TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS

PLANO DE RESPOSTA A INCIDENTES DE CIBERSEGURANÇA E PROTEÇÃO DE DADOS

(Versão 2.0)

Comitê Multissetorial de Apoio à Governança (CMAG)

Tema: Segurança da Informação e Crises Cibernéticas

(Portaria nº 313, de 18 de março de 2025)

Histórico de Versões

Data	Versão	Descrição	Autor	Aprovada por
10/04/2023	1.0	Primeira versão do Plano de Respostas a Incidentes do TRE-AM	NSI/STI	Comitê Gestor de Segurança da Informação e Crise Cibernética
30/05/2025	2.0	Atualização e inclusão de procedimentos para migração o plano inicial para o Plano de Resposta a Incidentes de Cibersegurança e Proteção de Dados	NSIP/AGG/DG	Comitê Multissetorial de Apoio à Governança

SUMÁRIO

1. APRESENTAÇÃO

A Justiça Eleitoral, em consonância com sua missão institucional, presta serviços essenciais à sociedade brasileira, com a responsabilidade de garantir a lisura, a segurança e a legitimidade dos processos eleitorais. Para cumprir esse papel, administra e protege a maior base de dados pessoais da América Latina[1], utilizada para a identificação segura do eleitorado e para assegurar a integridade do voto.

O Tribunal Regional Eleitoral do Amazonas (TRE-AM), como parte integrante da Justiça Eleitoral, adota controles rigorosos de segurança da informação, alinhados às melhores práticas nacionais e internacionais, com o objetivo de prevenir, detectar e responder a incidentes que possam comprometer a confidencialidade, integridade ou disponibilidade das informações institucionais.

Diante do avanço contínuo das ameaças cibernéticas e do aumento expressivo da complexidade e frequência dos ataques digitais, torna-se indispensável a adoção de estratégias de resposta estruturadas, que garantam uma atuação coordenada e tempestiva frente a eventos de risco.

Nesse contexto, o Núcleo de Segurança da Informação e Privacidade (NSIP) elaborou o presente Plano de Resposta a Incidentes de Segurança Cibernética, instituído originalmente em 2023 e agora atualizado em sua versão 2.0, de 20 de maio de 2025. Este plano define as fases, responsabilidades, procedimentos técnicos e fluxos de comunicação a serem seguidos em caso de incidentes que afetem ativos de informação do TRE-AM.

A versão atual foi revista e ampliada considerando as diretrizes da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), as recomendações do Conselho Nacional de Justiça (CNJ), as orientações do Comitê de Segurança da Informação e de Crises Cibernéticas do Tribunal, e os avanços tecnológicos e normativos da área.

O documento também contempla, quando cabível, os procedimentos para comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e a outras instâncias superiores, conforme a natureza e gravidade do incidente.

Por fim, este plano integra o conjunto de instrumentos de governança, gestão de riscos e continuidade institucional, reafirmando o compromisso do TRE-AM com a proteção das informações sob sua guarda e com a prestação de serviços públicos confiáveis, transparentes e resilientes.

[1] Segundo o Tribunal Superior Eleitoral, o cadastro eleitoral brasileiro conta com dados biométricos e biográficos de mais de 150 milhões de eleitores, sendo considerado a maior base de dados civis da América Latina. Fonte: TSE – https://www.tse.jus.br/eleitor/biometria/cadastro-biometrico.

2. OBJETIVOS

2.1. Objetivo Geral

Fornecer uma estrutura formal e eficaz para a resposta a incidentes de segurança cibernética, priorizando ações coordenadas, estabelecendo protocolos de comunicação com as partes envolvidas e promovendo o gerenciamento eficiente dos impactos sobre os ativos de informação e os serviços institucionais.

2.2. Objetivos Específicos

Para o alcance do objetivo geral, este plano estabelece os seguintes objetivos específicos:

1. **Desenvolver um processo estruturado de resposta a incidentes**, com definição clara das etapas de identificação, investigação, contenção, erradicação, recuperação e lições aprendidas, alinhado a protocolos técnicos, normativos e às boas práticas nacionais e internacionais em segurança da informação.

2. **Estabelecer diretrizes de comunicação estratégica** com as partes envolvidas, internas e externas, de forma a garantir a transparência, o alinhamento institucional e a atuação coordenada durante o tratamento de incidentes. Isso inclui a identificação prévia de interlocutores-chave e a definição de responsabilidades nos fluxos de informação.

3. **Assegurar a integração entre o Plano de Resposta a Incidentes e o Plano de Gestão de Continuidade de Negócios (PGCN)**, de modo a preservar os serviços essenciais e garantir a manutenção das operações críticas da instituição em situações de crise.

4. **Incorporar práticas de gestão de riscos à resposta a incidentes**, por meio da identificação e avaliação dos riscos associados, da definição de estratégias de mitigação e da priorização de ativos conforme sua criticidade e exposição a ameaças cibernéticas.

5. **Promover a melhoria contínua do processo de segurança cibernética**, por meio da documentação sistemática dos incidentes, da análise de causas, da revisão de processos e do uso das lições aprendidas para fortalecer a capacidadeinstitucional de prevenção, resposta e adaptação às novas ameaças.

3. ESCOPO

Este Plano de Resposta a Incidentes de Cibersegurança aplica-se a todos os fluxos de trabalho, sistemas, serviços, informações e ativos tecnológicos sob responsabilidade do Tribunal Regional Eleitoral do Amazonas (TRE-AM), sejam eles físicos ou virtuais, internos ou externos à infraestrutura do Tribunal.

Estão abrangidos por este plano:

- Dispositivos físicos e virtuais, incluindo servidores, estações de trabalho, dispositivos móveis e equipamentos de rede;
- Ativos hospedados localmente, em nuvem ou acessados por meio de redes privadas virtuais (VPN);
- Ambientes corporativos, sistemas críticos eleitorais e plataformas de apoio administrativo;
- Usuários e gestores responsáveis pelos ativos, incluindo administradores técnicos, equipes de suporte, desenvolvedores e terceiros contratados.

Este escopo estende-se a incidentes que afetem direta ou indiretamente a confidencialidade, integridade, disponibilidade ou autenticidade das informações institucionais, incluindo dados pessoais tratados sob a custódia do Tribunal.

Considerando a dinâmica do cenário de ameaças cibernéticas, este plano também incorpora diretrizes para a adaptação contínua frente a novos vetores de ataque, como ransomware, phishing, engenharia social, acesso indevido e exploração de vulnerabilidades em cadeia.

O escopo está alinhado com os princípios e recomendações da norma ABNT NBR ISO/IEC 27035, que orienta a gestão de incidentes de segurança da informação, e deve ser revisado periodicamente para refletir mudanças tecnológicas, organizacionais e regulatórias.

4. FASES

4.1. Preparação

A fase de preparação visa garantir que o ambiente institucional esteja adequadamente estruturado para responder a incidentes cibernéticos de forma eficaz, com base em práticas proativas, definição de responsabilidades, capacitação de pessoas e disponibilidade de recursos técnicos e operacionais.

O fluxo operacional do processo de resposta a incidentes encontra-se representado no **Anexo I – Fluxograma do Processo de Resposta a Incidentes**, que organiza visualmente as etapas descritas neste capítulo.

4.1.1. Estabelecimento de políticas, processos e equipe de resposta.

O Tribunal Regional Eleitoral do Amazonas (TRE-AM) deve manter formalmente estabelecidas suas políticas de segurança da informação e de gestão de riscos, com a definição clara de papéis, fluxos e processos voltados à prevenção, detecção, resposta e recuperação diante de incidentes cibernéticos.

A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), instituída por ato normativo próprio, é responsável pela execução técnica e operacional das ações previstas neste plano, durante todas as fases do tratamento de incidentes.

Com o objetivo de garantir efetividade, coordenação e governança, o presente plano estabelece a articulação entre diferentes instâncias institucionais, organizadas em três níveis (Figura 1):

- **CAMADA OPERACIONAL** – Equipe técnica responsável pela identificação, análise, contenção, erradicação e recuperação dos sistemas afetados;
- **CAMADA TÁTICA** – Comitê de Segurança da Informação e de Crises Cibernéticas, que no Tribunal teve funções ao Comitê Multissetorial de Apoio à Governança (CMAG), responsável pela deliberação conjunta em situações críticas e apoio à tomada de decisão estratégica;
- **CAMADA ESTRATÉGICA** – Alta Administração, responsável pela validação de medidas institucionais, comunicação pública e articulação com órgãos superiores e externos.

Figura 1 – Níveis de Comando do Plano de Resposta a Incidentes de ibersegurança

Desta forma, foi instituido o **modelo de implementação da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR)** no âmbito do TRE/AM, pela Portaria TRE-AM nº 146/2021, atualizada pela Portaria TRE-AM nº 302/2025, composta pelo(a)s o(a)s titulares das unidades abaixo relacionadas ou seus respectivos substitutos legais, em caso de afastamentos daqueles:

- Coordenadoria de Infraestrutura de Tecnologia – COINF (Responsável);
- Seção de Banco de Dados - SEBD;
- Seção de Redes e Telecomunicação - SERET;
- Coordenadoria de Soluções Corporativas- CSCOR;
- Assessoria de Comunicação - ASCOM;
- Coordenadoria de Registros, Contas e Jurisprudência - CAJUR;
- Gabinete de Polícia Judicial - GPJ; e
- Coordenadoria de Auditoria Interna - COAUD.

Além da ETIR, pela Portaria TRE-AM nº 313/2025, que revogou a Portaria TRE-AM nº 945/2022, foi instituido o Comitê Multissetorial de Apoio à Governança (CMAG), com comtetência para formular propostas para o aperfeiçoamento das políticas de gestão e de governança voltadas à segurança da informação e crises cibernéticas, com o(a)s titulares:

- Diretoria Geral – DG;
- Secretaria de Administração, Orçamento e Finanças - SAO;
- Secretaria Judiciária - SJD;
- Secretaria de Tecnologia da Informação - STI;
- Secretaria de Gestão de Pessoas - SGP;
- Assessoria de Governança e Gestão - AGG;
- Coordenadoria de Supervisão e Orientação - CSORI;
- Coordenadoria de Auditoria Interna – COAUD.

As atribuições que excedam as competências da ETIR e CMAG deverão ser submetidas ao Conselho de Governança - CGo/TRE-AM, intituido pela Portaria TRE-AM nº 217/2025, composto por:

- O(A) Presidente do Tribunal;
- (A) Vice-Presidente e Corregedor(a) Regional Eleitoral;
- O(A) Diretor(a)-Geral;
- O(A) Juiz(a) Presidente do Comitê Gestor Regional e Orçamentário de Atenção

Prioritária ao Primeiro Grau de Jurisdição - CGRO.

Além disso, foram editados no ambito do Tribunal outros normativos voltados a prevenção de incidentes de segurança da informação, conformr listados na tabela abaixo:

NORMATIVO	ASSUNTO
PORTARIA N° 600, DE 11 DE SETEMBRO DE 2019	Instituir, no âmbito do TRE-AM, a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI,** que visa assegurar os princípios básicos da segurança da informação, a integralidade, a confidencialidade e a acessibilidade de informações.
PORTARIA Nº 499, DE 29 DE MAIO DE 2023	Regulamenta a Política de Segurança da Informação (PSI) no âmbito do TRE-AM, em conformidade com a Resolução nº 23.644, de 1 de julho de 2021, do Tribunal Superior Eleitoral.
PORTARIA Nº 458, DE 29 DE MAIO DE 2023	Institui a Norma Complementar de Segurança da Informação para Gestão de Ativos, em consonância com a Política de Segurança da Informação (PSI) da Justiça Eleitoral.
PORTARIA Nº 177, DE 6 DE MARÇO DE 2023	Institui a Norma de Gestão de Identidade e Controle de Acesso Físico e Lógico relativa à segurança da informação e comunicação no âmbito do TRE-AM.
PORTARIA Nº 368, DE 17 DE ABRIL DE 2023	Institui a Instrução Normativa para a Gestão de Riscos de Segurança da Informação no âmbito do TRE-AM.
PORTARIA Nº 367, DE 17 DE ABRIL DE 2023	Institui a Política de Uso Aceitável dos Recursos de Tecnologia da Informação, para disciplinar as diretrizes, direitos e responsabilidades dos usuários dos recursos de TI no âmbito do TRE-AM.
PORTARIA Nº 104, DE 6 DE MARÇO DE 2023	Institui a Norma Complementar da Política de Segurança da Informação para Gerenciamento de Backup e Restauração de Dados e o Plano de Gerenciamento de Backup e Restauração de Dados.
PORTARIA Nº 609, DE 29 DE JUNHO DE 2023	Institui a Instrução Normativa para Continuidade de Serviços Essenciais de TI no âmbito do TRE-AM.
PORTARIA Nº 198, DE 10 DE ABRIL DE 2023	Institui a Instrução Normativa para a Gestão de Incidentes de Segurança da Informação no âmbito do TRE-AM.
PORTARIA Nº 558, DE 19 DE JUNHO DE 2023	Institui a Norma Complementar de Gerenciamento de Vulnerabilidades do TRE-AM.
PORTARIA Nº 610, DE 29 DE JUNHO DE 2023	Institui a Instrução Normativa para Gestão e Monitoramento de Registro de Atividades (logs) no âmbito do TRE-AM.
PORTARIA Nº 457, DE 29 DE MAIO DE 2023	Institui a Norma Complementar da Política de Segurança da Informação para Desenvolvimento Seguro de Software, com intuito de estabelecer padrões de segurança no desenvolvimento de software no âmbito do TRE-AM.
PORTARIA Nº 701, DE 18 DE JULHO DE 2023	Institui a Instrução Normativa para o Uso de Recursos Criptográficos, no âmbito do TRE-AM.
PORTARIA Nº 105, DE 6 DE MARÇO DE 2023	Institui a Norma Complementar da Política de Segurança da Informação para Gestão do Acesso Remoto e VPN.

4.1.2. Inventário e classificação dos ativos

A manutenção de um inventário atualizado dos ativos de informação é fundamental para a priorização de ações durante a ocorrência de incidentes cibernéticos. Esses ativos devem ser classificados com base em critérios de criticidade, sensibilidade e impacto à instituição, permitindo o direcionamento adequado dos esforços de proteção, mitigação e resposta.

A ETIR realizará o inventário e a classificação dos ativos conforme modelo constante no **Anexo II – Modelo de Inventário de Ativos**, que deverá estar disponível para pronta consulta em caso de incidentes.

4.1.3. Treinamento e conscientização

A capacitação contínua dos públicos estratégicos é essencial para garantir a eficácia da resposta a incidentes de segurança cibernética no âmbito do Tribunal Regional Eleitoral do Amazonas (TRE-AM). Nesse sentido, deverão ser realizados treinamentos periódicos voltados aos membros da Equipe de Tratamento e Resposta a Incidentes (ETIR), gestores de sistemas e usuários-chave, com foco em:

- Boas práticas de segurança da informação;
- Procedimentos institucionais de resposta, recuperação e comunicação de incidentes;
- Simulações de cenários reais, com posterior avaliação crítica e registro de lições aprendidas.

Com base nas características das funções exercidas e nas exigências legais e organizacionais, estabelece-se a seguinte periodicidade mínima recomendada para os treinamentos formais:

Público-Alvo	Periodicidade Recomendada	Justificativa
Comitê Multissetorial de Apoio à Governança (CMAG)	A cada 2 anos	Alinhamento com o ciclo bienal de gestão institucional e necessidade de atualização estratégica das lideranças.

Público-Alvo	Periodicidade Recomendada	Justificativa
Equipe de Tratamento e Resposta a Incidentes (ETIR)	A cada 2 anos	Devido à composição multissetorial por titulares de unidades estratégicas, cuja designação acompanha os ciclos de gestão bienal do TRE-AM, exige-se o nivelamento contínuo dos procedimentos e responsabilidades técnicas e legais.
Demais Colaboradores (servidores, magistrados, terceirizados, estagiários, etc.)	A cada 2 anos, com meta mínima de 50% ao ano	Visando assegurar a atualização periódica de todos os públicos internos, estabelece-se que, a cada exercício, ao menos 50% dos colaboradores devem ser capacitados. Dessa forma, ao final de dois anos, 100% do público-alvo terá sido treinado, garantindo cobertura integral com impacto operacional equilibrado.

As ações de conscientização do público geral — incluindo servidores, magistrados, terceirizados, estagiários e residentes — serão promovidas de forma contínua, por meio de campanhas internas, materiais educativos, comunicados institucionais e trilhas de aprendizado, conforme previsto no Plano de Comunicação da Segurança da Informação.

Além disso, todo novo colaborador do TRE-AM deverá, no prazo de até três meses do início de suas atividades, cumprir os seguintes requisitos obrigatórios:

- Assinar o Termo de Compromisso de Manutenção de Sigilo;
- Concluir os cursos de conscientização em segurança da informação e proteção de dados, disponibilizados pelo Tribunal por meio da sua plataforma de Educação a Distância (EAD) ou por meio de solução contratada.

Como parte da estratégia de fortalecimento da cultura de segurança, o TRE-AM firmou o Contrato nº 38/2024, de 07/12/2024, com a empresa HSC Desenvolvimento e Serviços em Tecnologia da Informação LTDA, para a prestação de serviço na modalidade Software as a Service (SaaS), com acesso a plataforma especializada em capacitação e conscientização em segurança da informação voltada a usuários de TIC.

As diretrizes completas de capacitação e conscientização institucional sobre segurança da informação e proteção de dados pessoais estão formalizadas no **Anexo VII – Plano de Capacitação e Conscientização**, o qual detalha os objetivos, públicos-alvo, periodicidades recomendadas, responsabilidades e instrumentos utilizados no âmbito do TRE-AM.

Fica estabelecido que, a contar da publicação deste plano, deverá ser disponibilizado curso introdutório sobre a Lei Geral de Proteção de Dados Pessoais (LGPD), voltado a todos os

servidores e colaboradores do TRE-AM, incluindo terceirizados, estagiários e residentes. A conclusão do curso será obrigatória no prazo máximo de três meses a contar da data de sua disponibilização.

A coordenação e o acompanhamento das ações de capacitação em segurança da informação e proteção de dados pessoais são de responsabilidade do Núcleo de Segurança da Informação e Privacidade (NSIP), unidade vinculada à Assessoria de Governança e Gestão da Diretoria Geral (AGG/DG), em articulação com a Seção de Capacitação (SECAP), integrante da Coordenadoria de Educação e Desenvolvimento da Secretaria de Gestão de Pessoas (COEDE/SGP). As unidades devem colaborar ativamente com o NSIP na execução das ações planejadas.

Destaca-se, ainda, a importância da inclusão de cursos regulares e atualizados sobre segurança da informação e proteção de dados pessoais no Plano Anual de Capacitação (PAC) do TRE-AM, como forma de institucionalizar essas ações no planejamento estratégico de desenvolvimento de pessoas.

4.1.4. Simulações e testes de resposta.

A realização periódica de simulações e testes de resposta a incidentes de segurança cibernética é obrigatória, conforme previsto nas melhores práticas (ISO/IEC 27035) e diretrizes do CNJ. Esses exercícios visam validar a eficácia dos procedimentos estabelecidos neste plano, testar a prontidão das equipes envolvidas e identificar oportunidades de melhoria nos processos e controles adotados.

As simulações devem contemplar cenários realistas, incluindo falhas técnicas, ataques externos (como ransomware), vazamentos de dados ou indisponibilidade de sistemas críticos.

Periodicidade mínima recomendada:

- Simulação completa (com todos os atores): a cada 2 anos
- Testes parciais e workshops técnicos (com ETIR): pelo menos 1 vez ao ano

A responsabilidade pela coordenação e execução dos exercícios é do Núcleo de Segurança da Informação e Privacidade (NSIP), em articulação com a ETIR e os gestores das áreas críticas. Os registros dos testes devem ser mantidos em repositório próprio e integrados ao ciclo de melhoria contínua.

Os resultados e aprendizados deverão ser documentados em relatório específico, vinculados ao processo de gestão de riscos e à atualização dos playbooks operacionais.

4.1.5. Definição de canais e protocolos de comunicação.

A comunicação durante a gestão de um incidente de segurança é um componente crítico para garantir a articulação entre as áreas envolvidas, o cumprimento de obrigações legais e a preservação da imagem institucional.

Devem ser formalmente estabelecidos e atualizados os canais seguros de comunicação (ex.: e-mail oficial, linha telefônica dedicada, grupos de resposta segura, formulários eletrônicos e sistemas de atendimento). Os fluxos e níveis de escalonamento constam no Anexo V – Modelos de Comunicação e no Anexo III – Fluxograma do Processo de Resposta.

Requisitos mínimos:

- Listagem atualizada de contatos das unidades técnicas e estratégicas;
- Definição de mensagens padrão para resposta inicial e normalização;
- Plano de comunicação com o público interno e, se necessário, externo (ANPD, imprensa, sociedade).

A comunicação institucional deverá ser coordenada pela Assessoria de Comunicação (ASCOM) e seguir as diretrizes do NSIP e da Alta Administração.

4.1.6. Criação de documentação e manuais operacionais.

A documentação de apoio à resposta a incidentes deve ser elaborada, atualizada e testada regularmente. Isso inclui manuais operacionais, fluxogramas, checklists por fase, termos de notificação, modelos de relatório, entre outros instrumentos de apoio.

Essa documentação é fundamental para garantir a padronização das respostas, o treinamento dos envolvidos e a rastreabilidade das ações tomadas.

Documentos mínimos recomendados:

- Playbooks por tipo de incidente (ransomware, acesso indevido, vazamento etc.);
- Checklists operacionais por fase (Anexo VI);
- Modelos de relatório de incidente (Anexo V);
- Manuais de escalonamento e atribuições (Anexo IV).

O conjunto completo da documentação deve ser mantido acessível à ETIR em repositório oficial e atualizado pelo NSIP sempre que houver mudanças nos procedimentos ou após lições aprendidas de incidentes.

Nota: As ações descritas nos itens 4.1.4, 4.1.5 e 4.1.6 deverão ser amadurecidas pelas unidades técnicas e de governança e gestão, com vistas à sua consolidação e divulgação na próxima versão deste plano.

4.2. Identificação e Notificação.

A fase de Identificação e Notificação tem como objetivo reconhecer, validar e registrar eventos que possam configurar incidentes de segurança cibernética. É fundamental garantir a rápida detecção de anomalias e a comunicação tempestiva às partes responsáveis, a fim de permitir a adoção de medidas adequadas nas fases seguintes do processo de resposta.

4.2.1. Monitoramento Contínuo

O ambiente tecnológico institucional deve ser monitorado de forma contínua, utilizando ferramentas automatizadas e análises técnicas que possibilitem a identificação de atividades anômalas. Fontes de monitoramento incluem:

- Sistemas de detecção e prevenção de intrusão (IDS/IPS);
- Antivírus, firewalls e soluções de endpoint;
- Ferramentas de gerenciamento de eventos e informações de segurança (SIEM);
- Relatos de usuários encaminhados à Central de Serviços de TI.

O monitoramento permite detectar comportamentos suspeitos e eventos fora do padrão, como acessos não autorizados, variações incomuns no tráfego de rede ou falhas de segurança.

4.2.2. Detecção de Atividades Anômalas ou Eventos Suspeitos

Uma vez detectada uma anomalia, a equipe técnica deve registrar e analisar o evento para verificar se há indícios de incidente cibernético. Entre os sinais comuns, destacam-se:

- Tentativas de acesso indevido;
- Comportamento anormal de sistemas ou aplicações;
- Comunicação com endereços externos não reconhecidos;
- Modificações não autorizadas em arquivos ou configurações.

Todo evento suspeito deve ser registrado como "evento de segurança", até que se confirme ou descarte sua elevação à condição de incidente.

4.2.3. Coleta de Informações

Ao identificar um evento suspeito, devem ser reunidas informações que possibilitem sua análise e categorização adequada. As evidências podem incluir:

- Data e hora do ocorrido;
- Equipamentos e sistemas envolvidos;
- Logs de acesso e de eventos do sistema;
- Relatos de usuários;
- Dados de rede e alertas de segurança.

Essas informações devem ser preservadas conforme critérios técnicos e legais, possibilitando sua utilização na análise técnica e, se necessário, em investigações formais.

4.2.4. Correlação de Logs e Alertas

A equipe técnica deve correlacionar os dados coletados com informações de outras fontes, como:

- Registros de sistemas;
- Alertas de antivírus e EDRs;
- Relatórios de vulnerabilidades;
- Tráfego de rede.

O objetivo da correlação é identificar a origem do incidente, os ativos afetados, os vetores utilizados e os possíveis impactos, subsidiando as decisões nas fases seguintes.

4.2.5. Classificação e Categorização do Incidente

Confirmado o incidente, ele deve ser classificado com base em:

- Tipo do incidente (ex.: malware, vazamento de dados, negação de serviço);
- Impacto no serviço, na confidencialidade, integridade e disponibilidade da informação;
- Escopo (quantidade de ativos ou usuários afetados);
- Severidade (baixo, médio ou alto).

A categorização do incidente deverá considerar os critérios definidos na **Matriz de Classificação e Gravidade de Incidentes Cibernéticos,** conforme modelo estabelecido **no Anexo III**.

4.2.6. Notificação aos Responsáveis e Partes Interessadas

Uma vez classificado o incidente, as partes envolvidas devem ser notificadas de forma

imediata e segura. A notificação deve seguir os protocolos definidos e incluir:

- Membros da Equipe de Tratamento e Resposta a Incidentes (ETIR);
- Gestores das áreas afetadas;
- Diretoria ou autoridade superior, conforme o nível de gravidade;
- Encarregado de Dados Pessoais (em casos com dados pessoais);
- Órgãos superiores (como o TSE) e, quando aplicável, a ANPD.

A comunicação deve ser documentada e realizada com o devido cuidado para preservar o sigilo, a integridade da informação e a imagem institucional.

Os modelos de comunicação institucional, incluindo notificações internas e externas, estão disponibilizados no **Anexo IV – Modelos de Comunicação**, que deve ser utilizado conforme o tipo e a criticidade do incidente.

4.2.7. Registro do Incidente

Todos os incidentes confirmados devem ser formalmente registrados, contendo, inicialmente:

- Descrição detalhada do ocorrido;
- Responsável pela identificação;
- Horários de detecção e tratamento;
- Classificação atribuída;
- Medidas preliminares tomadas;
- Evidências técnicas associadas.

Esse registro deve compor a base histórica de incidentes e alimentar o processo de melhoria contínua.

O registro formal do incidente deverá ser consolidado no **Relatório de Incidente de Segurança Cibernética (Anexo V)**, conforme as diretrizes deste plano.

4.3. Contenção

A fase de contenção visa limitar os danos causados por um incidente de segurança cibernética, impedindo sua propagação, evitando o agravamento da situação e permitindo a análise adequada do cenário. As ações devem ser coordenadas, baseadas na classificação do incidente e na criticidade dos ativos envolvidos, e planejadas de forma a reduzir os riscos sem comprometer a continuidade dos serviços essenciais.

4.3.1. Ações imediatas para limitar a propagação do incidente

Ao identificar um incidente, devem ser adotadas ações imediatas e criteriosas para impedir sua disseminação. Tais medidas podem incluir o bloqueio de acessos indevidos, a revogação de credenciais comprometidas, a desativação de serviços temporariamente e o redirecionamento de tráfego de rede. A rapidez e precisão nessas ações são cruciais para minimizar os impactos iniciais.

4.3.2. Contenção de curto prazo (emergencial)

A contenção emergencial busca interromper a atividade maliciosa com a menor interferência possível nas operações críticas. Essa abordagem deve ser baseada em procedimentos previamente definidos e executada pela equipe de resposta (ETIR), com apoio técnico das áreas envolvidas. As medidas podem incluir:

- Isolamento de máquinas afetadas;
- Aplicação de regras temporárias de firewall;
- Suspensão de contas de usuários comprometidas;
- Restrição de privilégios de acesso.

4.3.3. Contenção de longo prazo (planejada)

Após a estabilização inicial, deve-se implementar medidas mais abrangentes e sustentáveis, que visem restaurar a operação segura dos sistemas e prevenir recorrências. Essas ações envolvem:

- Correção de vulnerabilidades exploradas;
- Atualizações de segurança em sistemas e softwares;
- Redefinição de senhas e políticas de autenticação;
- Reconfiguração de serviços afetados.

Essas medidas devem ser executadas com base em análise técnica e alinhadas com os objetivos de continuidade institucional.

4.3.4. Isolamento de sistemas ou redes afetadas

Quando necessário, os sistemas ou redes impactadas devem ser isolados de forma controlada, para impedir a propagação do incidente e proteger os demais ativos. O isolamento pode ocorrer por meio de:

- Desconexão da rede;
- Remoção física de equipamentos;

- Segmentação lógica de redes;
- Bloqueios por dispositivos de segurança (firewalls, NAC etc.).

Esse processo deve ser registrado e coordenado com a área de infraestrutura de TI, com o mínimo impacto operacional possível.

4.3.5. Preservação de evidências

Durante a contenção, é fundamental garantir a integridade das evidências do incidente, visando subsidiar investigações internas ou externas e possíveis ações administrativas ou legais. A preservação deve considerar:

- Coleta e armazenamento seguro de logs;
- Registro fotográfico ou por vídeo dos eventos e telas;
- Proteção contra sobrescrita de dados;
- Documentação detalhada das ações realizadas.

A ETIR deve seguir práticas forenses adequadas, mantendo a cadeia de custódia das evidências e respeitando os critérios legais e normativos aplicáveis.

4.4. Erradicação

A fase de erradicação tem como objetivo remover as causas do incidente, eliminando artefatos maliciosos, corrigindo vulnerabilidades exploradas e garantindo que o ambiente esteja livre de riscos residuais. Trata-se de uma etapa essencial para restaurar a segurança dos ativos e evitar a recorrência do problema. As ações devem ser conduzidas de forma cuidadosa, documentada e baseada em análise técnica da ocorrência.

4.4.1. Remoção de artefatos maliciosos

Após a contenção, a equipe de resposta deve identificar e eliminar todos os arquivos, códigos maliciosos, backdoors e outros componentes relacionados ao incidente. Essa atividade pode envolver:

- Varreduras com ferramentas antivírus e antimalware atualizadas;
- Exclusão de arquivos e registros suspeitos;
- Desinstalação de softwares não autorizados;
- Verificação da integridade de arquivos e sistemas afetados.

A remoção deve ser validada com o apoio de ferramentas técnicas confiáveis e por profissionais qualificados.

4.4.2. Correção de vulnerabilidades exploradas

É indispensável corrigir as falhas que possibilitaram a ocorrência do incidente. As ações incluem:

- Aplicação de patches e atualizações de segurança;
- Reconfiguração de serviços, aplicações e dispositivos;
- Reforço nas permissões de acesso e nas políticas de autenticação;
- Análise e ajustes de regras de firewall, IDS/IPS e outros mecanismos de defesa.
-

A correção deve ser monitorada para garantir sua eficácia e evitar novas explorações.

4.4.3. Validação da limpeza dos sistemas

Após a remoção e correção, deve-se validar se os sistemas estão livres de códigos maliciosos e funcionam corretamente. As ações podem incluir:

- Novas varreduras completas nos ativos restaurados;
- Avaliação da integridade dos sistemas por meio de comparações com imagens de referência;
- Monitoramento temporário de logs e tráfego para identificar comportamentos suspeitos.

Essa validação é crítica antes da liberação para a fase de recuperação, assegurando que os riscos tenham sido devidamente eliminados.

4.5. Recuperação

A fase de recuperação consiste na restauração dos sistemas, serviços e dados afetados, com o objetivo de restabelecer a normalidade das operações institucionais de forma segura e controlada. Essa etapa deve ser conduzida com cautela, observando procedimentos técnicos, validações de integridade e coordenação entre os setores envolvidos, garantindo que não haja reinfecção ou recorrência do incidente.

4.5.1. Restauração de sistemas e serviços afetados

A recuperação deve priorizar os serviços essenciais da instituição, conforme definido no Plano de Continuidade de Negócios. As ações incluem:

- Reinstalação de sistemas operacionais e softwares;
- Restauração de configurações padrão ou seguras;
- Reconexão de sistemas isolados após validação de segurança;
- Sincronização com ambientes de contingência, se aplicável.

A reativação dos sistemas deve ser feita de forma gradual e controlada, com o devido acompanhamento técnico.

4.5.2. Recuperação de dados a partir de backups confiáveis

Os dados comprometidos devem ser restaurados a partir de cópias de segurança verificadas. É fundamental:

- Validar a integridade e atualidade dos backups;
- Garantir que as cópias não estejam contaminadas;
- Registrar todo o processo de recuperação;
- Realizar testes de consistência após a restauração.

A recuperação deve respeitar as políticas institucionais de backup e os critérios de confidencialidade, integridade e disponibilidade das informações.

4.5.3. Monitoramento pós-incidente

Após a retomada das operações, os sistemas restaurados devem ser monitorados com atenção redobrada, a fim de:

- Detectar possíveis sinais de reinfecção ou falhas remanescentes;
- Verificar a estabilidade e desempenho dos serviços;
- Avaliar se as correções aplicadas foram eficazes;
- Analisar os acessos e eventos pós-recuperação.

Esse monitoramento é essencial para garantir que o ambiente esteja plenamente seguro e funcional.

4.5.4. Comunicação da normalização às partes interessadas

Concluída a recuperação, é necessário comunicar a normalização dos serviços às partes interessadas, observando os seguintes cuidados:

- Utilizar os canais oficiais e protocolos definidos na fase de preparação;
- Informar o escopo do incidente, os serviços afetados e as medidas adotadas;

- Compartilhar orientações com os usuários sobre eventuais mudanças nos procedimentos ou senhas;
- Manter registros de todas as comunicações realizadas.

A comunicação transparente e tempestiva reforça a confiança dos usuários e a imagem institucional.

Os modelos de comunicação institucional, incluindo notificações internas e externas, estão disponibilizados no **Anexo V – Modelos de Comunicação**, que deve ser utilizado conforme o tipo e a criticidade do incidente.

4.6. Lições Aprendidas

Esta fase consiste na análise retrospectiva do incidente, com o objetivo de compreender suas causas, avaliar a eficácia da resposta adotada e identificar oportunidades de melhoria nos processos, controles e capacidades institucionais. A sistematização das lições aprendidas fortalece a resiliência organizacional e reduz a probabilidade de reincidência.

Como apoio à execução padronizada das ações previstas neste plano, recomenda-se o uso do **Anexo VI – Checklist Operacional por Fase**, que resume as principais atividades e responsáveis por etapa.

4.6.1. Condução de reunião de revisão pós-incidente

Deve ser realizada uma reunião com os envolvidos na resposta ao incidente, preferencialmente em até 10 dias úteis após a sua resolução, com o intuito de:

- Apresentar um resumo cronológico do ocorrido;
- Compartilhar percepções sobre a atuação de cada área;
- Identificar pontos fortes e fragilidades no processo de resposta;
- Estimular a comunicação aberta e colaborativa entre os participantes.

Essa reunião deve ser coordenada pela ETIR e registrada formalmente.

4.6.2. Documentação e registro das lições aprendidas

As informações coletadas na reunião e durante o tratamento do incidente devem ser consolidadas em um relatório de lições aprendidas, contendo:

- Descrição do incidente;

- Análise das causas raiz;
- Medidas adotadas e sua efetividade;
- Pontos de melhoria identificados;
- Recomendações para prevenção de novos incidentes;
- Plano de ação para correção de deficiências.

Toda ocorrência de incidente de segurança cibernética deverá ser formalmente registrada por meio do **Relatório de Incidente de Segurança Cibernética**, conforme o **modelo disponibilizado no Anexo V** deste plano.

O relatório deve ser elaborado pela Equipe de Tratamento e Resposta a Incidentes (ETIR) ou por profissional por ela designado, em até **10 dias úteis** após a resolução do incidente. Seu conteúdo subsidiará o processo de aprendizagem institucional e a melhoria contínua dos controles.

Esse relatório deve ser armazenado em repositório apropriado e acessível à área de governança e à alta administração.

4.6.3. Atualização de procedimentos e treinamentos

Com base nas lições aprendidas, deve-se:

- Atualizar os documentos operacionais e manuais da resposta a incidentes;
- Revisar políticas e controles afetados;
- Planejar ações de capacitação voltadas às fragilidades identificadas;
- Incluir os novos aprendizados nos programas de conscientização em segurança.

A melhoria contínua deve ser incorporada como parte da cultura institucional.

5. CONSIDERAÇÕES FINAIS

A elaboração e a manutenção deste Plano de Resposta a Incidentes de Cibersegurançademonstram o compromisso institucional do Tribunal Regional Eleitoral do Amazonas com a proteção de seus ativos de informação, a continuidade dos serviços essenciais à sociedade e o cumprimento das normas legais e regulatórias, como a Lei Geral de Proteção de Dados Pessoais (LGPD).

A resposta a incidentes requer atuação coordenada, tempestiva e baseada em evidências,

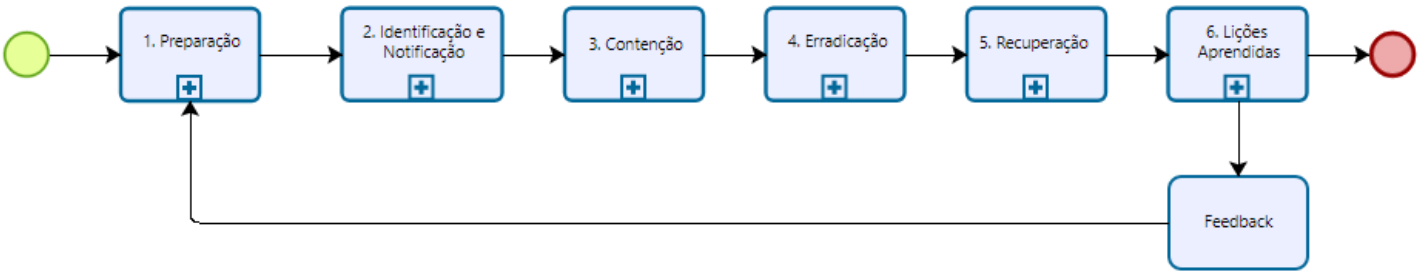
envolvendo diferentes áreas técnicas e de gestão, sob a condução da Equipe de Tratamento e Resposta a Incidentes (ETIR). O plano fornece a estrutura necessária para que essa resposta seja conduzida com eficiência, reduzindo impactos e promovendo a melhoria contínua da segurança da informação.

Ressalta-se a importância da adoção sistemática de treinamentos, simulações, revisões periódicas deste plano e atualização dos documentos de apoio, de forma a manter a prontidão organizacional diante de um cenário de ameaças cibernéticas em constante evolução.

Este documento deve ser compreendido como um instrumento dinâmico e complementar às demais políticas, planos e normativos de segurança da informação do TRE-AM.

Os anexos deste plano constituem instrumentos complementares e operacionais, devendo ser mantidos atualizados e integrados às rotinas do Núcleo de Segurança da Informação e Privacidade (NSIP).

ANEXO I – Fluxograma do Processo de Resposta a Incidentes



O fluxograma apresentado neste anexo ilustra, de forma sequencial, integrada e didática, as principais etapas operacionais do Processo de Resposta a Incidentes de Cibersegurança no âmbito do Tribunal Regional Eleitoral do Amazonas (TRE-AM), conforme definido nas fases detalhadas neste Plano.

As etapas refletem o modelo adotado pela Equipe de Tratamento e Resposta a Incidentes (ETIR), abrangendo desde a detecção e validação inicial do incidente, passando pela contenção, erradicação, recuperação e comunicação, até o encerramento do ciclo com a consolidação das lições aprendidas.

O fluxo permite visualizar as responsabilidades por camada (operacional, tática e estratégica), além de orientar as decisões e os registros necessários em cada fase, contribuindo para a coordenação eficiente da resposta e a preservação da continuidade dos serviços institucionais.

Nota: Os subprocessos e detalhamentos operacionais correspondentes a cada etapa estão disponíveis na página institucional do Núcleo de Segurança da Informação e Privacidade (NSIP), na intranet do TRE-AM, onde são mantidos atualizados em conformidade com os normativos vigentes.

ANEXO II - Modelo de Inventário de Ativos

Nº	Nome do Ativo	Tipo de Ativo	Localização / Responsável	Classificação de Criticidade[1]	Nível de Sensibilidade[2]	Impacto Potencial[3]	Medidas de Segurança Existentes	Observações
1	Servidor de Aplicações	Hardware	Data Center / STI	Alta	Alta	Alto	Backup diário, firewall	Sistema eleitoral
2	Sistema de Protocolo	Software	Nuvem / STI	Média	Média	Médio	Controle de acesso, logs	Acesso via VPN
3	Banco de Dados Eleitorais	Informação (Dados)	Ambiente restrito / STI	Alta	Alta	Muito Alto	Criptografia, controle físico	Dados pessoais e biométricos
4	E-mail Institucional	Serviço	Servidor Exchange / STI	Média	Baixa	Médio	Antivírus, autenticação MFA	Uso amplo
5	Estação de Trabalho	Hardware	Setor de Atendimento / Usuário	Baixa	Média	Baixo	Antivírus, senha complexa	Uso individual

Notas Explicativas:

1. Classificação de Criticidade:

Avaliação da importância do ativo para a continuidade das operações da instituição.

Categorias sugeridas: Baixa, Média, Alta.

2. Nível de Sensibilidade:

Define o grau de confidencialidade das informações processadas, armazenadas ou transmitidas.

Categorias sugeridas: Pública, Restrita, Confidencial, Alta Confidencialidade.

3. Impacto Potencial:

Consequências associadas à perda de confidencialidade, integridade ou disponibilidade do ativo.

Categorias sugeridas: Baixo, Médio, Alto, Muito Alto.

ANEXO III - Matriz de Classificação e Gravidade de Incidentes Cibernéticos

A matriz a seguir tem por finalidade auxiliar na categorização dos incidentes cibernéticos, considerando seu impacto e gravidade, e orientar as ações prioritárias da resposta. A classificação deve ser realizada pela ETIR, com apoio das áreas técnicas e envolvidas, sempre que possível.

1. Classificação do Tipo de Incidente

Tipo de Incidente	**Descrição**
Acesso não autorizado	Invasões, exploração de vulnerabilidades ou uso indevido de credenciais.
Vazamento de dados	Divulgação, acesso ou exposição indevida de dados pessoais ou sigilosos.
Interrupção de serviço (DoS/DDoS)	Queda ou degradação de sistemas ou serviços provocada intencionalmente.
Código malicioso (malware, ransomware)	Infecção de sistemas por software malicioso, com ou sem criptografia.
Engenharia social / phishing	Tentativas de enganar usuários para obter acesso ou dados sensíveis.
Uso indevido de recursos	Utilização dos ativos institucionais para fins não autorizados.
Outros	Incidentes que não se enquadrem nas categorias anteriores.

2. Avaliação do Impacto (Eixo Vertical)

Nível	**Descrição**
Crítico	Causa paralisação de serviços essenciais ou compromete dados sensíveis em grande escala.
Alto	Afeta significativamente serviços institucionais ou um número relevante de usuários/dados.
Moderado	Afeta serviços ou sistemas de forma localizada, com impacto limitado e reversível.
Baixo	Impacto mínimo, com pouca ou nenhuma interrupção de serviço e sem comprometimento de dados.

3. Avaliação da Probabilidade (Eixo Horizontal)

Nível	**Descrição**
Muito alta	Vulnerabilidade amplamente explorada, sem controle implementado.
Alta	Ameaça conhecida com poucos controles existentes.
Moderada	Alguns controles existem, mas ainda há riscos remanescentes.

Baixa	Ameaça pouco provável ou com controles eficazes implementados.

4. Matriz de Gravidade do Incidente

Impacto \ Probabilidade	**Baixa**	**Moderada**	**Alta**	**Muito Alta**
Crítico	Médio	Alto	Crítico	Crítico
Alto	Médio	Alto	Alto	Crítico
Moderado	Baixo	Médio	Alto	Alto
Baixo	Baixo	Baixo	Médio	Médio

5. Níveis de Gravidade e Ações Sugeridas

Nível de Gravidade	**Ações Prioritárias**
Crítico	Acionamento imediato da ETIR; comunicação à alta gestão e, se aplicável, às autoridades competentes.
Alto	Resposta urgente coordenada pela ETIR; notificação das áreas afetadas e contenção imediata.
Médio	Análise e resposta no prazo de até 24h; monitoramento contínuo e documentação das ações.
Baixo	Registro e tratamento conforme rotina; ações corretivas e preventivas, se necessário.

ANEXO IV – Modelos de Comunicação

Modelo 1 – Notificação Interna do Incidente

Assunto: **Notificação de Incidente de Segurança Cibernética**

Prezados,

Informamos que foi identificado um incidente de segurança cibernética no [sistema/serviço], ocorrido em [data/hora]. A Equipe de Tratamento e Resposta a Incidentes (ETIR) está conduzindo a análise e aplicando as medidas cabíveis.

Recomendamos atenção a comportamentos suspeitos e colaboração na coleta de informações.

Atenciosamente,

[Responsável/Coordenação ETIR]

Modelo 2 – Comunicação à Alta Administração

Assunto: **Relato de Incidente Crítico de Segurança**

Senhores(as),

Comunicamos a ocorrência de um incidente classificado como crítico, identificado em [data], que impactou [sistema/serviço afetado]. A equipe técnica está atuando nas fases de contenção e recuperação.

Detalhes preliminares:

- Tipo de incidente: [ex: ransomware]
- Impacto: [ex: indisponibilidade temporária]
- Medidas tomadas: [ex: isolamento de sistemas, acionamento de backup]

Atualizações serão fornecidas conforme a evolução da resposta.

Atenciosamente,

[Coordenador ETIR / STI]

Modelo 3 – Comunicação à ANPD (quando aplicável)

Assunto: **Comunicação de Incidente de Segurança com Dados Pessoais – Art. 48 da LGPD**

Prezados,

O Tribunal Regional Eleitoral do Amazonas comunica, nos termos do art. 48 da Lei Geral de Proteção de Dados Pessoais (LGPD), a ocorrência de incidente de segurança envolvendo dados pessoais.

Informações iniciais:

- Data do incidente: [dd/mm/aaaa]
- Natureza dos dados afetados: [ex: nome, CPF, e-mail]
- Medidas técnicas e administrativas adotadas: [ex: isolamento de sistemas, investigação da causa]
- Riscos envolvidos e medidas de mitigação: [descrever]

Permaneço à disposição para esclarecimentos.

Atenciosamente,
[Encarregado de Dados / Representante do TRE-AM]

ANEXO V – Modelo de Relatório de Incidente de Segurança Cibernética

Este modelo deve ser utilizado para registrar formalmente os incidentes de segurança cibernética ocorridos no âmbito do TRE-AM, visando subsidiar as ações de resposta, comunicação, lições aprendidas e melhoria contínua dos controles institucionais.

1. Identificação do Incidente

Data e hora da identificação: _____
Unidade/Setor responsável pela identificação: _____
Nome do responsável pela comunicação: _____

2. Descrição do Incidente

Resumo do ocorrido:
Sistemas e/ou ativos afetados:
Impacto percebido (disponibilidade, integridade, confidencialidade, imagem):

3. Classificação do Incidente

Tipo de incidente (Ex.: ransomware, vazamento, acesso indevido, etc.):
Classificação conforme matriz (Anexo III):
Nível de criticidade: ( ) Baixo ( ) Médio ( ) Alto ( ) Crítico

4. Ações Imediatas Executadas

Descrição das ações de contenção adotadas:
Equipes acionadas:
Sistemas isolados, backups verificados, etc.:

5. Investigação e Análise Técnica

Vetores de ataque identificados:
Origem provável do incidente:
Outras vulnerabilidades detectadas:
Ferramentas utilizadas na análise:

6. Erradicação e Recuperação

Medidas de correção aplicadas:
Dados restaurados com sucesso? ( ) Sim ( ) Não
Prazo estimado para normalização completa:

7. Comunicação

Partes internas notificadas:

Autoridades externas notificadas (ANPD, TSE, etc.):
Data e forma da comunicação:

8. Lições Aprendidas e Recomendações

Causa raiz identificada:
Controles que devem ser aprimorados:
Propostas de atualização de procedimentos, treinamentos ou sistemas:

9. Anexos

Capturas de tela, logs, documentos de análise, e-mails, etc.:

10. Assinaturas

Responsável pela ETIR: _____
Analista responsável pelo relatório: _____
Data: ____/____/_____

ANEXO VI – Checklist Operacional por Fase

- **FASE DE IDENTIFICAÇÃO**

  - ✓ - O incidente foi detectado e registrado?
  - ✓ - Há logs e evidências disponíveis?
  - ✓ - Foi atribuída uma prioridade inicial?

- **FASE DE ANÁLISE**

  - ✓ - A causa raiz foi identificada?
  - ✓ - Houve impacto em dados pessoais?
  - ✓ - O escopo foi delimitado?

- **FASE DE CONTENÇÃO**

  - ✓ - A propagação foi interrompida?
  - ✓ - Os acessos indevidos foram revogados?
  - ✓ - Sistemas comprometidos foram isolados?

- **FASE DE ERRADICAÇÃO**

  - ✓ - O código malicioso foi removido?
  - ✓ - As vulnerabilidades foram corrigidas?
  - ✓ - Atualizações e patches foram aplicados?

- **FASE DE RECUPERAÇÃO**

  - ✓ - Sistemas foram restaurados a partir de backups seguros?
  - ✓ - A operação normal foi retomada?
  - ✓ - Há monitoramento ativo após o incidente?

- **FASE DE LIÇÕES APRENDIDAS**

  - ✓ - Reunião de revisão foi realizada?
  - ✓ - Relatório de incidente foi concluído?
  - ✓ - Medidas preventivas foram propostas?

ANEXO VII – Plano de Capacitação e Conscientização em Segurança da Informação e Proteção de Dados Pessoais

Este plano estabelece as diretrizes para a capacitação e conscientização contínuas dos públicos estratégicos e gerais do Tribunal Regional Eleitoral do Amazonas (TRE-AM), com foco na segurança da informação e proteção de dados pessoais. Seu objetivo é promover uma cultura institucional de prevenção, resposta e conformidade, alinhada à LGPD, ISO/IEC 27001, ISO/IEC 27035 e às diretrizes do CNJ e da ANPD.

1. Objetivos

- Estabelecer periodicidades mínimas de treinamento por público.
- Garantir capacitação obrigatória dos novos colaboradores.
- Promover campanhas permanentes de conscientização.
- Manter trilhas de aprendizado atualizadas e acessíveis.
- Subsidiar o Plano de Resposta a Incidentes com equipes preparadas.

2. Públicos-Alvo e Periodicidade Recomendada

Público-Alvo	Periodicidade Recomendada	Justificativa
Comitê de Monitoramento da Área de Gestão (**CMAG**)	A cada 2 anos	Alinhamento com o ciclo bienal de gestão institucional e necessidade de atualização estratégica das lideranças.
Equipe de Tratamento e Resposta a Incidentes (**ETIR**)	A cada 2 anos	Devido à composição multissetorial por titulares de unidades estratégicas, cuja designação acompanha os ciclos de gestão bienal do TRE-AM, exige-se o nivelamento contínuo dos procedimentos e responsabilidades técnicas e legais.
Demais Colaboradores (servidores, magistrados, terceirizados, estagiários, etc.)	A cada 2 anos, com meta mínima de 50% ao ano	Visando assegurar a atualização periódica de todos os públicos internos, estabelece-se que, a cada exercício, ao menos 50% dos colaboradores devem ser capacitados. Dessa forma, ao final de dois anos, 100% do público-alvo terá sido treinado, garantindo cobertura integral com impacto operacional equilibrado.

3. Responsabilidades

A coordenação e o acompanhamento das ações de capacitação em segurança da informação e proteção de dados pessoais são de responsabilidade do Núcleo de Segurança da Informação e Privacidade (NSIP), unidade vinculada à Assessoria de

Governança e Gestão da Diretoria Geral (AGG/DG), em articulação com a Seção de Capacitação (SECAP), integrante da Coordenadoria de Educação e Desenvolvimento da Secretaria de Gestão de Pessoas (COEDE/SGP).

Destaca-se, ainda, a importância da inclusão de cursos regulares e atualizados sobre segurança da informação e proteção de dados pessoais no Plano Anual de Capacitação (PAC) do TRE-AM, como forma de institucionalizar essas ações no planejamento estratégico de desenvolvimento de pessoas. As unidades devem colaborar ativamente com o NSIP na execução das ações planejadas.

4. Capacitação Inicial Obrigatória

Todos os novos colaboradores do TRE-AM (magistrados, servidores, estagiários, terceirizados, residentes, etc.) deverão, no prazo de até dois meses do início das atividades, assinar o Termo de Compromisso de Manutenção de Sigilo e concluir os cursos obrigatórios de segurança da informação, disponibilizados na plataforma EAD do Tribunal ou por meio de solução contratada.

5. Contrato de Apoio à Capacitação (SaaS)

O TRE-AM firmou o Contrato nº 38/2024 com a empresa HSC Desenvolvimento e Serviços em Tecnologia da Informação LTDA, para fornecimento de conteúdo educacional na modalidade Software as a Service (SaaS), com foco em treinamentos de segurança da informação. A plataforma contratada será utilizada como ferramenta principal para a execução das trilhas de capacitação.