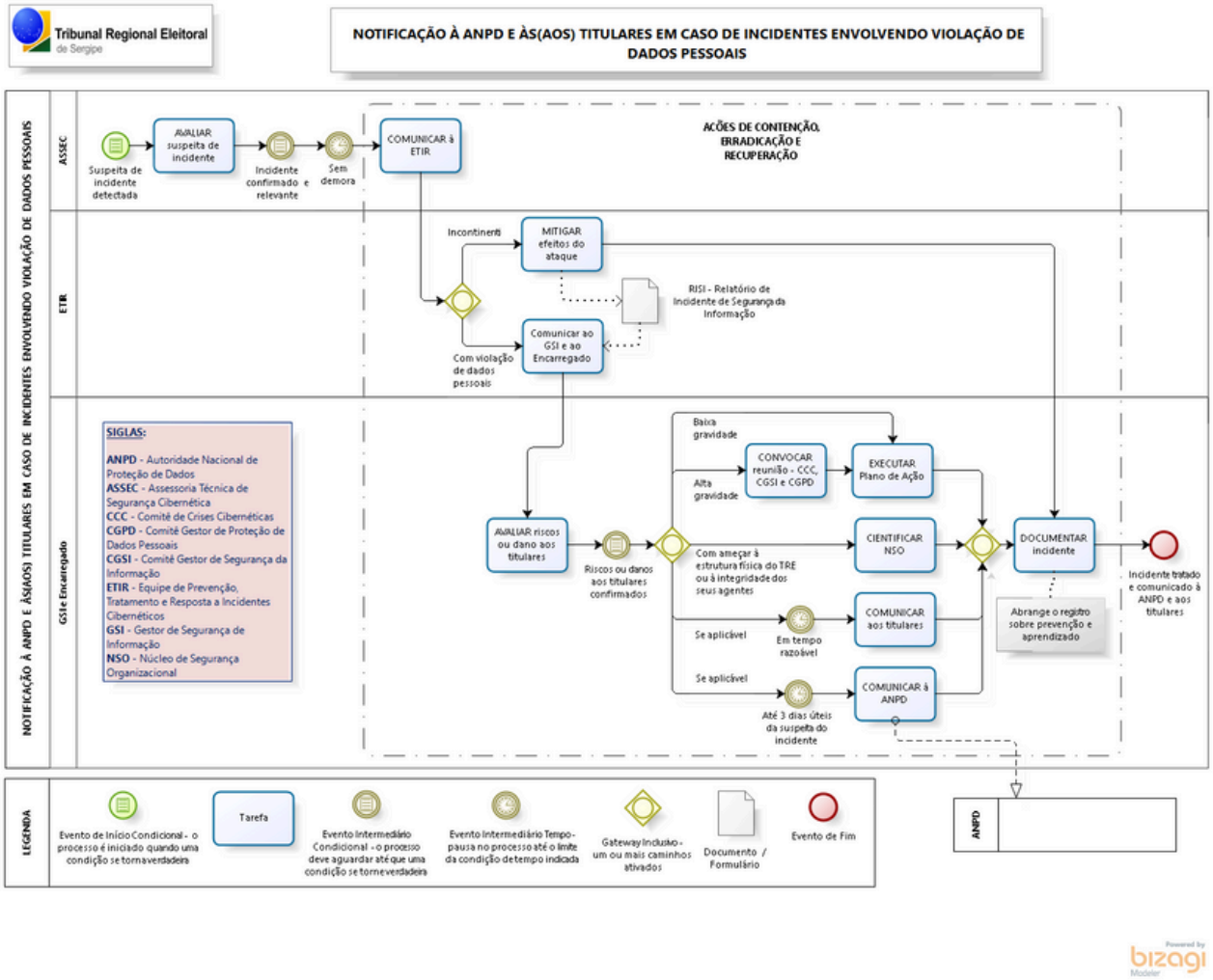
10 Normas de Instituição e Composição da ETIR e dos Comitês

Unidade	Link de Acesso
Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do TSE (ETIR/TSE)	Instituição: Portaria 700/2021 Composição: Portaria 707/2021
Comitê Gestor de Crises (CGC)	Instituição: Resolução 17/2021 Composição: Portaria 683/2021
Comitê de Crises Cibernéticas (CCC)	Instituição: Portaria 117/2022 Composição: Portaria 121/2022
Comitê Gestor de Segurança da Informação (CGSI)	Instituição: Portaria 601/2021 Composição: Portaria 603/2021
Comitê Gestor de Tratamento e Proteção de Dados Pessoais (CGTPDP)	Instituição: Resolução 24/2022 Composição: Portaria 680/2022

PLANO DE AÇÃO

11 Anexos

FLUXOGRAMA INSTITUCIONAL DE NOTIFICAÇÃO À ANPD E ÀS(AOS) TITULARES EM CASO DE INCIDENTE ENVOLVENDO VIOLAÇÃO DE DADOS PESSOAIS



Orientações para preenchimento do RELATÓRIO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO – RISI*

Número:

Data:

Descrição: (identificar resumidamente o que ocorreu)

Período em que ocorreu o incidente:

Data de início: hora início:
data fim: hora fim:

Grau de Gravidade do Incidente
( ) Altíssimo ( ) Alto
( ) Médio ( ) Baixo

Tipo de impacto
( ) Confidencialidade
( ) Integridade
( ) Disponibilidade

Houve notificação ao CCC?
( ) Não
( ) Sim: Data: _____ hora:_____

Houve notificação ao CGC?
( ) Não
( ) Sim: Data: _____ hora:_____

Houve notificação ao Presidente do TRE/SE?
( ) Não
( ) Sim: Data: _____ hora:_____

Origem: (informar quem ou qual sistema acusou o incidente)

Detalhamento do Incidente: (informar a categoria do incidente. Descrever o que ocorreu, extensão e impactos do incidente, as causas do incidente, áreas envolvidas na investigação do incidente).

Tratamento do incidente: Descrever as ações executadas para contenção e/ou contorno do problema/incidente, equipes/pessoas envolvidas.

Análise e encerramento do incidente: Descrever se necessárias outras ações e recursos necessários para finalizar o tratamento do incidente e/ou para evitar que o incidente volte a ocorrer, informando, se possível, prazos e responsáveis para execução.
Lições aprendidas.
Considerar também a necessidade de: reversão da solução de controle; implementação de uma correção para a causa-raiz do problema. Implantação de um novo serviço/sistema. Substituição do ativo/sistema afetado. Revisão de procedimentos/processos.

Adaptação do Relatório de Incidente de Segurança da Informação – RISI produzido pelo TJ/MT.

RELATÓRIO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO – RISI

Número:

Data:

Descrição:

Período em que ocorreu o incidente:

Data de início: **hora início:**
data fim: **hora fim:**

Grau de Gravidade do Incidente
( ) Altíssimo **( ) Alto**
( ) Médio **( ) Baixo**

Tipo de impacto
( ) Confidencialidade
( ) Integridade
( ) Disponibilidade

Houve notificação ao CCC?
( ) Não
( ) Sim: Data: _____ hora:_____

Houve notificação ao CGC?
( ) Não
( ) Sim: Data: _____ hora:_____

Houve notificação ao Presidente do TRE/SE?
( ) Não
( ) Sim: Data: _____ hora:_____

Origem:

Detalhamento do Incidente:

Tratamento do incidente:

Análise e encerramento do incidente:

Sobre o Plano

Versão 3.0:

- Elaborado pela Diretoria-Geral (DG), por meio de seu Núcleo de Segurança da Informação e Proteção de Dados Pessoais (NSI), maio de 2025.

Tribunal Regional Eleitoral
de Sergipe