SUMÁRIO

1. OBJETIVO

Esta Política tem como objetivo preparar a DTI para lidar com a gestão de incidentes no ambiente de TI garantindo que as respostas sejam rápidas, organizadas e eficientes ao evento, minimizando suas consequências para todos os envolvidos no Tribunal. O nível das respostas dependerá do tipo e da complexidade do tratamento aplicado resguardando as evidências que possam auxiliar na prevenção de novos incidentes e no atendimento às diretrizes de comunicação e transparência.

2. ABRANGÊNCIA

A Política de Resposta a Incidentes de TI abrange todos os colaboradores, sejam eles próprios ou cedidos, pessoas e empresas públicas e privadas com os quais a DTI tenha ou possa vir a ter relacionamento direto ou indireto e os que atuam a serviço ou em nome dela, tais como terceiros, prestadores de serviços e fornecedores.

3. REFERÊNCIAS

Manual de Classificação e Tratamento de Informações Sigilosas;

Manual de Gerenciamento de Permissões de Acesso;

Norma ABNT ISO/IEC 20000:2018 para Gerenciamento de Serviços de TI;

Norma ABNT ISO/IEC 27001:2022 para Gestão da Segurança da Informação, Segurança Cibernética e Proteção à Privacidade;

Norma ABNT ISO/IEC 29134:2017 - Tecnologia da Informação - Técnicas de Segurança, Avaliação de Impacto de Privacidade;

Norma ABNT NBR ISO/IEC 27005:2023 - Gestão de Riscos de TI;

Norma ABNT NBR 14724: 2011 – Informação e Documentação – Apresentação Trabalhos Acadêmicos;

Plano Diretor de Tecnologia da Informação PDTI (2024-2026);

Política Corporativa de Segurança da Informação do TCE-AL;

Política de Controle de Acesso Lógico e Físico;

Política de Desenvolvimento Seguro na DTI do TCE-AL;

Política de Gestão de Ativos de TI na DTI do TCE-AL;

Política de Gestão de Riscos de TI;

Política de Governança de TI;

Política de Privacidade e Proteção de Dados Pessoais do TCE-AL;

Política de Respostas à Incidente de TI;

Política de Tecnologia da Informação do TCE-AL;

Procedimento Operacional de Gestão de Incidentes e Requisições;

Procedimento Operacional de Gestão de Mudanças;

Processo de Gestão e Análise de Vulnerabilidades de TI;

4. CONCEITOS E DEFINIÇÕES

Para fins de compreensão dos termos utilizados neste processo serão aplicados os seguintes conceitos e definições:

Ativos de TI: insumos tangíveis e intangíveis tais como: bases de dados, documentos, equipamentos, locais físicos, força de trabalho, sistemas, unidades organizacionais, processos corporativos etc.;

Ataque: evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

Base de Conhecimento: repositório de processos, instruções de trabalho contendo diretrizes orientativas na resposta e tratamento aos incidentes de TI;

Incidente: evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações;

Incidente de TI: qualquer interrupção não planejada ou redução da qualidade de um determinado serviço de TI;

Incidente de Segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

IP: protocolo da Internet, número utilizado para identificar um dispositivo de tecnologia da informação em uma rede ou Internet;

Log: processo de registro de eventos relevantes num sistema computacional;

Malware: é um termo genérico para qualquer tipo de software malicioso projetado para se infiltrar em dispositivos eletrônicos sem o devido conhecimento do usuário;

Sistemas: hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pela DTI para dar suporte na execução de suas atividades;

Spam: termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

Usuário: alguém que usa os serviços de TI no dia a dia, às vezes, informalmente referido como o cliente;

Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;

Worm: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

5. ATRIBUIÇÕES E RESPONSABILIDADES

Nesta política são estabelecidas funções e responsabilidades no sentido de assegurar confiabilidade nas respostas aos incidentes de TI, sempre prezando pela disponibilidade dos sistemas e processos internos da DTI, proteção dos ativos de tecnologia da informação e credibilidade nos serviços prestados, conforme seguem:

a) **Da Diretoria DTI -** tendo como base a assessoria técnica e especializada das equipes de resposta a incidentes e encarregado da privacidade e proteção de dados, a DTI atua nas seguintes funções:

- orientar e liderar as equipes técnicas e demais colaboradores no cumprimento dos requisitos descritos na Política de Resposta a Incidentes de TI;
- estabelecimento e aprimoramento contínuo de processos e sistemas para prevenção de incidentes de TI;
- estabelecimento e aprimoramento do programa de capacitação e avaliação da equipe em resposta a incidente de TI.

b) **Dos Usuários/Colaboradores de TI**: atuar proativamente no cumprimento dos requisitos descritos na Política de Resposta a Incidentes de TI e demais normativos internos da DTI, identificando situações que possam configurar incidentes e aplicando as ações necessárias nas devidas correções que assegurem a preservação do ambiente computacional, bem como, desenvolvendo sistemática de mitigação de riscos em conformidade com as diretrizes definas na **Política de Gestão de Riscos de TI**., implementado medidas de prevenção a exemplo dos backup regulares dentro dos requisitos da **Política de Gestão de Backup e Recuperação de Dados**, atualização de softwares mantendo as práticas definidas na **Política de Desenvolvimento Seguro**, prospecção, configuração e implantação de ferramentas de detecção de ameaças, firewalls, entre outras medidas também voltadas para cibersegurança.

c) **Do Encarregado de Proteção de Dados (Incidentes de Segurança da Informação):** atuar na resposta aos incidentes de segurança que envolvam dados pessoais ou que possam potencialmente envolvê-los.

d) **Da Equipe de Resposta aos Incidentes:** equipe especializada com acessos, habilidades, responsabilidades, treinamento e conhecimentos para responder aos mais variados tipos de incidentes de TI.

6. CICLO DE VIDA DE RESPOSTAS A INCIDENTES DE TI

O conceito de respostas a incidentes de TI é baseado em um conjunto de ações que podem ser tomadas para recuperar o sistema (ambiente de TI, software ou processo) do evento ocorrido. O ciclo de vida de resposta a incidentes costuma ser conduzido a partir das seguintes fases explicadas a seguir:

a) Preparação: consiste em todo o trabalho de preparação para a resposta ao incidente, incluindo a orientação contínua de todos os colaboradores, com base nas diretrizes definidas no **Procedimento Operacional de Gestão de Incidentes e Requisições**, sobre como proceder em situações de incidentes de TI e quem deve ser comunicado de forma imediata na DTI.

Nesta fase é recomendado que a equipe de resposta a incidentes tenha acesso a ferramentas que venham auxiliar e apoiar todo o tratamento, conforme seguem:

- lista com contatos de outros integrantes da equipe de resposta a incidentes, fornecedores e plantonistas de outras equipes, além de ferramentas para acionamento;
- ferramenta para registro dos incidentes, ações da equipe de tratamento de incidentes, upload de logs e evidências, e status do incidente;

- ferramenta que tenha a capacidade de rastrear incidentes recorrentes e novos, com repositório de informações referentes aos tratados anteriormente e suas respectivas evidências de tratamento;
- repositório de procedimentos (base de conhecimento) para resolução de incidentes;
- local para reunião de equipes durante a resolução de incidentes graves, chamada informalmente de "sala de guerra" ou "sala de crise";
- equipamentos de tecnologia como impressoras, estações de trabalho e sobressalentes para uso emergencial em caso de necessidade;
- ferramentas para recuperação de backup de sistemas e dados.

b) Deteção e Análise do Incidente: é a fase na qual os incidentes reportados ou identificados são analisados, estudados e categorizados. É a mais importante pois direciona os tipos de ações utilizadas na próxima fase. Para realizar a detecção de alguma anomalia no ambiente de TI podem ser utilizadas ferramentas de monitoramento que auxiliam na visualização do problema e na posterior análise.

Cabe ressaltar que para identificar uma ocorrência como incidente é importante conhecer o comportamento esperado da utilização dos sistemas e da rede, para então comparar com a situação suspeita. Após identificada alguma irregularidade na utilização dos recursos é realizada a categorização do incidente, tais como:

- "Negação de Serviço",
- "Código Malicioso",
- "Acesso não autorizado",
- "Uso Inapropriado" ou outra categoria.

Também é possível que um incidente possua mais de uma categoria, por exemplo: uma máquina infectada por um malware pode causar uma negação de serviço em uma outra máquina da mesma rede.

c) Contenção, Erradicação e Recuperação: nesta fase ações importantes são executadas, conforme segue:

- contenção do ambiente infectado para prevenir que mais danos sejam causados;
- eliminação, dentro do possível, da causa raiz do incidente para que o problema não volte a ocorrer no mesmo ambiente;
- recuperação do ambiente a fim de voltar à normalidade das atividades;
- revogação de acesso seguindo as práticas da **Política de Controle de Acesso Lógico e Físico**;
- bloqueio dos canais de comunicação comprometidos;
- monitoramento sistemático dos ativos seguinte as práticas da **Política de Gestão de Ativos de TI**;
- isolamento dos sistemas afetados e notificação às partes interessadas.

As três ações supracitadas, se executadas sistematicamente, contribui para o tratamento efetivo do problema causado pelo incidente. Cabe ressaltar que diferentes tipos de incidentes podem necessitar de métodos de tratamentos distintos, a exemplo dos descritos abaixo:

- "Negação de Serviço" – configurar os servidores para proteção contra excesso de requisições HTTP, bloquear IPs identificados como originários dessas requisições;
- "Código Malicioso (malware)" – isolar a(s) máquina(s) infectadas o mais breve possível, a fim de evitar novas infecções, realizar uma varredura na rede para verificar se existem outras máquinas comprometidas;
- "Acesso não autorizado" – detectar, monitorar e investigar as tentativas de acesso, principalmente dos usuários que possuem acesso a informações

sensíveis e/ou críticas e dos usuários que possuem privilégios no sistema, bem como, bloquear tentativas de acesso identificadas como ilegítimas.

d) Ações de melhoria após ocorrência de incidentes (lições aprendidas, documentação e comunicação): é fundamental que os mesmos erros não voltem a acontecer, ou seja, os incidentes precisam ser documentados, especificando quais foram as ações de respostas utilizadas para contorná-los, de forma a manter um histórico das ocorrências.

Uma sistemática de comunicação e documentação dos incidentes, detalhando as informações obtidas (quando foi identificado, qual sua natureza, danos ou potenciais danos causados, a extensão, a relevância e a repercussão desses danos, etc.), atores envolvidos, evidências, conclusões, decisões, autorizações e ações executadas, conduz a uma maior eficiência na proteção contra ameaças.

Da mesma forma e com base nas informações acima documentadas, torna-se essencial a realização de reuniões periódicas a título de lições aprendidas para revisar como o evento ocorreu, o que foi feito durante as tratativas e se as ações efetivamente surtiram efeito positivo.

Neste sentido e, contribuindo para a padronização das ações de respostas a incidentes de TI, destaca-se um modelo de lista de verificação com a sequência lógicas das ações voltadas ao tratamento dos incidentes. Ressalta-se que a aplicabilidade da mesma não é obrigatória, sendo responsabilidade da DTI optar pela adoção e/ou personalizá-la:

AÇÕES DE RESPOSTA A INCIDENTES DE TI	
Preparação	
1	Definir a equipe técnica que irá atuar nas ações
2	Selecionar ferramentas de rastreamento e registro e tratamento de incidentes

3	Consultar procedimentos que orientam o tratamento de incidentes
Deteção e Análise	
4	Determinar se ocorreu um incidente
4.1	Analisar os antecessores
4.2	Buscar por informações correlatas
4.3	Realizar pesquisa do incidente (via mecanismos de busca e bases de conhecimento)
4.4	Documentar, investigar e reunir de evidências assim que a equipe identificar a ocorrência do incidente
5	Priorizar o tratamento com base em sua relevância (impacto de negócio, impacto de informação e recuperabilidade)
6	Comunicar o incidente às equipes internas envolvidas e, quando aplicável, aos externos
Contenção, Erradicação e Recuperação	
7	Adquirir, preservar, proteger e documentar as evidências
8	Conter o incidente
9	Erradicar o incidente
9.1	Identificar e mitigar todas as vulnerabilidades
9.2	Remover malware e outros componentes
9.3	Se mais sistemas/processos afetados forem descobertos, repetir as etapas de detecção e análise (4.1, 4.2), para então conter (8) e erradicar (9) o incidente
10	Recuperar-se do incidente
10.1	Retornar os sistemas afetados ao estado operacional
10.2	Confirmar se os sistemas afetados estão funcionando normalmente

10.3	Se necessário, implementar monitoração adicional para encontrar futuras atividades relacionadas
Atividades Pós-Incidente	
11	Elaborar relatório de acompanhamento
12	Realizar reunião de lições aprendidas (tal reunião é obrigatória para incidentes graves e opcional para os demais incidentes)
13	Realizar análise pós-incidente para prevenir sua recorrência por meio da identificação de lições aprendidas e ações de acompanhamento

7. PARTES INTERESSADAS ENVOLVIDAS NAS RESPOSTAS AOS INCIDENTES

Nas atividades de resposta aos incidentes de TI normalmente é requerida a formação de uma equipe técnica multidisciplinar com experiência em plataformas e aplicativos tecnológicos. Contudo, também deve haver especialistas em infraestrutura, redes, banco de dados, desenvolvimento de softwares e pessoas com especialização em segurança da informação.

Na área de Governança e Gestão de TI e, em conformidade com as diretrizes definidas na **Política de Governança de TI**, a equipe deve incluir, dentro do possível, um gestor/coordenador de incidentes. No entanto, ele deve ser capaz de fazer com que os membros da equipe com diferentes perspectivas, agendas e objetivos trabalhem em direção a metas comuns. Não obstante, também deve haver um responsável na equipe encarregado de lidar com a comunicação de e para a Diretoria DTI. Contudo, essa função requer uma pessoa com habilidade em traduzir requisitos técnicos para o idioma que facilite a tomada de decisões.

Na ausência da possibilidade de nominação dos representantes acima citados, as equipes envolvidas na gestão dos serviços de tecnologia da informação na DTI devem assegurar que os incidentes identificados sejam tratados seguindo as diretrizes das políticas e procedimentos referenciados no **Item 3. REFERÊNCIAS**.

8. DOS TIPOS GERAIS DE INCIDENTES EM TI

Na área de TI incidentes são classificados e categorizados como uma interrupção não prevista ou ainda uma queda da qualidade de um serviço prestado. Visando garantir a continuidade de suas operações e a resposta ágil a possíveis gargalos que surgem na gestão dos serviços, a DTI têm atuado proatividade em garantir o bom funcionamento das ferramentas e ativos, resolvendo, de maneira eficiente, as possíveis falhas que ocorrerem, em conformidade com as diretrizes abordadas no **Processo de Gestão e Análise de Vulnerabilidades de TI**.

Neste sentido listamos abaixo alguns tipos mais comuns de incidentes em ambientes de TI que podem se manifestar de diversas formas e em diferentes níveis de gravidade:

8.1. SEGURANÇA DA INFORMAÇÃO

Os tipos de incidentes de segurança da informação mais frequentes são:

a) **Violação de dados:** intrusão não autorizada em um sistema ou rede que resulte no acesso não autorizado, roubo ou comprometimento de informações confidenciais, como dados pessoais;

b) **Ataques de malware:** software malicioso, como vírus, worms, ransomware ou spyware, que infecta os sistemas, causando interrupção das operações, perda de dados ou outros danos;

c) **Ataques de negação de serviço (DDoS):** resulta em uma sobrecarga dos recursos de rede ou sistema, levando à interrupção dos serviços;

d) **Acesso não autorizado:** indivíduo com acesso não autorizado a sistemas, redes ou contas de usuário tentando acessar informações confidenciais ou áreas restritas;

e) **Phishing e engenharia social:** tentativa de enganar os usuários para que divulguem informações confidenciais, como senhas, através de e-mails fraudulentos e sites falsos;

f) **Comportamento incomum do sistema:** sistema apresentando um comportamento incomum, como uma lentidão excessiva ou falhas frequentes;

g) **Mensagens de erro incomuns:** sistema emitindo mensagens de erro incomuns, como erros de segurança ou de privacidade;

h) **Alertas de segurança:** alertas ou notificações do software antivírus ou firewall;

i) **Mudanças em dados ou arquivos:** mudanças inesperadas em dados ou arquivos, como a exclusão de informações importantes ou a adição de arquivos suspeitos;

j) **Atividade de rede suspeita:** tráfego de rede incomum ou suspeito, como uma grande quantidade de dados sendo transferidos para fora da sua rede;

k) **Roubo ou Perda de Dispositivos Físicos:** quando o usuário e/ou colaborador de TI perde ou é furtado o seu notebook corporativo onde nele contém informações confidenciais expondo dados importantes.

8.2. INFRAESTRUTURA DE TI

Os tipos de incidentes em ambiente de infraestrutura mais frequentes são:

a) **Segmentação das conexões WI-FI**: ausência ou falhas na segmentação das conexões de rede resulta em fragilidades e acesso não autorizado aos ativos estratégicos de TI;

b) **Gestão das contas de usuários**: permissões e gerenciamento contas descumprindo os critérios do **Manual de Gerenciamento de Permissões de Acesso**;

c) **Logs de uso da rede**: ausência ou falhas em configurar os dispositivos para registro dos logs de utilização, bem como, falta da realização de testes por amostragem dos arquivos de logs objetivando checar as irregularidades no ambiente de TI;

d) **Configuração do DNS**: mudanças no DNS muitas vezes não são identificadas pelo usuário e podem causar um grande impacto na confiabilidade da conexão e no dia a dia das atividades;

e) **Falhas em serviço de e-mail:** ausência ou falhas nas regras de configuração para detecção de vírus e derivados, recebimento de SPAMs, análise de conteúdo do email e anexos com tamanhos excessivos.

8.3. DESENVOLVIMENTO E SUSTENTAÇÃO DE APLICAÇÕES

Os tipos de incidentes em desenvolvimento e sustentação de aplicações mais frequentes são:

a) **Desconfiguração/erro de software**: configurações incompletas ou incorretas para integração entre diferentes sistemas, aplicação de regras concorrentes, etc.;

b) **Método de desenvolvimento e codificação:** ausência e falhas no rastreamento de códigos de erro durante a compilação de software;

c) **Revisão de código**: ausência ou falhas na definição de modelos de ameaças durante a definição do desenho e construção do software, bem como, testes e revisões de código com uso de ferramentas automatizadas;

d) **Erros de Confiabilidade e Disponibilidade**: quando a aplicação que frequentemente se desconecta ou fica fora do ar causando perda de dados ou interrupção do serviço para os usuários;

e) **Incidentes de Deploy (Implantação):** deploy malsucedido que resulta em indisponibilidade temporária do sistema ou em erros de regressão, onde funcionalidades anteriormente estáveis deixam de funcionar após uma atualização. A DTI adotada uma postura bem firme e cautelosa em relação a algumas migrações de versões de banco de dados para que não afetem funcionalidades dos sistemas que antes já estavam estáveis, a exemplo de migrações no sistema AUDORA.

8.4. BANCO DE DADOS

Os tipos de incidentes em banco de dados mais frequentes são:

a) **Configurações incorretas em banco de dados**: ausência ou falhas nas configurações de credenciais padrão para acesso, criptografia de dados e critérios para backup e recuperação de dados;

b) **Inventário inconsistente das bases de dados**: ausência ou falhas nos mecanismos de rastreamento e inventário de dados, bem como, definição das regras de classes de dados por nível criticidade.

9. BOAS PRÁTICAS DE PREVENÇÃO A INCIDENTES DE TI

A equipe especializada e dedicada às ações de resposta a incidentes de TI pode ter capacidade de identificar problemas dos quais a Diretoria não está ciente. Logo, possui potencial de desempenhar um importante papel na identificação de vulnerabilidades e avaliação de riscos.

A seguir, são apresentadas algumas boas práticas para a prevenção e proteção de todo ambiente de TI (redes, sistemas e aplicativos):

a) Avaliação de riscos: realizar avaliações de riscos de forma periódica, em conformidade com as diretrizes estabelecidas na **Política de Gestão de Riscos de TI**, visando levantar o cenário de exposição a ameaças e vulnerabilidades;

b) Segurança de processamento e transmissão de dados (host): o ambiente computacional deve ser protegido de forma apropriada, usando configurações adequadas. Além disso, é essencial manter as regras de privilégios mínimos, conforme diretrizes definidas no **Manual de Gerenciamento de Permissões de Acesso**, concedendo aos usuários somente os perfis necessários para execução de tarefas previamente autorizadas. É importante manter habilitadas as funções de auditoria para que os logs registrem eventos considerados significativos à segurança;

c) Segurança de rede: estabelecer e configurar o perímetro de segurança de rede a fim de negar quaisquer tentativas de acessos não permitidas;

d) Prevenção contra malware: instalar software de detecção, bloqueio e remoção de malwares em todos os hosts e serviços de e-mail do Tribunal;

e) Conscientização e capacitação de usuários: manter os usuários cientes das principais ameaças do mundo digital e das **Políticas de Tecnologia da Informação, Segurança da Informação**, **Controle de Acesso Lógico e Físico**, no que tange ao uso adequado de equipamentos, redes de Internet e Intranet, sistemas e acesso adequado as instalações físicas;

f) Gestão de Vulnerabilidades: é considerado uma prática de prevenção o ato de resolver e mitigar vulnerabilidades existentes nos sistemas o que dificulta a ação maliciosa de usuários, visto que há diminuição de brechas a serem exploradas conforme diretrizes definidas no **Processo de Gestão e Análise de Vulnerabilidades de TI**.

10. PENALIDADES

Esta Política de Resposta a Incidentes de TI, juntamente com os documentos descritos no **Item 3. REFERÊNCIAS,** compõem o conjunto de normativos da DTI os quais direcionam atitudes e comportamentos exigidos aos colaboradores no tocante à proteção dos ativos de TI devendo ser rigorosamente observados.

O descumprimento desta Política será considerado infração disciplinar e poderá acarretar a aplicação de sanções previstas nos normativos da DTI e disposições contratuais.

11. IMPLEMENTAÇÃO E ATUALIZAÇÃO

Espera-se que a política de resposta a incidentes de TI seja revisada continuamente e, em intervalos planejados, seguindo as regras dos normativos internos da DTI, não se restringindo apenas a estes. Caso uma parte interessada identifique uma melhoria ela deve ser desenvolvida e implantada dentro do possível e onde for aplicável.

A DTI deve assegurar que as revisões desta política sejam amplamente divulgadas com objetivo de promover a sua observância e cumprimento. Ademais, recursos humanos e tecnológicos devem ser disponibilizados para garantir a execução das regras nela contidos.

12. CONTROLE DE DOCUMENTOS E REGISTRO

Código	Responsável pela guarda	Permissão de acesso	Meio de arquivo	Indexação	Local de arquivo	Tempo de Arquivo	Forma de Disposição
PL-DTI-008	DTI	Restrito ao setor	Eletrônico	Alfabética	Base de Conhecimento	Permanente	Não aplicável

13. ANEXOS

Não se aplica.

14. HISTÓRICO DAS REVISÕES

Revisão	Descrição das alterações	Data
00	Emissão Inicial	26/07/2024
01	Ajustes em todo o texto de acordo com as anotações dos Líderes de Serviços e Governança Coordenação.	24/10/2024

Elaborado por: **Equipe de Processos e Projetos**	Analisado e Aprovado por: **Diretoria DTI**
Data da Elaboração: 26/07/2024	Data da Aprovação: 21/11/2024