PODER JUDICIÁRIO
DO ESTADO DE RORAIMA
Secretaria de Tecnologia
da Informação

Plano de Resposta de Incidentes Cibernéticos

Fevereiro de 2024

TRIBUNAL DE JUSTIÇA DO ESTADO DE RORAIMA

(Composição)

Des. Jésus Rodrigues do Nascimento
Presidente

Des. Ricardo de Aguiar Oliveira
Vice- Presidente

Esdras Silva Pinto
Juiz Auxiliar da Presidência

Des. Mozarildo Monteiro Cavalcanti
Corregedor – Geral de Justiça

Des. Erick Cavalcanti Linhares Lima
Ouvidor – Geral de Justiça

Des. Cristóvão José Suter Correia da Silva
Diretor da Escola do Poder Judiciário de Roraima

Membros

Des. Mauro José do Nascimento Campello
Des. Almiro José Mello Padilha
Desa. Tânia Maria Brandão Vasconcelos
Desa. Elaine Cristina Bianchi
Des. Leonardo Pache de Faria Cupello

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Secretário de Tecnologia da Informação

Tiago Mendonça Lobo

Secretário Adjunto

Gabriel Vieira

Subsecretários

Boniek Amurim de Souza

Felippi Tuan da Silva Figueiredo

Paulo Adriano Brito Oliveira

Paulo Richard Perdiz Itapirema

Roodger Nathanael Schau Menezes Araújo de Sousa

Targino Carvalho Peixoto

Chefes de Setor

Akauã da Silva Carvalho

Carlos Vinicius da Silva Souza

Cinara da Conceição Araújo

George Wilson Lima Rodrigues

Jádila Costa Cotrim

Marco Aurélio Carvalho Feitosa

Marlon Daniel Brands

Vitor Rodrigues de Oliveira

Histórico de Versões

Versão	Data	Descrição	Autor
1.0	01/09/2023	Elaboração	Tatiana Brandão Carlos Roberto Dias
1.0	02/2024	Aprovação	Tiago Lobo – Secretário de TI CGSI

Sumário

1. INTRODUÇÃO

Vazamentos de Dados e ataques cibernéticos tornaram-se comuns e estão cada vez mais sofisticados. Diante disso, o Tribunal de Justiça do Estado de Roraima está consciente de que incidentes de segurança são passíveis de acontecer e que devem ser evitados com medidas de garantia e prevenção.

O Plano de Resposta a Incidentes Cibernéticos inclui estratégias, habilidades, pessoas, processos e as ferramentas para identificar, tratar e restaurar os serviços o mais rápido possível. Isso assegura que objetivos relevantes sejam atingidos, tais como conquistar a confiança dos servidores e dos cidadãos e cumprir com exigências apresentadas nos normativos de segurança da informação e privacidade de dados.

2. OBJETIVOS

O Plano de Respostas a Incidentes Cibernéticos tem como objetivo principal orientar quanto aos procedimentos de resposta para emergências de forma documentada e confiável, resguardando as evidências para prevenir novos incidentes e atender às exigências legais de comunicação e transparência.

3. TERMOS E DEFINIÇÕES:

Para facilitar o entendimento na compreensão deste Plano de Resposta a Incidentes Cibernéticos são adotadas as seguintes definições:

AGENTE DE TRATAMENTO: de acordo com a LGPD, são agentes de tratamento aqueles que podem ter alguma ação no tratamento de um incidente que coloque em risco a segurança dos dados pessoais.

ATIVIDADES CRÍTICAS: atividades que devem ser executadas para garantir a consecução dos produtos e serviços fundamentais do órgão, de maneira que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

ATIVO: qualquer coisa que represente valor para uma instituição, tal como a informação.

ATIVOS DE INFORMAÇÃO: meios de armazenamento, transmissão e processamento de informação, sistemas de informação e locais onde se encontram esses meios e as pessoas que a eles têm acesso.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: os arts. 55-A e seguintes da LGPD definem a Autoridade Nacional de Proteção de Dados (ANPD), entidade responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional, conforme as atribuições descritas no art. 55-J da LGPD e no Decreto nº 10.474, de 26 de agosto de 2020.

CONTINUIDADE DE SERVIÇOS DE TI - TECNOLOGIA DA INFORMAÇÃO: abordagem que garante a recuperação dos ativos de TI e a continuidade das atividades críticas ante um desastre, interrupção ou outro incidente maior.

CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Na administração pública federal, os órgãos exercem as funções típicas do controlador.

CRISE CIBERNÉTICA: crise decorrente de incidente em dispositivos, serviços e redes de computadores, que causa dano material ou de imagem, atrai a atenção do público e da mídia e foge ao controle direto da organização.

CRISE: evento ou série de eventos graves que apresentam propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas que eles geram e que apresentam implicações que afetam uma proporção considerável da organização, bem como de seus constituintes.

DADO PESSOAL: é toda informação relacionada a pessoa natural identificada ou identificável.

ETIR: Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética.

ENCARREGADO: pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

APF: Administração Pública Federal.

EVENTO: qualquer ocorrência observável num sistema ou rede da organização.

GERENCIAMENTO DE CRISE: decisões e atividades coordenadas que ocorrem na organização durante crise corporativa, incluindo crises cibernéticas.

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO: processo que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar riscos nos ativos de informação e para equilibrá-los com os custos operacionais e financeiros envolvidos.

INCIDENTE GRAVE: evento que tenha causado dano, colocado em risco ativos críticos de informação ou interrompido a execução de atividades críticas.

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

PROCEDIMENTO: conjunto de ações sequenciadas e ordenadas para o atingimento de um determinado fim.

PROCESSO DE GESTÃO DE INCIDENTES: atividades executadas para prevenir e tratar a ocorrência de evento adverso de segurança da informação, avaliar o impacto, determinar a resposta inicial e restabelecer a normalidade.

TRATAMENTO: qualquer operação ou conjunto de operações efetuadas sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização.

VAZAMENTO DE DADOS: qualquer quebra de sigilo ou vazamento de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado.

VIOLAÇÃO DE PRIVACIDADE: qualquer violação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita dos dados, bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento.

4. PAPÉIS E RESPONSABILIDADES

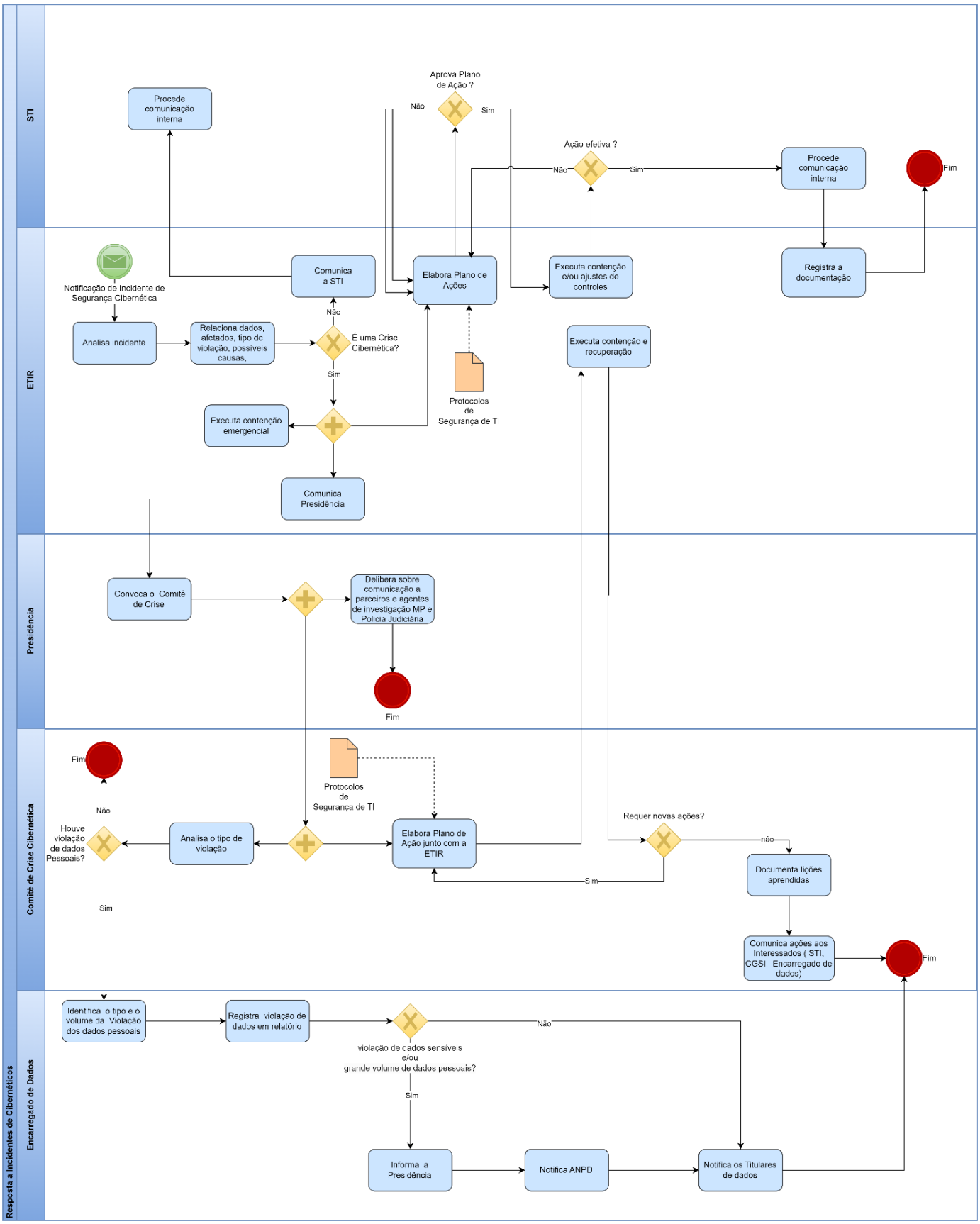
Identificação dos principais atores seus papéis e responsabilidades individuais e em grupo, pela proteção dos ativos:

- Comitê de Governança de Segurança da Informação - CGSI: responsável, dentre outras atribuições, por acompanhar os processos de segurança da informação (Portaria N.° 1256, de 28 de dezembro de 2022);
- Comitê Gestor de Proteção e Privacidade de Dados: responsável pela avaliação dos mecanismos de tratamento e proteção de dados existentes e pela proposição de ações voltadas ao seu aperfeiçoamento, com vistas ao cumprimento das disposições da Lei 13.709, de 14 de agosto de 2018. (Portaria N.° 547, de 16 de dezembro de 2020);
- Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR): grupo de servidores com responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação em ambiente tecnológico (Portaria N.° 961, de 29 de setembro de 2022 e Portaria N.° 962, de 29 de setembro de 2022);

- Encarregado de Dados - Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD). Deverá atuar em todas as questões relativas à privacidade e proteção de dados pessoais .

5. FLUXO DO PROCESSO DE RESPOSTA A INCIDENTES CIBERNÉTICOS

Resposta a Incidentes Cibernéticos



6. DESCRIÇÃO DO PROCESSO DE RESPOSTA A INCIDENTES CIBERNÉTICOS

ETIR

1. Início o Processo – Os incidentes de segurança cibernética devem ser registrados na Central de Serviços e serão tratados como Incidente Crítico e/ ou ser comunicados diretamente quando urgentes
2. Após receber a notificação, a ETIR analisa o incidente
3. Relaciona os dados afetados, tipo de violação e possíveis causas
4. É uma crise cibernética?
    - Se sim comunica a Presidência
    - Se não comunica a STI

STI

5. Procede com a comunicação interna

ETIR

6. Elabora Plano de Ação

STI

7. Aprova plano de Ação ?
    - Se sim

ETIR

8. Executa contenção e/ou ajustes de controles Ação efetiva?
    - Se sim
        - STI procede comunicação interna
        - ETIR registra e documenta as ações
        - FIM
    - Se não
        - Volta no item 6

Presidência

9. Convoca Comitê de Crise e paralelamente delibera sobre comunicação a parceiros e agentes de investigação MP e Polícia Judiciária:

Comitê de Crise

10. Paralelamente analisa o tipo de violação e Elabora Plano de ação JUnto com a ETIR
11. Analisa tipo de violação item 18
12. Elabora Plano de Ação junto com a Etir conforme o Protocolo de Segurança de TI
13. Etir executa contenção e recuperação
14. Requer novas ações?
    - Se sim volta ao item 11
    - Se não
15. Documentar lições aprendidas
16. Comunicar ações aos interessados (STI, CGSI, Encarregado de dados) – Fim do Processo

17. Verifica se houve violação de dados pessoais

a. Se sim– item 18

b. Se não - fim

Encarregado de dados

18. Identifica o Tipo e o volume da violação de dados pessoais

19 Registra a violação de dados no relatório

20 Houve violação de dados sensíveis e/ou um grande volume de dados pessoais?

- Se sim:
  - Informar à presidência;
  - Notificar a ANPD;
  - Notificar os titulares de dados.

Se não:

- Notificar os titulares de dados.

FIM

7. COMUNICAÇÃO:

As comunicações internas e que necessitem de publicidade através dos meios de comunicação oficiais serão realizadas pelo NUCRI (Núcleo de Comunicação e Relações Institucionais), com orientação do Comitê de Crise e aprovação da alta gestão, dessa forma dando publicidade e informando medidas de contenção e mitigação de seus efeitos.

O Comitê de crise decidirá sobre a comunicação dos incidentes a comunidade interna e a Presidência deliberará sobre comunicações a comunidade externa

Quando for necessário proceder com a comunicação à ANPD e ao titular de dados pessoais sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o Encarregado de Dados providenciará a comunicação dentro do prazo, mencionando no mínimo: a descrição da natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados; os riscos relacionados ao incidente; os motivos da demora, no caso da comunicação não ter sido imediata; e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

8. INDICADORES DOS PROCESSOS

Indicador	Descrição	Métrica
Número de Incidentes de Segurança Cibernética identificados.	Número total de incidentes registrados e classificados pela Central de Atendimento como incidente cibernético	Resultado: número absoluto Periodicidade: mensal Fonte: SUBCS
Número de Incidentes de Segurança Cibernética solucionados	Número total de incidentes registrados e classificados pela Central de Atendimento como incidente cibernético solucionado	Resultado: número absoluto Periodicidade: mensal Fonte: SUBCS

Número de Incidentes de Segurança Cibernética não solucionados	Número total de incidentes registrados e classificados pela Central de Atendimento como incidente cibernético não solucionado	Resultado: número absoluto Periodicidade: mensal Fonte: SUBCS
Tempo médio de respostas aos incidentes identificados	Tempo médio de atendimento dos incidentes identificados	Resultado: número absoluto em horas Periodicidade: mensal Fonte: SUBCS

9. PRESERVAÇÃO DAS EVIDÊNCIAS

Após ocorrido um incidente, caso seja necessário a preservação de evidências, será mantido todo material coletado durante o tratamento do incidente pelo período mínimo de 1 (um) ano, com base no art. 13 da Lei Federal nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

Tal procedimento é prática, antes de se iniciar as ações de restauração de operação do ambiente, a preservação de provas para identificação correta da causa raiz do incidente e, posteriormente, a realização da recuperação dos sistemas afetados.

10. CONCLUSÃO

Este plano descreve um processo para tratar os incidentes cibernéticos do TJRR, que venham ocasionar algum impacto aos ativos mantidos pela STI. Desta forma, o documento enaltece os passos necessários para uma resposta ágil e precisa, atendendo as exigências legais de comunicação e transparência para segurança da informação e privacidade.

Com enfoque consistente e efetivo para gerenciar os incidentes cibernéticos, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

Outrossim, pretende-se alcançar os objetivos de detecção de eventos de incidentes cibernéticos e seu tratamento, prover a identificação, avaliação e resposta adequada, minimizando os efeitos dos incidentes, tratando-os o mais rápido possível.

11. REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação. Rio de Janeiro: 2013;

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001: Tecnologia da informação - Técnicas de segurança - Sistema de gestão da segurança da informação - Requisitos. Rio de Janeiro: 2013;

BRASIL. **Lei N.° 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

TJRR. Portaria N.° 1248/2022 - http://diario.tjrr.jus.br/dpj/dpj-20221229.pdf

TJRR. Portaria N.° 1249/2022 - https://diario.tjrr.jus.br/dpj/dpj-20221227.pdf

TJRR. Portaria N.° 1250/2022 - https://diario.tjrr.jus.br/dpj/dpj-20221227.pdf

TJRR. Portaria N.° 961/2022 - http://diario.tjrr.jus.br/dpj/dpj-20220930.pdf

TJRR. Portaria N.° 962/2022 - http://diario.tjrr.jus.br/dpj/dpj-20220930.pdf

TJRR. Portaria N.° 1256/2022 - https://diario.tjrr.jus.br/dpj/dpj-20221229.pdf

TJRR. Portaria N.° 547/2020 - https://diario.tjrr.jus.br/dpj/dpj-20201217.pdf

TJRR. Resolução TJRR/TP N.° 70/2022 - https://diario.tjrr.jus.br/dpj/dpj-20221228.pdf