ANEXO VII
NORMA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
PORTARIA-TJ nº 47312022	
PORTARIA-CNJ nº 1622021	ANEXOS

Versionamento:

Versão:	2.0
Data:	22/04/2024
Criada por:	Grupo de Trabalho Técnico (GTT) do CGSI
Aprovada por:	Comitê de Governança de Segurança da Informação (CGSI)
Aprovada em:	22/04/2024

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações
14/08/2023	1.0		
22/04/2024	2.0	GTT do CGSI	Conforme arquivo de registro de alterações (changelog).

1. INTRODUÇÃO

A Norma de Gestão de Incidentes de Segurança da Informação complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para administrar eventos ou incidentes de segurança que estejam impactando ou possam vir a impactar ativos e/ou recursos de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário do Estado do Maranhão (PJMA).

Para fins desta norma aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I - Glossário da PSI.

2. OBJETIVOS

Assegurar uma resposta rápida, eficiente, eficaz e ordenada aos incidentes de segurança da informação, incluindo a comunicação interna e externa sobre os eventos ocorridos e procedimentos de continuidade do serviço prestado.

Assegurar a efetiva categorização e priorização de eventos de segurança da informação.

Reduzir a probabilidade ou as consequências de incidentes.

Assegurar uma gestão consistente e eficaz das evidências relacionadas a incidentes de segurança da informação para fins de ações disciplinares e legais.

Realizar práticas e simulações de incidentes para efetivar o aprimoramento contínuo do processo de gestão de incidentes.

Utilizar tecnologia que favoreça o conhecimento de ameaças cibernéticas em redes de informação, especialmente em fóruns e comunidades virtuais, inclusive de iniciativa privada.

Estabelecer troca de informações e boas práticas com outros membros do poder público em geral e do setor privado de forma colaborativa.

3. DIRETRIZES

As violações ou tentativas de violação da Política de Segurança da Informação, de normas ou de controles de segurança da informação, intencionais ou não, poderão ser consideradas incidentes de segurança.

Os incidentes de segurança poderão ser identificados por processos de monitoramento da Diretoria de Informática e Automação (DIA) ou por usuários(as) que observem fragilidades, anomalias ou violações que coloquem a segurança do PJMA em risco.

A lista a seguir exemplifica, mas não esgota os possíveis incidentes de segurança da informação tratados nesta política:

I - qualquer evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, bem como estruturas físicas e lógicas, que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente do PJMA;

II - indisponibilidade do ambiente tecnológico em virtude de ataque de código malicioso interno e/ou externo;

III - vazamento de dados, tais como: informações restritas e/ou confidenciais, dados pessoais, propriedade intelectual, dentre outros;

IV - tentativas internas ou externas de ganhar acesso não autorizado a sistemas, a dados ou até mesmo de comprometer o ambiente de TIC;

V - ato de violar, explícita ou implicitamente, diretrizes da Política de Segurança da Informação e normativos correlatos;

VI - uso ou acesso não autorizado a um sistema, a rede de dados corporativa ou a ativos críticos de TIC;

VII - modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio da Diretoria de Informática e Automação (DIA);

VIII - vazamentos e/ou compartilhamento de senhas, intencionais ou não.

O conteúdo da notificação precisará ser claro, em formato simples e incluir todas as informações necessárias para a rápida e correta identificação e solução do problema.

Não serão considerados incidentes de segurança da informação:

I - eventos acidentais não intencionais;

II - eventos não maliciosos;

III - comportamento inadequado de usuários(as) que não resulte em violação de políticas ou comprometimento da segurança da informação;

IV - eventos relacionados a falhas de hardware ou software que não comprometam a segurança da informação;

V - problemas de rede não relacionados a ataques ou violações de segurança;

VI - incidentes que não envolvam ativos de TIC, como incidentes puramente físicos ou operacionais;

VII - eventos relacionados a situações de emergência ou desastres naturais que não tenham impacto direto na segurança da informação.

4. PROTOCOLO DE PREVENÇÃO DE INCIDENTES CIBERNÉTICOS

O protocolo de prevenção de incidentes cibernéticos do PJMA é um processo constante de ações proativas com o objetivo de reduzir a probabilidade de ataques cibernéticos bem-sucedidos. Entre essas ações, enfatizam-se as de definição e de implementação de controles de segurança, de gerenciamento de vulnerabilidades, bem como de conscientização e de capacitação.

4.1 Definição e Implementação de Controles de Segurança Preventivos

Os controles de segurança preventivos constituem-se em: organizacionais, de pessoas, físicos e tecnológicos.

Os controles organizacionais serão fundamentais para garantir a contínua adequação, suficiência e efetividade da direção na gestão e suporte à segurança da informação conforme os requisitos comerciais, legais, estatutários, regulamentares e contratuais. Dentre os principais controles, destacam-se a Política de Segurança da Informação (PSI) e as normas específicas por tema, as quais deverão ser definidas, aprovadas, publicadas, comunicadas e revisadas periodicamente pela direção.

Os controles de pessoas deverão abranger, por exemplo, verificações de antecedentes de todos os candidatos aprovados por meio de concurso público antes de serem admitidos e de forma contínua, conforme exigido pelas leis e regulamentos aplicáveis. Esses controles deverão ser proporcionais aos requisitos do cargo, à classificação das informações e aos riscos percebidos.

Os controles físicos terão como objetivo prevenir o acesso não autorizado a áreas restritas e proteger os ativos de TIC que contenham informações críticas ou sensíveis contra danos e interferências. Entre os principais controles físicos estão a definição dos perímetros de segurança física, monitoramento, proteção contra ameaças físicas e ambientais, bem como a proteção e localização de equipamentos.

Os controles tecnológicos serão essenciais para reduzir vulnerabilidades em ativos de TIC, sistemas e softwares. Incluem os dispositivos finais dos(as) usuários(as), restrição de acesso, autenticação segura, proteção contra códigos maliciosos, cópias de segurança das informações (backup) e monitoramento de eventos, segurança de redes e criptografia.

4.2 Gerenciamento de Vulnerabilidades

O gerenciamento de vulnerabilidades é um processo contínuo e proativo que visa controlar riscos, realizar monitoramento, corrigir falhas e proteger contra ataques cibernéticos e violações de dados. O objetivo principal deste processo é reduzir a exposição geral do PJMA a riscos, mitigando o maior número possível de vulnerabilidades.

Para tanto, deverão ser observadas as diretrizes definidas no ANEXO XI - Norma de Gestão de Vulnerabilidades Técnicas da Política de Segurança da Informação.

4.3 Conscientização e Capacitação (Educação Cibernética)

Visando aprimorar a educação em segurança da informação, é fundamental implementar ações de conscientização e de capacitação em todo âmbito do PJMA.

O PJMA deverá estabelecer um processo contínuo de divulgação de boas práticas sobre o tema segurança da informação. As informações relacionadas à prevenção deverão ser encaminhadas pelos canais oficiais de comunicação, utilizando uma linguagem adequada ao público-alvo.

Será necessário que a conscientização sobre a segurança da informação contemple os seguintes aspectos:

I - compromisso da alta administração com a segurança da informação;

II - responsabilização dos(as) usuários(as) por ações e omissões; e

III - familiarização e conformidade em relação às regras e obrigações aplicáveis de segurança da informação.

Com relação à capacitação, será necessário:

I - preparação de um plano de treinamento e capacitação adequado para usuários(as) e para equipes técnicas, cujos papéis requerem habilidades e conhecimentos específicos;

II - constante atualização e aprimoramento do conhecimento técnico e profissional.

Para alcançar esses objetivos poderão ser realizadas iniciativas no âmbito do próprio PJMA, tais como seminários, treinamentos, palestras, informes, competições, premiações, dentre outros.

Além das ações direcionadas para públicos-alvo específicos do PJMA deverão ser estabelecidas concomitantemente as seguintes ações: campanhas, produção de folderes, cartazes, folhetos, notas informativas e/ou boletins, periódicos e testes de segurança.

5. DETECÇÃO

A detecção terá o objetivo de reduzir o impacto do incidente cibernético, antecipando o início do processo de tratamento e de resposta. Portanto, pressupõe o estabelecimento de linhas de base, o monitoramento contínuo e a comunicação dos incidentes cibernéticos.

5.1 Estabelecimento de Linhas de Base

A Diretoria de Informática e Automação (DIA) necessitará estabelecer linhas de base que caracterizem o uso normal da rede. As anormalidades serão consideradas indícios de incidente e, se identificadas, deverão ser investigadas. Os critérios para analisar e caracterizar uma anormalidade como suposto incidente serão essenciais para a eficácia do processo.

5.2 Monitoramento Contínuo

A Diretoria de Informática e Automação (DIA) deverá estabelecer o monitoramento contínuo de seus ativos e/ou recursos de TIC, cabendo a verificação contínua de:

I - alteração de comportamento pela comparação com as linhas de base;

II - acesso de usuários(as), particularmente quanto a horários e quais ativos de TIC foram acessados;

III - volumetria do tráfego de saída;

IV - registro de eventos (logs);

V - funcionamento e atualização das ferramentas de segurança cibernética;

VI - execução não autorizada de serviço, software ou código.

Este processo poderá ser complementado com ações de detecção proativa, que incluem: testes de invasão, análise de vulnerabilidades, análise de logs, correlação de eventos e monitoramento proativo de rede.

Uma vez identificada uma anomalia, as informações referentes ao evento adverso deverão ser encaminhadas para a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) para investigar a atividade suspeita.

5.3 Recebimento de Comunicação

Os(as) usuários(as) deverão ser capazes de identificar e relatar incidentes ou suspeitas de incidentes de segurança da informação assim que perceberem. Caso detectem qualquer evento de segurança ou fragilidade que possa resultar em prejuízos, interrupções, mau funcionamento, imprecisão ou vazamento de dados e/ou informações nos sistemas do PJMA, será imprescindível que o incidente seja imediatamente notificado.

Os incidentes deverão ser reportados através do endereço eletrônico ctir@tjma.jus.br.

Havendo indisponibilidade da comunicação por meio do correio eletrônico, excepcionalmente, poderão ser utilizados outros canais de comunicação oficiais do PJMA. A notificação dos incidentes poderá ser feita através dos seguintes canais:

I - sistema: acessando o portal do SENTINELA pelo endereço eletrônico https://sistemas.tjma.jus.br/sentinela/ fazendo uso do sistema DIGIDOC:

a) a requisição deverá constar o assunto “SOLICITAÇÃO DE AÇÃO DE TECNOLOGIA DA INFORMAÇÃO”, o objeto “INCIDENTE DE

SEGURANÇA DA INFORMAÇÃO" e no campo observação uma descrição breve do incidente.

b) no caso de existir indícios do incidente, os mesmos deverão ser anexados na requisição.

II - canais de voz ou telefone: (98) 2055-2055;

III - correspondências oficiais: memorandos, ofícios, etc., devidamente protocolados;

IV - pessoalmente: em casos emergenciais.

6. TRATAMENTO DE INCIDENTES CIBERNÉTICOS

O tratamento de incidentes cibernéticos deverá ser iniciado imediatamente após a detecção ou a notificação de provável ocorrência destes, pelo processo de triagem, seguido pelo processo de análise.

6.1 Triagem

O processo de triagem consistirá em:

I - verificar se a ocorrência (evento) se trata de um incidente cibernético, para aceitação ou descarte;

II - verificar se há correlação com outros eventos e/ou incidentes;

III - dimensionar a severidade e a relevância para priorizar o tratamento e a resposta do incidente;

IV - registrar o incidente na base de incidentes cibernéticos;

V - atribuir o tratamento do incidente à ETIR ou ao especialista.

6.2 Análise

O processo de análise consistirá nas atividades abaixo:

I - validar as informações coletadas na triagem, ratificando-as, complementando-as ou retificando-as;

II - identificar e avaliar atividades suspeitas ou atípicas em relação à linha de base conhecida;

III - identificar pelo menos uma parte da cadeia de ataque para permitir a definição das atividades de resposta;

IV - complementar e adicionar novos dados a partir da colaboração das fontes utilizadas na detecção;

V - incluir todos os dados coletados na documentação sobre o incidente para viabilizar as ações de pós-incidente.

7. AVALIAÇÃO DE IMPACTO

A priorização do tratamento de incidentes será crucial para a correta alocação de recursos em áreas e sistemas que sejam fundamentais para o contexto do PJMA.

7.1 Impacto no Negócio

A ETIR deverá considerar como o incidente em tratamento poderá impactar negativamente o negócio do PJMA, realizando uma avaliação que leve em consideração os impactos futuros que o mesmo poderá trazer. A seguir, compartilha-se um quadro com os possíveis níveis de impacto no negócio:

Categoria	Definição
Nenhum	Não afeta a capacidade do PJMA de fornecer os serviços aos(às) usuários(as) e/ou público externo.
Baixo	O PJMA ainda consegue fornecer os serviços essenciais para os(as) usuários(as) e/ou público externo, mas sua eficiência foi comprometida.
Médio	O PJMA perdeu a capacidade de fornecer um serviço crítico a um subconjunto de usuários(as) e/ou pessoas.
Alto	O PJMA encontra-se incapaz de fornecer alguns serviços essenciais aos(às) usuários(as) e/ou ao público externo.
Crítico	O PJMA não consegue fornecer nenhum dos serviços essenciais aos(às) usuários(as) e/ou ao público externo.

Quadro 1: Níveis de impacto no negócio

7.2 Impacto em Dados e Informações

Os incidentes poderão afetar a confidencialidade, a integridade e a disponibilidade dos dados e informações do PJMA. A equipe da ETIR deverá, diante das opções para tratamento, mensurar os impactos que tais alternativas poderão gerar tanto para o próprio PJMA como para outros entes parceiros. A seguir, compartilha-se o quadro com os possíveis níveis de impacto em dados e informações:

Categoria	Definição
Nenhum	Nenhuma informação relevante foi exposta, alterada, excluída ou comprometida.
Violação de privacidade	Informações confidenciais de identificação pessoal foram acessadas ou expostas.
Violação proprietária	Informações proprietárias não classificadas, como informações de infraestrutura crítica protegida, foram acessadas ou expostas.
Perda de integridade	Informações confidenciais ou proprietárias foram alteradas ou excluídas.

Quadro 2: Níveis de impacto em dados e informações

8. RESPOSTA

O processo de resposta a um incidente cibernético envolve ações de contenção, erradicação e recuperação. Essas ações deverão ser guiadas pelo ANEXO XVI - Plano de Gestão de Continuidade de Negócios da PSI, considerando critérios a seguir:

I - criticidade dos ativos de TIC afetados;

II - tipo e gravidade do incidente;

III - necessidade de preservar a evidência;

IV - importância de quaisquer sistemas afetados para processos de negócio críticos;

V - recursos necessários para implementar a estratégia.

8.1 Contenção

O objetivo da contenção será limitar os danos causados pelo incidente ocorrido e evitar outros. Deverão ser aplicadas medidas de segurança para mitigar o incidente, evitando-se a destruição de provas que possam servir de subsídios para possível processo cível, penal ou administrativo.

A ação de contenção poderá envolver, minimamente, as seguintes atividades:

I - contenção a curto prazo, que consistirá em:

a) limitar os danos, para evitar que o incidente piore;

b) segmentar a rede;

c) executar desvio de tráfego de rede para os recursos que estejam saudáveis e disponíveis (failover routing);

d) observar as disposições do ANEXO II - Norma de Controle de Acesso e Gestão de Identidade no que diz respeito às credenciais de acesso de usuários(as) ou de unidades judiciais e/ou administrativas;

e) avaliar a possibilidade de desconectar os sistemas afetados da rede para evitar a propagação do incidente e descrever o método de isolamento utilizado.

II - realização de imagem forense do ambiente afetado, caso possível;

III - contenção a longo prazo, que consistirá em:

a) identificar vulnerabilidades exploradas pelos atacantes e os mecanismos que permitiram o ataque;

b) aplicar correções temporárias que permitam a normalização do funcionamento dos sistemas afetados.

A extensão dos danos do incidente de segurança deverá ser avaliada para, em seguida, ser identificado o melhor curso de ação para a erradicação completa do incidente e restauração dos ativos de TIC afetados.

8.2 Erradicação

A ação de erradicação consiste em remover ou inutilizar artefatos utilizados pelos atacantes e poderá envolver as seguintes atividades:

I - restauração completa das imagens de unidades de armazenamento, implicando na exclusão de todos os dados atuais;

II - recuperação dos dados a partir das cópias de segurança (backups) existentes, observando as diretrizes do ANEXO VIII - Norma de Cópias de Segurança da Informação da Política de Segurança da Informação (PSI) e procedimentos internos a ela relacionados;

III - identificação das principais causas que originaram o incidente;

IV - realização dos procedimentos necessários para limpar a unidade de armazenamento, removendo ou isolando os artefatos utilizados pelos atacantes;

V - correção das vulnerabilidades encontradas, observando as diretrizes do ANEXO XI - Norma de Gestão de Vulnerabilidades Técnicas da PSI.

Após a erradicação completa do incidente, será realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

8.3 Recuperação

Os impactos de um incidente determinam os recursos e o tempo necessários para a recuperação. A ETIR terá o papel de identificar e avaliar os recursos disponíveis, bem como a relevância da recuperação do incidente para o PJMA. Compartilha-se a seguir o quadro com os níveis de recuperabilidade:

Categoria	Definição
Regular	O tempo de recuperação é previsível com os recursos existentes.
Suplementado	O tempo de recuperação é previsível com recursos adicionais.
Estendido	O tempo de recuperação é imprevisível; ajuda externa e recursos adicionais poderão ser necessários.
Não Recuperável	A recuperação do incidente não é possível (por exemplo, dados confidenciais expostos e postados publicamente); deve ser

	lançada investigação.

Quadro 3: Níveis de recuperabilidade

O objetivo da recuperação será restabelecer o pleno funcionamento do ambiente afetado após garantir que as ameaças foram neutralizadas ou removidas. A ação de recuperação poderá envolver as seguintes atividades:

I - definição de cronograma para a restauração das operações pelos responsáveis pelos ativos de informação afetados, com base em subsídios apresentados pela ETIR;

II - realização de varredura completa do ambiente recuperado, de forma a garantir que este esteja apto para uso seguro;

III - realização de testes de funcionamento do ambiente recuperado, validando os resultados com as linhas de base definidas, à medida em que estão novamente disponibilizados para uso;

IV - monitoramento do ambiente recuperado, a ser executado num período após o incidente cibernético, de forma a verificar comportamentos atípicos ou anormalidade nas operações.

8.4 Envio de Comunicação

A ETIR deverá encaminhar, tempestivamente, em função do tipo e do impacto, os dados relativos ao incidente cibernético para o Comitê de Crises Cibernéticas (CCCiber) para que sejam adotadas as medidas legais cabíveis, incluindo a comunicação para as autoridades competentes. São eles:

I - agentes atacantes e atacados(as);

II - agentes envolvidos(as) no tratamento e resposta do incidente;

III - evidências coletadas;

IV - Indicadores de Comprometimento (IoCs);

V - Táticas, Técnicas e Procedimentos (TTPs) utilizados pelo atacante;

VI - ativos de infraestrutura, serviços e total de usuários(as) afetados(as);

VII - volume de dados vazados;

VIII - cronologia dos fatos;

IX - medidas de contenção, erradicação e recuperação adotadas; e

X - medidas preventivas propostas para ocorrências similares.

Em caso de incidentes envolvendo dados pessoais e dados pessoais sensíveis, o(a) encarregado(a) de proteção de dados do PJMA deverá notificar a Autoridade Nacional de Proteção de Dados (ANPD) em até 03 (três) dias úteis, observando as diretrizes previstas na Resolução-GP nº 05/2024 - TJMA ou posterior que a substitua, na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) e/ou no ANEXO XIII - Norma de Proteção de Dados Pessoais da Política de Segurança da Informação.

9. PÓS-INCIDENTE

O objetivo desta fase será realizar a análise da documentação dos incidentes, do processo de comunicação e das regras de proteção do ambiente para evitar incidentes semelhantes e aperfeiçoar os processos existentes.

9.1. Melhoria Contínua dos Processos

No intuito de evoluir em maturidade e nas ações perante incidentes cibernéticos, a ETIR deverá realizar a análise dos processos de prevenção, detecção, tratamento e resposta do incidente.

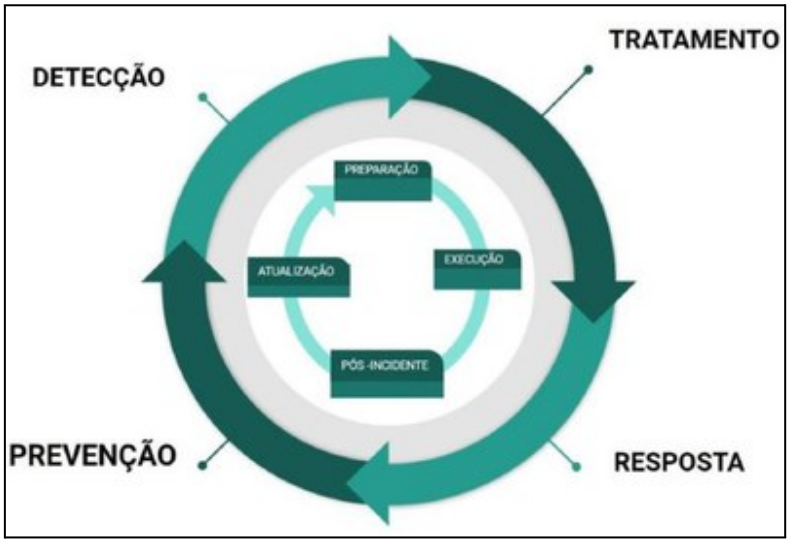

Figura 1: Ciclo de melhoria contínua do processo de gestão de incidente cibernético

A figura acima representa o ciclo de melhoria contínua, representado no anel interno, que ocorre simultaneamente com os processos de gestão de incidentes cibernéticos, representado no anel externo.

Os principais objetivos da análise pós-incidente incluem:

I - confirmar que a causa raiz foi eliminada ou mitigada;

II - estabelecer medidas preventivas para incidentes similares;

III - identificar os erros ou ausências de infraestrutura a serem resolvidos;

IV - identificar as oportunidades de melhoria na política de segurança da informação, normativos ou nos processos e procedimentos;

V - revisar e atualizar as funções, as responsabilidades, o processo de comunicação e a autoridade da ETIR para garantir a resposta oportuna e adequada;

VI - identificar necessidades de treinamento técnico ou operacional;

VII - melhorar as ferramentas, ações e capacidades necessárias para realizar a prevenção, a detecção, o tratamento e a resposta.

A ETIR deverá atualizar as atividades preparatórias e os processos de prevenção, detecção, tratamento e resposta com base nas análises do pós-incidente, com as seguintes diretrizes:

I - identificar os Indicadores de Comprometimento (IoCs) ou Técnicas, Táticas e Procedimentos (TTPs) da ameaça;

II - adicionar critérios adicionais para detecção e triagem da ameaça;

III - identificar e propor soluções para lacunas identificadas durante o incidente.

10. PROTOCOLO DE GERENCIAMENTO DE CRISE CIBERNÉTICA

O protocolo de gerenciamento de crise cibernética do PJMA prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente

de segurança cibernética não será mitigado rapidamente e poderá durar dias, semanas ou meses.

Considerado o incidente como crise cibernética, o CCCiber deverá ser acionado. O gerenciamento de crise se inicia quando:

I - ficar caracterizado grave dano material ou de imagem;

II - restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período;

III - o incidente impactar a atividade fim ou o serviço crítico mantido pelo PJMA;

IV - o incidente atrair grande atenção da mídia e da população em geral.

10.1 Planejamento da Crise

Para melhor lidar com uma crise cibernética, é necessário que o PJMA realize uma preparação prévia e adequada, seguindo as orientações do ANEXO XVI - Plano de Gestão de Continuidade de Negócios da PSI, e contemple:

I - definir as atividades críticas que são fundamentais para a atividade fim do PJMA;

II - identificar os ativos de TIC críticos, ou seja, aqueles que suportam as atividades primordiais, incluindo as pessoas, os processos, a infraestrutura e os recursos de TIC;

III - avaliar continuamente os riscos a que as atividades críticas estão expostas e que possam impactar diretamente na continuidade do negócio;

IV - categorizar os incidentes e estabelecer procedimentos de resposta específicos (playbooks) para cada tipo de incidente, de forma a apoiar equipes técnicas e de liderança em casos de incidentes cibernéticos;

V - priorizar o monitoramento, acompanhamento e tratamento dos riscos de maior criticidade; e

VI - realizar simulações e testes para validação dos planos e procedimentos.

Deverá ser definida a sala de situação e acionar o Comitê de Crises Cibernéticas (CCCiber), composto por representantes da alta administração com suporte da ETIR e de especialistas de várias áreas, tais como: jurídica, administrativa, de comunicação, de tecnologia da informação e comunicação, de privacidade de dados pessoais, de segurança da informação, de finanças, de segurança institucional, dentre outras.

10.2 Durante a Crise (Execução)

A comunicação interna entre as áreas envolvidas será fator fundamental para o PJMA reagir a uma crise cibernética de longa duração ou de grande impacto.

Assim que a ETIR identificar que um incidente constitui uma crise cibernética, o Comitê de Crises Cibernéticas deverá se reunir imediatamente na sala de situação previamente definida.

Os planos de continuidade existentes, caso aplicáveis, deverão ser colocados em prática imediatamente, visando garantir a continuidade dos serviços prestados.

O CCCiber será presidido(a) pelo(a) presidente do CGSI e do CGPD, com autoridade e autonomia para tomar decisões sobre conteúdo de comunicação a serem divulgados, bem como delegar atribuições, estabelecer metas e prazos de ações.

A sala de situação deverá dispor dos meios e equipamentos necessários e estar preferencialmente próxima a um local onde se possa fazer declarações públicas à imprensa e com acesso restrito ao CCCiber e a outros entes eventualmente convidados a participar das reuniões.

A sala de situação deverá ser um ambiente que permita ao CCCiber deliberar com tranquilidade e que possua uma equipe dedicada à execução de atividades administrativas para o período da crise.

As etapas e os procedimentos de resposta serão diferentes a depender do tipo de crise. Dessa forma, são necessárias reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

Deverá ser elaborado Relatório de Comunicação de Incidente de Segurança Cibernética, que contenha a descrição e o detalhamento da crise, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.

10.3 Pós-crise (Melhoria Contínua)

Após o retorno das operações à normalidade, a ETIR o Comitê de Crises Cibernéticas deverá realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.

Para a identificação das lições aprendidas e a elaboração de relatório final, deverá ser objeto de avaliação:

I - a identificação e análise da causa-raiz do incidente;

II - a linha do tempo das ações realizadas;

III - a avaliação do impacto nos dados, sistemas e operações de negócios importantes durante a crise;

IV - os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;

V - o escalonamento da crise;

VI - a investigação e preservação de evidências;

VII - a efetividade das ações de contenção;

VIII - a coordenação da crise, liderança das equipes e gerenciamento de informações;

IX - a tomada de decisão e as estratégias de recuperação.

As lições aprendidas serão utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta (playbooks) e para a melhoria do processo de preparação para crises cibernéticas.

11. PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS

O protocolo de investigação para ilícitos cibernéticos do PJMA tem por finalidade estabelecer os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao órgão de polícia judiciária com atribuição para o início da persecução penal.

Este protocolo deverá observar a norma ABNT NBR ISO/IEC 27037 que fornece diretrizes para atividades específicas de identificação, coleta, aquisição e preservação de evidência digital.

11.1 Requisitos para Adequação dos Ativos de TIC

Deverão ser observadas as diretrizes e prazos de retenção estabelecidos no ANEXO XIV - Norma de Registro de Eventos da Política de Segurança da Informação para as situações abaixo:

I - ajuste do horário dos ativos de TIC;

II - registro dos eventos nos ativos de TIC;

III - registros dos eventos das trilha de auditoria para componentes de sistema de informação;

IV - registro dos eventos nos ativos de TIC críticos ou que contenham dados sensíveis.

Os ativos de TIC que não propiciem os registros dos eventos listados no item acima deverão ser mapeados e documentados quanto ao tipo e formato de registros de auditoria permitidos e armazenados.

Os sistemas e as redes de comunicação de dados deverão ser monitorados, registrando-se, minimamente, os seguintes eventos de segurança, sem prejuízo de outros considerados relevantes:

I - utilização de usuários, perfis e grupos privilegiados;

II - inicialização, suspensão e reinicialização de serviços;

III - acoplamento e desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis;

IV - modificações da lista de membros de grupos privilegiados;

V - modificações de política de senhas, como, por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico, etc.;

VI - acesso ou modificação de arquivos ou sistemas considerados críticos; e

VII - eventos obtidos por meio de quaisquer mecanismos de segurança existentes.

Os ativos de informação são configurados de forma a armazenar seus registros de auditoria não apenas localmente, mas também remotamente, por meio do uso de tecnologia aplicável.

11.2 Coleta e Preservação de Evidências

A ETIR durante o processo de tratamento do incidente penalmente relevante, deverá, sem prejuízo de outras ações, coletar e preservar:

I - as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses;

II - os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM);

III - todos os registros de eventos citados no tópico 11.1.

Nos casos de inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados ou das suas respectivas imagens forenses, em razão da necessidade de pronto restabelecimento do serviço afetado, a ETIR deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original e os “metadados” desses arquivos, como data, hora de criação e permissões.

O agente responsável pela ETIR deverá fazer constar em relatório a eventual impossibilidade de preservação das mídias afetadas e listar todos os procedimentos adotados.

Para garantir a preservação dos arquivos coletados durante uma investigação de ilícitos cibernéticos, será essencial seguir os seguintes procedimentos:

I - gerar um arquivo contendo a lista dos resumos criptográficos de todos os arquivos coletados;

II - gravar os arquivos coletados juntamente com o arquivo contendo a lista dos resumos criptográficos mencionados no item anterior;

III - gerar um resumo criptográfico para cada arquivo coletado.

Todo material coletado deverá ser lacrado e custodiado por um membro da ETIR, o qual é responsável por preencher o Termo de Custódia dos Ativos de TIC relacionado ao incidente de segurança penalmente relevante. O material coletado ficará à disposição das autoridades competentes.

11.3 Envio de Comunicação

Deverá ser definido um Plano de Comunicação de Incidentes de Segurança da Informação que esteja de acordo com a classificação e o nível de criticidade do incidente. Em casos mais simples e de baixa criticidade apenas o gestor responsável pela informação, ativo e/ou recurso de TIC deverá ser comunicado. Em casos mais graves, a alta administração e os setores envolvidos serão comunicados.

Nenhum tipo de informação sobre incidentes de segurança da informação poderá ser divulgado para entidades ou pessoas externas ao Poder Judiciário do Estado do Maranhão, sem aprovação expressa e formal do CCCiber.

Todos os incidentes cibernéticos graves serão comunicados ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça, através do endereço eletrônico de e-mail abuse@cnj.jus.br. A depender do tipo de incidente, poderá ainda ser comunicado o órgão de polícia judiciária, de preferência especializado em crimes cibernéticos, com devida atribuição e para apuração dos fatos.

Havendo indisponibilidade da comunicação por meio do correio eletrônico, excepcionalmente, poderão ser utilizados outros canais para comunicação, como:

I - voz (telefone, celular);

II - mensagem instantânea;

III - reunião por videoconferência ou presencial;

IV - sítios eletrônicos e mídias sociais institucionais.

As principais mensagens que serão transmitidas por meio desses canais de comunicação dizem respeito a notificação de incidentes cibernéticos e deverão ocorrer com a maior brevidade possível.

Após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante, o responsável pela ETIR deverá elaborar Relatório de Comunicação de Incidente de Segurança Cibernética, descrevendo detalhadamente os eventos verificados.

O Relatório de Comunicação de Incidente de Segurança Cibernética tem por objetivo registrar de forma detalhada os eventos relacionados a incidentes cibernéticos, fornecendo informações essenciais para a análise e resposta adequada às ocorrências. O relatório deverá conter as seguintes informações, sem prejuízo de outras julgadas relevantes:

I - nome do responsável pela preservação dos dados do incidente, com informações de contato;

II - nome do agente responsável pela ETIR e informações de contato;

III - órgão comunicante com sua localização e informações de contato;

IV - número de controle da ocorrência;

V - relato sobre o incidente que descreva o que ocorreu, como foi detectado e quais dados foram coletados e preservados;

VI - descrição das atividades de tratamento e resposta ao incidente e todas as providências tomadas pela ETIR, incluindo as ações de preservação e coleta, a metodologia e as ferramentas utilizadas e o local de armazenamento das informações preservadas;

VII - resumo criptográfico dos arquivos coletados;

VIII - Termo de Custódia dos Ativos de TIC relacionados ao incidente de segurança;

IX - número de lacre de material físico preservado, se houver; e

X - justificativa sobre a eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, diante da impossibilidade de mantê-las.

O Relatório de Comunicação de Incidente de Segurança em Redes Computacionais deverá ser assinado pelo agente responsável pela ETIR e encaminhado formalmente à autoridade responsável pelo órgão do Poder Judiciário afetado.

Deverá constar no documento formal de encaminhamento a que se refere o parágrafo acima, apenas a informação de que se trata de comunicação de evento relacionado à segurança da informação, sem a descrição dos fatos.

12. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

12.1 Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação

São responsabilidades da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR):

I - aconselhar o CCCiber sobre os eventos e incidentes de segurança da informação;

II - decidir sobre os procedimentos técnicos a serem adotados na resposta a incidentes da informação;

III - diligenciar para coletar e proteger evidências;

IV - detectar, receber, analisar, classificar, tratar, responder e documentar as notificações e atividades relacionadas a incidentes de segurança;

V - definir os procedimentos de compartilhamento de informações relevantes para a proteção de outros tribunais com base nas informações colhidas sobre o incidente;

VI - elaborar plano de retorno à normalidade.

12.2 Comitê de Crise Cibernética

São responsabilidades do Comitê de Crise Cibernética (CCCiber):

I - entender claramente o incidente que gerou a crise, sua gravidade e seus impactos negativos;

II - levantar soluções alternativas para a crise, avaliando sua viabilidade e consequências;

III - avaliar a necessidade de suspender serviços e/ou sistemas informatizados;

IV - centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas;

V - realizar comunicação tempestiva e eficiente, de forma a evidenciar o trabalho diligente das equipes e enfraquecer boatos ou investigações paralelas que alimentem notícias falsas;

VI - definir estratégias de comunicação com a imprensa e/ou redes sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso;

VII - solicitar a colaboração de especialistas ou de centros de resposta a incidentes de segurança;

VIII - avaliar a necessidade de recursos adicionais extraordinários a fim de apoiar as equipes de resposta;

IX - orientar sobre as prioridades e estratégias do PJMA para recuperação rápida e eficaz;

X - avaliar e validar o plano de retorno à normalidade elaborado pela ETIR.

12.3 Assessoria de Comunicação da Presidência

É responsabilidade da Assessoria de Comunicação da Presidência (ASSCOM):

I - aprovar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação.

12.4 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação (DIA):

I - apoiar a ETIR no tratamento de ocorrências e incidentes de segurança da informação.

13. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

14. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

15. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.