ATA-GabDesJMGN - 42023
Código de validação: 160FB2214F

ATA DE REUNIÃO
COMITÊ DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO – CGSI e do COMITÊ GESTOR DE PROTEÇÃO DE DADOS – CGPD

Ata da 6ª Reunião de 2023 (14/08/2023)

Aos quatorze dias do mês de agosto do ano de dois mil e vinte e três, na sala de videoconferência da DIA, utilizando a ferramenta ZOOM, às 09:00h, sob a presidência do desembargador Jamil de Miranda Gedeon Neto, reuniram-se os membros do Comitê de Governança de Segurança da Informação (CGSI) e do Comitê Gestor de Proteção de Dados (CGPD), instituídos, respectivamente, pelas Resoluções RESOL-GP - 1132022 e RESOL-GP - 132021.

Como membros(as), registraram-se as presenças do desembargador JAMIL DE MIRANDA GEDEON NETO (TJMA - presidente do CGSI e CGPD), do juiz FRANCISCO SOARES REIS JÚNIOR (TJMA - Coordenador do CGPD e membro do CGSI), do juiz JOSÉ JORGE FIGUEIREDO DOS ANJOS JÚNIOR (CGJ - Membro do CGSI e CGPD), do diretor CLÁUDIO HENRIQUE CARNEIRO SAMPAIO (Diretoria de Informática e Automação - Membro do CGSI e CGPD), do diretor LAÉRCIO LEÃO AMARAL (Diretoria Judiciária - Membro do CGPD), da diretora MILENA VIEIRA DE OLIVEIRA (Diretoria de Recursos Humanos - Membra do CGSI e CGPD) e do diretor ANDRÉ MENEZES MENDES (Diretoria do FERJ - Membro do CGPD).

Estavam ausentes os(as) membros(as): - o juiz JOSÉ NILO RIBEIRO FILHO (TJMA - Coordenador do CGSI e membro do CGPD), o diretor ALEXANDRE MAGNO DE SOUSA NUNES (Diretoria de Segurança Institucional e Gabinete Militar - Membro do CGSI e CGPD), substituído por EDUARDO HELDER PACÍFICO PINHEIRO, a diretora CÉLIA REGINA PEREIRA DA SILVA (Diretoria Financeira - Membra do CGPD), substituída por FERNANDO ANTÔNIO CARVALHO MARQUES, a diretora JUREMA MAMEDE DE PAIVA SANTOS (Diretoria de Auditoria Interna - Membra do CGPD), substituída por PATRICIA FONSECA PEREIRA DOS SANTOS, a diretora KEILA FONSECA DA SILVA (Diretoria Administrativa - Membra do CGSI e CGPD), substituída por LUIZ GUSTAVO SANTOS NASCIMENTO, o diretor CARLOS ANDERSON DOS SANTOS FERREIRA (Diretoria Geral - Membro do CGSI), substituído por LISIANE SEBA SALOMÃO DA SILVA, o diretor MAYCO MURILO PINHEIRO (Diretoria de Engenharia - Membro do CGPD), substituído por DÉBORA CRISTINA COUTINHO VILAS BOAS e a assessora ISABELLA CAROLINA SILVA E SILVA (Assessoria de Comunicação da Presidência - Membra do CGSI), substituída por THAÍSE ADRIANA SOUZA LUZ.

Como convidados, registraram-se as presenças do GIVANILDO MARQUES (Coordenadoria de Atendimento ao Usuário), ADRIANO VALPORTO (Gabinete do Des. Jamil de Miranda Gedeon Neto) e HALLYSON CARLOS (INTEROP).

A apresentação foi conduzida inicialmente pelo diretor CLÁUDIO HENRIQUE CARNEIRO SAMPAIO com participação do Técnico Judiciário JAIRO FERREIRA ROCHA, servidor da Diretoria de Informática e Automação. A reunião seguiu com a pauta abaixo:

- Ações da ENSEC-PJ - Relatório de progresso;
- Normas da PSI (ANEXOS) - minutas para aprovação:

a) ANEXO I - Glossário;
b) ANEXO VII - Norma de Gestão de Incidentes de Segurança da Informação;
c) ANEXO XIII - Norma de Proteção de Dados Pessoais;
d) ANEXO XV - Norma de Gestão de Riscos de Segurança da Informação;
e) ANEXO XVI - Plano de Gestão de Continuidade de Negócios;
f) Termo de Responsabilidade e Confidencialidade (PSI) - DRH.

- Ações da LGPD - Relatório de progresso;
- Ações futuras.

O Sr. Jairo Rocha saudou a todos(as) e apresentou o relatório de progresso da ENSEC-PJ demonstrando sua evolução. O progresso, focado na conclusão, evoluiu de 48,9% (24.07.2023) para 72,3% (08.08.2023).

Discorreu-se sobre a intenção de unificar os comitês de Segurança da Informação e de Proteção de Dados, além de adicionar o Comitê de Crise Cibernética (CCC), definido nos protocolos da ENSEC-PJ e já descrito na norma de Gestão de Incidentes de Segurança da Informação. Acordou-se que o CCC será detalhado em reunião posterior.

Falou-se resumidamente sobre as normas de Gestão de Incidentes de Segurança da Informação, de Proteção de Dados Pessoais, de Gestão de Riscos de Segurança da Informação e sobre o Plano de Gestão de Continuidade de Negócios, anexas a esta ata. Além do Glossário e do Termo de Responsabilidade e Confidencialidade, também anexos a esta ata. Pontuou-se sobre algumas questões de incidentes de segurança, tais como vazamento de credenciais e phishing. O MM. Francisco Reis colocou em pauta as observações realizadas por ele na norma de Proteção de Dados Pessoais e foi acordado com o desembargador Jamil que os tratamentos seriam realizados após a reunião. O Sr. Cláudio discorreu sobre o Plano de Gestão de Continuidade de Negócio da área da Diretoria de Informática de Automação e se disponibilizou a apresentá-lo. Superadas essas questões, os normativos, termo, glossário e plano foram colocados em votação pelos membros dos comitês e foram aprovados por unanimidade.

Discorreu-se sobre o andamento das ações da LGPD de forma sucinta e o MM. Francisco Reis reportou sobre os ajustes realizados com a empresa FAC Tecnologia para intensificar essas ações. Serão realizados workshops para setores agrupados e seguirão com a realização dos mapeamentos desses setores, andando de forma paralela.

Por fim, voltando à condução da apresentação, o Sr. Jairo Rocha falou sobre as ações futuras, com ações específicas do Grupo de Trabalho Técnico em Segurança da Informação (GTT - SI), e encerrou a mesma, passando a vez para o Sr. Cláudio Sampaio que franqueou espaço para os demais membros se manifestarem e não tendo mais assuntos a serem tratados, o desembargador Jamil de Miranda Gedeon Neto agradeceu a todos(as) e encerrou a reunião, tendo eu, Cláudio Henrique Carneiro Sampaio, designado secretário ad hoc do Comitê, lavrado a presente ata que, depois de lida e aprovada, vai assinada pelos(as) membros(as) dos comitês.

PALÁCIO DA JUSTIÇA "CLÓVIS BEVILÁCQUA" DO ESTADO DO MARANHÃO

São Luís, 14 de agosto de 2023.

ANEXO VII
NORMA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
PORTARIA-TJ - 47312022	
PORTARIA-CNJ Nº 162 de 10/06/2021	ANEXOS

Versionamento:

Versão:	1.0
Data:	XX/04/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	14/08/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

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 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.

Os incidentes de segurança da informação deverão ser documentados, triados,

classificados e priorizados conforme sua criticidade e comunicados à Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), conforme definição da Portaria TJ 47312022 ou posterior que a substitua.

A autonomia da ETIR descreve o escopo de atuação e o nível de responsabilidade que a equipe tem sobre as suas próprias ações e sobre as atividades de resposta e tratamento dos incidentes de segurança cibernética.

A ETIR terá autonomia compartilhada, ou seja, trabalhará em acordo com os outros setores do PJMA a fim de participar do processo de tomada de decisão sobre quais medidas deverão ser adotadas, recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de um incidente e debaterá sobre as ações a serem tomadas, seus impactos e a repercussão, caso as recomendações não sejam seguidas.

A ETIR poderá solicitar apoio multidisciplinar para responder aos incidentes de segurança de maneira adequada e tempestiva.

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, 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 - compartilhamento de senhas.

O conteúdo da notificação precisará ser claro, em formato simples e deverá

incluir as informações necessárias para a rápida e correta identificação do problema e da ação requerida.

Os eventos abaixo não serão considerados incidentes de segurança da informação:

I - eventos acidentais não intencionais;

II - eventos não maliciosos.

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: tecnológicos, organizacionais e físicos.

Os controles tecnológicos são aqueles utilizados para reduzir vulnerabilidades nos ativos de TIC e nos sistemas e/ou softwares. Entre os principais controles tecnológicos estão: dispositivos finais do(a) usuário(a), restrição de acesso à informação, autenticação segura, proteção contra códigos maliciosos, cópia de segurança das informações, atividades de monitoramento, tais como, registro de eventos (logs), segurança de redes e uso de criptografia.

Os controles organizacionais serão utilizados para assegurar a adequação contínua e efetiva da gestão de segurança da informação. Entre os principais controles organizacionais estão: Política de Segurança da Informação e normativos correlatos, definição de papéis e responsabilidades no âmbito da segurança da informação, gestão de ativos de TIC, controles de acesso, classificação e tratamento de informações e gestão de riscos de segurança da informação.

Por fim, os controles físicos têm por finalidade prevenir ou evitar o acesso não autorizado a áreas restritas, bem como danos e interferências em ativos que contenham informações críticas ou sensíveis. Entre os principais controles físicos estão: definição dos perímetros de segurança física, monitoramento de segurança física, proteção contra ameaças físicas e ambientais, proteção e localização de equipamentos, segurança de ativos fora das instalações do PJMA e manutenção de ativos.

4.2 Gerenciamento de Vulnerabilidades

Trata-se de um processo contínuo e proativo que visa controlar riscos, realizar monitoramento, corrigir falhas e proteger contra ataques cibernéticos e violação de dados. O objetivo desse 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 na norma de gestão de vulnerabilidades técnicas.

4.3 Conscientização e Capacitação (Educação Cibernética)

Visando aprimorar a educação em segurança da informação, deverão ser desenvolvidas 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 relativas à prevenção deverão ser encaminhadas pelos canais oficiais de comunicação, além de possuírem linguagem adequada ao público-alvo.

É 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, é 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, etc.

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 tem 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 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 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 estar aptos a identificar e relatar incidentes e/ou suspeitas de incidentes de segurança da informação assim que os perceberem. Caso notem 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, é imprescindível que o mesmo seja 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.

6. TRATAMENTO DE INCIDENTES CIBERNÉTICOS

O tratamento de incidentes cibernéticos inicia-se 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 consiste 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 ao especialista ou à ETIR.

6.2 Análise

O processo de análise consiste nas atividades listadas abaixo:

I - validar as informações tratadas 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 é importante para a correta alocação de recursos em áreas e sistemas que sejam chave 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, devendo realizar 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 poderá fornecer os serviços essenciais para os(as) usuários(as) e/ou público externo, mas perdeu eficiência.
Médio	O PJMA perdeu a capacidade de fornecer um serviço crítico a um subconjunto de usuários(as) e/ou pessoas.
Alto	O PJMA não é mais capaz de fornecer alguns serviços essenciais a nenhum(a) usuário(a) 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 de alguma maneira comprometida.
Violação de	Informações confidenciais de identificação pessoal foram

privacidade	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 consiste em ações de contenção, erradicação e recuperação. As ações deverão observar o plano de gestão de continuidade de negócios em segurança da informação e os critérios abaixo:

I - criticidade dos ativos 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 é 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 consiste 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).

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

III - contenção a longo prazo, que consiste 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 da norma de cópias de segurança da informação e procedimentos internos a ela relacionados;

III - identificação das causas principais que originaram o ataque;

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 da norma de gestão de vulnerabilidades técnicas.

Após a erradicação completa do incidente, deverá ser 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 tem 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; recursos adicionais e ajuda externa poderão ser necessários.
Não Recuperável	A recuperação do incidente não é possível (por exemplo, dados confidenciais expostos e postados publicamente); lançar investigação.

Quadro 3: Níveis de recuperabilidade

O objetivo da recuperação é 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 (CCC) para que sejam adotadas as medidas legais cabíveis, incluindo a comunicação para as autoridades competentes. São eles:

I - atores atacantes e atacados;

II - atores envolvidos 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 05 (cinco) dias úteis, observando as diretrizes previstas na Resolução GP nº 13/2021 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 na norma de proteção de dados pessoais do PJMA.

9. PÓS-INCIDENTE

O objetivo desta fase é 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.

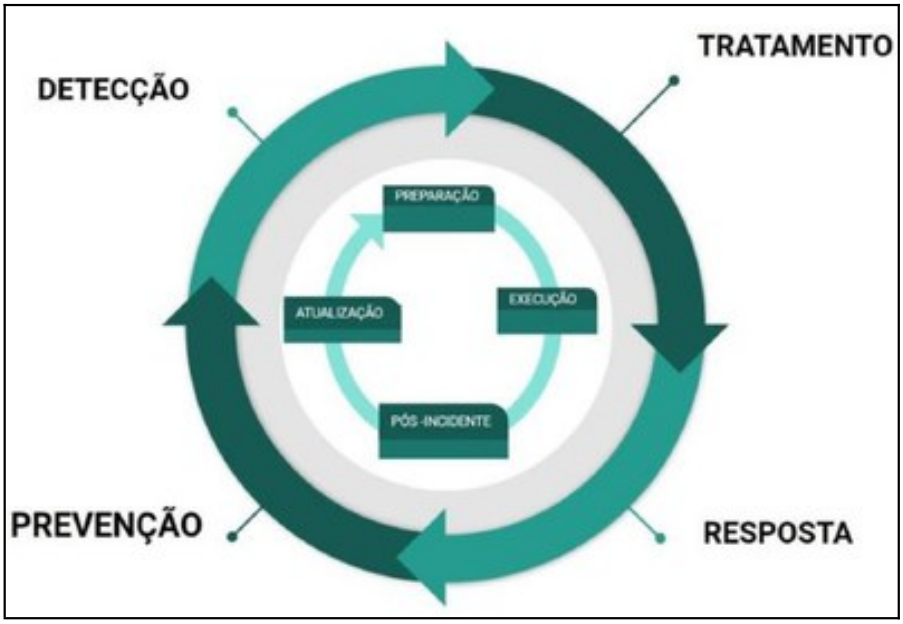

Figura 1: Ciclo de melhoria contínua do processo de gestão de incidente cibernético

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 a partir das análises do pós-incidente,

devendo:

I - identificar os IoCs ou TTPs da ameaça;

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

III - identificar e propor soluções para situações omissas verificadas no 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 CCC 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 finalística 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 prévia e adequada preparação, sendo fundamental que o PJMA estabeleça um Plano de Gestão da Continuidade de Serviços que contemple as seguintes atividades:

I - definir as atividades críticas que são fundamentais para a atividade finalística 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 criar o Comitê de Crises Cibernéticas (CCC), 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 é 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 contingência existentes, caso aplicáveis, deverão ser colocados em prática imediatamente, visando à continuidade dos serviços prestados.

A chefia do Comitê de Crises Cibernéticas deverá ficar a cargo do membro indicado pelo Presidente do PJMA, 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 CCC e a outros entes eventualmente convidados a participar das reuniões.

A sala de situação deverá ser um ambiente que permita ao CCC 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 são 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, 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, deverão ser objeto de avaliação:

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

II - a linha do tempo das ações realizadas;

III - a escala 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 deverão ser 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.

O 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 estabelecidas na norma de registro de eventos 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.

Habilitar nos ativos de TIC do PJMA, onde houver suporte para essa atividade, os registros de eventos, devendo ser armazenados por no mínimo 180 (cento e oitenta) dias, exceto ativos de TIC que necessitem manter o registro de eventos por mais tempo, para atender algum normativo interno ou para cumprir alguma exigência legal.

Os registros de eventos de ativos de TIC deverão ser criados e retidos na medida necessária para permitir o monitoramento, análise, investigação e relatório de

atividades suspeitas ou não autorizadas. Os registros de eventos serão armazenados em pelo menos um repositório central.

Assegurar que os eventos dos ativos de TIC classificados como críticos, serão registrados, armazenados e mantidos por pelo menos 365 (trezentos e sessenta e cinco) dias, a contar do registro de cada evento.

Os ativos de informação serão 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.

As ações de restabelecimento do serviço não deverão comprometer a coleta e a preservação da integridade das evidências.

Para a preservação dos arquivos coletados, dever-se-á:

I - gerar arquivo que contenha a lista dos resumos criptográficos de todos os arquivos coletados;

II - gravar os arquivos coletados, acompanhados do arquivo com a lista dos resumos criptográficos descritos na alínea a deste subitem; e

III - gerar resumo criptográfico do arquivo a que se refere a deste subitem.

Todo material coletado deverá ser lacrado e custodiado por um membro da ETIR, o qual deverá preencher o Termo de Custódia dos Ativos de TIC relacionados ao incidente de segurança penalmente relevante. O material coletado ficará à disposição da autoridade responsável pelo órgão do Poder Judiciário competente.

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 ou outros setores pertinentes deverão ser 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 CCC.

Todos os incidentes cibernéticos graves deverão ser 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 ao órgão de polícia judiciária, de preferência especializado em crimes cibernéticos, com atribuição 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 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 acondicionado em envelope lacrado e rubricado pelo agente responsável pela ETIR, protocolado 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 (ETIR)

São responsabilidades da ETIR:

I - aconselhar o CCC sobre quais informações sobre eventos e incidentes de segurança da informação poderão ser divulgadas para públicos internos e externos;

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

III - diligenciar para coletar e proteger evidências;

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

12.2 Comitê de Crise Cibernética:

São responsabilidades do Comitê de Crise Cibernética:

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

II - levantar as informações relevantes, verificando fatos e descartando boatos;

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

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

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

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

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

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

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

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

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

XII - elaborar plano de retorno à normalidade.

12.3 Assessoria de Comunicação

É responsabilidade da Assessoria de Comunicação:

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:

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.

ANEXO XIII
NORMA DE PROTEÇÃO DE DADOS PESSOAIS

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
Resolução nº 13/2021-GP	

Versionamento:

Versão:	1.0
Data:	02/05/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	14/08/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A norma de proteção de dados pessoais complementa a Política de Segurança da Informação (PSI), estabelecendo princípios que devem nortear o tratamento de dados pessoais, físicos e digitais, no âmbito do Poder Judiciário do Estado do Maranhão (PJMA), a fim de garantir a proteção de dados e a privacidade de seus(suas) titulares.

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

As orientações da norma de proteção de dados pessoais serão baseadas nos princípios da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) e também seguirão as diretrizes que constam na Resolução GP nº 13/2021 ou posterior que a substitua.

2. OBJETIVO

Assegurar o cumprimento dos requisitos legais, estatutários, regulamentares e contratuais relacionados aos aspectos de segurança da informação da proteção de dados pessoais.

3. DIRETRIZES

Orientações da norma de proteção de dados pessoais.

3.1 Princípios de Proteção de Dados Pessoais

Esta seção descreve os princípios que deverão ser observados no tratamento de dados pessoais pelo PJMA, atendendo aos padrões de proteção de dados no âmbito institucional.

3.1.1 Legalidade, Transparência e Não Discriminação

O PJMA tratará os dados pessoais de forma transparente, justa, em conformidade com legislação e regulamentação aplicáveis e sempre vinculado a finalidade do tratamento às hipóteses legais permitidas, abaixo elencadas, sendo obrigatório informar aos(às) titulares dos dados a razão e a forma, pela qual seus dados estarão sendo tratados:

I - mediante o fornecimento de consentimento pelo(a) titular;

II - cumprimento de obrigação legal ou regulatória, ao qual o PJMA está sujeito;

III - para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

IV - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o(a) titular, a pedido do(a) titular dos dados;

V - quando necessário para atender aos interesses legítimos do PJMA ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do(a) titular que exijam a proteção dos dados pessoais;

VI - para tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

VII - para a proteção da vida ou da incolumidade física do(a) titular ou de terceiro(a);

VIII - para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

O consentimento dos(as) titulares para o tratamento de seus dados pessoais deverá ser obtido de forma específica, livre, inequívoca e informada.

O PJMA, através das unidades administrativas e/ou judiciais, deverá coletar, armazenar e gerenciar as respostas de consentimento de maneira organizada e acessível, para que sua comprovação possa ser fornecida pelo(a) encarregado(a), quando necessário.

Para quaisquer hipóteses em que os dados se tornem manifestamente públicos pelo(a) seu(sua) titular será dispensada a exigência de consentimento, ficando resguardados os direitos do(a) titular e os princípios previstos na Política de Privacidade dos Dados das Pessoas Físicas do PJMA, na legislação e/ou nesta norma.

As atividades de tratamento de dados pessoais deverão observar o princípio da não discriminação, proibindo qualquer forma de tratamento que tenha como finalidade a discriminação ilícita ou abusiva dos(as) titulares dos dados.

O PJMA poderá ter a necessidade de tratar dados pessoais sensíveis, quais sejam:

I - relacionados à saúde ou à vida sexual;

II - relacionado a dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - que evidenciem a origem racial ou étnica;

IV - referente a convicção religiosa;

V - referente a opinião política;

VI - referente à filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

O tratamento de dados pessoais sensíveis, somente poderá ocorrer nos casos específicos descritos abaixo, devendo observar padrões de segurança mais robustos do que aos demais dados:

I - quando o(a) titular ou seu(sua) responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do(a) titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo PJMA;

b) tratamento e uso compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

d) proteção da vida ou da incolumidade física do(a) titular ou de terceiro(a);

e) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

f) garantia da prevenção à fraude e à segurança do(a) titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos do(a) titular mencionados em legislação específica, exceto nos casos de prevalecerem direitos e liberdades fundamentais do(a) titular que exijam a proteção dos dados pessoais.

3.1.2 Limitação e Adequação da Finalidade

O tratamento de dados pessoais deverá ser realizado de maneira compatível com a finalidade original para qual os dados foram coletados, ou seja, somente poderão ser utilizados para o propósito para o qual foram solicitados inicialmente, vedando-se a coleta com uma finalidade e utilização para outra sem o consentimento específico do(a) titular, garantindo assim a proteção dos direitos e da privacidade dos(as) titulares.

O tratamento também deverá ser limitado ao mínimo necessário para o

cumprimento da finalidade específica, não podendo ser excessivo ou desproporcional. Portanto, serão priorizados os modos de tratamento menos invasivos/abusivos à privacidade dos(as) titulares de dados pessoais.

O compartilhamento de dados pessoais com outra área, empresa ou órgão, somente será possível dentro das hipóteses legais.

3.1.3 Princípio da Necessidade (Minimização dos Dados)

O PJMA somente poderá tratar dados pessoais, limitando-se ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

3.1.4 Exatidão (Qualidade dos Dados)

O PJMA deverá adotar medidas razoáveis para assegurar que os dados pessoais em sua posse sejam mantidos precisos e atualizados em relação às finalidades para as quais foram coletados. Dessa forma, será disponibilizado ou facilitado ao(à) titular dos dados pessoais canais para requerimento de correção dos dados imprecisos ou desatualizados.

3.1.5 Retenção e Limitação do Armazenamento de Dados

O PJMA deverá ter conhecimento de suas atividades de tratamento, períodos de retenção estabelecidos e processos de revisão periódica, não podendo manter os dados pessoais por prazo superior ao necessário para atender as finalidades pretendidas.

A retenção da informação, no que couber, deverá observar os prazos definidos no Plano de Classificação e Tabelas de Temporalidade do PJMA, que constam na Resolução GP nº 31/2015 ou posterior que a substitua.

3.1.6 Livre Acesso, Prevenção e Segurança

As atividades de tratamento de dados pessoais deverão observar:

I - livre acesso: garantia, aos(às) titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a plenitude de seus dados pessoais;

II - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

III - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Dentre algumas técnicas, no que refere-se às questões de proteção de dados pessoais, podem ser descritas:

I - a anonimização;

II - a pseudoanonimização.

3.1.7 Responsabilização e Prestação de Contas

O PJMA é responsável e deverá demonstrar o cumprimento desta norma, assegurando a implementação de diversas medidas que incluem, mas não se limitam, a:

I - garantia de que os(as) titulares dos dados pessoais poderão exercer os seus direitos conforme descritos nesta norma;

II - registro de dados pessoais, incluindo:

a) registros de atividades de tratamento de dados pessoais, com a descrição dos propósitos/finalidades, os destinatários do compartilhamento dos dados e os prazos pelos quais o PJMA deverá retê-los;

b) registros de incidentes e violações de dados pessoais.

III - garantia de que os(as) prestadores(as) de serviços terceirizados que sejam operadores(as) de dados pessoais estarão agindo em conformidade com esta norma e com a legislação e regulamentação aplicáveis;

IV - garantia de que o PJMA cumprirá as exigências e solicitações de qualquer autoridade de supervisão à qual esteja sujeita.

3.2 Padrões de Segurança

O PJMA estará comprometido com a adequação dos padrões de segurança da informação e com a proteção de dados pessoais com vistas a garantir o direito fundamental do indivíduo à autodeterminação da informação.

Os(As) agentes de tratamento deverão adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

3.2.1 Garantir a Segurança dos Dados Pessoais

A confidencialidade, integridade e disponibilidade, bem como autenticidade,

responsabilidade e não-repúdio, deverão ser observados para a segurança dos dados pessoais tratados pelo PJMA.

A Autoridade Nacional de Proteção de Dados Pessoais (ANPD) poderá solicitar ao PJMA a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais.

3.2.2 Obrigação do Sigilo de Dados Pessoais

Todos(as) os(as) servidores(as), prestadores(as) de serviço, colaboradores(as), terceirizados(as), agentes públicos(as) externos(as) e estagiários(as) com acesso a dados pessoais estarão obrigados(as) aos deveres de manter a confidencialidade dos dados pessoais por eles(as) tratados.

3.2.3 Privacidade de Dados Pessoais por Concepção (privacy by design) e por Padrão (privacy by default)

Ao implementar novos processos, procedimentos ou sistemas que envolvam o tratamento de dados pessoais, o PJMA deverá adotar medidas que garantam que as regras de privacidade e proteção de dados serão aplicadas durante todo o ciclo de vida do tratamento dos dados pessoais (coleta, armazenamento, uso, manutenção e descarte).

3.2.4 Direito dos(as) Titulares de Dados Pessoais

O PJMA deverá estar comprometido com os direitos dos(as) titulares de dados pessoais, os quais incluem:

I - confirmação da existência de tratamento de seus dados;

II - o acesso aos dados pessoais que o PJMA detenha sobre eles(as);

III - a correção de seus dados pessoais se estiverem incompletos, inexatos ou desatualizados;

IV - a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade. Isso poderá incluir, mas não se limita a, circunstâncias em que não é mais necessário que o PJMA retenha seus dados pessoais para os propósitos para os quais foram coletados;

V - a eliminação dos dados pessoais após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

a) cumprimento de obrigação legal ou regulatória pelo PJMA;

b) transferência a terceiro(a), desde que respeitados os requisitos de tratamento de dados dispostos na LGPD; ou

c) uso exclusivo do PJMA, vedado seu acesso por terceiro(a), e desde que anonimizados os dados.

VI - informação das entidades públicas e privadas com as quais o PJMA realizou o uso compartilhado de dados;

VII - a revogação do consentimento a qualquer momento, se o tratamento dos dados pessoais se basear no consentimento do indivíduo para um propósito específico;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

3.2.5 Prestadores(as) de Serviço, Colaboradores(as) e Terceirizados(as)

Os(As) prestadores(as) de serviço, colaboradores(as) e terceirizados(as), identificados(as) como operadores(as) de dados, que tratam dados pessoais sob as instruções do PJMA estarão sujeitos às obrigações de acordo com a legislação e regulamentação de proteção de dados pessoais vigentes.

O PJMA deverá garantir que no contrato de prestação de serviços sejam contempladas as cláusulas de privacidade e proteção de dados que exijam que o(a) operador(a) de dados implemente medidas de segurança cabíveis. Além disso, o PJMA deverá assegurar controles técnicos e administrativos apropriados para garantir a confidencialidade, a integridade e a segurança dos dados pessoais e especifiquem que o(a) operador(a) está autorizado(a) a tratar dados pessoais apenas quando seja formalmente solicitado pelo PJMA.

Nos casos em que o(a) operador(a) de dados estiver localizado(a) fora do país em que o dado pessoal foi tratado, cláusulas contratuais deverão ser incluídas no contrato de proteção de dados pessoais como um anexo para garantir que as devidas salvaguardas exigidas pela legislação e regulamentação aplicáveis de proteção de dados sejam atendidas.

3.2.6 Gerenciamento de Violação de Dados

Todos(as) os(as) usuários(as) deverão estar cientes de suas responsabilidades pessoais de encaminhar e escalonar possíveis problemas, bem como de denunciar violações ou suspeitas de violações de dados pessoais assim que as identificarem. No momento em que um incidente ou violação real for descoberto, é essencial que os incidentes sejam informados e formalizados de forma tempestiva.

As violações de dados pessoais incluem, mas não se limitam a, qualquer perda, exclusão, roubo ou acesso não autorizado de dados pessoais tratados pelo PJMA.

O PJMA deverá comunicar à Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e ao(à) próprio(a) titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos(às) titulares.

Quando houver infração à LGPD em decorrência do tratamento de dados pessoais realizados pelo PJMA, a ANPD poderá enviar informe com medidas cabíveis para fazer cessar a violação.

A comunicação à ANPD será feita em prazo razoável e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os(as) titulares envolvidos(as);

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, caso a comunicação não seja imediata;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente.

Na impossibilidade de comunicação individual ao(à) titular de dados pessoais, o PJMA providenciará publicação em mídias de massa, com o propósito de garantir minimamente condições de que os(as) afetados(as) sejam notificados(as) do vazamento.

3.2.7 Auditorias de Proteção de Dados

O PJMA deverá garantir que existam revisões periódicas a fim de confirmar que as iniciativas de privacidade, seus sistemas, medidas, processos, precauções e outras atividades incluindo o gerenciamento de proteção de dados pessoais são efetivamente implementados e mantidos e estão em conformidade com a legislação e regulamentação aplicáveis.

4. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

4.1 Comitê Gestor de Proteção de Dados Pessoais - CGPD

São responsabilidades do Comitê Gestor de Proteção de Dados Pessoais:

I - avaliar os mecanismos de tratamento e proteção dos dados existentes e propor políticas, estratégias e metas para a conformidade do PJMA, com as disposições da LGPD;

II - formular princípios e diretrizes para a gestão de dados pessoais e propor sua regulamentação;

III - supervisionar a execução dos planos, dos projetos estratégicos e ações aprovadas para viabilizar a implantação das diretrizes previstas na LGPD;

IV - prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com diretrizes estabelecidas na LGPD e nas normas internas;

V - promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos;

VI - sugerir medidas de transparência do tratamento de dados;

VII - analisar a disponibilização no sítio eletrônico do PJMA de fácil acesso aos(às) usuários(as), informações básicas sobre aplicação da LGPD, incluindo os requisitos para o tratamento legítimo de dados, as obrigações dos controladores de dados e os direitos dos(as) titulares;

VIII - analisar o plano de ação para adequação da LGPD;

IX - apresentar proposta de disponibilização pública dos registros de tratamentos de dados pessoais;

X - orientar os(as) usuários(as) do PJMA, a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

4.2 Encarregado(a) pelo Tratamento de Dados Pessoais

São responsabilidades do(a) encarregado(a) pelo tratamento de dados pessoais:

I - aceitar reclamações e comunicações dos(as) titulares de dados pessoais, prestar esclarecimentos e adotar as providências necessárias;

II - receber comunicações da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e adotar as providências necessárias;

III - atender as demais atribuições definidas em normas complementares publicadas pelo PJMA, conforme orientação da ANPD;

IV - apoiar o CGPD em suas deliberações;

V - identificar e avaliar as principais ameaças à proteção de dados, bem como propor e, quando aprovado, apoiar a implantação de medidas corretivas para mitigação dos riscos;

VI - tomar as ações cabíveis para se fazer cumprir os termos desta norma;

VII - apoiar a gestão das violações de dados pessoais, garantindo tratamento adequado e comunicando, em prazo razoável, a ANPD e os(as) titulares afetados(as) pela violação sempre que esta representar risco ou dano relevante aos(às) titulares.

4.3 Diretoria de Informática e Automação (DIA)

São responsabilidades da Diretoria de Informática e Automação:

I - adotar medidas de segurança, técnicas e/ou administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado, conforme padrões mínimos recomendados pela ANPD.

4.4 Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR)

São responsabilidades da ETIR:

I - realizar o tratamento de incidentes de segurança da informação que envolvam o tratamento de dados pessoais, garantindo sua detecção, contenção, eliminação e recuperação dentro de um prazo razoável;

II - apoiar o(a) encarregado(a) pelo tratamento de dados pessoais na comunicação à ANPD e ao(à) titular dos dados em casos de ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos(às) titulares.

4.5 Usuários(as)

São responsabilidades dos(as) usuários(as) da informação do PJMA:

I - ler, compreender e cumprir integralmente os termos da norma de proteção de dados pessoais, bem como os procedimentos que dela poderão decorrer;

II - encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a norma de proteção de dados pessoais e seus procedimentos ao(à) encarregado(a) pelo tratamento de dados pessoais ou, quando pertinente, ao Comitê Gestor de Proteção de Dados Pessoais;

III - comunicar ao(à) encarregado(a) qualquer evento que viole esta norma ou coloque em risco os dados pessoais tratados pelo PJMA;

IV - responder pela inobservância da norma de proteção de dados pessoais e procedimentos correlatos ao assunto, assegurado o contraditório e a ampla defesa.

5. INFRAÇÕES E PENALIDADES

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

6. REVISÕES

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

7. APROVAÇÃO

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

ANEXO XV
NORMA DE GESTÃO DE RISCO DE SEGURANÇA DA INFORMAÇÃO

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
Resolução nº 44/2022-GP	

Versionamento:

Versão:	1.0
Data:	02/05/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	14/08/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A gestão de riscos é uma metodologia contínua, que consiste no conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar riscos que poderão afetar as rotinas do Poder Judiciário do Estado do Maranhão (PJMA) nos níveis estratégico, tático e operacional.

Esta norma obedecerá ao escopo definido na Política de Segurança da Informação (PSI) e deverá observar, no que couber, as diretrizes que constam na Resolução GP nº 44/2022 ou posterior que a substitua.

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

2. OBJETIVOS

Contextualizar e identificar os riscos.

Analisar e estabelecer ordem prioritária dos riscos.

Avaliar e priorizar as ações para reduzir a ocorrência dos riscos.

Tratar periodicamente os riscos.

Monitorar os riscos.

Comunicar os riscos aos responsáveis.

Envolver as partes interessadas nas decisões de gestão de riscos.

Coletar informações de forma a melhorar a abordagem da gestão de riscos.

3. DIRETRIZES

Sugere-se que o processo de gestão de riscos de segurança da informação observe as seguintes diretrizes:

I - ser parte integrante dos processos organizacionais de Tecnologia da Informação e Comunicação (TIC);

II - ser parte da tomada de decisões;

III - ser sistemático, estruturado e oportuno;

IV - ser baseado nas melhores informações disponíveis;

V - considerar fatores humanos e culturais;

VI - ser transparente e inclusivo;

VII - ser dinâmico, interativo e capaz de reagir às mudanças tempestivamente;

VIII - contribuir para a melhoria contínua do PJMA.

O processo de gestão de riscos será baseado nos conceitos de governança corporativa, na norma ABNT NBR ISO/IEC 27005 e alinhado ao modelo denominado PDCA (Plan-Do-Check-Act).

4. GESTÃO DE RISCO

A gestão de riscos de segurança da informação deverá apoiar as unidades administrativas e/ou judiciais (organizacionais) do PJMA no sentido de:

I - aprimorar o processo de tomada de decisão, com o propósito de incorporar a visão de riscos em conformidade com as melhores práticas de mercado;

II - melhorar a alocação de recursos;

III - aprimorar os controles internos;

IV - alinhar a tolerância aos riscos e à estratégia adotada;

V - resguardar a alta administração e os(as) gestores(as) quanto à tomada de decisão e à prestação de contas;

VI - identificar, avaliar e reagir às oportunidades e ameaças; e

VII - melhorar a eficiência operacional por meio do gerenciamento de riscos.

4.1 Avaliação de Risco

O processo de avaliação de risco será coordenado pelo(a) gestor(a) de risco, sendo necessário que o(a) mesmo(a) tenha responsabilidade e autoridade compatíveis com a execução das atividades relativas à gestão de risco.

O primeiro passo será estabelecer o contexto no que se refere ao entendimento do ambiente em que o(a) gestor(a) de risco estará inserido(a). Em seguida, o(a) gestor(a) deverá identificar os ativos e/ou processos que poderão ter os princípios da segurança da informação afetados no âmbito do PJMA e associá-los aos seus respectivos riscos.

No passo seguinte, o(a) gestor(a) de risco associará as ameaças e vulnerabilidades para cada identificação realizada. Todo ativo e/ou processo poderá estar associado a várias ameaças e cada ameaça poderá estar relacionada a várias vulnerabilidades. Existem exemplos de ameaças e vulnerabilidades disponíveis na norma ABNT NBR ISO/IEC 27005, porém o(a) gestor(a) de risco terá a flexibilidade de

associar os ativos e/ou processos com outras ameaças e vulnerabilidades identificadas e não catalogadas.

Em seguida, o(a) gestor(a) de risco deverá analisar os impactos (Quadro 1) decorrentes de cada combinação das ameaças e vulnerabilidades, as quais estarão associadas a cada mapeamento realizado, caso o risco identificável se concretize:

Insignificante	**1**	Impacto mínimo nos objetivos do processo.
Menor	**2**	Impacto pequeno nos objetivos do processo.
Moderado	**3**	Impacto moderado nos objetivos do processo, porém recuperável.
Significativo	**4**	Impacto significativo nos objetivos do processo, de difícil reversão.
Forte	**5**	Impacto catastrófico nos objetivos do processo, de forma irreversível.

Quadro 1: Escala de impacto

Após a avaliação do impacto, é necessário avaliar a probabilidade (Quadro 2) de ocorrência de tal risco, ou seja, a probabilidade de uma ameaça explorar a vulnerabilidade:

Raro	**1**	Em situações excepcionais o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.
Improvável	**2**	De forma inesperada ou casual o evento poderá ocorrer, pois as circunstâncias indicam pouca possibilidade.
Possível	**3**	De alguma forma o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.
Provável	**4**	De forma esperada o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.
Quase certo	**5**	De forma garantida o evento ocorrerá, pois as circunstâncias indicam claramente essa possibilidade.

Quadro 2: Escala de probabilidade

Ao inserir os valores de impacto (I) e probabilidade (P), o nível de risco (R) será

calculado automaticamente multiplicando os dois valores (P x I). Os controles de segurança já existentes deverão ser levados em consideração no processo de avaliação de risco.

A matriz de risco (Quadro 3), representa os possíveis resultados da combinação das escalas de probabilidade e impacto (P x I), determinando o nível de risco (R):

		PROBABILIDADE x IMPACTO (P x I)				
PROBABILIDADE	Quase certo (5)					
	Provável (4)					
	Possível (3)					
	Improvável (2)					
	Raro (1)					
		Insignificante (1)	Menor (2)	Moderado (3)	Principal (4)	Forte (5)
		IMPACTO				

Quadro 3: Matriz de riscos

Vale destacar que quanto maior a probabilidade e o impacto, maior será a medida de risco. Desse modo, com base nos níveis de impacto e probabilidade será estabelecido o nível de criticidade (Quadro 4) dos riscos identificados:

CRITICIDADE
Menor
Moderada
Maior
Severa

Quadro 4: Criticidade do risco

Diante disso, o(a) gestor(a) de risco deverá avaliar os riscos, determinando se são aceitáveis ou se requerem tratamento. Os riscos classificados com as criticidades “menor” e “moderada” serão considerados aceitáveis e deverão ser monitorados constantemente pelo(a) gestor(a). Enquanto os riscos classificados com as criticidades “maior” e “severa” serão considerados inaceitáveis e deverão ser tomadas ações para tratá-los.

4.2 Tratamento de Risco

O tratamento de risco envolverá a escolha de estratégias para alterar o nível de cada risco identificado, bem como o desenvolvimento de planos de tratamento que, uma vez executados, resultarão na implementação de novos controles internos ou na modificação dos controles existentes.

As opções de tratamento de riscos incluem evitar, reduzir ou mitigar, transferir ou compartilhar e aceitar ou tolerar o risco. Uma ou mais opções de tratamento deverão ser selecionadas para riscos classificados com criticidade “maior” e/ou “severa”. São elas:

I - evitar o risco: decide-se não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

II - reduzir ou mitigar o risco: adotar ações para reduzir a probabilidade ou a consequência negativa associada a um risco. Exemplo: adoção de controles de segurança;

III - transferir ou compartilhar os riscos: o ônus associado a um risco é compartilhado com outra entidade. Exemplo: contratação de seguros, terceirização de atividades, etc.;

IV - aceitar ou tolerar o risco: assumem-se as responsabilidades caso o risco se materialize. Esse item só será permitido se outras opções de tratamento tiverem custo maior do que o impacto potencial.

Deve-se entender, que o apetite pelo risco, definido como a quantidade de risco que uma organização está disposta a buscar ou aceitar, poderá variar de organização para organização. São fatores que afetam o apetite pelo risco de uma organização:

tamanho, complexidade e setor. Convém que o apetite pelo risco seja definido e regularmente analisado, criticamente, pela Alta Administração do PJMA.

Diante disso, o(a) gestor(a) de risco deverá avaliar o custo-benefício de cada opção de tratamento e definir as ações prioritárias a serem implementadas, bem como, o prazo de execução e avaliação dos resultados obtidos.

No caso da opção pelo item II acima, poderá ser necessário avaliar o novo valor de impacto e probabilidade no processo de tratamento de risco, a fim de avaliar a eficácia dos controles implementados.

O tratamento de risco relacionado aos processos terceirizados deverá ser abordado por meio dos contratos estabelecidos juntos às partes interessadas.

4.3 Monitoramento dos Riscos

O(A) gestor(a) de risco deverá monitorar, detectar falhas, rever e atualizar os processos de avaliação e tratamento de risco. Cada gestor(a) estabelecerá indicadores de acompanhamento e informes dos planos de ação instituídos. Após concretizados, os riscos e controles deverão ser reavaliados e revistos ao longo do tempo para identificar preventivamente o surgimento de riscos novos ou emergentes.

Os riscos deverão ser monitorados e analisados criticamente, a fim de verificar regularmente, no mínimo, as seguintes mudanças:

a) nos critérios de avaliação e aceitação dos riscos;

b) no ambiente;

c) nos ativos e/ou processos;

d) nos fatores de risco (ameaça, vulnerabilidade, probabilidade e impacto).

A revisão será realizada pelo menos uma vez por ano, ou com maior frequência no caso de mudanças organizacionais significativas, nas tecnologias utilizadas, nos objetivos de negócio ou no ambiente de negócios do PJMA.

4.4 Registro e Comunicação

O(A) gestor(a) de risco deverá registrar os resultados da avaliação e tratamento de risco dos ativos sob sua responsabilidade e todas as revisões ou evoluções

subsequentes.

A comunicação sobre os riscos deverá ser realizada de forma clara, objetiva e eficiente, garantindo que as informações sejam compartilhadas com as partes envolvidas e interessadas.

5. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

5.1 Gestor(a) de Risco

Compete ao(à) gestor(a) de risco:

I - realizar a escolha dos ativos e/ou processos que terão os riscos gerenciados e tratados;

II - propor os níveis aceitáveis de exposição ao risco;

III - definir as ações de tratamento a serem implementadas, bem como o prazo de implementação e avaliação dos resultados obtidos;

IV - implementar o plano de ação definido para o tratamento de risco dos ativos e/ou processos mapeados;

V - realizar as atividades de identificação e avaliação de riscos dos ativos e/ou processos sob sua responsabilidade;

VI - gerenciar os riscos inerentes dos ativos e/ou processos, de forma a mantê-los em nível de exposição aceitável;

VII - comunicar novos riscos que não fazem parte da relação de riscos dos ativos e/ou processos já identificados.

6. INFRAÇÕES E PENALIDADES

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

7. REVISÕES

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

8. APROVAÇÃO

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

ANEXO XVI
PLANO DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo

Versionamento:

Versão:	1.0
Data:	02/05/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	14/08/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A implantação do processo gestão de continuidade de negócios busca minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do Poder Judiciário do Estado do Maranhão (PJMA), além de recuperar perdas de ativos de Tecnologia da Informação e Comunicação (TIC) a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

A gestão de continuidade de negócios poderá envolver ações mais abrangentes do que as definidas no âmbito da gestão de segurança da informação, especialmente devido aos requisitos estratégicos de continuidade relativos às pessoas, à infraestrutura, aos processos e às atividades operacionais.

O Plano de Gestão de Continuidade de Negócios (PGCN) está limitado ao escopo das ações de segurança da informação implementadas no PJMA.

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

2. OBJETIVO

Planejar, implementar, manter e testar a prontidão do plano baseado nos objetivos e requisitos de continuidade de negócios.

3. DIRETRIZES

Orientações do Plano de Gestão de Continuidade de Negócios (PGCN).

3.1 PROCEDIMENTOS

A elaboração do PGCN envolve os seguintes procedimentos:

I - definir as atividades críticas do PJMA;

II - avaliar os riscos a que estas atividades críticas estão expostas;

III - definir as estratégias de continuidade para as atividades críticas;

IV - desenvolver e implementar os procedimentos previstos no plano de gestão de continuidade de negócios, para respostas tempestivas a interrupções;

V - realizar exercícios, testes e manutenção periódica dos procedimentos, promovendo as revisões necessárias;

VI - desenvolver a cultura de continuidade de negócios no PJMA.

Os procedimentos previstos no PGCN serão executados em conformidade com

os requisitos de segurança da informação necessários à proteção dos ativos de TIC críticos, tratando as atividades de forma abrangente, o que inclui as pessoas, os processos, a infraestrutura e os recursos de TIC.

Recomenda-se que o Plano de Gestão de Continuidade de Negócios do PJMA seja composto, no mínimo, pelos seguintes procedimentos abaixo, de acordo com as suas necessidades específicas, de forma a assegurar a disponibilidade dos ativos de TIC e a recuperação das atividades críticas.

I - Plano de Gerenciamento de Incidentes (PGI);

II - Plano de Continuidade Operacional (PCO);

III - Plano de Recuperação de Desastres (PRD).

Os planos serão executados e testados periodicamente, bem assim os resultados documentados de forma a garantir a sua efetividade.

O PJMA deverá assegurar que os contratos firmados com empresas terceirizadas e/ou prestadores de serviços, que suportem atividades críticas, contenham cláusula segundo a qual as mesmas possuam planos de continuidade dos seus negócios, bem como as evidências dos testes realizados.

5. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

5.1 Alta Administração

São responsabilidades da Alta Administração do PJMA:

I - aprovar as diretrizes estratégicas que norteiam a elaboração do Plano de Gestão de Continuidade de Negócios;

II - avaliar a relação custo/benefício das estratégias de continuidade propostas e dos planos que compõem o PGCN e decida sobre sua implementação;

III - garantir os recursos necessários para estabelecer, implementar, operar e manter o PGCN;

VI - desenvolver a cultura de Gestão de Continuidade de Negócios.

5.2 Superior Imediato(a) ou Gestor(a) da Unidade Judicial ou Administrativa

As seguintes atribuições deverão ser conferidas ao(à) superior imediato(a) ou gestor(a) da unidade onde foram identificadas atividades críticas para o PJMA:

I - propor as diretrizes estratégicas do PGCN;

II - elaborar os planos previstos no PGCN relacionados às atividades críticas;

III - avaliar a norma de gestão de riscos de segurança da informação;

IV - realizar, periodicamente, a Análise de Impacto nos Negócios (AIN);

V - administrar a contingência quando da interrupção de atividades, com base nos planos desenvolvidos;

VI - supervisionar a elaboração, implementação, testes e atualização dos planos;

VII - propor os recursos necessários para a implantação e o desenvolvimento das ações relacionadas à continuidade das atividades, bem como para a realização dos testes e dos exercícios dos planos;

VIII - avaliar e aprimorar os planos a partir dos resultados dos testes e exercícios;

IX - propor melhorias na implantação de novos controles relativos ao PGCN.

6. INFRAÇÕES E PENALIDADES

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

7. REVISÕES

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

A revisão dos planos poderá ser realizada nas seguintes situações:

I - no mínimo, uma vez por ano;

II - em função dos resultados dos testes realizados;

III - após alguma mudança significativa nos ativos de TIC, nas atividades ou em algum de seus componentes.

8. APROVAÇÃO

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

ANEXO I
GLOSSÁRIO

Versionamento:

Versão:	2.0
Data:	03/04/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	14/08/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A lista de termos com suas respectivas definições constantes neste glossário é aplicável no âmbito da Política de Segurança da Informação e de suas normas e procedimentos correlatos produzidos e/ou aprovados pelo Comitê de Governança de Segurança da Informação (CGSI) do Poder Judiciário do Estado do Maranhão (PJMA).

0-9

- **2FA:** processo de autenticação em que dois fatores de autenticação são combinados/utilizados.

A

- **Administradores(as) das cópias de segurança da informação:** servidores(as) da Coordenadoria de Infraestrutura e Telecomunicações e da Coordenadoria de Sistemas de Informação, subordinados à Diretoria de Informática e Automação.
- **Adware:** software que exibe anúncios indesejados em um dispositivo ou sistema, geralmente gerando lucro para os desenvolvedores por meio de cliques ou visualizações de anúncios.
- **Agentes de tratamento:** o controlador e o operador envolvidos no tratamento de dados.
- **Agente público externo:** toda e qualquer pessoa que exerce uma atribuição pública em sentido lato, seja ocupante de função, cargo ou emprego público.
- **Agente responsável pela ETIR:** servidor público do Poder Judiciário incumbido de chefiar e gerenciar a ETIR.
- **Algoritmo:** conjunto de regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas.
- **Alias:** endereço de encaminhamento que faz todos os e-mails endereçados a ele serem enviados para uma ou mais contas específicas. O alias em si não tem caixa de entrada, início de sessão (login) e não pode ser utilizado para enviar e-mails. Também é conhecido como apelido da conta de e-mail.
- **Alta Administração:** unidades organizacionais com poderes deliberativos ou normativos no âmbito do PJMA.
- **Ambiente corporativo:** têm-se por definição, o ambiente de trabalho de todos os servidores(as), colaboradores(as), terceirizados(as) formado por diferentes unidades judiciais e/ou administrativas do PJMA. Além disso, cada uma dessas unidades trabalha para objetivos compartilhados de acordo com os valores compartilhados do PJMA.
- **Ameaças:** conjunto de fatores externos ou causa potencial de um incidente indesejado que pode resultar em dano para o PJMA.
- **Análise de Impacto nos Negócios (AIN):** visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho do PJMA, bem como as técnicas para quantificar e qualificar esses

impactos. Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.

- **Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
- **Apetite ao risco:** nível de risco que o PJMA está disposto a aceitar para atingir os objetivos identificados no contexto analisado.
- **Aquisição de evidência**: processo de coleta e cópia das evidências de incidente de segurança em redes computacionais.
- **Área de armazenamento de dados:** trata de espaço reservado, limitado, acessível através de rede de computadores ou nuvem, onde os(as) usuários(as) podem guardar suas informações digitais, preferencialmente documentos de trabalho.
- **Ativo**: qualquer coisa que tenha valor para o PJMA, material ou não.
- **Ativo de TIC:** todo elemento que manipula e processa a informação, inclusive a própria informação, o meio em que ela é armazenada, os equipamentos com os quais ela é manuseada, transportada e descartada. Figuram como ativos, além da informação, pessoas, computadores/notebooks e seus acessórios, impressoras, servidores de rede, dispositivos de armazenamento de dados, sistemas de informação, equipamentos de conexão de rede, dispositivos e equipamentos de transmissão de dados ou quaisquer outros dispositivos que venham a processar informação ou prover acesso aos recursos computacionais.
- **Ativo de TIC crítico**: recursos computacionais que processam, armazenam e transmitem informações essenciais para que o Poder Judiciário do Estado do Maranhão alcance seus objetivos mais importantes e sensíveis no tempo, tais como aplicações, sistemas de informação, computadores, servidores de rede e equipamentos de conectividade da infraestrutura.
- **Atividades críticas**: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do PJMA, de maneira que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.
- **Auditoria**: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos.
- **Autenticação**: processo de identificação das partes envolvidas em um processo.
- **Autenticidade**: propriedade indicativa de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.
- **Autoridade Nacional de Proteção de Dados Pessoais (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018) em todo território nacional brasileiro.
- **Autorização**: processo que visa a garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso.

B

- **Backdoor:** forma de acesso não autorizado a um sistema, aplicativo ou dispositivo que evita os mecanismos normais de autenticação e segurança.
- **Banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- **Bloqueio:** refere-se a uma medida ou mecanismo de proteção temporária que impede o acesso não autorizado a recursos, sistemas, redes ou informações confidenciais.
- **Bloqueio (Norma de Proteção de Dados Pessoais):** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

C

- **Caixa de correio eletrônico corporativo ou caixa postal de correio eletrônico corporativo:** caixa de correio atribuída a um(uma) usuário(a): - magistrado(a), servidor(a) efetivo(a) ou requisitado(a), ocupante de cargo em comissão sem vínculo efetivo e/ou estagiário(a) ou a uma unidade organizacional (administrativa ou judicial) do TJMA.
- **Caixa de correio eletrônico de serviço:** caixa de correio atribuída a uma atividade específica, exercida no âmbito de uma unidade organizacional ou por um grupo de trabalho.
- **Classificação da informação:** atribuição, pela autoridade competente, de grau de sigilo dado à informação, ao documento, ao material, etc.
- **Coleta de evidências de segurança em redes computacionais:** processo de obtenção de itens físicos que contém potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Esse processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente.
- **Comitê de Crises Cibernéticas (CCC):** composto por representantes da alta administração com suporte da ETIR e de especialistas de várias áreas.
- **Comitê de Governança de Segurança da Informação (CGSI):** Comitê de trabalho multidisciplinar permanente, instituído pelo PJMA, que tem por finalidade realizar a promoção da cultura de segurança da informação, inclusive no que tange à prevenção, ao gerenciamento, ao tratamento de crises cibernéticas de forma contínua, assim como a sua investigação, estabelecendo um modelo de gestão que cria um sistema eficiente de segurança da informação em todas as suas variáveis.
- **Comitê Gestor de Proteção de Dados Pessoais (CGPD):** Comitê de trabalho multidisciplinar permanente, efetivado pelo Poder Judiciário do Estado do Maranhão, que tem por finalidade tratar questões ligadas à Proteção de Dados Pessoais.
- **Competência:** habilidade para aplicar conhecimentos e habilidades para atingir

resultados pretendidos.

- **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizada.
- **Conformidade:** preenchimento de um requisito.
- **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
- **Continuidade de serviços:** capacidade estratégica e tática do PJMA de se planejar e de responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos de TIC das atividades críticas, de forma a manter suas operações em nível aceitável, previamente definido.
- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- **Controle:** providência que modifica o risco, incluindo qualquer processo, política, dispositivo, prática ou ação.
- **Controles criptográficos:** sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração.
- **Cópia de segurança completa (full):** é realizada uma cópia completa de todos os arquivos, pastas ou volumes para destinos previamente estabelecidos.
- **Cópia de segurança diferencial:** é executada primeiro uma cópia de segurança (backup) completa com a cópia de todos os dados, e depois outras execuções subsequentes, onde serão copiados apenas os dados que foram alterados.
- **Cópia de segurança incremental:** é realizada uma cópia completa de todos os arquivos uma única vez, todas as outras cópias de segurança (backups) só carregam os dados alterados desde o último carregamento.
- **Correio eletrônico ou e-mail:** serviço de comunicação de mensagens eletrônicas entre usuários(as), composto por programas de computador e equipamentos centrais de processamento, responsáveis pelo envio e recebimento das mensagens, bem como pela administração das caixas de correio corporativa ou individual.
- **Credencial de acesso:** combinação do login e senha, utilizada, ou não, em conjunto com outro mecanismo de autenticação, que visa legitimar e conferir autenticidade ao usuário na utilização da infraestrutura e recursos de informática.
- **Credencial de acesso à rede:** combinação do login e senha, utilizada, ou não, em conjunto com outro mecanismo de autenticação, que visa legitimar e conferir autenticidade do usuário na rede corporativa do PJMA.
- **Credencial de acesso ao e-mail:** combinação do login e senha, utilizada ou não, em conjunto com outro mecanismo de autenticação, que visa legitimar e conferir autenticidade usuário(a) ou da unidade administrativa/judicial para acessar os serviços de correio eletrônico e de ambiente colaborativo do Google Workspace (armazenamento remoto, calendário, videoconferência e bate-papo).
- **Criptografia:** conjunto de princípios e técnicas empregadas para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às chaves combinadas.
- **Crise:** um evento ou série de eventos danosos que apresenta propriedades

emergentes capazes de exceder as habilidades do PJMA em lidar com as demandas de tarefas que eles geram e que apresenta implicações que afetam proporção considerável do PJMA e de seus constituintes.
- **Crise cibernética:** crise que pode ocorrer em decorrência de incidente(s) em dispositivos, serviços e redes de computadores, causando dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto do PJMA.

D

- **Dado anonimizado:** dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- **Dados pessoais:** informação relacionada à pessoa natural identificada ou identificável.
- **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **Desastre:** evento, seja previsto ou imprevisto, que causa um desvio não planejado e negativo da expectativa de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação.
- **Disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.
- **Dispositivos móveis:** equipamentos digitais que permitem a mobilidade e o acesso à internet. Pode-se citar como exemplos os celulares, smartphones e tablets.
- **Download:** termo utilizado para recebimento de arquivos através de uma rede de computadores que utiliza os padrões TCP/IP, de um computador remoto para um computador local.
- **Drive compartilhado:** pastas especiais no Google Drive que o usuário pode usar para armazenar, pesquisar e acessar arquivos com uma equipe.

E

- **Eliminação:** exclusão de dados ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
- **Encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- **Endereço eletrônico de e-mail:** é formado pelo nome de usuário (username) e o nome de domínio a que ele pertence, por exemplo, fulano.ciclano@tjma.jus.br.
- **Endereço IP (Internet Protocol):** refere-se ao conjunto de elementos

numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores.

- **Erro emergencial:** qualquer comportamento anômalo gerado pelo sistema que impeça de forma imperativa sua utilização, comprometendo a capacidade operacional de uma atividade crítica ou área do PJMA. Caso exista uma operação alternativa no sistema ou no setor que possa mitigar o erro em questão, o mesmo não será considerado emergencial.
- **Estação de trabalho:** computadores e/ou notebooks e seus respectivos acessórios utilizados pelo(a) usuário(a) para execução de suas atividades administrativas e judiciais (laborais).
- **Estratégia de continuidade de serviços:** abordagem do órgão que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou com outro incidente maior.
- **Escopo de auditoria:** extensão e fronteiras de uma auditoria.
- **Equipe de Tratamento e Resposta a Incidentes de Segurança de Cibernética (ETIR):** denominação tradicionalmente atribuída a grupos de resposta a incidentes de segurança da informação. Também conhecida como Computer Security Incident Response Team (CSIRT).
- **Evento:** ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.
- **Evidência digital:** informação ou dado armazenado ou transmitido eletronicamente, na forma binária, que pode ser reconhecida como parte de um evento.
- **Evidência de auditoria:** registros, declarações de fato ou outras informações verificáveis e relevantes para os critérios de auditoria.

F

- **Feed de ameaças:** refere-se a um serviço ou fonte de dados que fornece informações atualizadas sobre ameaças, vulnerabilidades e atividades maliciosas. Esse tipo de feed é essencial para a detecção e resposta a incidentes de segurança cibernética.

G

- **Gerenciamento de crise:** decisões e atividades coordenadas que ocorrem no PJMA durante uma crise corporativa, incluindo crises cibernéticas.
- **Gestão de continuidade:** processo de gestão global que identifica as potenciais ameaças para o PJMA e os impactos nas operações que essas ameaças, concretizando-se, poderiam causar, fornecendo e mantendo nível aceitável de serviço diante de rupturas e desafios à operação normal do dia a

dia.

- **Gestão de riscos de segurança da informação:** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e para equilibrá-los com os custos operacionais e financeiros envolvidos.
- **Gestão de segurança da informação:** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.
- **Gestor da informação:** responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades. O gestor da informação poderá ser: um(a) usuário(a), uma unidade administrativa ou judicial, um(a) superior imediato(a), qualquer pessoa que crie uma informação utilizando os ativos de TIC do PJMA.
- **Gestor(a) de riscos:** responsável por determinada unidade administrativa e/ou judicial, em seu respectivo âmbito e escopo de atuação. É considerado(a) gestor(a) de riscos os responsáveis pelos processos de trabalho, projetos e ações desenvolvidos nos níveis estratégico, tático e operacional do PJMA.
- **Gestor de segurança da informação:** responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da administração pública federal.

I

- **Impacto do risco:** efeito resultante da ocorrência do risco.
- **Incidente de segurança:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.
- **Incidente grave:** evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação.
- **Incidente de segurança da Informação:** quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de segurança da informação: confidencialidade, integridade, disponibilidade e conformidade.
- **Informação:** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato. É um ativo que tem valor para o PJMA e necessita ser adequadamente protegido.
- **Informação sigilosa:** informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado e aquela abrangida pelas demais hipóteses legais de sigilo.
- **Integridade:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

- **Internet:** sistema global de redes de computadores interligadas que utilizam um conjunto próprio de protocolos, com o propósito de servir progressivamente usuários no mundo inteiro.
- **Intranet:** ambiente de rede interna do Poder Judiciário do Estado do Maranhão, composta pelo conjunto de redes locais e seus ativos e recursos de informática utilizados para sua formação.
- **Inventário de ativos de TIC:** refere-se a um registro detalhado e abrangente de todos os ativos relacionados à Tecnologia da Informação e Comunicação no âmbito do PJMA. Esses ativos podem incluir hardware, software, equipamentos de rede, sistemas de armazenamento, bancos de dados, aplicativos, servidores, dispositivos móveis e qualquer outro componente de TIC utilizado para suportar as operações e os processos do PJMA.

L

- **Log (registro de auditoria):** registro de eventos relevantes em um dispositivo ou sistema computacional.
- **Login:** parte da credencial do usuário com prévio cadastramento através de sua matrícula ou identificador único, no sistema, software ou serviço, de modo a garantir a individualização do seu proprietário.
- **Login Único (Single Sign-On - SSO):** função de gerenciamento de acesso que permite aos(às) usuários(as) fazer o login com um único conjunto de credenciais de identidade para várias contas, software, sistemas e recursos.
- **Logoff ou Logout:** refere-se ao processo de desconexão de um(a) usuário(a) de uma sessão ativa em um determinado ativo de TIC. Quando uma usuário(a) faz logoff, todas as aplicações abertas são fechadas e todos os dados não salvos são perdidos. Isso garante que o(a) próximo(a) usuário(a) que acessar o sistema comece com uma sessão limpa e segura, sem acesso aos dados do(a) usuário(a) anterior.

M

- **Malware:** termo genérico que abrange uma ampla variedade de programas de computador projetados para causar danos, comprometer a segurança ou obter acesso não autorizado a sistemas, dispositivos ou dados de usuários(as).
- **Mensagens eletrônicas:** consiste na utilização de mensagens para estabelecer a comunicação síncrona ou assíncrona entre aplicações.
- **Metadados:** conjunto de dados estruturados que descrevem informação primária.
- **Menor privilégio:** estabelece que os(as) usuários(as) devem receber apenas as permissões mínimas necessárias para realizar suas atividades administrativas e judiciais (laborais).
- **Mineração de textos e dados:** processo de extração e análise de grandes quantidades de dados ou de trechos parciais ou integrais de conteúdo textual, a partir dos quais são extraídos padrões e correlações que gerarão informações

relevantes para o desenvolvimento ou utilização de sistemas de inteligência artificial.
- **Multi Nuvem:** empresa que implementa o serviço de vários provedores de serviço de nuvens.
- **Múltiplo Fator de Autenticação (MFA):** método de autenticação que exige que o usuário forneça dois ou mais fatores de verificação para obter acesso a um recurso, como um aplicativo, conta online ou VPN.

N

- **Não-repúdio:** refere-se a uma situação em que a autoria de uma declaração não pode ser contestada.
- **Navegadores de internet:** também conhecidos como browsers, são programas de computador que permitem que os(as) usuários(as) acessem e visualizem páginas da rede mundial de computadores. Com eles os(as) usuários(as) poderão navegar na internet, realizar pesquisas, acessar sítios eletrônicos, assistir vídeos, fazer download/upload de arquivos e muito mais.
- **Negação de serviço:** refere-se a um tipo de ataque cibernético projetado para sobrecarregar um sistema, rede ou serviço, tornando-o inacessível para usuários(as) legítimos(as). O objetivo principal de um ataque de negação de serviço é interromper ou diminuir significativamente a disponibilidade de um recurso ou serviço, prejudicando sua capacidade de responder a solicitações válidas.
- **Nível de risco:** magnitude do risco, expressa pelo produto das variáveis impacto e probabilidade.
- **Network Time Protocol (NTP):** protocolo de Tempo de Rede, que é utilizado para sincronizar os relógios dos dispositivos em uma rede de computadores. Ele permite que os dispositivos obtenham uma referência de tempo precisa e consistente, garantindo que todos os sistemas estejam sincronizados.
- **Nuvem comunitária:** infraestrutura de nuvem dedicada para uso exclusivo de uma comunidade, ou de um grupo de usuários(as) de órgãos ou de entidades não vinculados, que compartilham a mesma natureza de trabalho e obrigações, e sua propriedade e seu gerenciamento podem ser de organizações da comunidade, de terceiros ou de ambos.
- **Nuvem híbrida:** infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações.
- **Nuvem privada (ou interna):** infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos(as) usuários(as), e sua propriedade e seu gerenciamento podem ser do próprio PJMA, de terceiros ou de ambos.
- **Nuvem pública (ou externa):** infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de organizações públicas, privadas ou de ambas.

O

- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

P

- **Patches:** refere-se a uma modificação ou melhoria aplicada a um software, sistema operacional, firmware ou qualquer outro tipo de programa de computador. Com o objetivo de fornecer correções de bugs, melhorias de desempenho, novos recursos ou para abordar questões de segurança.
- **Pentest ou penetration testing:** também conhecido como "teste de invasão" ou "teste de intrusão", o pentest é uma atividade realizada para avaliar a segurança de um sistema, rede ou aplicativo, simulando ataques reais que um potencial invasor poderia explorar.
- **Pessoa natural:** todo ser humano, nascido com vida.
- **Plano de Continuidade Operacional (PCO):** plano de ação integrante do PGCN que contém os procedimentos e informações necessárias para que se atue no contingenciamento do ativo impactado que suporta o processo de negócio crítico, após o tempo limite ter sido atingido, objetivando restaurar o serviço a um nível mínimo aceitável.
- **Plano de Gerenciamento de Incidentes (PGI):** plano de ação integrante do PGCN que contém os procedimentos e informações necessárias na identificação e resposta ao incidente, visando restaurar o serviço ao nível normal através da recuperação do ativo em produção, dentro de um tempo limite previamente definido.
- **Plano de Gestão de Continuidade de Negócios (PGCN):** processo abrangente e contínuo de gestão e governança que identifica ameaças potenciais e, caso as mesmas venham a se concretizar, visa a orientação sobre como responder a um incidente e a recuperar e restaurar a entrega de serviços a fim de garantir a continuidade de negócios.
- **Plano de Recuperação de Desastre (PRD):** plano de ação integrante do PGCN que contém os procedimentos e informações necessárias sobre como atuar para restaurar o serviço ao nível normal através da recuperação do ativo principal que estava fora de operação.
- **Política de Segurança da Informação (PSI):** conjunto de diretrizes, podendo incluir normas, procedimentos e políticas auxiliares, que regulamentam o uso adequado dos ativos e/ou recursos de TIC.
- **Preservação de evidência de incidentes em redes computacionais:** processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações.
- **Prestador de serviço:** toda e qualquer pessoa que possui uma relação

contratual ou de convênio com o Judiciário.

- **Probabilidade do risco:** possibilidade de ocorrência do risco.
- **Procedimento:** conjunto de ações sequenciadas e ordenadas para o atingimento de um determinado fim.
- **Processo de elaboração, acompanhamento e revisão da PSI:** processo de gestão de TI que visa instituir os procedimentos para elaboração, revisão e acompanhamento do cumprimento das diretrizes da PSI.
- **Projeto Open Web Application Security Project (OWASP):** projeto aberto de segurança em aplicações web. É uma fundação sem fins lucrativos dedicada à melhora da segurança na internet.
- **Pseudoanonimização:** processo pelo qual os dados pessoais não mais se relacionam diretamente com uma pessoa identificável (por exemplo, mencionando seu nome), mas não é anônimo, porque ainda é possível, com informações adicionais, que são mantidas separadamente, identificar uma pessoa.

Q

- **Quebra de segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

R

- **Ransomware:** tipo de malware que criptografa arquivos em um dispositivo ou sistema, impedindo o acesso do usuário a esses arquivos. Os atacantes exigem um resgate em troca da chave de descriptografia.
- **Recursos de TIC:** são todos os recursos tecnológicos que o PJMA utiliza para processar, armazenar, transmitir e receber informações. Isso inclui computadores, servidores de rede, dispositivos móveis, dispositivos de armazenamento, dispositivos de rede e todos os tipos de equipamentos de TIC.
- **Rede de dados corporativa:** é a infraestrutura de rede que permite que o PJMA conecte seus recursos de TIC e forneça acesso seguro e confiável a esses recursos para seus funcionários(as) e usuários(as) autorizados(as).
- **Rede local:** é considerada como o ambiente de rede interna de cada edificação do Poder Judiciário do Estado do Maranhão, composta por seus ativos e recursos de informática, assim como seus meios físicos e lógicos de conexão.
- **Rede Privada Virtual (Virtual Private Network – VPN):** é um serviço que cria uma conexão on-line segura e criptografada, na qual permite que um(a) usuário(a) envie e receba dados com segurança pela internet.
- **Relatório de impacto à proteção de dados pessoais:** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

- **Releases:** disponibilização de uma nova versão de um sistema para uso, normalmente aplicada a melhorias e evoluções.
- **Requisito:** necessidade ou expectativa declarada, geralmente implícita ou obrigatória.
- **Resiliência:** poder de recuperação ou capacidade do PJMA resistir aos efeitos de um incidente.
- **Resumo criptográfico:** é um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho desta, gera resultado único e de tamanho fixo, também chamado de hash.
- **Risco:** combinação da probabilidade e impacto de um evento ocorrer.
- **Risco de Tecnologia da Informação e Comunicação (TIC):** evento capaz de afetar positiva ou negativamente os objetivos do PJMA nos níveis estratégico, tático e operacional.
- **Robustez:** capacidade do PJMA de resistir aos efeitos de um incidente de continuidade de negócios.

S

- **Sala de situação:** local a partir do qual serão geridas as situações de crise cibernética do PJMA.
- **Segurança cibernética:** é um conjunto de práticas que protege informações armazenadas em computadores e aparelhos de computação e transmitidas através das redes de comunicação, como a Internet.
- **Segurança da Informação (SI)**: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações.
- **Senha:** parte da credencial do(a) usuário(a), formada por um conjunto de caracteres alfabéticos, numéricos ou alfanuméricos, de caráter pessoal, confidencial e intransferível, para uso nos sistemas, softwares e serviços de informática.
- **Serviço de correio eletrônico corporativo:** sistema de mensagens utilizado para criar, encaminhar, responder, transmitir, arquivar, manter, copiar, ler ou imprimir informações, com o propósito de estabelecer comunicações, relacionadas com as funções institucionais do TJMA, entre redes de computadores, entre pessoas e entre grupo de pessoas.
- **Serviço de Diretório (Active Directory - AD):** é um conjunto de atributos sobre recursos e serviços existentes na rede, como por exemplo, usuários(as), computadores, impressoras, servidores entre outros recursos de rede.
- **Sistema de Gestão de Segurança da Informação (SGSI)**: políticas, procedimentos, manuais e recursos associados e atividades coletivamente gerenciadas pelo PJMA na busca de proteger seus ativos de informação.
- **Sistema de inteligência artificial:** sistema computacional, com graus diferentes de autonomia, desenhado para inferir como atingir um dado conjunto de objetivos, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento, por meio de dados de entrada

provenientes de máquinas ou humanos, com o objetivo de produzir previsões, recomendações ou decisões que possam influenciar o ambiente virtual ou real.
- **Software:** qualquer programa ou conjunto de programas de computador.
- **Software malicioso:** termo coletivo para descrever programas com intenções maliciosas, incluindo vírus, worms, trojans ou qualquer outra praga digital que ponham em risco a confidencialidade, integridade e disponibilidade das informações.
- **Spam:** termo utilizado para referir-se a mensagens não solicitadas, enviadas a um grande número de indivíduos e com conteúdo geralmente comercial, fraudulento ou impróprio.
- **Spyware:** software malicioso que coleta informações sobre a atividade do(a) usuário(a), como histórico de navegação, senhas, dados pessoais e informações bancárias, sem o consentimento do(a) mesmo(a).
- **Suporte criptográfico:** dispositivo portátil especializado – composto de processador eletrônico criptográfico assimétrico – que contém o certificado digital e é inserido no computador para efetivar a assinatura digital.

T

- **Tecnologia da Informação e Comunicação (TIC):** ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações.
- **Tempo Objetivo de Recuperação (RTO):** período de tempo após um incidente em que o processo de negócio pode ficar interrompido sem causar impacto.
- **Titular:** pessoa natural a quem se referem os dados pessoais que são objetos de tratamento.
- **Tolerância a risco:** margem que a administração permite aos gestores de suportar o impacto de determinado risco em troca de benefícios específicos, ainda que esse seja superior ao “apetite ao risco” determinado pelo PJMA.
- **Transferência internacional de dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.
- **Trabalho remoto:** refere-se a todas as formas de trabalho fora do escritório, incluindo ambientes de trabalho não tradicionais, como aqueles referidos como: “local de trabalho flexível", “trabalho remoto” e “trabalho virtual”.
- **Tratamento da informação classificada:** conjunto de ações referentes à produção, à recepção, à classificação, à utilização, ao acesso, à reprodução, ao transporte, à transmissão, à distribuição, ao arquivamento, ao armazenamento, à eliminação, à avaliação, à destinação ou ao controle de informação classificada em qualquer grau de sigilo.
- **Tratamento de dados pessoais:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- **Trojans:** programas que se disfarçam como softwares legítimos, mas possuem

funcionalidades maliciosas ocultas. Eles podem permitir o acesso remoto não autorizado, roubar informações confidenciais ou abrir portas para outros malwares.

U

- **Upload:** termo utilizado para envio de arquivos através de rede de computadores que utiliza os padrões TCP/IP, de um computador local para um computador remoto (ação inversa do download).
- **Uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.
- **Usuário(a):** termo que se refere ao magistrado(a), servidor(a) efetivo(a) ou requisitado(a) e ocupante de cargo em comissão sem vínculo efetivo do PJMA. Prestador(a) de serviço, colaborador(a), terceirizado(a), agente público(a) externo(a) e estagiário(a) será considerado(a) usuário(a), em caráter temporário, se for previamente autorizado(a) por procedimento formal.

V

- **Violação de dados pessoais:** situação em que dados pessoais são processados violando um ou mais requisitos relevantes de proteção da privacidade.
- **Vírus:** programas que se replicam e se espalham anexando-se a outros arquivos ou programas. Eles são capazes de se auto-duplicar e se espalhar para outros dispositivos quando os arquivos infectados são compartilhados.
- **Vulnerabilidades:** conjunto de fatores internos ou causa potencial de um incidente indesejado que pode resultar em risco para o PJMA, os quais podem ser evitados por uma ação interna de segurança da informação.

W

- **Worms:** programas maliciosos independentes que se espalham por redes e sistemas, explorando vulnerabilidades e explorando mecanismos de distribuição, como e-mails ou mensagens instantâneas.

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

Pelo presente instrumento, eu _ , matrícula _ _ _ _ _ _ _ _ _ e lotado(a) no(a) _ deste órgão, DECLARO, sob pena das sanções cabíveis nos termos da Resolução 39/2023 ou posterior que a substitua, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito do Poder Judiciário do Estado do Maranhão (PJMA), que assumo as responsabilidades por:

I - tratar o(s) ativo(s) de Tecnologia da Informação e Comunicação (TIC) como patrimônio do Poder Judiciário do Estado do Maranhão (PJMA);

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, nos interesses dos serviços do PJMA;

III - utilizar as credenciais, as permissões de acesso concedidas e os ativos e/ou recursos de TIC em conformidade com a legislação vigente e com as normas específicas do PJMA;

IV - acessar a rede corporativa de dados, computadores/notebooks, internet e/ou e-mail, somente com autorização, por necessidade de serviço ou por determinação expressa do(a) superior imediato(a), realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições publicadas;

V - não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior, e desde que não contrarie as legislações vigentes;

VI - manter a necessária cautela quando da exibição de dados em tela, impressos ou gravados em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

VII - não me ausentar sem bloquear a estação de trabalho, sem encerrar a sessão de uso do navegador, bem como encerrar a sessão do cliente de correio (e-mail), garantindo assim a impossibilidade de acessos indevidos por terceiros;

VIII - não revelar a(s) senha(s) da(s) credencial(is) de acesso à rede, correio eletrônico (e-mail), sistemas e/ou acesso remoto a ninguém e tomar o máximo de cuidado para que essa senha permaneça somente sob meu conhecimento;

IX - responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha(s) credencial(is) ou das transações a que tenha acesso, garantidos a ampla defesa e o contraditório.

Estou ciente e de acordo que, tanto os ativos e/ou recursos de TIC, quanto a infraestrutura tecnológica do PJMA somente poderão ser utilizados para fins exclusivamente profissionais e relacionados às atividades fins do PJMA.

Estou ciente de que, de acordo com as leis vigentes, é realizado o monitoramento de todos os acessos e comunicações realizados por meio da infraestrutura tecnológica do PJMA.

Tenho conhecimento e aceito os termos, as diretrizes, os conceitos e as condições de uso da Política de Segurança da Informação do Poder Judiciário do Estado do Maranhão, bem como das demais normas e procedimentos de Segurança da Informação e Privacidade de Dados necessários ao meu trabalho, que se encontram disponíveis no portal corporativo, às quais li na íntegra e me comprometo a cumprir integralmente.

São Luís, MA, ___de _____de _____.

_____
Assinatura do(a) servidor(a)

Desembargador JAMIL DE MIRANDA GEDEON NETO
Matrícula 53991

FRANCISCO SOARES REIS JÚNIOR
Juiz Auxiliar de Entrância Final
Gabinete do Juiz Auxiliar Francisco Soares Reis Júnior
Matrícula 93856

JOSÉ JORGE FIGUEIREDO DOS ANJOS JUNIOR
Diretor da Secretaria da CGJ
Gabinete do Diretor da Secretaria da CGJ
Matrícula 155846

CLÁUDIO HENRIQUE CARNEIRO SAMPAIO
Diretor de Informática e Automação
Diretoria de Informática e Automação
Matrícula 99176

LAÉRCIO LEÃO AMARAL
Diretor Judiciário
Diretoria Judiciária
Matrícula 128835

MILENA VIEIRA DE OLIVEIRA
Diretora de Recursos Humanos
Diretoria de Recursos Humanos
Matrícula 99671

ANDRE MENEZES MENDES
Diretor do FERJ
Diretoria do FERJ
Matrícula 114819

ALEXANDRE MAGNO DE SOUSA NUNES
Diretor de Segurança Institucional e Gabinete Militar
Diretoria de Segurança Institucional e Gabinete Militar

Matrícula 145979

CÉLIA REGINA PEREIRA DA SILVA
Diretora Financeira
Diretoria Financeira
Matrícula 99382

JUREMA MAMEDE DE PAIVA SANTOS
Diretora de Auditoria Interna
Diretoria de Auditoria Interna
Matrícula 107318

KEILA FONSECA DA SILVA
Diretora Administrativa
Diretoria Administrativa
Matrícula 204057

CARLOS ANDERSON DOS SANTOS FERREIRA
Diretor Geral da Secretaria do Tribunal de Justiça
Gabinete do Diretor Geral
Matrícula 193474

MAYCO MURILO PINHEIRO
Diretor de Engenharia e Arquitetura
Diretoria de Engenharia e Arquitetura
Matrícula 114389

ISABELLA CAROLINA SILVA E SILVA
Assessora Chefa da Assessoria de Comunicação da Presidência
Assessoria de Comunicação da Presidência
Matrícula 198986

Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 05/09/2023 16:07 (CÉLIA REGINA PEREIRA DA SILVA)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 05/09/2023 16:10 (MILENA VIEIRA DE OLIVEIRA)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 05/09/2023 17:36 (ISABELLA CAROLINA SILVA E SILVA)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 05/09/2023 17:37 (CLÁUDIO HENRIQUE CARNEIRO SAMPAIO)
Documento assinado. SÃO LUÍS - ENTRÂNCIA FINAL, 05/09/2023 20:15 (FRANCISCO SOARES REIS JÚNIOR)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 06/09/2023 07:46 (ALEXANDRE MAGNO DE SOUSA NUNES)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 06/09/2023 08:22 (ANDRE MENEZES MENDES)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 06/09/2023 12:56 (CARLOS ANDERSON DOS SANTOS FERREIRA)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 06/09/2023 17:59 (MAYCO MURILO PINHEIRO)

Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 08/09/2023 16:36 (KEILA FONSECA DA SILVA)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 11/09/2023 10:02 (LAÉRCIO LEÃO AMARAL)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 11/09/2023 10:21 (JUREMA MAMEDE DE PAIVA SANTOS)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 12/09/2023 15:07 (JOSÉ JORGE FIGUEIREDO DOS ANJOS JUNIOR)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 15/09/2023 12:01 (JAMIL DE MIRANDA GEDEON NETO)