ATA-GabDesJMGN - 22024
Código de validação: CC994226BA

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

Ata da 8ª Reunião de 2024 (22/04/2024)

Aos vinte e dois dias do mês de abril do ano de dois mil e vinte e quatro, na sala do Pleninho do Tribunal de Justiça do Estado do Maranhão e na sala de videoconferência da DIA, utilizando a ferramenta ZOOM, às 11:00h, sob a presidência do Desembargador Jamil de Miranda Gedeon Neto, reuniram-se os(as) membros(as) do Comitê de Governança de Segurança da Informação (CGSI) e do Comitê Gestor de Proteção de Dados (CGPD), instituídos, respectivamente, pela Resolução-GP nº 14/2024, do Tribunal de Justiça do Estado do Maranhão (TJMA).

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 em exercício BRUNO JORGE PORTELA SILVA COUTINHO (Diretoria de Informática e Automação - membro do CGSI e CGPD), do diretor ALEXANDRE MAGNO DE SOUSA NUNES (Diretoria de Segurança Institucional e Gabinete Militar - membro do CGSI e CGPD), da diretora MILENA VIEIRA DE OLIVEIRA (Diretoria de Recursos Humanos - membra do CGSI e CGPD).

Estavam ausentes os(as) membros(as): - a diretora JUREMA MAMEDE DE PAIVA SANTOS (Diretoria de Auditoria Interna - membra do CGPD), substituída por PATRÍCIA FONSECA PEREIRA DOS SANTOS, a diretora CÉLIA REGINA PEREIRA DA SILVA (Diretoria Financeira - membra do CGPD), substituída por CRISTIANO DE JESUS SOUSA DE ABREU, a diretora MÁIRA AZEVEDO DA CRUZ VIDAL (Diretoria do FERJ - membro do CGPD), substituída por FABRICYO CASTRO COTRIM.

Não enviaram substitutos(as) ou representantes o diretor JONAS JÚLIO FERREIRA FRANCA (Diretoria Judiciária - membro do CGPD), a diretora KEILA FONSECA DA SILVA (Diretoria Administrativa - membra do CGSI e CGPD), o diretor CARLOS ANDERSON DOS SANTOS FERREIRA (Diretoria Geral - membro do CGSI), o diretor MAYCO MURILO PINHEIRO (Diretoria de Engenharia - membro do CGPD) e a assessora ISABELLA CAROLINA SILVA E SILVA (Assessoria de Comunicação da Presidência - membra do CGSI).

Como convidados, registraram-se as presenças da Sra. TICIANY GEDEON MACIEL PALACIO, do Sr. JAIRO FERREIRA ROCHA (Diretoria de Informática e Automação), do Sr. LEANDRO CAVALCANTE MENDONCA LIMA (Divisão de Serviços de TI), do Sr. ANDERSON MAIA DE LIMA CARVALHO (Diretoria de Informática e

Automação), do Sr. GIVANILDO MARQUES (Coordenadoria de Atendimento ao Usuário), do Sr. MARCOS AURÉLIO FERREIRA NAVA (Divisão de Serviços de TI) e do Sr. HALLYSON CARLOS (INTEROP).

A apresentação foi conduzida inicialmente pelo Desembargador Jamil de Miranda Gedeon Neto e pelo Juiz Francisco Soares Reis Júnior com participação do servidor Jairo Ferreira Rocha. A reunião seguiu com a pauta abaixo:

- **Segurança da Informação - deliberação e aprovação dos documentos abaixo relacionados:**

a. 2ª (segunda) versão das normas da Política de Segurança da Informação:

ANEXO I - Glossário;
ANEXO II - Norma de Controle de Acesso e Gestão de Identidade;
ANEXO III - Norma de Classificação e Tratamento da Informação;
ANEXO IV - Norma de Segurança Física no Ambiente de TIC;
ANEXO V - Norma de Gestão de Ativos;
ANEXO VI - Norma de Uso Aceitável de Ativos;
ANEXO VII - Norma de Gestão de Incidentes de Segurança da Informação;
ANEXO VIII - Norma de Cópias de Segurança da Informação;
ANEXO XI - Norma de Gestão de Vulnerabilidades Técnicas;
ANEXO XII - Norma de Desenvolvimento Seguro;
ANEXO XIII - Norma de Proteção de Dados Pessoais.

b. Guias de uso para usuários(as): Acesso à Internet, Correio Eletrônico Corporativo, Ativos de TIC, Proteção de Dados Pessoais e Controle de Acesso e Gestão de Identidade.

- **Proteção de Dados Pessoais - deliberação e aprovação dos documentos abaixo relacionados:**

a. Plano de Comunicação e seus Anexos:

ANEXO I - TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE 2023/2024;
ANEXO II - RELATÓRIO DE ATIVIDADES DA ADEQUAÇÃO LGPD – PJMA 2023/2024.

b. Cartilha da LGPD;
c. Resumo das ações da empresa de consultoria - FAC Tecnologia.

Na reunião, foram esclarecidos alguns pontos da versão 2.0 das normas e do glossário, e abriu-se a votação, tendo sido aprovadas por unanimidade.

O Sr. Givanildo pediu a palavra e pontuou sobre a desativação automática implantada no PJe e SISCONDJ a partir do sistema MentoRH.

O MM. Francisco Soares Reis Júnior sugeriu criar um Grupo de Trabalho para aprimorar o controle de acesso dos(as) magistrados(as).

Em seguida, foram apresentados os 05 (cinco) guias de uso das normas para os(as) usuários(as), os quais foram colocados em pautas para votação e aprovados por unanimidade.

O MM. Francisco Soares Reis Júnior apresentou o Plano de Comunicação e seus Anexos, juntamente com a Cartilha da LGPD, e os submeteu para votação, os quais também foram aprovados por unanimidade. Além disso, foram destacadas as ações realizadas pela empresa FAC Tecnologia e delineados os próximos passos. Ressaltou ainda a necessidade dos Comitês possuírem uma secretária e de uma melhor estruturação para execução das atividades pertinentes aos Comitês.

O Sr. Jairo Ferreira Rocha sugeriu que os guias e a cartilha sejam submetidos para Assessoria de Comunicação da Presidência para revisão final antes da publicação.

Por fim, após a saída do Desembargador Jamil de Miranda Gedeon Neto, o MM. Francisco Reis encerrou a apresentação e franqueou espaço para os(as) demais membros(as) se manifestarem e não tendo mais assuntos a serem tratados, agradeceu a todos e todas e encerrou a reunião, tendo eu, Bruno Jorge Portela Silva Coutinho, designado secretário ad hoc dos Comitês, lavrado a presente ata que, depois de lida e aprovada, vai assinada pelos(as) membros(as) dos CGSI e CGPD.

**PALÁCIO DA JUSTIÇA "CLÓVIS BEVILÁCQUA" DO ESTADO DO MARANHÃO**

São Luís, 24 de abril de 2024.

# ANEXO I
# GLOSSÁRIO

## Versionamento:

| | |
|---|---|
| Versão: | 2.0 |
| Data: | 22/04/2024 |
| Criada por: | Grupo de Trabalho Técnico SGSI - DIA |
| Aprovada por: | Comitê de Governança de Segurança da Informação |
| Aprovada em: | 22/04/2024 |

## Histórico de mudanças:

| Data | Versão | Alterado por | Descrição das alterações |
|---|---|---|---|
| 14/08/2023 | 1.0 | | |
| 22/04/2024 | 2.0 | GTT do CGSI | Atualização da lista de termos. |
| | | | |
| | | | |
| | | | |

## 1. INTRODUÇÃO

A lista de termos com suas respectivas definições constantes neste glossário é aplicável no âmbito da Política de Segurança da Informação, seus normativos anexos e procedimentos correlatos produzidos e/ou aprovados pelo Comitê de Governança de Segurança da Informação (CGSI) e Comitê Gestor de Proteção de Dados Pessoais (CGPD) do Poder Judiciário do Estado do Maranhão (PJMA).

# 0-9

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

# A

- **Administração executiva:** formada pelos(as) diretores(as) e assessores(as)-chefes do Poder Judiciário do Estado do Maranhão (PJMA).
- **Administração superior:** composta pelo(a) Presidente, Vice-Presidente(s) e Corregedor(a) Geral da Justiça.
- **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, softwares, 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.
- **Autodeterminação Informativa:** confere à pessoa titular de dados o direito de

controlar seus próprios dados pessoais, com base nos preceitos da boa-fé e da transparência.

- **Autoridade Nacional de Proteção de Dados Pessoais (ANPD):** Autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal, responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709, de 14 de agosto de 2018, em todo o território nacional.
- **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.
- **Ciclo de vida dos dados:** todas as etapas de manuseio dos dados, desde o surgimento destes no TJMA até o respectivo descarte ou o arquivamento.
- **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.
- **Controle de acesso:** medida técnica para garantir que os dados sejam acessados somente por pessoas autorizadas, que consiste em processos de autenticação, autorização e auditoria.
- **Cookies:** Arquivos instalados no dispositivo de um usuário que permitem a coleta de determinadas informações, inclusive de dados pessoais em algumas situações, visando ao atendimento de finalidades diversas.
- **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.
- **Dado pessoal:** 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:** procedimento técnico contínuo, que consiste no desenvolvimento de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar eventos potencialmente capazes de comprometer o alcance dos objetivos organizacionais.
- **Gestão de riscos de Segurança da Informação (SI):** 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 (SI):** 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 (SI):** 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 (SI):** 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

- **Legítimo interesse:** hipótese legal que autoriza o tratamento de dados pessoais de natureza não sensível quando necessário ao atendimento de interesses legítimos do controlador ou de terceiros, “exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.”
- **Lei Geral de Proteção de Dados Pessoais (LGPD):** Lei que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento

da personalidade da pessoa natural.

- **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 ou 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).
- **Medidas de segurança:** medidas 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.
- **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 jurídica:** conjunto de pessoas ou bens, dotada de personalidade jurídica própria e constituída na forma da lei.
- **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 cookies:** Declaração pública que disponibilize informações aos usuários de um site ou aplicativo sobre, entre outros aspectos, as finalidades específicas que justificam a coleta de dados por meio de cookies, o período de retenção e se há compartilhamento com terceiros.
- **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.
- **Princípio:** nortear a atuação de magistrados(as), servidores(as), estagiários(as), terceirizados(as) e demais pessoas ou instituições estabeleçam relações com o TJMA.

- **Privacidade:** esfera íntima ou particular do(a) indivíduo(a).
- **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.
- **Programa:** conjunto de mecanismos e procedimentos administrados de forma integrada, reunidos em documento único, no qual são previstas ações articuladas e dinâmicas para atingir determinado objetivo.
- **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.
- **Pseudonimização:** tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
- **Público externo:** usuários(as) dos serviços do TJMA.
- **Público interno:** magistrados(as), servidores(as), estagiários(as), terceirizados(as) e colaboradores(as).

# 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 (RIPD):** 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.
- **Serviço em nuvem:** prestação de serviços de computação pela Internet, incluindo servidores, armazenamento, bancos de dados, rede, software, análise

e inteligência.

- **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
- **Termo de Custódia dos Ativos de TIC**: documento formal que estabelece a responsabilidade pela guarda e proteção dos ativos de TIC de uma organização. Ele descreve os ativos de TIC que estão sob custódia de uma determinada equipe, departamento ou indivíduo, especificando suas responsabilidades, deveres e procedimentos para manter a segurança, integridade e disponibilidade desses ativos, que podem incluir hardware, software, dados, redes e outros recursos relacionados à tecnologia.
- **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.
- **Wipe:** procedimento consiste em apagar, bit a bit, todo o espaço de armazenamento de dados no dispositivo de armazenamento de dados (formatação de baixo nível). Os dados contidos nos setores apagados são normalmente substituídos por zeros ou valores aleatórios.

# ANEXO II
# NORMA DE CONTROLE DE ACESSO E GESTÃO DE IDENTIDADE

**Normativos relacionados:**

| Ato normativo | Capítulo / Seção / Artigo |
|---|---|
| Resolução nº 27/2013-TJ | |
| | |
| | |

**Versionamento:**

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

**Histórico de mudanças:**

| Data | Versão | Alterado por | Descrição das alterações |
|---|---|---|---|
| 12/06/2023 | 1.0 | | |
| 22/04/2024 | 2.0 | GTT do CGSI | Conforme arquivo de registro de alterações (changelog). |
| | | | |
| | | | |
| | | | |

## 1. INTRODUÇÃO

A Norma de Controle de Acesso e Gestão de Identidade complementa a Política de Segurança da Informação (PSI) e define diretrizes para a gestão de identidade, assim como para o controle de acesso visando garantir níveis adequados de proteção aos ativos e/ou recursos de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário do Estado do Maranhão (PJMA).

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

Esta norma está alinhada com o escopo definido na Política de Segurança da Informação (PSI). As diretrizes específicas para o controle de acesso físico são tratadas no ANEXO IV - Norma de Segurança Física no Ambiente de TIC da PSI.

## 2. OBJETIVOS

Assegurar o acesso autorizado e mitigar o acesso não autorizado a informações, ativos e/ou recursos de TIC do PJMA.

Permitir a identificação única de indivíduos que acessam informações, ativos e/ou recursos de TIC do PJMA com a cessão adequada dos direitos de acesso.

## 3. DIRETRIZES

Disponibilizar credenciais de acesso aos(às) usuários(as) autorizados(as) para utilização de ativos e/ou recursos de TIC do PJMA, de acordo com seu cargo, função, necessidade ou atribuições, para execução de atividades administrativas, funcionais e/ou judiciais (atividades laborais).

Estabelecer e manter gerenciador de identidade de usuários(as), que permitam inventariar credenciais de acesso.

Centralizar o controle de acesso para ativos e/ou recursos de TIC do PJMA por meio de um serviço de diretório (Active Directory - AD, Lightweight Directory Access Protocol - LDAP, entre outros), serviço de identidade ou provedor de Login Único (Single Sign-On - SSO), caso a tecnologia esteja disponível.

## 4. CONTROLE DE ACESSO

As credenciais de acesso abordadas nesta norma são pessoais e intransferíveis. Qualquer ação realizada pelos(as) usuários(as) utilizando uma credencial específica será de responsabilidade exclusiva do mesmo(a), devendo zelar pelos princípios da segurança da informação.

Os(As) usuários(as) tratados(as) nesta norma e as respectivas credenciais de

acesso:

I - magistrados(as), servidores(as) efetivos(as) ou requisitados(as), servidores(as) ocupantes de cargo em comissão sem vínculo efetivo, estagiários(as):

a) credenciais de acesso à rede;

b) credenciais de acesso ao e-mail;

c) credenciais de acesso a sistemas administrativos;

d) credenciais de acesso a sistemas judiciais;

e) credenciais de acesso remoto, exceto estagiários(as).

II - colaboradores(as) e terceirizados(as):

a) credenciais de acesso à rede;

b) credenciais de acesso a sistemas administrativos;

c) credenciais de acesso a sistemas judiciais;

d) credenciais de acesso remoto, com autorização da Diretoria de Informática e Automação (DIA).

III - unidades administrativas e/ou judiciais:

a) credenciais de acesso à rede;

b) credenciais de acesso ao e-mail.

Excepcionalmente, de acordo com o princípio do privilégio mínimo, poderão ser concedidas credenciais de acesso temporário à rede para prestadores(as) de serviço, agentes públicos externos(as), visitantes e outras pessoas não previstas, para execução de atividades laborais relacionadas ao PJMA. A concessão, autorizada pela DIA, considera quaisquer responsabilidades legais durante sua utilização.

Os direitos e permissões de acesso requeridos serão avaliados pela Diretoria de Informática e Automação, que habilitará os(as) usuários(as) exclusivamente aos ativos e/ou recursos de TIC necessários à execução de atividades laborais.

Qualquer utilização ou tentativa de utilização não autorizada de credenciais de acesso poderá ser tratada como um incidente de segurança da informação.

O controle de acesso e a gestão de identidade dispostos nesta norma aplicam-

se às seguintes categorias:

- Ativos e/ou Recursos de TIC;
- Sistemas de Informação;
- Acesso Remoto;
- Administrador de Redes;
- Senhas de Acesso;
- Autorização de Acesso;
- Restrição de Acesso.

## 4.1 Ativos e/ou Recursos de TIC

A identificação dos(as) usuários(as) ao acessar ativos e/ou recursos de TIC será realizada por meio de credencial de acesso ou certificado digital, quando aplicável, sendo de uso pessoal e intransferível.

Os(As) usuários(as) poderão acessar os ativos e/ou recursos de TIC através de:

I - credencial de acesso à rede, utilizando login e senha, para uso dos computadores de mesa (desktops) ou notebooks, rede de dados corporativa, intranet, internet, rede sem fio e/ou acesso remoto;

II - credencial de acesso ao e-mail, utilizando login e senha, para uso dos serviços de correio eletrônico e de ambiente colaborativo (armazenamento remoto, agenda/calendário, bate-papo, videoconferência e suíte de escritório).

Os(As) usuários(as), bem como as unidades administrativas e/ou judiciais possuem acesso a uma caixa de correio eletrônico corporativo, única e exclusiva, que deverá ser acessada através da credencial de acesso ao e-mail.

As unidades administrativas e judiciais poderão ter mais de uma caixa de correio eletrônico corporativo, alinhadas às necessidades de seus organogramas. O acesso regular da caixa deverá ser realizado pelo(a) gestor(a), secretário(a) judicial, superior imediato(a) ou pelos(as) usuários(as) da unidade, devidamente autorizados(as).

Após aprovação da DIA, poderá ser criada caixa de correio eletrônico de serviço para sistemas ou serviços relacionados a uma atividade específica no âmbito de uma unidade administrativa e/ou judicial, com acesso concedido por meio de credencial de acesso ao e-mail.

Caso haja necessidade de criar endereços eletrônicos de e-mail destinados a eventos ou projetos no âmbito do PJMA, esses endereços serão configurados, preferencialmente, como grupos ou listas, com a atribuição adequada dos(as) membros(as) participantes e responsáveis.

Mediante análise e autorização da DIA, poderá ser criado um grupo ou lista para

um conjunto específico de usuários(as), conforme necessidade.

A utilização do Múltiplo Fator de Autenticação (MFA) será obrigatória para todas as credenciais de acesso nos serviços de correio eletrônico (e-mail) e ambiente colaborativo, quando houver suporte para essa tecnologia.

## 4.2 Sistemas de Informação

A identificação dos(as) usuários(as) ao acessarem os sistemas de informação administrativos ou judiciais do PJMA, para execução de atividades laborais, será realizada por meio de credencial de acesso ou, quando aplicável, mediante uso de certificado digital.

Os(As) usuários(as) poderão utilizar os sistemas de informação através de:

I - credencial de acesso a sistemas administrativos, utilizando matrícula e senha;

II - credencial de acesso a sistemas judiciais, utilizando CPF e senha, ou certificado digital.

O uso do Múltiplo Fator de Autenticação (MFA) será obrigatório para todas as credenciais de acesso ao utilizar os sistemas de informação do PJMA ou de terceiros, caso o recurso esteja disponível.

No caso de sistemas de informação acessados com certificado digital, o mesmo deverá ser fornecido aos(às) usuários(as), seguindo as regras da Resolução-GP nº 27/2013 - TJMA ou posterior que a substitua.

Deverá ser priorizada a utilização de credencial única para acesso a serviços de diretório corporativo e para acesso aos sistemas de informação, com o objetivo de uniformizar e garantir uma experiência única de interação dos(as) usuários(as) com ativos e/ou recursos de TIC do PJMA.

## 4.3 Acesso Remoto

O acesso remoto à rede de dados corporativa do PJMA será concedido por meio de uma Rede Privada Virtual (Virtual Private Network - VPN), destinada ao desempenho de atividades laborais. Esse acesso será fornecido com as permissões mínimas necessárias, utilizando credenciais de acesso remoto alinhadas às responsabilidades e atribuições dos(as) usuários(as).

O(a) superior imediato(a) deverá justificar e encaminhar a solicitação do acesso remoto pelo sistema DIGIDOC à Diretoria de Informática e Automação (DIA), anexando a portaria que autorizou o trabalho remoto dos(as) usuários(as). A DIA será a responsável por autorizar e implementar esse acesso.

O Múltiplo Fator de Autenticação (MFA) deverá ser utilizado obrigatoriamente

nas credenciais de acesso remoto à rede de dados corporativa do PJMA, caso o recurso esteja disponível.

### 4.4 Administrador de Redes

Somente os(as) servidores(as) lotados(as) na Diretoria de Informática e Automação (DIA), devidamente identificados(as) e autorizados(as), possuem credencial de acesso de administrador de redes para acessar ativos e/ou recursos de TIC do PJMA, incluindo os considerados críticos.

Os(As) usuários(as) que possuem credencial de acesso de administrador de redes deverão utilizar essa permissão exclusivamente para a execução de atividades administrativas que exijam esse nível de acesso.

O Múltiplo Fator de Autenticação (MFA) deverá ser utilizado nas credenciais de acesso de administrador de redes do PJMA, caso o recurso esteja disponível.

### 4.5 Senhas de Acesso

As senhas associadas às credenciais de acesso aos ativos e/ou recursos de TIC do PJMA são de uso pessoal e intransferível. Os(As) usuários(as) deverão zelar pela sua guarda e sigilo, garantindo assim o princípio da confidencialidade.

A Diretoria de Informática e Automação será a responsável por fornecer a senha de acesso inicial aos(as) usuários(as), que deverá ser imediatamente alterada no momento do primeiro acesso. Após essa troca, os(as) servidores(as) da DIA não terão mais acesso à senha.

Os(as) usuários(as) serão encorajados(as) a utilizarem uma ferramenta de gerenciamento de senhas para armazenar e gerir suas credenciais de acesso.

Os(As) usuários(as) deverão alterar a senha imediatamente e notificar seu(sua) superior imediato(a) e a DIA caso haja indicações de que suas credenciais de acesso foram vazadas, acessadas e/ou utilizadas indevidamente por pessoa não autorizada, para que a DIA possa tomar as providências cabíveis.

#### 4.5.1 Prazo de Validade

O prazo de validade das senhas estará alinhado conforme as categorias de usuários(as) e seus respectivos tipos de credenciais de acesso, definidos no tópico 4, como segue:

I - 180 (cento e oitenta) dias para:

a) administradores(as) de redes;

b) estagiários(as);

c) colaboradores(as) e terceirizados(as).

II - 365 (trezentos e sessenta e cinco) dias para:

a) magistrados(as);

b) servidores(as) efetivos(as) ou requisitados(as);

c) servidores(as) ocupantes de cargo em comissão sem vínculo efetivo;

d) unidades administrativas e judiciais.

As senhas das credenciais de acesso serão programadas para serem alteradas na data de aniversário dos(as) usuários(as), preferencialmente. Para prestadores(as) de serviço, agentes públicos externos(as), visitantes e outras pessoas não previstas, a validade será flexibilizada conforme a duração do serviço ou da visita, com possibilidade de prorrogação mediante análise da DIA.

Quando o prazo de validade expira, uma notificação será automaticamente gerada para que os(as) usuários(as) realizem a troca da senha. Além disso, os(as) usuários(as) terão a liberdade de alterar a senha a qualquer momento, conforme julgue conveniente.

### 4.5.2 Complexidade e Tamanho

As senhas das credenciais de acesso deverão ter no mínimo 10 (dez) caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais ($, %, &, #, !, …).

A senha da credencial de administrador de redes deverá ter no mínimo 14 (quatorze) caracteres, combinando letras maiúsculas, minúsculas, números e caracteres especiais ($, %, &, #, !, …).

### 4.5.3 Recomendações para Elaboração de Senhas

Na criação das senhas das credenciais de acesso, os(as) usuários(as) não deverão:

I - utilizar partes de sua credencial de acesso;

II - reutilizar suas senhas em diferentes credenciais de acesso;

III - usar números repetidos, sequência de letras ou de números crescentes e/ou decrescentes na composição da senha. Exemplos: 222999, TTTJJJ, 123456 e 098765;

IV - utilizar informações pessoais suas ou de familiares, tais como nome, sobrenome, placas de carro, datas de aniversário, endereços, números de telefone, nomes de times de futebol ou de animais de estimação, dentre outros;

V - aplicar partes ou variações do nome do Poder Judiciário do Estado do Maranhão, Tribunal de Justiça do Estado do Maranhão e Corregedoria Geral da Justiça do Estado do Maranhão ou qualquer outra variação dos itens descritos, tais como: duplicação ou escrita invertida. Exemplos: PJ, PJMA, PJMAPJMA, AMJP, TJ, TJMA, TJMATJMA, AMJT e assim sucessivamente;

VI - anotar, guardar em locais de fácil acesso ou compartilhar suas senhas com outras pessoas.

As senhas usadas para fins particulares não deverão ser utilizadas para fins laborais.

## 4.6 Autorização de Acesso

A autorização e o nível de acesso aos ativos e/ou recursos de TIC do Poder Judiciário do Estado do Maranhão seguem o modelo de controle de acesso baseado no método RBAC (Role-Based Access Control), que define o nível de privilégio dos(as) usuários(as) baseado em papéis. Esse modelo adere aos princípios de privilégio mínimo e segregação de funções, objetivando mitigar acessos indevidos e vazamentos de informações.

Será responsabilidade da Diretoria de Informática e Automação realizar, anualmente ou quando necessário, a revisão do controle de acesso de ativos e/ou recursos de TIC do PJMA para validar se todas as credenciais de acesso estão devidamente autorizadas de acordo com o nível de permissão necessária para realização das atividades laborais dos(as) usuários(as).

## 4.7 Restrição de Acesso

A DIA estabelece e segue um processo para revogar ou restringir o acesso aos ativos e/ou recursos de TIC do PJMA, por meio da redefinição das credenciais de acesso dos(as) usuários(as).

Para garantir a segurança das contas e evitar acessos não autorizados, o gerenciador de identidade não permitirá a reutilização das últimas 03 (três) senhas utilizadas pelos(as) usuários(as).

### 4.7.1 Bloqueios

As credenciais de acesso dos(as) usuários(as) serão bloqueadas nos seguintes casos:

I - por solicitação formal do(a) superior imediato(a) com a devida justificativa;

II - quando houver suspeita de mau uso dos ativos e/ou recursos de TIC disponibilizados pelo PJMA ou descumprimento da PSI e das normas correlatas em vigência;

III - devido à falta de uso regular ou em casos de aposentadoria, desligamento ou falecimento;

IV - após 05 (cinco) tentativas de acesso com senhas inválidas, permanecendo assim por, no mínimo, 15 (quinze) minutos.

Após 05 (cinco) tentativas de acesso com senhas inválidas, o desbloqueio da credencial de acesso deverá ser solicitado à DIA:

a) para usuários(as): pelo(a) próprio(a) usuário(a) ou por seu(sua) superior imediato(a);

b) para unidades administrativas ou judiciais: pelo(a) superior imediato(a) ou pelo gestor(a) da credencial da unidade.

Ambos os pedidos deverão ser formalizados através dos canais oficiais de comunicação ou solicitação do PJMA.

Para garantir a segurança, as credenciais de acesso serão bloqueadas se não forem utilizadas regularmente pelos(as) usuários(as), de acordo com os seguintes prazos:

I - superior a 30 (trinta) dias para:

a) servidores(as) ocupantes de cargo em comissão sem vínculo efetivo;

b) unidades administrativas ou judiciais;

c) estagiários(as);

d) colaboradores(as) e terceirizados(as), somente credencial de acesso à rede.

II - superior a 60 (sessenta) dias para:

a) magistrados(as);

b) servidores(as) efetivos(as) ou requisitados(as).

O desbloqueio das credenciais de acesso por falta de uso regular será realizado pela Diretoria de Informática e Automação (DIA) mediante solicitação formal justificada realizada pelo(a) superior imediato(a) do(a) usuário(a) ou pelo(a) gestor(a) da

credencial da unidade administrativa e/ou judicial, utilizando os canais oficiais de comunicação ou solicitação do PJMA.

Para preservar as trilhas de auditoria, as credenciais de acesso deverão permanecer bloqueadas, e as exclusões dessas credenciais serão avaliadas pela Diretoria de Informática e Automação (DIA).

### 4.7.2 Exclusões

Caso não seja identificado o uso regular da credencial de acesso ao e-mail pelos(as) usuários(as), a respectiva credencial poderá ser excluída, respeitando os tempos de bloqueio definidos no item 4.7.1, com os prazos abaixo:

I - superior a 15 (quinze) dias para:

a) estagiários(as), com exclusão após 45 (quarenta e cinco) dias.

II - superior a 30 (trinta) dias para:

a) servidores(as) ocupantes de cargo em comissão sem vínculo efetivo, com exclusão após 60 (sessenta) dias;

b) unidades administrativas ou judiciais, com exclusão após 60 (sessenta) dias.

III - superior a 120 (cento e vinte) dias para:

a) magistrados(as), com exclusão após 180 (cento e oitenta) dias;

b) servidores(as) efetivos(as) ou requisitados(as), com exclusão após 180 (cento e oitenta) dias.

Nos casos de desligamento, aposentadoria ou falecimento, as credenciais de acesso serão bloqueadas imediatamente e as credenciais de acesso ao e-mail serão excluídas após o prazo de:

I - 15 (quinze) dias para:

a) estagiários(as).

II - 45 (quarenta e cinco) dias para:

a) servidores(as) ocupantes de cargo em comissão sem vínculo efetivo.

III - 90 (noventa) dias para:

a) magistrados(as);

b) servidores(as) efetivos(as) ou requisitados(as).

Durante o período em que a credencial de acesso ao e-mail estiver bloqueada, os(as) usuários(as) poderão solicitar uma cópia de segurança das mensagens e arquivos eletrônicos de sua caixa de correio. Para fazer essa solicitação os(as) usuários(as) deverão entrar em contato com a Diretoria de Informática e Automação (DIA).

Após a exclusão da credencial de acesso ao e-mail dos(as) usuários(as), o(a) administrador(a) do ambiente colaborativo poderá recuperar as mensagens e os arquivos eletrônicos em até 20 (vinte) dias.

### 4.7.3 Exceções

Em casos de afastamentos superiores a 180 (cento e oitenta) dias, a Diretoria de Recursos Humanos (DRH) deverá notificar formalmente a Diretoria de Informática e Automação (DIA) para evitar a exclusão da credencial de acesso ao e-mail dos(as) usuários(as) afastados(as).

Em caso de extinção da unidade administrativa e/ou judicial à qual uma credencial de acesso ao e-mail está vinculada, compete à DIA decidir sobre as medidas a serem tomadas em relação à credencial, bem como às mensagens e arquivos eletrônicos contidos na caixa de correio associada a ela.

## 5. PAPÉIS E RESPONSABILIDADES

Os(As) usuários(as) deverão observar as responsabilidades e deveres desta norma, podendo ser responsabilizados(as) por quaisquer danos, diretos ou indiretos, causados ao PJMA ou a terceiros(as). As responsabilidades poderão ser apuradas em processo administrativo disciplinar, sem prejuízo das ações cíveis e penais cabíveis.

### 5.1 Diretoria De Recursos Humanos

Compete à Diretoria de Recursos Humanos:

I - comunicar à DIA a nomeação, afastamento, mudança de lotação, retorno, desligamento, exoneração, aposentadoria, falecimento ou qualquer outra mudança no quadro funcional dos(as) usuários(as) para que as credenciais de acesso e permissões sejam redefinidas;

II - apoiar revisões periódicas relacionadas à validade das credenciais de acesso dos(as) usuários(as) para uso dos ativos e/ou recursos de TIC do PJMA.

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

Compete ao(à) superior imediato(a) ou gestor(a) da unidade, através dos canais oficiais de comunicação ou solicitação do PJMA:

I - solicitar à Diretoria de Informática e Automação (DIA) a concessão de acesso a novos(as) usuários(as) aos ativos e/ou recursos de TIC para execução de atividades laborais, considerando o cargo ou funções exercidas;

II - requerer à DIA a definição ou redefinição das permissões da credencial de acesso dos(as) usuários(as) aos ativos e/ou recursos de TIC conforme atividades laborais, cargo ou funções exercidas;

III - comunicar à DRH qualquer ocorrência de mudança de lotação, afastamento, retorno ou desligamento de servidores(as) lotados(as) em sua unidade;

IV - requisitar à DIA a concessão de acesso a colaboradores(as), terceirizados(as), estagiários(as), prestadores(as) de serviço, agentes públicos externos(as), visitantes ou outras pessoas não previstas sob sua supervisão, justificando a necessidade de acesso aos ativos e/ou recursos de TIC, conforme as definições, exceções e prazos estabelecidos nesta norma;

V - informar imediatamente à DIA quando do encerramento do contrato com colaboradores(as), terceirizados(as) e/ou estagiários(as) que fazem uso de ativos e/ou recursos de TIC para a devida revogação da credencial de acesso;

VI - solicitar à DIA, com a devida justificativa, a concessão dos(as) usuários(as) ao acesso remoto, anexando a portaria que os(as) designaram para o trabalho remoto.

## 5.3 Diretoria de Informática e Automação

A habilitação, manutenção e concessão de permissões dos(as) usuários(as) para uso dos ativos e/ou recursos de TIC será realizada pela Diretoria de Informática e Automação (DIA).

Compete à Diretoria de Informática e Automação:

I - analisar as solicitações formais para cadastramento de credenciais de acesso ou definição de permissões de usuários(as) e unidades judiciais e/ou administrativas para uso dos ativos e/ou recursos de TIC do PJMA;

II - bloquear, quando solicitado e justificado, as credenciais de acesso ou permissões dos(as) usuários(as) ou das unidades judiciais e/ou administrativas do PJMA;

III - suspender as credenciais de acesso dos(as) usuários(as) ou das unidades judiciais e/ou administrativas quando constatado o uso indevido de ativos e/ou recursos de TIC do PJMA, dando ciência ao(à) usuário(a) e ao(à) superior imediato(a) ou gestor(a) da unidade para apuração formal;

IV - realizar a revisão periódica das credenciais de acesso dos(as) usuários(as) e das unidades judiciais e/ou administrativas do PJMA;

V - elaborar e implementar mecanismos de auditoria, com o objetivo de garantir a exatidão dos registros de acesso e avaliar a conformidade baseando-se na legislação e normas vigentes;

VI - auditar e periciar as credenciais de acesso dos(as) usuários(as) e das unidades judiciais e/ou administrativas do PJMA, quando necessário;

VII - elaborar e aplicar modelo de padronização das credenciais de acesso que utilizam os ativos e/ou recursos de TIC do PJMA;

VIII - gerir as credenciais de acesso dos(as) usuários(as) e unidades judiciais e/ou administrativas do PJMA;

IX - realizar a gestão dos níveis de permissões de acesso dos(as) usuários(as) e das unidades judiciais e/ou administrativas aos ativos e/ou recursos de TIC do PJMA.

## 6. INFRAÇÕES E PENALIDADES

As 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 III
# NORMA DE CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

**Normativos relacionados:**

| Ato normativo | Capítulo / Seção / Artigo |
|---|---|
| Resolução-GP nº 31/2015 | |
| | |
| | |

**Versionamento:**

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

**Histórico de mudanças:**

| Data | Versão | Alterado por | Descrição das alterações |
|---|---|---|---|
| 12/06/2023 | 1.0 | | |
| 22/04/2024 | 2.0 | GTT do CGSI | Melhoria textual e correções ortográficas no tópico 1 e nos itens 3.1, 3.2 e 3.3. |
| | | | |
| | | | |
| | | | |

## 1. INTRODUÇÃO

A Norma de Classificação e Tratamento da Informação complementa a Política de Segurança da Informação (PSI) e define diretrizes para a classificação, rotulagem, manuseio, guarda, descarte seguro e transferência de informações em formato digital ou em formato físico do Poder Judiciário do Estado do Maranhão (PJMA).

Esta norma visa garantir a privacidade e a segurança das informações sensíveis e proteger a imagem do PJMA, evitando assim perdas reputacionais, financeiras e jurídicas, obedecendo o escopo definido na PSI.

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

## 2. OBJETIVO

Garantir a identificação e o entendimento das necessidades de proteção das informações de acordo com a sua relevância para a organização.

## 3. DIRETRIZES

Orientações da Norma de Classificação e Tratamento da Informação.

### 3.1 Classificação da Informação

A classificação da informação deverá ser levada em consideração pelo nível de impacto que seu comprometimento tem para o Poder Judiciário do Estado do Maranhão (PJMA).

Para efeitos de classificação da informação, serão utilizadas as seguintes categorias:

I - pública: informações disponibilizadas para o público em geral pelo Poder Judiciário do Estado do Maranhão. A divulgação deste tipo de informação causa danos mínimos ou nenhum prejuízo e poderá ser compartilhada livremente, desde que sua integridade seja mantida e os direitos autorais sejam respeitados;

II - de uso interno: informações disponibilizadas para usuários(as), unidades administrativas e/ou judiciais do Poder Judiciário do Estado do Maranhão, empresas contratadas (terceirizadas) e órgãos parceiros. Não deverão ser compartilhadas com o público em geral, salvo mediante autorização expressa do(a) gestor(a) da informação. A divulgação deste tipo de informação poderá acarretar pequenos danos e prejuízos à reputação e às operações do PJMA;

III - de uso restrito: informações restritas a um grupo específico de usuários(as) do Poder Judiciário do Estado do Maranhão, necessárias para a execução de suas atividades administrativas e/ou judiciais, independentemente do cargo

ocupado. Estas informações deverão ser protegidas adequadamente contra acessos internos e externos não autorizados. A divulgação deste tipo de informação poderá causar sérios danos de privacidade, reputação e operações ao PJMA;

IV - confidencial: informações de caráter sigiloso, que deverão ser comunicadas exclusivamente a usuários(as) autorizados(as) pelo Poder Judiciário do Estado do Maranhão, os(as) quais necessitam conhecê-las para o desempenho de suas atividades administrativas e/ou judiciais. A divulgação ou alteração não autorizada deste tipo de informação poderá acarretar graves danos e prejuízos para o PJMA e a sociedade, portanto, seu compartilhamento deverá ser restrito e realizado de maneira controlada.

### 3.2 Rotulagem da Informação

Os rótulos (tags) deverão seguir o padrão definido no ANEXO A – MODELO PARA ROTULAGEM DE INFORMAÇÕES detalhado na página 7 e também obedecerão às regras abaixo:

I - para a informação pública, utilizar um rótulo simples contendo sua classificação;

II - para a informação de uso interno, de uso restrito ou confidencial, a classificação deverá constar individualmente em cada rótulo, seguida pela identificação da unidade administrativa e/ou judicial criadora da informação, quando aplicável.

#### 3.2.1 Em mensagens eletrônicas

Os rótulos das informações das mensagens eletrônicas dos e-mails deverão ser sinalizadas antes da informação escrita.

#### 3.2.2 Em documentos eletrônicos

Os rótulos das informações dos documentos eletrônicos deverão constar no rodapé de cada página, sempre alinhados à direita.

### 3.3 Manuseio da Informação

Os documentos de uso interno, de uso restrito ou confidenciais em formato físico deverão ser guardados em gavetas ou armários com trancas durante os períodos de ausência do local de trabalho dos(as) usuários(as), impedindo o acesso de pessoas não autorizadas.

Os documentos de uso interno, de uso restrito ou confidenciais em formato eletrônico ou digital deverão ser armazenados em ambientes com acesso controlado através de credencial de acesso que utilize senha e Múltiplo Fator de Autenticação

(MFA), caso disponível.

### 3.4 Guarda da Informação

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

### 3.5 Descarte da Informação

O descarte seguro da informação deverá ser realizado de forma a impedir a recuperação da mesma, independente do seu formato de armazenamento original, conforme método de descarte estabelecido pelo PJMA.

### 3.6 Transferência da Informação

Ao realizar a transferência de informação no ambiente interno do PJMA ou com qualquer parte externa interessada, seja no formato físico (papéis, contratos, etc.) ou digital (arquivos, e-mails, etc.), os(as) usuários(as) deverão observar os princípios da segurança da informação e seguir as boas práticas para prevenir acessos não autorizados.

## 4. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

### 4.1 Gestor da Informação

Será de responsabilidade do(a) gestor(a) da informação classificar as informações considerando os requisitos de confidencialidade, integridade e disponibilidade, segundo a categorias abaixo:

I - pública;

II - de uso interno;

III - de uso restrito;

IV - confidencial.

## 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 A – MODELO PARA ROTULAGEM DE INFORMAÇÕES

Os padrões a seguir representam os rótulos que deverão ser exibidos nos rodapés de documentos de acordo com o nível de classificação da informação.

A fonte utilizada deverá ser do tipo Arial e o texto definido em tamanho 12. Na forma escrita não deverá existir espaços e as letras sempre serão maiúsculas. As cores da fonte e do fundo seguirão o padrão de código de cores em HEX.

| INFORMAÇÃO | RÓTULO | COR DA FONTE (HEX) | COR DO FUNDO (HEX) |
|---|---|---|---|
| PÚBLICA | PÚBLICA | #FFFFFF | #4D4D4D |
| DE USO INTERNO | INTERNA | #FFFFFF | #006400 |
| DE USO RESTRITO | RESTRITA | #000000 | #F4B400 |
| CONFIDENCIAL | CONFIDENCIAL | #FFFFFF | #CC0000 |

**2. RODAPÉ**

**TJMA/CGJMA – RÓTULO [UNIDADE ADMINISTRATIVA OU JUDICIAL]**

**EXEMPLOS:**

**TJMA – PÚBLICA**

**TJMA – INTERNA [Diretoria de Recursos Humanos]**

**CGJMA – RESTRITA [Coordenadoria das Serventias]**

# ANEXO IV
# NORMA DE SEGURANÇA FÍSICA NO AMBIENTE DE TIC

**Normativos relacionados:**

| Ato normativo | Capítulo / Seção / Artigo |
|---|---|
| Resolução-GP nº 115/2022 | |
| | |
| | |

**Versionamento:**

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

**Histórico de mudanças:**

| Data | Versão | Alterado por | Descrição das alterações |
|---|---|---|---|
| 12/06/2023 | 1.0 | | |
| 22/04/2024 | 2.0 | GTT do CGSI | Correção da numeração dos tópicos. |
| | | | |
| | | | |
| | | | |

## 1. INTRODUÇÃO

A Norma de Segurança Física no Ambiente de Tecnologia da Informação e Comunicação (TIC) complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para a segurança física dos ativos de TIC críticos do Poder Judiciário do Estado do Maranhão (PJMA).

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

Esta norma obedece ao escopo definido na Política de Segurança da Informação.

## 2. OBJETIVO

Mitigar acesso físico não autorizado, danos e interferências nas informações, ativos e/ou recursos de TIC críticos do PJMA.

## 3. DIRETRIZES

Orientações da Norma de Segurança Física no Ambiente de TIC.

### 3.1 Segurança física

Os ativos de TIC críticos serão mantidos em áreas restritas, denominadas áreas restritas de TIC, cujo perímetro é fisicamente protegido contra o acesso não autorizado, danos e quaisquer interferências de origem humana ou natural.

No que se refere ao controle de acesso, circulação e permanência de pessoas nas dependências do PJMA, deverão ser observadas as diretrizes definidas na Resolução-GP nº 115/2022 - TJMA ou posterior que a substitua.

Os crachás de identificação fornecidos pelo PJMA, inclusive provisórios, são pessoais e intransferíveis, não sendo permitido o seu compartilhamento sob nenhuma circunstância.

Quanto à segurança física das área restritas de TIC, deverão ser observadas as seguintes disposições:

I - todo acesso às áreas restritas de TIC deverá, obrigatoriamente, ser autorizado pela DIA, registrando a data e horário de início e fim do acesso para posteriores averiguações em caso de ocorrências;
II - os(as) servidores(as) do PJMA autorizados(as) pela DIA a acessarem as áreas restritas de TIC, deverão portar seus crachás funcionais, fixados em local de fácil visualização;

III - os(as) terceirizados(as), prestadores(as) de serviço e colaboradores(as)

registrados(as), após identificação na recepção do prédio sede ou prédios remotos do PJMA, preferencialmente uniformizados(as), portando crachás da empresa, e fixados em local de fácil visualização, deverão ser autorizados(as) pela DIA para acessarem as áreas restritas de TIC do PJMA;

IV - os(as) visitantes registrados(as), devidamente identificados(as) na recepção do prédio sede ou prédios remotos do PJMA, portando crachás provisórios fornecidos pelo PJMA, e fixados em local de fácil visualização, deverão ser autorizados(as) pela DIA para acessarem as áreas restritas de TIC do PJMA;

V - terceirizados(as), prestadores(as) de serviço, colaboradores(as) e visitantes nunca deverão ficar sem acompanhamento ou supervisão nas áreas restritas de TIC do PJMA;

VI - é proibida qualquer tentativa de obtenção ou permissão de acesso de indivíduos(as) não autorizados(as) às áreas restritas de TIC do PJMA;

VII - é resguardado ao PJMA o direito de inspecionar malas, maletas, mochilas, cargas, volumes e similares, assim como quaisquer equipamentos, incluindo dispositivos móveis, antes de permitir a entrada ou saída de terceirizados(as), prestadores(as) de serviço ou colaboradores(as) autorizados(as) a acessar áreas restritas de TIC, incluindo os(as) próprios(as) servidores(as) do PJMA, conforme disposto na Resolução-GP nº 115/2022 - TJMA ou posterior que a substitua;

VIII - é resguardado ao PJMA o direito de, a qualquer momento, abordar pessoas em atitude de fundada suspeita, a fim de realizar procedimentos necessários à vigilância ou à manutenção das áreas restritas de TIC, conforme determinado na Resolução-GP nº 115/2022 - TJMA ou posterior que a substitua;

IX - é resguardado ao PJMA o direito de monitorar as áreas restritas de TIC;

X - não será permitido consumir qualquer tipo de alimento, bebida ou fumar nas áreas restritas de TIC;

XI - armazenar em salas com chave e/ou mobília segura (cofres, armários e gaveteiros com chave) as informações sensíveis das áreas restritas de TIC;

XII - as áreas restritas de TIC deverão conter proteções físicas implementadas contra: incêndio, inundação, umidade, poeira, descarga elétrica, explosão, etc., observando legislações e normativos técnicos vigentes, de acordo com o grau de restrição de cada área;

XIII - as áreas restritas de TIC deverão permanecer livres de quaisquer equipamentos, materiais e/ou objetos que não sejam estritamente necessários à sua finalidade.

Em caso de perda, roubo ou furto de ativos de TIC, sob sua responsabilidade, nas dependências do PJMA, o(a) usuário(a) deverá procurar auxílio das Diretorias Administrativa e de Segurança Institucional e Gabinete Militar para que sejam tomadas as medidas cabíveis, dando ciência para a Diretoria de Informática e Automação através dos canais oficiais de comunicação ou solicitação do PJMA.

## 4. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

### 4.1 Diretoria de Informática e Automação

É responsabilidade da Diretoria de Informática e Automação:

I - analisar e autorizar solicitações formais de acesso às áreas restritas de TIC do PJMA;

II - gerir e monitorar as instalações físicas das salas de servidores, salas de racks, data centers e salas afins, onde são mantidos os ativos de TIC críticos;

III - manter o registro de acesso, lógico e/ou físico, às áreas restritas de TIC do PJMA;

IV - gerir, monitorar e autorizar o acesso físico de pessoas às áreas restritas de TIC, como salas de servidores, salas de racks, data centers e salas afins, utilizando controles de acesso, tais como biometria, cartões de acesso, senhas, entre outros;

V - realizar testes regulares de segurança física nas áreas restritas de TIC para identificação e mitigação de vulnerabilidades;

VI - treinar e conscientizar os(as) usuários(as) sobre a importância da segurança física nas áreas restritas de TIC, bem como das medidas de proteção adotadas pelo PJMA.

### 4.2 Diretoria de Segurança Institucional e Gabinete Militar

É competência da Diretoria de Segurança Institucional e Gabinete Militar:

I - gerir sistemas de monitoramento e vigilância, como câmeras de segurança e alarmes, incluindo o alarme de incêndio, para detectar e prevenir intrusões e incidentes de segurança nas áreas restritas de TIC;

II - realizar inspeções regulares para garantir que as portas, janelas e outras entradas físicas das áreas restritas de TIC estejam seguras e em bom estado de conservação e uso;

III - manter registros de acesso físico e lógico para visitantes, fornecedores(as), terceirizados(as), prestadores(as) de serviço ou colaboradores(as) que entram nas dependências do PJMA;

IV - fornecer apoio técnico, por meio de sistema de segurança eletrônica e outros recursos disponíveis, para investigações em andamento de possíveis ilícitos relacionados aos ativos de TIC, incluindo os críticos, mantidos nas áreas restritas de TIC do PJMA.

### 4.3 Diretoria Administrativa

Compete à Diretoria Administrativa:

I - tomar medidas administrativas a respeito de ativos de TIC (computadores de mesa, impressoras, notebooks, celulares, smartphones, tablets, etc.), dispositivos de armazenamento removível, suportes criptográficos (tokens) e outros ativos de TIC disponibilizados ao(à) usuário(a), que tenham sido objetos de perda, roubo ou furto nas dependências do PJMA.

### 4.4 Superior Imediato(a) ou Gestor(a) da Unidade Judicial ou Administrativa

Compete ao(à) superior imediato(a) ou gestor(a) da unidade:

I - manter o controle de acesso e guarda das chaves de salas, cofres, armários e gaveteiros, onde estão armazenadas informações sensíveis;

II - solicitar formalmente à DIA, através dos canais oficiais de comunicação ou solicitação do PJMA, a liberação de usuários(as) que necessitam de acesso às áreas restritas de TIC com a devida justificativa.

## 5. INFRAÇÕES E PENALIDADES

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 V
# NORMA DE GESTÃO DE ATIVOS

**Normativos relacionados:**

| Ato normativo | Capítulo / Seção / Artigo |
|---|---|
| Resolução-GP nº 5/2017 | |
| | |
| | |

**Versionamento:**

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

**Histórico de mudanças:**

| Data | Versão | Alterado por | Descrição das alterações |
|---|---|---|---|
| 12/06/2023 | 1.0 | | |
| 22/04/2024 | 2.0 | GTT do CGSI | Conforme arquivo de registro de alterações (changelog). |
| | | | |
| | | | |
| | | | |

## 1. INTRODUÇÃO

A Norma de Gestão de Ativos define diretrizes para identificar ativos e/ou recursos de Tecnologia da Informação e Comunicação (TIC) adequadamente, a fim de recomendar controles de segurança, obedecendo ao escopo definido na Política de Segurança da Informação (PSI).

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

As diretrizes que se referem a utilização dos ativos e recursos de TIC serão detalhadas na Resolução-GP nº 5/2017 - TJMA ou posterior que a substitua e no ANEXO VI - Norma de Uso Aceitável de Ativos da Política de Segurança da Informação (PSI).

Esta norma obedece ao escopo definido na Política de Segurança da Informação.

## 2. OBJETIVO

Identificar as informações, ativos e/ou recursos de TIC da organização, a fim de preservar a segurança da informação e atribuir propriedades adequadas.

## 3. DIRETRIZ

Identificar e inventariar os ativos de TIC do Poder Judiciário do Estado do Maranhão, que deverão subsidiar os processos de gestão de risco e de gestão de continuidade do negócio nos aspectos relativos à segurança da informação.

## 4. INVENTÁRIO

Os seguintes ativos deverão ser considerados no processo de inventário de ativos de TIC no PJMA:

I - ativos de TIC, como computadores de mesa, dispositivos de armazenamento removível, dispositivos móveis, periféricos ou hardwares e demais equipamentos de TIC que compõem o patrimônio do TJMA;

II - ativos críticos de TIC, como servidores de rede, sistemas de informação e equipamentos de conectividade da infraestrutura de rede, tais como: switches, roteadores, firewalls, modems, etc.;

III - sistemas de gerenciamento de banco de dados;

IV - níveis de permissões;

V - serviços da rede de dados corporativa e de nuvem;

VI - sistemas e/ou softwares desenvolvidos, adquiridos ou recebidos em doação;

VII - dados armazenados e trafegados nas redes operacionalizadas pelo PJMA;

VIII - procedimentos, contratos, documentação de sistemas, manuais, planos e guias.

O inventário resultante do processo de mapeamento de ativos de TIC deverá conter, minimamente, para cada ativo:

I - a identificação e descrição;

II - a categoria e subcategoria;

III - o responsável (gestor);

IV - o nível de criticidade (alta, média e baixa);

V - a localização.

Os ativos de TIC tratados nesta norma deverão ser classificados de acordo com o nível de criticidade, sendo determinado por:

I - requisitos legais;

II - valor financeiro;

III - seu potencial de agregar valor ao negócio;

IV - sua vida útil.

A classificação do inventário deverá ser aprovada pelos gestores dos ativos de TIC.

## 5. PAPÉIS E RESPONSABILIDADES

Todos os ativos de TIC deverão ter um(a) proprietário(a) designado(a) no inventário de ativos.

O(A) proprietário(a) do ativo de TIC será responsável pela confidencialidade, integridade e disponibilidade das informações no ativo em questão.

### 5.1 Superior Imediato(a) ou Gestor(a) da Unidade Judicial ou Administrativa

Compete ao(à) superior imediato(a) ou gestor(a) da unidade:

I - identificar os ativos sob sua responsabilidade;

II - identificar potenciais ameaças e vulnerabilidades relacionadas aos ativos;

III - consolidar informações resultantes da análise do nível de segurança da informação de cada ativo;

IV - avaliar os riscos dos ativos;

V - estabelecer e monitorar os processos em torno do gerenciamento de mudança e de configuração dos ativos;

VI - sugerir controles de segurança para tratamento do risco dos ativos sob sua gestão;

VII - garantir que os ativos de TIC disponibilizados pelo PJMA, sejam devidamente protegidos, utilizados e manuseados;

VIII - excluir as informações confidenciais armazenadas no ativo sob sua responsabilidade;

IX - devolver os ativos de TIC, disponibilizados pelo PJMA, em bom estado de conservação.

## 5.2 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação:

I - estabelecer e manter um inventário preciso, detalhado e atualizado dos ativos e/ou recursos de TIC do PJMA;

II - disponibilizar ferramentas de descoberta ativa e/ou passiva para identificar dispositivos conectados à rede de dados corporativa do PJMA e automaticamente atualizar o inventário de ativos de TIC do PJMA, excetuando os equipamentos particulares;

III - implementar mecanismos para lidar com ativos não autorizados, com opções de remover o ativo da rede, negar que se conecte remotamente à rede de dados corporativa ou colocá-lo em modo de espera (quarentena);

IV - utilizar ferramentas de gerenciamento de endereços IP (Internet Protocol) para atualizar o inventário de ativos do PJMA, a exemplo do Dynamic Host Configuration Protocol (DHCP);

V - assegurar que apenas softwares suportados, licenciados e autorizados sejam designados no inventário de ativos de TIC do PJMA;

VI - assegurar que softwares não autorizados sejam retirados de uso em ativos

de TIC do PJMA;

VII - utilizar controles técnicos, como lista de permissões de aplicações, para garantir que apenas softwares autorizados possam ser executados ou acessados;

VIII - assegurar que os ativos de TIC inventariados possuam contrato de suporte em vigor.

## 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 VI
# NORMA DE USO ACEITÁVEL DE ATIVOS

**Normativos relacionados:**

| Ato normativo | Capítulo / Seção / Artigo |
|---|---|
| Resolução-GP nº 27/2013 | |
| Portaria-GP nº 97/2019 | |
| | |

**Versionamento:**

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

**Histórico de mudanças:**

| Data | Versão | Alterado por | Descrição das alterações |
|---|---|---|---|
| 12/06/2023 | 1.0 | | |
| 22/04/2024 | 2.0 | GTT do CGSI | Conforme arquivo de registro de alterações (changelog). |
| | | | |
| | | | |
| | | | |

## 1. INTRODUÇÃO

A Norma de Uso Aceitável de Ativos complementa a Política de Segurança da Informação (PSI) e estabelece diretrizes para os(as) usuários(as) devidamente autorizados(as) quanto à utilização adequada dos ativos de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário do Estado do Maranhão (PJMA).

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

Esta norma obedece ao escopo definido na Política de Segurança da Informação.

## 2. OBJETIVOS

Assegurar que as informações, ativos e/ou recursos de TIC da organização sejam devidamente protegidos, utilizados e/ou manuseados.

Reduzir os riscos de acessos não autorizados, perdas e danos às informações em mesas, telas e em outros locais acessíveis durante e fora do horário de expediente.

Manter a segurança das informações transferidas dentro da organização e com qualquer parte externa interessada.

Elaborar requisitos específicos de segurança cibernética relativos aos ativos de TIC sob sua jurisdição, incluindo ambientes centralizados, endpoints, equipamentos intermediários ou finais conectados em rede ou a algum sistema de comunicação, inclusive equipamentos portáteis e dispositivos móveis.

Elaborar requisitos específicos de segurança cibernética relacionados com o acesso remoto.

Certificar a utilização adequada dos recursos de TIC, no que se refere ao uso do correio eletrônico, dos sistemas de informação, da internet e do ambiente colaborativo (armazenamento remoto, agenda/calendário, videoconferência, bate-papo e suíte de escritório).

Garantir a inserção, divulgação, modificação, manutenção ou remoção de informações apenas de forma autorizada sobre as mídias de armazenamento.

## 3. DIRETRIZES

Fornecer uma direção clara e objetiva sobre como os(as) usuários(as) deverão utilizar ativos e/ou recursos de TIC do PJMA, observando os princípios de segurança da informação.

Identificar comportamentos esperados e inaceitáveis dos(as) usuários(as) ao utilizarem os ativos e/ou recursos de TIC do PJMA.

Regulamentar as permissões e proibições quanto ao uso dos ativos e/ou recursos de TIC do PJMA pelos(as) usuários(as).

## 4. ATIVOS E/OU RECURSOS DE TIC

Os(As) usuários(as) deverão utilizar os ativos e/ou recursos de TIC, de propriedade do Poder Judiciário do Estado do Maranhão (PJMA), para desenvolvimento de atividades administrativas, funcionais e/ou judiciais (atividades laborais), fazendo uso exclusivo de sua credencial de acesso ou certificado digital.

O Poder Judiciário do Estado do Maranhão (PJMA) poderá, a seu critério, conceder aos(às) usuários(as) ativos de TIC, como dispositivos móveis, certificados digitais ou dispositivos de armazenamento removíveis, para execução de suas atividades laborais, que poderão ser utilizados fora das dependências do PJMA.

Os(As) usuários(as) deverão:

I - zelar pelo uso dos ativos e/ou recursos de TIC disponibilizados pelo PJMA, a fim de garantir sua preservação física e lógica;

II - fechar, desconectar ou sair de aplicativos ou sistemas, efetuar o logoff da rede ou bloquear a tela do computador de mesa (desktop) ou do notebook quando:

a) não estiver mais utilizando o ativo de TIC;

b) ausentar-se do local de trabalho por um curto período de tempo.

III - desligar computadores de mesa (desktops) ou notebooks:

a) ao final do expediente;

b) ausentar-se do local de trabalho por um longo período de tempo.

IV - informar quaisquer fragilidades, incidentes ou eventos que indiquem um possível incidente conforme o ANEXO VII - Norma de Gestão de Incidentes de Segurança da Informação da Política de Segurança da Informação (PSI).

Os computadores de mesa (desktops) ou notebooks que não forem desligados ao final do expediente poderão sofrer reinícios ou desligamentos remotos por servidores(as) lotados(as) da Diretoria de Informática e Automação (DIA) a fim de receberem atualizações de sistemas operacionais, softwares, sistemas, antivírus, etc.

O bloqueio de tela, protegido por senha, deverá ser ativado automaticamente sempre que o computador de mesa (desktop) ou notebook ficar inativo por mais de 10

(dez) minutos.

Qualquer dano aos ativos de TIC do PJMA, sob responsabilidade do(a) usuário(a), deverá ser devidamente analisado pela DIA. Caso seja constatado que tal dano decorreu da falta de zelo, negligência ou imprudência, caberá a este(a) adotar as medidas necessárias para reparação do prejuízo, por meio das ações cabíveis.

Os(As) usuários(as) não deverão:

I - conectar equipamentos particulares na rede de dados corporativa do PJMA, seja em segmentos cabeados ou sem fio, sem avaliação e autorização formal da Diretoria de Informática e Automação (DIA), tais como: computadores de mesa (desktops), equipamentos portáteis, dispositivos móveis (notebooks, celulares, smartphones, tablets, smartwatches, etc.), impressoras, câmeras, switches, roteadores, modems**,** etc.;

II - executar comando, instrução ou aplicativo que possa causar indisponibilidade dos ativos e/ou recursos de TIC do PJMA;

III - realizar alterações e/ou manutenções em qualquer ativo de TIC de propriedade do PJMA, cedido ou não, sob sua guarda, salvo com autorização expressa da DIA;

IV - utilizar os ativos e/ou recursos de TIC disponibilizados pelo PJMA para fins particulares ou não relacionados com as atividades laborais;

V - copiar materiais originais ou qualquer conteúdo protegido por direitos autorais, sem a devida licença ou autorização, incluindo músicas, filmes, jogos, emuladores de jogos, vídeos, sistemas operacionais, softwares ou aplicativos, etc.;

VI - utilizar a rede elétrica estabilizada de informática para ligação de bebedouros, ventiladores, frigobares, cafeteiras, micro-ondas, carregadores de celulares/smartphones e outros utensílios elétricos/eletrônicos.

Os equipamentos, softwares ou qualquer outro ativo de TIC de propriedade particular, quando utilizados nas dependências do PJMA, deverão ter registro de entrada e saída nas dependências da Diretoria de Informática e Automação ou nas direções dos órgãos onde serão utilizados.

O uso aceitável de ativos e/ou recursos de TIC disposto nesta norma aplica-se às seguintes categorias:

- Telefones;
- Dispositivo Móvel Corporativo;
- Acesso Remoto (Conexão Remota);
- Dispositivo de Armazenamento Removível;

- Armazenamento de Arquivos;
- Certificado Digital;
- Equipamentos de Impressão e Fotocópia;
- Mesa Limpa e Tela Limpa;
- Acesso à Internet;
- Serviço de Ambiente Colaborativo;
- Serviço de Correio Eletrônico Corporativo;
- Sistemas de Informação;
- Propriedade Intelectual;
- Aplicativos de Mensagens, Redes Sociais e Serviço de Correio Eletrônico Pessoal;
- Inteligência Artificial.

## 4.1 Telefones

O Poder Judiciário do Estado do Maranhão (PJMA) disponibilizará telefones analógicos ou digitais exclusivamente para uso laboral.

Os(as) usuários(as) deverão priorizar o uso dos telefones fornecidos para realizar chamadas relacionadas às suas atividades laborais. Em situações excepcionais, onde seja necessário fazer chamadas pessoais, é recomendável que utilizem seus dispositivos móveis pessoais, como celulares, respeitando as normas de uso estabelecidas pelo PJMA.

## 4.2 Dispositivo Móvel Corporativo

O Poder Judiciário do Estado do Maranhão (PJMA) poderá, a seu critério exclusivo, fornecer dispositivos móveis corporativos, como notebooks, celulares, smartphones, tablets, smartwatches, etc., aos(as) usuários(as) para execução de atividades laborais.

Ao fazer uso do dispositivo móvel corporativo, os(as) usuários(as) deverão:

I - utilizar criptografia obrigatoriamente ao armazenar informações restritas e confidenciais, quando o dispositivo assim permitir;

II - habilitar o mecanismo de bloqueio de segurança pessoal (bloqueio de tela) no dispositivo, utilizando preferencialmente recursos biométricos, para evitar acesso não autorizado em caso de perda, roubo ou furto;

III - manter o sistema operacional e os aplicativos atualizados;

IV - evitar que os dados do dispositivo sejam acessados por pessoas não autorizadas;

V - realizar cópias de segurança dos dados do dispositivo periodicamente;

VI - utilizar redes de comunicação seguras, preferencialmente criptografadas.

Ao se deslocar com dispositivo móvel corporativo, os(as) usuários(as) deverão:

I - guardá-lo de forma segura, como em mochila, maleta, case ou capa;

II - mantê-lo sempre à vista e atento(a) à sua segurança;

III - acomodá-lo em local seguro e fora do alcance da visão de terceiros ao transportá-lo em veículos automotores;

IV - levá-lo consigo para evitar deixá-lo desacompanhado dentro do veículo.

Os dispositivos móveis corporativos deverão estar em conformidade com o ANEXO X - Norma de Proteção Contra Códigos Maliciosos da PSI, ANEXO XI - Norma de Gestão de Vulnerabilidades Técnicas da PSI e com níveis adequados de proteção.

Os(As) usuários(as) poderão utilizar seus dispositivos móveis pessoais para fins laborais durante o expediente, desde que não interfiram na própria concentração nem na dos(as) demais usuários(as), não violem legislações, políticas ou normas vigentes, e não gerem riscos ao PJMA. No entanto, os notebooks pessoais, em caso de necessidade de serem conectados na rede corporativa de dados do PJMA, deverão ser avaliados e autorizados pela Diretoria de Informática e Automação (DIA).

Em caso de perda, roubo ou furto do dispositivo móvel corporativo ou pessoal utilizado para fins laborais, os(as) usuários(as) deverão procurar a ajuda das autoridades policiais para registrar um boletim de ocorrência e notificar imediatamente o(a) superior imediato(a). Este, por sua vez, deverá comunicar, via DIGIDOC, a Diretoria Administrativa e a Diretoria de Informática e Automação para que sejam tomadas as providências cabíveis.

### 4.3 Acesso Remoto (Conexão Remota)

O acesso remoto à rede de dados corporativa do Poder Judiciário do Estado do Maranhão (PJMA) será disponibilizado através de Virtual Private Network (VPN) e será restrito aos(às) usuários(as) do PJMA para a execução de suas atividades laborais de forma remota. Esse acesso será atribuído com as permissões mínimas necessárias e poderá ser realizado através dos computadores de mesa (desktops) e/ou notebooks corporativos ou pessoais.

Os computadores de mesa (desktops) ou notebooks corporativos deverão estar em conformidade com as normas vigentes, em especial o ANEXO X - Norma de Proteção Contra Códigos Maliciosos e o ANEXO XI - Norma de Gestão de Vulnerabilidades Técnicas da Política de Segurança da Informação (PSI).

Ao utilizar o computador de mesa ou notebook pessoal, inspecionado e autorizado pela DIA, para realizar acesso remoto à rede de dados corporativa, os(as) usuários(as) deverão seguir recomendações de boas práticas de segurança, incluindo:

I - utilizar aplicativos e sistemas operacionais originais e licenciados, com exceção dos baseados em softwares livres;

II - manter o sistema operacional e os aplicativos atualizados;

III - obter aplicativos de fontes confiáveis e lojas oficiais;

IV - usar ferramentas ou recursos de segurança, como antivírus e firewall local;

V - manter a data e hora corretas, sincronizado com o fuso horário local;

VI - ser cuidadoso(a) ao clicar em endereços eletrônicos (links) e baixar arquivos;

VII - proteger suas credenciais de acesso;

VIII - criar uma conta padrão, sem privilégios de administrador, e usá-la em tarefas rotineiras, utilizando a conta com privilégio superior somente quando necessário;

IX - fazer cópias de segurança (backups) pessoais periódicas;

X - ativar a criptografia de disco, quando disponível;

XI - utilizar travas físicas ao utilizá-los em locais públicos;

XII - compartilhar recursos apenas pelo tempo necessário e estabelecer senhas e permissões de acesso adequadamente;

XIII - ser cauteloso(a) ao enviá-los para serviços de reparo e manutenção;

XIV - evitar o acesso em redes sem fio (wireless) públicas, como as disponibilizadas em hotéis, restaurantes, aeroportos e locais similares, ao fazer login nos sistemas do PJMA ou realizar trabalhos associados.

Caso seja identificado que o computador de mesa ou notebook pessoal não esteja em conformidade, minimamente, com os itens de I a V informados acima, o acesso remoto poderá ser bloqueado ou revogado, com notificação ao(à) superior imediato(a) do(a) usuário(a).

Caso os computadores de mesa ou notebooks pessoais sejam de servidores(as), estagiários(as), terceirizados(as) e/ou colaboradores(as) lotados na

Diretoria de Informática e Automação (DIA) para realizar acesso remoto à rede de dados corporativa do PJMA, o acesso e uso desses ativos de TIC poderá ser disciplinado através de Portaria, a qual poderá incluir novas recomendações ou recomendações adicionais de segurança.

A Diretoria de Informática e Automação (DIA) poderá, sem aviso prévio, monitorar e/ou registrar para fins de auditoria como o acesso remoto está sendo utilizado, notificando, e eventualmente responsabilizando, os(as) usuários(as) que estejam utilizando indevidamente este tipo de acesso.

## 4.4 Dispositivo de Armazenamento Removível

O PJMA poderá, a seu critério exclusivo, fornecer dispositivos de armazenamento removíveis (mídias de CD's, DVD's e/ou BLU-RAY, pendrives e discos rígidos externos) aos(às) seus(suas) usuários(as) para execução de atividades laborais.

Os(As) usuários(as) ao fazerem uso do dispositivo de armazenamento removível, deverão:

I - utilizar criptografia, obrigatoriamente, ao armazenar informações de uso restrito e confidenciais, quando o dispositivo assim permitir;

II - realizar, regularmente, cópias de segurança (backups) das informações nos locais de armazenamento de arquivos cedidos pelo PJMA, minimizando impactos em caso de perda ou roubo do dispositivo;

III - zelar pela segurança dos ativos de TIC, certificando-se da inexistência de códigos maliciosos nos dispositivos antes de utilizá-los.

O uso de dispositivos de armazenamento removíveis deverá ser realizado somente em computadores de mesa (desktops) ou notebooks com níveis de segurança em conformidade com padrões estabelecidos pelo PJMA.

Será estritamente proibido que os(as) usuários(as) cancelem a verificação da ferramenta de proteção contra códigos maliciosos para os dispositivos de armazenamento removíveis, visando manter a integridade dos dados destes dispositivos e garantindo a proteção da rede de dados corporativa do PJMA.

## 4.5 Armazenamento de Arquivos

O Poder Judiciário do Estado do Maranhão disponibiliza aos(às) seus(suas) usuários(as) áreas de armazenamento de arquivos, não sendo permitido o uso de qualquer outro tipo de armazenamento de arquivos, que não sejam os oficiais adotados pelo PJMA.

Os(As) usuários(as) deverão armazenar os arquivos em uma das seguintes

áreas:

I - interna, na rede de dados corporativa, através do espaço disponibilizado pelos servidores de arquivos disponibilizados pela DIA;

II - externa, em nuvem, remotamente através do espaço disponibilizado pelo ambiente colaborativo do Google Workspace, pelo aplicativo Google Drive.

Os(As) usuários(as), ao utilizarem as áreas de armazenamento de arquivos, não deverão:

I - criar, manipular, armazenar, acessar, copiar, distribuir, divulgar, disponibilizar ou transmitir qualquer material protegido por direitos autorais sem a devida licença ou autorização, incluindo músicas, filmes, jogos, emuladores de jogos, vídeos, sistemas operacionais, aplicativos, e arquivos com conteúdo inadequado, incluindo material pornográfico, agressivo, preconceituoso, discriminatório, terrorista, injurioso, difamatório, de práticas de aborto, de drogas ilícitas ou não, de pirataria, com credenciais de acesso, informações protegidas por segredo de estado ou outro estatuto legal, assim como qualquer outro que possa infringir a legislação, políticas e normas vigentes;

II - criar, manipular, armazenar, acessar, copiar, distribuir, divulgar, disponibilizar ou transmitir arquivos particulares ou não pertinentes aos interesses do PJMA, sob pena de serem excluídos definitivamente, sem aviso prévio;

III - usar as áreas de armazenamento de forma a consumir sua capacidade de forma desnecessária, enfraquecendo seu desempenho ou representando uma ameaça à segurança do ambiente.

Os arquivos não deverão ser armazenados localmente nos computadores de mesa (desktops) ou notebooks, pois a cópia de segurança (backup) desses arquivos não será realizada pela Diretoria de Informática e Automação (DIA), sendo esse procedimento de única e exclusiva responsabilidade dos(as) usuários(as).

O PJMA tem propriedade legal sobre todos os arquivos criados ou produzidos em seus ativos de TIC e/ou áreas de armazenamento de arquivos, reservando-se o direito de manter, a seu critério, histórico de acessos e transações realizadas através das conexões de rede, intranet ou internet, quando considerado necessário, por motivos de segurança ou para fins de auditoria.

O espaço de armazenamento de arquivos disponibilizado internamente, na rede de dados corporativa, observará os limites para:

I - usuários(as): 50 (cinquenta) GigaBytes (GB);

II - unidades administrativas e/ou judiciais - 500 (quinhentos) GigaBytes (GB).

O espaço de armazenamento de arquivos disponibilizado remotamente, no Google Drive, obedecerá os limites para:

I - usuários(as): 01 (um) TeraByte (TB);

II - magistrados(as) e unidades administrativas e judiciais: ilimitado, observando os limites de criação de objetos estabelecidos pelo Google.

O espaço de armazenamento de arquivos disponibilizado remotamente no Google Drive será compartilhado com outros aplicativos do ambiente colaborativo do Google Workspace do PJMA.

Os drives compartilhados terão o limite de 01 (um) Terabyte (TB), exceto nas situações que necessitem de mais espaço, devidamente justificadas pelo(a) solicitante e autorizadas pelo(a) superior imediato(a) e pela Diretoria de Informática e Automação (DIA).

Os(As) usuários(as), ao utilizarem drives compartilhados, serão responsáveis por:

I - gerir o acesso (permissões, compartilhamento, etc.) dos drives compartilhados;

II - evitar o mau uso decorrente de acesso indevido concedido, preservando a integridade do PJMA;

III - disponibilizar arquivos eletrônicos ou áreas de armazenamento apenas para indivíduos(as):

a) dentro do domínio do PJMA;

b) fora do domínio do PJMA, desde que para atender às atividades judiciais e/ou administrativas, sem causar danos à segurança da informação e em conformidade com as políticas e normas vigentes do PJMA.

## 4.6 Certificado Digital

O PJMA poderá, a seu critério, fornecer certificado digital aos(às) usuários(as) para a execução de atividades laborais.

Para emissão e uso do certificado digital, os(as) usuários(as) do PJMA deverão observar a Resolução-GP nº 27/2013 - TJMA e a Portaria-GP nº 97/2019 - TJMA ou posteriores que as substituam.

## 4.7 Equipamentos de Impressão e Fotocópia

Os(As) usuários(as) deverão observar as seguintes disposições quanto ao uso de equipamentos de impressão e fotocópia:

I - retirar imediatamente da impressora ou fotocopiadora, o documento que tenha solicitado para impressão, transmissão ou cópia que contenha informação classificada como de uso interno, de uso restrito ou confidencial;

II - não reaproveitar, em nenhuma hipótese, páginas já impressas e contendo informações classificadas como de uso restrito ou confidenciais, devendo as mesmas serem descartadas de acordo com os procedimentos adotados pelo PJMA.

## 4.8 Mesa Limpa e Tela Limpa

Toda informação classificada como de uso interno, de uso restrito e confidencial especificada no ANEXO III - Norma de Classificação e Tratamento da Informação será considerada sensível neste item.

Os(As) usuários(as) deverão:

I - manter a mesa de trabalho (mobília) e outros móveis, bem como os ativos de TIC, como impressoras, digitalizadores, fotocopiadoras, etc., organizados e livres de papéis (documentos físicos) com informações sensíveis;

II - guardar em mobília segura (cofres, armários e gaveteiros com chave) os papéis, dispositivos de armazenamento removíveis, como mídias de CD's, DVD's e/ou BLU-RAY, pendrives e discos rígidos externos, e outros ativos de TIC sob sua responsabilidade e que possuam informações sensíveis;

III - adotar métodos seguros de descarte para papéis, utilizando triturador, e para dispositivos de armazenamento removíveis, empregando formatação de baixo nível (wipe), de acordo com a classificação das informações;

IV - manter a área de trabalho do computador de mesa (desktop) ou do notebook livre de arquivos que contenham informações sensíveis;

V - armazenar apropriadamente as informações sensíveis nas áreas de armazenamento de arquivos adotadas oficialmente pelo PJMA;

VI - limpar informações de uso restrito ou confidencial em quadros brancos e outros tipos de recursos de exibição quando não for mais necessário.

## 4.9 Acesso à Internet

O acesso à internet, fornecido por meio cabeado ou sem fio, será disponibilizado através da rede corporativa do PJMA para os(as) usuários(as)

observando a necessidade de uso responsável para o desenvolvimento de suas atividades laborais.

O acesso à internet dos ativos de TIC do PJMA, por meio de equipamentos ou dispositivos de acesso direto à internet de operadoras não contratadas pelo PJMA, sob responsabilidade da Diretoria de Informática e Automação (DIA), é permanentemente proibido.

Os(As) usuários(as) deverão:

I - acessar à internet através de sua credencial de acesso à rede, devidamente autorizada e identificada;

II - navegar na internet por meio de navegadores homologados pelo PJMA, na sua versão mais recente sempre que possível;

III - comunicar à DIA, qualquer controle aplicado que restrinja o acesso a conteúdos relacionados às atividades laborais, para as providências cabíveis.

O acesso à internet aos sítios eletrônicos, disponibilizado aos(às) usuários(as) do PJMA, será monitorado pela Diretoria de Informática e Automação (DIA). Os registros de acessos à internet seguirão as diretrizes do ANEXO XIV - Norma de Registros de Eventos da PSI e serão preservados em conformidade com a legislação e normas vigentes.

Durante uso da internet, os(as) usuários(as) não deverão acessar arquivos, conteúdos ou sítios eletrônicos que contenham:

I - exploração sexual, infantil, racial, étnica, etc.;

II - materiais adultos, eróticos, pornográficos ou de relacionamentos íntimos;

III - ameaças, chantagens e assédio moral ou sexual;

IV - atos ofensivos, agressivos, terroristas, subversivos, injuriosos, difamatórios, bem como aqueles que atentem contra a honra, moral, bons costumes e os direitos humanos, além de quaisquer outros que possam infringir as legislações, políticas e/ou normas vigentes, incluindo aqueles que incitem à violência ou intolerância;

V - preconceitos ou discriminações, especialmente os baseados em: cor, sexo, idade, orientação sexual, raça, origem, condição social, crença ou religião, deficiências e/ou necessidades especiais;

VI - promoção de consumo de bebidas alcoólicas, cigarros, substâncias entorpecentes, sejam estas lícitas ou não;

VII - promoção de compras e/ou uso de armas de fogo;

VIII - práticas e/ou incitação de crimes, contravenções penais e/ou pirataria;

IX - práticas de atividades comerciais desleais e anúncios;

X - desrespeito aos direitos de propriedade intelectual ou direitos autorais, incluindo áudios, vídeos, jogos, emuladores de jogos, sistemas operacionais e aplicativos;

XI - softwares de compartilhamento do tipo Peer-To-Peer (P2P), como Kazaa, BitTorrent, eMule, Ares e similares;

XII - práticas de atividades relacionadas a jogos eletrônicos, jogos de azar e qualquer outra forma de jogo ou aposta ilegal;

XIII - criação, execução ou disseminação de códigos maliciosos (malwares);

XIV - portais e páginas inseguras ou suspeitas, que ofereçam riscos de contaminação por códigos maliciosos (malwares) ou outras ameaças para o ambiente da rede de dados corporativa do PJMA;

XV - utilização de recursos ou serviços que tentem evitar controles internos de acesso à internet, como descriptografia de tráfegos de rede (proxy e afins), VPNs, IPs dinâmicos, entre outros;

XVI - redes sociais, exceto para os(as) usuários(as) devidamente autorizados(as) que necessitem desse tipo de acesso para realização de atividades de interesse do PJMA;

XVII - mineração de criptomoedas (bitcoins, etc.) e aplicativos de acesso remoto;

XVIII - serviços de streaming, como rádios online, podcasts, áudios e vídeos, exceto os que sejam de interesse do PJMA;

XIX - desrespeito à imagem institucional do PJMA;

XX - serviços de armazenamento de arquivos externo (em nuvem), exceto aqueles contratados ou licenciados pelo PJMA.

Ao constatar o acesso a sítios eletrônicos com os conteúdos acima relacionados, a DIA poderá comunicar o fato ao Comitê de Governança de Segurança da Informação (CGSI) para as providências necessárias, reportando o(a) superior imediato(a) do(a) usuário(a).

Os casos de liberação de acesso de usuários(as) serão analisados pela

Diretoria de Informática e Automação (DIA), mediante solicitação justificada do(a) superior imediato(a) utilizando os canais oficiais de comunicação do PJMA.

Os(As) juízes(as), desembargadores(as) ou servidores(as) por eles(as) indicados(as) poderão precisar de acesso a sítios eletrônicos restritos para conduzir investigações legítimas e promover a justiça. Nessas circunstâncias, os(as) magistrados(as) ou servidores(as), devidamente autorizados(as) conforme as leis e regulamentos aplicáveis, terão a prerrogativa de acessar esses sítios eletrônicos.

O CGSI poderá autorizar, após parecer técnico da Diretoria de Informática e Automação (DIA), a criação de grupos de usuários(as) com permissões especiais de acesso à internet.

Durante o monitoramento, a DIA resguarda o direito de, sem qualquer notificação ou aviso prévio, aplicar controles necessários para identificar, filtrar e bloquear o acesso a arquivos ou sítios eletrônicos considerados inadequados ou não relacionados às atividades laborais dos(as) usuários(as).

A DIA poderá realizar perícias e auditorias para finalidades administrativas, judiciais e extrajudiciais, incluindo investigações cíveis ou criminais de toda informação trafegada ou armazenada, que seja originada na rede interna (rede de dados corporativa) e destinada às redes externas, ou o contrário.

## 4.10 Serviço de Ambiente Colaborativo

O Poder Judiciário do Estado do Maranhão fornecerá exclusivamente aos(as) usuários(as) e unidades administrativas/judiciais o serviço de ambiente colaborativo (armazenamento remoto, agenda/calendário, videoconferência, bate-papo e suíte de escritório) para desempenho de suas atividades laborais.

No serviço de ambiente colaborativo do Google Workspace (GW) estarão disponibilizados os seguintes aplicativos:

I - Gmail: serviço de correio eletrônico (e-mail);

II - Agenda: serviço de agenda e calendário;

III - Google Drive: serviço de armazenamento de arquivos remoto (em nuvem);

IV - Google Docs: suíte de escritório com pacote de aplicativos de edição de textos, planilhas e apresentações;

V - Google Meet: serviço de comunicação por videoconferência;

VI - Chat do Google: serviço de comunicação por envio de mensagens diretas de texto (bate-papo);

VII - Jamboard: serviço de quadro interativo;

VIII - Google Keep: serviço de anotações;

IX - Grupos: serviço de grupos, listas ou fóruns de e-mails.

Novos aplicativos poderão ser disponibilizados aos(às) usuários(as) do PJMA para execução de atividades laborais, desde que atendam a todos os itens abaixo:

I - sejam homologados e/ou disponibilizados pela empresa Google;

II - sejam compatíveis com o ambiente do Google Workspace;

III - não gerem custos adicionais ao contrato vigente;

IV - sejam devidamente avaliados e autorizados pela DIA.

São responsabilidades dos(as) usuários(as):

I - manter o sigilo da senha de sua credencial de acesso;

II - conhecer a classificação e tratar, de maneira prévia, todas as informações (mensagens, arquivos e documentos) acessadas, manipuladas, armazenadas, produzidas, compartilhadas, copiadas, transmitidas, distribuídas, divulgadas, incluídas, disponibilizadas, publicadas, visualizadas, baixadas e/ou enviadas na área de armazenamento de arquivos remoto;

III - monitorar a capacidade da área de armazenamento de arquivos remoto, utilizado pelo aplicativo Google Drive, e realizar a limpeza desta área, quando necessário, a fim de garantir o seu funcionamento contínuo;

IV - reportar à DIA, através dos canais oficiais de comunicação ou solicitação do PJMA, qualquer ocorrência que comprometa a segurança e/ou a disponibilidade do serviço de ambiente colaborativo.

Quando os(as) usuários(as) fizerem uso do serviço de ambiente colaborativo do Poder Judiciário do Estado do Maranhão, não será permitido:

I - utilizar o serviço em caráter pessoal ou para fins que não sejam de interesse do PJMA.

## 4.11 Serviço de Correio Eletrônico Corporativo

O Poder Judiciário do Estado do Maranhão (PJMA) fornecerá serviço de correio eletrônico corporativo (e-mail) para seus(suas) usuários(as) e unidades administrativas e/ou judiciais, destinado ao desempenho de atividades laborais. O uso de serviço de correio eletrônico pessoal será permitido e disciplinado no item 4.14.2.

As caixas de correio eletrônico corporativo das unidades administrativas e judiciais deverão ser utilizadas para as comunicações oficiais e serão divulgadas através da intranet e internet, conforme necessidade.

No caso de afastamento temporário ou provisório do(a) usuário(a) autorizado(a) ou responsável a acessar a caixa de correio eletrônico corporativo da unidade administrativa ou judicial, caberá ao(à) usuário(a) substituto(a) manter o acesso regular à caixa de correio eletrônico corporativo.

São deveres dos(as) usuários(as):

I - utilizar a caixa de correio eletrônico corporativo disponibilizada pelo PJMA apenas para transmitir e receber informações relacionadas às atividades laborais;

II - manter o sigilo da senha de sua credencial de acesso ao e-mail;

III - acessar sua caixa de correio eletrônico corporativo regularmente, observando os prazos de bloqueio e exclusão definidos no ANEXO II - Norma de Controle de Acesso e Gestão de Identidade da PSI;

IV - acessar o serviço de correio eletrônico corporativo por meio de navegadores de internet e/ou aplicativos de e-mail homologados pelo PJMA, nas suas versões mais recentes;

V - ser cauteloso(a) ao ler mensagens eletrônicas, baixar e/ou executar arquivos anexados, acessar sítios eletrônicos (links ou URLs), principalmente quando recebidas de fontes externas, desconhecidas ou suspeitas;

VI - verificar e dar a correta destinação às mensagens eletrônicas recebidas em sua caixa de correio eletrônico corporativo, inclusive as classificadas como spam, phishing e correlatas;

VII - monitorar a capacidade de armazenamento disponível de sua caixa de correio eletrônico corporativo e realizar a limpeza da mesma, quando necessário, a fim de garantir o seu funcionamento contínuo;

VIII - denunciar mensagens eletrônicas suspeitas, indesejadas, casos de violação ou mau uso do serviço de correio corporativo levando ao conhecimento da Diretoria de Informática e Automação (DIA), através dos canais oficiais de comunicação ou solicitação do PJMA, para que sejam tomadas as medidas cabíveis;

IX - evitar a exposição indevida de endereços eletrônicos de e-mail organizacionais quando enviados/copiados para destinatários de domínios externos (redes externas) ao Poder Judiciário do Estado do Maranhão.

Quando os(as) usuários(as) fizerem uso do serviço de correio eletrônico corporativo do PJMA, não será permitido:

I - utilizar o serviço de correio eletrônico em caráter pessoal ou para fins que não sejam de interesse do PJMA;

II - usar termos obscenos ou palavras de baixo calão na redação de mensagens eletrônicas;

III - enviar informações classificadas como de uso restrito ou confidencial, incluindo credenciais de acesso, para endereços eletrônicos de e-mail de domínios externos ao Poder Judiciário do Estado do Maranhão, exceto em atividades que exijam esse tipo de envio, atendendo aos interesses do PJMA;

IV - incluir o endereço eletrônico de e-mail fornecido pelo PJMA em sítios eletrônicos externos, listas de distribuição, grupos de discussão e/ou fóruns que não estejam relacionados com atividades laborais ou que não sejam de interesse deste órgão;

V - fazer uso de qualquer procedimento de falsificação, manipulação de cabeçalho ou alteração do conteúdo de mensagens eletrônicas de outros(as) usuários(as) do PJMA ou de endereços eletrônicos de e-mail de domínios externos;

VI - realizar interceptação do conteúdo da mensagem eletrônica de outros(as) usuários(as) ou de terceiros(as), a menos que autorizada por autoridade competente;

VII - enviar mensagem eletrônica não solicitada, indesejada ou ilícita ao serviço de correio eletrônico do PJMA ou para domínios externos;

VIII - enviar mensagem eletrônica, de forma intencional, contendo arquivo ou código malicioso, qualquer forma de rotinas ou códigos de programação prejudiciais e danosas aos ativos e/ou recursos de TIC do PJMA ou para domínios externos, excetuando as mensagens eletrônicas suspeitas direcionadas à DIA para análise;

IX - disseminar mensagens eletrônicas de entretenimento ou do tipo “correntes”;

X - transmitir mensagens eletrônicas com conteúdo inadequado, incluindo material sexualmente explícito, ofensivo, agressivo, preconceituoso, discriminatório, terrorista, subversivo, injurioso, difamatório ou de qualquer outra forma ilegal;

XI - emitir comunicados gerais com caráter eminentemente político-partidário

ou com anúncios publicitários;

XII - executar outras atividades lesivas, tendentes a comprometer a intimidade dos(as) usuários(as), a segurança e a disponibilidade de ativos e/ou recursos de TIC, ou a imagem institucional do PJMA.

O serviço de correio eletrônico do PJMA será monitorado pela Diretoria de Informática e Automação (DIA) com objetivo de proteger a organização contra ameaças virtuais, como phishing, spam e outras ameaças existentes, além de produzir evidências relacionadas a eventuais violações das normas e/ou da legislação vigente.

Durante o monitoramento, a DIA, dentro dos limites legais, reserva-se o direito de, sem qualquer notificação ou aviso prévio, processar as mensagens eletrônicas enviadas ou recebidas pelos(as) usuários(as) através do serviço de correio eletrônico corporativo para atender finalidades administrativas, judiciais e extrajudiciais, incluindo investigações cíveis ou criminais.

As caixas de correio eletrônico corporativo dos(as) usuários(as) do PJMA deverão adotar a assinatura padrão, formatada de acordo com o seguinte modelo:

01. Nome completo
02. Cargo
03. Função
04. Setor
05. E-mail
06. Telefone Fixo Corporativo e Ramal

Ao final do e-mail, após a assinatura padrão, deverá ser exibido o seguinte aviso de confidencialidade:

*"A informação contida neste e-mail, assim como em seus anexos, é CONFIDENCIAL e reservada exclusivamente ao(s)/a(s) seu(s)/sua(s) destinatário(s)/destinatária(s), podendo conter informações sigilosas e/ou legalmente protegidas. Qualquer armazenagem, divulgação, distribuição, impressão ou cópia deste e-mail e/ou de seus anexos é absolutamente PROIBIDA. Se você não é o(s)/a(s) destinatário(s)/destinatária(s), por favor, informe imediatamente o(a) remetente, respondendo a esta mensagem, e em seguida apague/destrua permanentemente o original desta mensagem e seus anexos."*

A veiculação de campanhas internas de caráter social ou informativo de grande relevância através do serviço de correio eletrônico deverá ser incentivada e realizada pela Assessoria de Comunicação da Presidência e outros setores autorizados pela Administração do TJMA, observando sempre o disposto nesta norma.

## 4.12 Sistemas de Informação

O Poder Judiciário do Estado do Maranhão (PJMA) disponibiliza aos(às) usuários(as) acesso aos sistemas de informação para o desenvolvimento de suas atividades laborais.

O uso dos sistemas de informação será obrigatório pelos(as) usuários(as), que deverão incluir de forma fidedigna e tempestiva todas as informações processuais e administrativas. Isso possibilita maior transparência e celeridade nos métodos e procedimentos processuais utilizados.

Para acessar os sistemas de informação que requerem certificado digital, os(as) usuários(as) deverão obtê-lo observando as disposições da Resolução-GP nº 27/2013 - TJMA e a Portaria-GP nº 97/2019 - TJMA ou posteriores que as substituam.

Os(As) usuários(as) poderão acessar os sistemas de informação através de:

I - credencial de acesso aos sistemas administrativos, utilizando matrícula e senha;

II - credencial de acesso aos sistemas judiciais, utilizando CPF e senha, ou certificado digital.

Os registros de acessos aos sistemas de informação serão preservados em conformidade com a legislação e normas vigentes e estarão sujeitos a monitoramento pela Diretoria de Informática e Automação (DIA).

A DIA poderá realizar perícias e auditorias para finalidades administrativas, judiciais e extrajudiciais, incluindo investigações cíveis ou criminais de toda informação registrada nos sistemas de informação do PJMA.

São responsabilidades dos(as) usuários(as):

I - manter em sigilo as senhas das credenciais de acesso;

II - utilizar os sistemas do PJMA com cautela;

III - preservar a confidencialidade de fatos ou informações às quais tenha acesso em decorrência de suas atribuições, exceto aquelas de acesso público, salvo quando exigido por lei ou ordem judicial;

IV - não interferir no trabalho de outros(as) usuários(as) ou não comprometer o desempenho e a segurança das informações do PJMA.

Será considerado uso indevido dos sistemas de informação, sujeito às penalidades:

I - a instalação, distribuição e uso de aplicativos ou sistemas não homologados pela Diretoria de Informática e Automação na rede corporativa de dados do

PJMA;

II - a utilização de softwares que permitam ou facilitem o acesso não autorizado aos sistemas, às bases de dados existentes na rede corporativa de dados do PJMA e aos recursos físicos e lógicos, restritos aos administradores dos sistemas de informação deste Tribunal.

Além das hipóteses acima, incorre em uso indevido dos sistemas de informação, qualquer outra prática não autorizada expressamente pela DIA, que importe em dano ao sistema, base de dados ou recursos da rede corporativa de dados do PJMA, especialmente aqueles destinados ao controle de processos judiciais e ao fluxo dos procedimentos administrativos.

## 4.13 Propriedade Intelectual

Os(As) usuários(as) estarão autorizados a fazer uso apenas de ativos ou recursos de TIC que tenham sido oficialmente adquiridos, contratados ou licenciados pelo Poder Judiciário do Estado do Maranhão (PJMA).

Visando cumprir os termos de uso ou serviço, respeitar a propriedade intelectual, garantir a segurança e integridade dos sistemas de informação do PJMA, será expressamente proibida a instalação de softwares ou sistemas adquiridos particularmente nos ativos de Tecnologia da Informação e Comunicação (TIC) do PJMA.

O uso inadequado de licenças poderá resultar em violações de licenciamento e acarretar possíveis consequências legais para o PJMA e para os(as) usuários(as).

## 4.14 Aplicativos de Mensagens, Redes Sociais e Serviço de Correio Eletrônico Pessoal

Os(As) usuários(as) serão responsáveis pelo uso e pela guarda de suas senhas de acesso a redes sociais, aplicativos de mensagens e serviços de correio eletrônico pessoal.

O uso de redes sociais, aplicativos de mensagens e serviços de correio eletrônico pessoal na rede corporativa do Poder Judiciário do Estado do Maranhão (PJMA) poderá ser monitorado pela Diretoria de Informática e Automação (DIA) para garantir a segurança da informação, respeitando a privacidade e confidencialidade dos conteúdos nas comunicações dos(as) usuários(as).

A Diretoria de Informática e Automação (DIA) poderá realizar perícias e auditorias para fins administrativos, judiciais e extrajudiciais, incluindo investigações cíveis ou criminais de toda informação registrada ao utilizar redes sociais, aplicativos de mensagens e serviços de correio eletrônico pessoal através da rede corporativa do PJMA.

### 4.14.1 Aplicativos de Mensagens e Redes Sociais

O uso de aplicativos de mensagens, como WhatsApp e Telegram, será permitido nas dependências do Poder Judiciário do Estado do Maranhão (PJMA). O uso de redes sociais, como Facebook, Instagram, etc., nas dependências do PJMA será permitido exclusivamente para atividades laborais, mediante justificativa do(a) superior imediato(a) e autorização da Diretoria de Informática e Automação (DIA).

Os(As) usuários(as) autorizados(as), ao utilizarem aplicativos de mensagens e/ou redes sociais, não deverão:

I - divulgar, enviar ou publicar dados, arquivos ou informações sensíveis, restritas ou confidenciais do ambiente interno, exceto quando de interesse do PJMA;

II - prejudicar o exercício de suas atividades laborais ou de outros(as) usuários(as) do PJMA;

III - compartilhar, postar, divulgar ou expor imagens, fotos, vídeos ou sons captados nas dependências internas, exceto quando de interesse do PJMA;

IV - compartilhar, postar, divulgar ou expor comentários ou textos que revelem ou induzam terceiros(as) a crerem que se trata de opinião ou posicionamento do PJMA;

V - compartilhar, postar, divulgar ou expor mensagens pornográficas, ofensivas, agressivas, preconceituosas, discriminatórias, terroristas, subversivas, injuriosas, difamatórias, de práticas de aborto, ou que incentivem o uso de drogas ilícitas ou não, assim como qualquer outra que possa infringir as legislações, políticas e/ou normas vigentes.

### 4.14.2 Serviço de Correio Eletrônico Pessoal

O uso de serviços de correio eletrônico pessoal, como Hotmail, Google, Yahoo, ProtonMail, dentre outros, será permitido nas dependências do PJMA.

Os(As) usuários(as), ao usarem o serviço de correio eletrônico pessoal, não deverão:

I - enviar mensagens eletrônicas não solicitadas, indesejadas ou ilícitas para o serviço de correio eletrônico do PJMA ou de domínios externos;

II - enviar mensagens eletrônicas com arquivos ou códigos maliciosos, qualquer forma de rotinas ou códigos de programação prejudiciais e danosas aos ativos de TIC, rede de dados corporativa ou para o serviço de correio eletrônico do PJMA ou de domínios externos;

III - disseminar ou transmitir mensagens eletrônicas pornográficas, ofensivas, agressivas, preconceituosas, discriminatórias, terroristas, subversivas, injuriosas, difamatórias, de práticas de aborto, que incentive o uso de drogas ilícitas ou não, ou que violem as legislações, políticas e/ou normas vigentes.

## 4.15 Inteligência Artificial

Os(As) usuários(as) ao utilizarem sítios eletrônicos que dispõem de serviços de Inteligência Artificial (IA), como ChatGPT, Bard, Gemini, dentre outros, não deverão:

I - compartilhar informações confidenciais do PJMA, como objetivos estratégicos, metas, transações financeiras e indicadores;

II - submeter códigos-fonte de sistemas ou aplicações do PJMA;

III - compartilhar credenciais de acesso corporativas, códigos de autenticação ou informações de acesso;

IV - divulgar informações sobre segredos comerciais e de propriedade intelectual;

V - compartilhar detalhes médicos pessoais;

VI - fornecer dados pessoais, tais como: números de documentos de identificação, nome, endereço, entre outros;

VII - submeter dados biométricos, como impressões digitais ou reconhecimento facial;

VIII - fornecer dados bancários, tais como números de cartões de crédito, números de contas bancárias, códigos de segurança, detalhes de transações financeiras, etc.;

IX - utilizar os serviços de IA para disseminar conteúdo que viole as políticas de uso estabelecidas pelo PJMA ou que possa prejudicar a reputação da instituição.

## 5. PAPÉIS E RESPONSABILIDADES

O uso indevido de quaisquer ativos e/ou recursos de TIC disponibilizados implicará na suspensão imediata dos acessos do(a) usuário(a), seguido pela notificação ao(à) seu(sua) superior imediato(a).

Os(As) usuários(as) deverão observar as responsabilidades e deveres desta norma, podendo ser responsabilizados(as) por quaisquer danos, diretos ou indiretos, causados ao PJMA ou a terceiros(as). Tais responsabilidades poderão ser apuradas por meio de processo administrativo disciplinar, sem prejuízo das ações cíveis e penais

cabíveis.

## 5.1 Superior Imediato(a) ou Gestor(a) da Unidade Judicial ou Administrativa

Compete ao(à) superior imediato(a) ou gestor(a) da unidade:

I - solicitar formalmente à Diretoria de Informática e Automação (DIA), através dos canais oficiais de comunicação ou solicitação do PJMA, a concessão ou restrição de permissões quanto ao uso dos ativos e/ou recursos de TIC do PJMA pelos(as) usuários(as), principalmente, em relação às categorias tratadas nesta norma.

## 5.2 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação (DIA):

I - analisar solicitações formais para concessão ou restrição de permissões dos(as) usuários(as), relacionado ao uso dos ativos e/ou recursos de TIC do PJMA;

II - gerir o uso dos ativos e/ou recursos de TIC do PJMA garantindo os princípios da segurança da informação;

III - gerir o acesso remoto, as áreas de armazenamento de arquivos, o acesso à internet, o serviço de correio eletrônico corporativo, o ambiente colaborativo, os sistemas de informação e outros recursos de TIC oferecidos aos(às) usuários(as) do PJMA;

IV - estabelecer horários de restrição para acesso à internet aos sítios eletrônicos, caso necessário;

V - revisar, quando necessário e observando o disposto nesta norma, os limites, regulações e controles estabelecidos, mediante solicitação do(a) superior imediato(a) do(a) usuário(a), acompanhada da devida justificativa;

VI - realizar alterações e/ou manutenções nos ativos e/ou recursos de TIC de propriedade do PJMA;

VII - disseminar conhecimento de boas práticas de Segurança da Informação;

VIII - reportar ao Comitê de Governança de Segurança da Informação o uso indevido dos(as) usuários(as) aos ativos e/ou recursos de TIC do PJMA que tome conhecimento, para as providências cabíveis;

IX - estabelecer requisitos para uso de computadores de mesa ou notebooks pessoais dos(as) usuários(as) habilitados(as) a realizar o acesso remoto à rede de dados corporativa do PJMA;

X - estabelecer restrições de acesso externo aos ativos e/ou recursos de TIC do PJMA para determinados países, caso necessário.

Casos não previstos deverão ser analisados pela Diretoria de Informática e Automação, mediante solicitação do(a) superior imediato(a) ou gestor(a) da unidade administrativa e/ou judicial.

### 5.3 Diretoria Administrativa

Compete à Diretoria Administrativa:

I - tomar medidas administrativas a respeito de dispositivos móveis (notebooks, celulares, smartphones, tablets, smartwatches, etc.), dispositivos de armazenamento removível, suportes criptográficos (tokens) e outros ativos de TIC disponibilizados aos(às) usuários(as), que tenham sido objetos de perda, roubo ou furto.

### 5.4 Diretoria de Segurança Institucional e Gabinete Militar

Compete à Diretoria de Segurança Institucional e Gabinete Militar:

I - fornecer apoio técnico, por meio de sistema de segurança eletrônica e outros recursos disponíveis, para investigações em andamento de possíveis ilícitos relacionados aos ativos de TIC nas dependências do PJMA.

### 5.5 Assessoria de Comunicação da Presidência

Compete à Assessoria de Comunicação da Presidência:

I - promover e divulgar campanhas de conscientização de segurança da informação para os(as) usuários(as) do PJMA, de caráter social ou informativo, em parceria com a Diretoria de Informática e Automação (DIA) e a Escola Superior da Magistratura do Estado do Maranhão (ESMAM), observando o disposto nesta norma.

### 5.6 Escola Superior da Magistratura do Estado do Maranhão

Compete à Escola Superior da Magistratura do Estado do Maranhão:

I - promover cursos de capacitação e de conscientização sobre segurança da informação para os(as) usuários(as) do PJMA, em parceria com a Diretoria de Informática e Automação (DIA) e a Assessoria de Comunicação da Presidência (ASSCOM), sempre observando o disposto nesta norma.

## 6. INFRAÇÕES E PENALIDADES

As 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 VII
# NORMA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

**Normativos relacionados:**

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

**Versionamento:**

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

**Histórico de mudanças:**

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

## 1. INTRODUÇÃO

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

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

## 2. OBJETIVOS

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

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

Reduzir a probabilidade ou as consequências de incidentes.

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

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

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

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

## 3. DIRETRIZES

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

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

A lista a seguir exemplifica, mas não esgota os possíveis incidentes de

segurança da informação tratados nesta política:

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

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

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

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

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

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

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

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

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

Não serão considerados incidentes de segurança da informação:

I - eventos acidentais não intencionais;

II - eventos não maliciosos;

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

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

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

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

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

## 4. PROTOCOLO DE PREVENÇÃO DE INCIDENTES CIBERNÉTICOS

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

### 4.1 Definição e Implementação de Controles de Segurança Preventivos

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

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

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

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

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

### 4.2 Gerenciamento de Vulnerabilidades

O gerenciamento de vulnerabilidades é um processo contínuo e proativo que visa controlar riscos, realizar monitoramento, corrigir falhas e proteger contra ataques cibernéticos e violações de dados. O objetivo principal deste processo é reduzir a

exposição geral do PJMA a riscos, mitigando o maior número possível de vulnerabilidades.

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

### 4.3 Conscientização e Capacitação (Educação Cibernética)

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

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

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

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

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

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

Com relação à capacitação, será necessário:

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

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

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

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

## 5. DETECÇÃO

A detecção terá o objetivo de reduzir o impacto do incidente cibernético,

antecipando o início do processo de tratamento e de resposta. Portanto, pressupõe o estabelecimento de linhas de base, o monitoramento contínuo e a comunicação dos incidentes cibernéticos.

## 5.1 Estabelecimento de Linhas de Base

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

## 5.2 Monitoramento Contínuo

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

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

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

III - volumetria do tráfego de saída;

IV - registro de eventos (logs);

V - funcionamento e atualização das ferramentas de segurança cibernética;

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

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

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

## 5.3 Recebimento de Comunicação

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

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

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

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

a) a requisição deverá constar o assunto “SOLICITAÇÃO DE AÇÃO DE TECNOLOGIA DA INFORMAÇÃO”, o objeto “INCIDENTE DE SEGURANÇA DA INFORMAÇÃO” e no campo observação uma descrição breve do incidente.

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

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

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

IV - pessoalmente: em casos emergenciais.

## 6. TRATAMENTO DE INCIDENTES CIBERNÉTICOS

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

### 6.1 Triagem

O processo de triagem consistirá em:

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

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

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

IV - registrar o incidente na base de incidentes cibernéticos;

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

### 6.2 Análise

O processo de análise consistirá nas atividades abaixo:

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

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

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

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

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

## 7. AVALIAÇÃO DE IMPACTO

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

### 7.1 Impacto no Negócio

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

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

| | |
|---|---|
| Crítico | O PJMA não consegue fornecer nenhum dos serviços essenciais aos(às) usuários(as) e/ou ao público externo. |

Quadro 1: Níveis de impacto no negócio

## 7.2 Impacto em Dados e Informações

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

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

Quadro 2: Níveis de impacto em dados e informações

## 8. RESPOSTA

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

I - criticidade dos ativos de TIC afetados;

II - tipo e gravidade do incidente;

III - necessidade de preservar a evidência;

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

V - recursos necessários para implementar a estratégia.

## 8.1 Contenção

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

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

I - contenção a curto prazo, que consistirá em:

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

b. segmentar a rede;

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

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

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

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

III - contenção a longo prazo, que consistirá em:

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

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

A extensão dos danos do incidente de segurança deverá ser avaliada para, em seguida, ser identificado o melhor curso de ação para a erradicação completa do

incidente e restauração dos ativos de TIC afetados.

## 8.2 Erradicação

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

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

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

III - identificação das principais causas que originaram o incidente;

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

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

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

## 8.3 Recuperação

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

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

| | |
|---|---|
| Recuperável | lançada investigação. |

Quadro 3: Níveis de recuperabilidade

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

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

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

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

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

## 8.4 Envio de Comunicação

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

I - agentes atacantes e atacados(as);

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

III - evidências coletadas;

IV - Indicadores de Comprometimento (IoCs);

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

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

VII - volume de dados vazados;

VIII - cronologia dos fatos;

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

X - medidas preventivas propostas para ocorrências similares.

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

## 9. PÓS-INCIDENTE

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

### 9.1. Melhoria Contínua dos Processos

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

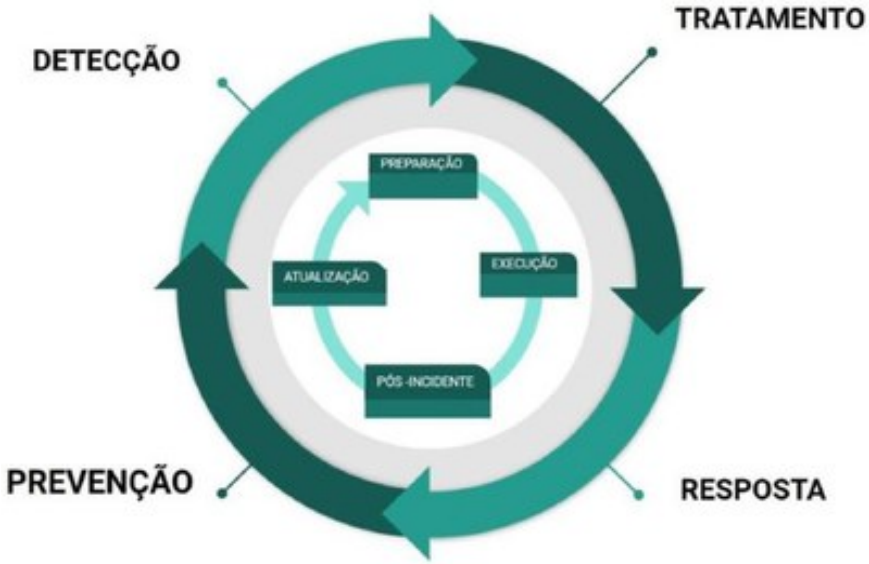



Figura 1: Ciclo de melhoria contínua do processo de gestão de incidente cibernético

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

Os principais objetivos da análise pós-incidente incluem:

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

II - estabelecer medidas preventivas para incidentes similares;

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

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

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

VI - identificar necessidades de treinamento técnico ou operacional;

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

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

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

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

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

## 10. PROTOCOLO DE GERENCIAMENTO DE CRISE CIBERNÉTICA

O protocolo de gerenciamento de crise cibernética do PJMA prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente e poderá durar dias, semanas ou meses.

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

I - ficar caracterizado grave dano material ou de imagem;

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

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

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

## 10.1 Planejamento da Crise

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

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

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

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

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

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

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

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

## 10.2 Durante a Crise (Execução)

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

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

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

O CCCiber será presidido(a) pelo(a) presidente do CGSI e do CGPD, com

autoridade e autonomia para tomar decisões sobre conteúdo de comunicação a serem divulgados, bem como delegar atribuições, estabelecer metas e prazos de ações.

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

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

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

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

### 10.3 Pós-crise (Melhoria Contínua)

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

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

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

II - a linha do tempo das ações realizadas;

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

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

V - o escalonamento da crise;

VI - a investigação e preservação de evidências;

VII - a efetividade das ações de contenção;

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

informações;

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

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

## 11. PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS

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

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

### 11.1 Requisitos para Adequação dos Ativos de TIC

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

I - ajuste do horário dos ativos de TIC;

II - registro dos eventos nos ativos de TIC;

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

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

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

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

I - utilização de usuários, perfis e grupos privilegiados;

II - inicialização, suspensão e reinicialização de serviços;

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

IV - modificações da lista de membros de grupos privilegiados;

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

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

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

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

## 11.2 Coleta e Preservação de Evidências

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

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

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

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

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

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

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

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

arquivos coletados;

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

III - gerar um resumo criptográfico para cada arquivo coletado.

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

### 11.3 Envio de Comunicação

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

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

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

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

I - voz (telefone, celular);

II - mensagem instantânea;

III - reunião por videoconferência ou presencial;

IV - sítios eletrônicos e mídias sociais institucionais.

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

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

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

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

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

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

IV - número de controle da ocorrência;

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

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

VII - resumo criptográfico dos arquivos coletados;

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

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

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

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

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

## 12. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

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

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

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

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

III - diligenciar para coletar e proteger evidências;

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

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

VI - elaborar plano de retorno à normalidade.

### 12.2 Comitê de Crise Cibernética

São responsabilidades do Comitê de Crise Cibernética (CCCiber):

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

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

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

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

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

VI - definir estratégias de comunicação com a imprensa e/ou redes sociais e

estabelecer qual a mídia mais adequada para se utilizar em cada caso;

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

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

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

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

### 12.3 Assessoria de Comunicação da Presidência

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

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

### 12.4 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação (DIA):

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

## 13. INFRAÇÕES E PENALIDADES

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

## 14. REVISÕES

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

## 15. APROVAÇÃO

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

# ANEXO VIII
# NORMA DE CÓPIAS DE SEGURANÇA DA INFORMAÇÃO

**Normativos relacionados:**

| Ato normativo | Capítulo / Seção / Artigo |
|---|---|
| Resolução-GP nº 31/2015 | |
| | |
| | |

**Versionamento:**

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

**Histórico de mudanças:**

| Data | Versão | Alterado por | Descrição das alterações |
|---|---|---|---|
| 12/06/2023 | 1.0 | | |
| 22/04/2024 | 2.0 | GTT do CGSI | Conforme arquivo de registro de alterações (changelog). |
| | | | |
| | | | |
| | | | |

## 1. INTRODUÇÃO

A Norma de Cópias de Segurança da Informação complementa a Política de Segurança da Informação (PSI), definindo as diretrizes de gestão das cópias de segurança produzidas pelo Poder Judiciário do Estado do Maranhão (PJMA).

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

Esta norma obedece ao escopo definido na Política de Segurança da Informação, aplicando-se a todos os dados produzidos internamente e externamente no contexto do PJMA, incluindo dados armazenados em serviços de nuvem pública ou privada.

## 2. OBJETIVOS

Providenciar a realização de cópias de segurança atualizadas e segregadas de forma automática em local protegido, de forma que permita a investigação de incidentes.

Realizar a guarda, preservação ou eliminação de cópias de segurança seguindo tempo de retenção estabelecido.

Possibilitar a recuperação da perda de dados ou sistemas através das cópias de segurança realizadas.

Realizar testes de recuperação a fim de garantir a efetividade da realização das cópias de segurança.

## 3. DIRETRIZES

A Diretoria de Informática e Automação (DIA) não garantirá a realização de cópia de segurança (backup) ou a recuperação de arquivos armazenados localmente nos computadores de mesa (desktop) e notebooks dos(as) usuários(as) ou em quaisquer outros dispositivos fora das áreas de armazenamento disponibilizadas pela DIA, conforme estabelecido no ANEXO VI - Norma de Uso Aceitável de Ativos da PSI.

As cópias de segurança em formato eletrônico pertencentes a ativos e/ou recursos de Tecnologia da Informação e Comunicação (TIC) do PJMA, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deverão estar garantidas nos acordos ou contratos que formalizam a relação entre os envolvidos.

As rotinas de cópia de segurança serão projetadas para garantir a restauração dos arquivos no menor tempo possível, especialmente em situações de indisponibilidade de ativos e/ou recursos de TIC. Essas rotinas utilizarão soluções próprias e especializadas, automatizando o processo, e possuirão requisitos mínimos

diferenciados de acordo com o tipo de serviço de TIC ou dado armazenado, dando prioridade aos ativos e/ou recursos de TIC críticos do Poder Judiciário do Estado do Maranhão (PJMA).

A infraestrutura de rede para cópias de segurança deverá ser separada, tanto logicamente quanto fisicamente, dos sistemas críticos do PJMA. E, deverá ser garantido reserva de recursos para testes de restauração das informações armazenadas.

A armazenagem das cópias de segurança deverá ser realizada em um local fisicamente separado do ambiente principal de Tecnologia da Informação e Comunicação (TIC). Essa prática possibilita preservar cópias adicionais dos principais serviços e informações que sejam considerados críticos.

Em situações onde a confidencialidade seja considerada importante, é recomendável que as cópias de segurança sejam protegidas por criptografia.

## 4. FREQUÊNCIA E RETENÇÃO

As cópias de segurança do PJMA deverão ser realizadas utilizando-se as seguintes frequências temporais:

I - diária;

II - semanal;

III - mensal;

IV - anual;

V - temporalidade personalizada, a depender de necessidades específicas.

As cópias de segurança deverão ser mantidas sob um padrão mínimo, o qual observará a correlação estabelecida da frequência e da retenção. As especificidades das cópias de segurança poderão demandar frequência e tempo de retenção diferenciados.

A cópia de segurança dos arquivos eletrônicos produzidos na rede de dados corporativa do PJMA será realizada pela DIA, considerando os requisitos de serviço, de segurança da informação e de proteção de dados envolvidos, bem como a criticidade da informação para a continuidade da operação do PJMA, e deverá explicitar, no mínimo, os seguintes requisitos técnicos:

I - escopo (arquivos eletrônicos internos, base de dados, máquinas virtuais, sistemas, etc.);

II - tipo da cópia de segurança (completa, incremental, diferencial);

III - frequência temporal de realização da cópia de segurança (diária, semanal, mensal, anual e personalizada);

IV - tempo de retenção individual, conforme escopo definido;

V - Recovery Point Objective - RPO, que diz respeito à quantidade de informação que é tolerável perder no caso de uma parada nas operações;

VI - Recovery Time Objective - RTO, que diz respeito à quantidade de tempo que as operações levam para voltar ao normal após uma parada.

Os(As) administradores(as) das cópias de segurança da informação deverão zelar pelo cumprimento das diretrizes dos tempos de retenção estabelecidos em procedimento interno da DIA.

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

## 5. TIPOS DE CÓPIAS DE SEGURANÇA

O Poder Judiciário do Estado do Maranhão (PJMA) adotará os seguintes tipos de cópias de segurança:

I - completa (*full*);

II - incremental;

III - diferencial.

## 6. USO DA REDE

Os(As) administradores(as) das cópias de segurança da informação deverão considerar o impacto da execução das rotinas de cópias sobre o desempenho da rede de dados corporativa e dos serviços, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais ativos e/ou recursos de TIC do PJMA.

A execução das cópias de segurança deverá considerar, preferencialmente, os períodos estabelecidos e as informações de frequência e tipo para realização das mesmas.

O período de realização das cópias de segurança será determinado pelos administradores(as) das cópias em procedimento interno detalhado.

## 7. TRANSPORTE E ARMAZENAMENTO

As unidades de armazenamento utilizadas na preservação dos dados deverão considerar as seguintes características:

I - a criticidade dos dados armazenados;

II - o tempo de retenção dos dados;

III - a probabilidade de necessidade de restauração;

IV - o tempo esperado para restauração;

V - o custo de aquisição da unidade de armazenamento de cópia de segurança (backup);

VI - a vida útil da unidade de armazenamento da cópia de segurança.

Técnicas de compressão de dados poderão ser utilizadas, desde que o aumento no tempo de restauração dos mesmos seja considerado aceitável pelos(as) administradores(as) das cópias de segurança da informação.

A execução das rotinas de cópias de segurança da informação deverá envolver a previsão de ampliação da capacidade dos ativos de TIC envolvidos no armazenamento.

As unidades de armazenamento das cópias de segurança serão acondicionadas em locais apropriados, com proteções físicas implementadas contra: incêndio, inundação, umidade, poeira, pressão, descarga elétrica, explosão, campos eletromagnéticos, etc. e com acesso restrito a servidores(as) da DIA devidamente autorizados(as). As condições ambientais deverão ser observadas e estar alinhadas com aquelas descritas pelo fabricante das unidades de armazenamento.

Quando da necessidade de descarte de unidades de armazenamento das cópias de segurança, tais recursos deverão ser logicamente e fisicamente destruídos, atentando-se aos procedimentos de descarte seguro do PJMA.

As mídias de armazenamento (fitas magnéticas, discos rígidos externos e outras) contendo as cópias de segurança deverão ser transportadas e armazenadas seguindo as orientações abaixo:

I - a mídia será identificada e armazenada em área segura acessível apenas para servidores(as) da DIA devidamente autorizados(as);

II - a mídia não será deixada sem supervisão durante o transporte;

III - as cópias de segurança completas diárias, semanais, mensais e anuais serão mantidas pelo período e local informados em procedimento interno da

DIA.

## 8. TESTES DAS CÓPIAS DE SEGURANÇA

As cópias de segurança da informação deverão ser verificadas periodicamente e seguir as seguintes orientações:

I - os registros de eventos (logs) das cópias de segurança da informação serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho da cópia de segurança;

II - ações corretivas serão tomadas quando problemas nas cópias de segurança forem identificados, a fim de reduzir os riscos associados a cópias com falha;

III - os registros de eventos (logs) das cópias de segurança e testes de restauração serão mantidos para demonstrar conformidade com esta norma.

Os testes de restauração das cópias de segurança deverão ser realizados, por amostragem, uma vez a cada 03 (três) meses, atendendo aos ambientes de homologação e produção de forma alternada, levando em consideração os recursos de TIC disponíveis.

Os registros de teste de recuperação de cópias de segurança deverão incluir, no mínimo:

I - o tipo de ativo e/ou recurso de TIC, como Máquina Virtual ou Virtual Machine (VM), sistema, serviço ou Banco de Dados, que teve o seu restabelecimento testado;

II - a data da realização do teste;

III - o tempo gasto para finalização do teste (retorno da cópia de segurança);

IV - a situação do procedimento, indicando se foi concluído com sucesso ou se ocorreu alguma falha;

V - uma avaliação se foram atendidos os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs, considerando os diferentes tipos de ambiente (produção, homologação, etc.) do PJMA e os recursos de TIC disponíveis para cada ambiente.

## 9. RESTAURAÇÃO DE CÓPIAS DE SEGURANÇA

Os(As) administradores(as) das cópias de segurança da informação terão a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com as atividades laborais, cabendo recurso da negativa ao superior imediato(a) ou gestor(a) da unidade administrativa ou judicial.

O atendimento de solicitações de restauração de cópias deverá obedecer a um processo de restauração, que estará definido em procedimento interno detalhado da DIA.

A recuperação de mensagens e arquivos eletrônicos da rede corporativa do PJMA e do ambiente colaborativo deverá ser solicitada para a Diretoria de Informática e Automação (DIA), através dos canais oficiais de comunicação ou solicitação pelo(a) superior imediato(a) ou gestor(a) da unidade administrativa ou judicial.

## 9.1 Área de Armazenamento de Arquivos Interna

Os arquivos eletrônicos armazenados na rede corporativa de dados do PJMA, na área disponibilizada pela DIA, que forem excluídos pelos(as) usuários(as) terão possibilidade de recuperação em até 30 (trinta) dias, a contar da data da exclusão dos mesmos.

A restauração de arquivos eletrônicos dos(as) usuários(as) na rede corporativa do PJMA só será possível se estiverem incluídos na rotina de cópia de segurança do dia anterior.

## 9.2 Área de Armazenamento de Arquivos Externa (Nuvem)

As mensagens e os arquivos eletrônicos produzidos ou recebidos no ambiente colaborativo fornecido pelo PJMA que forem excluídos pelos(as) usuários(as), deverão observar as orientações abaixo:

I - os(as) usuários(as) poderão recuperar, no prazo de 30 (trinta) dias, as mensagens e os arquivos eletrônicos colocados na lixeira;

II - decorridos os 30 (trinta) dias da exclusão ou após a execução do procedimento de “esvaziar a lixeira” realizada pelos(as) usuários(as), o(a) administrador(a) de cópias de segurança terá 25 (vinte e cinco) dias para recuperar as mensagens e/ou os arquivos eletrônicos deletados.

Após o vencimento dos prazos mencionados, as mensagens e arquivos eletrônicos serão automaticamente excluídos pelo serviço do ambiente colaborativo, sem possibilidade de recuperação. Apenas as contas dos magistrados(as) ou das unidades administrativas/judiciais terão a capacidade de restaurar mensagens e arquivos eletrônicos após os prazos informados.

Se uma credencial de acesso ao e-mail for excluída, observando os prazos de bloqueio e exclusão definidos no ANEXO II - Norma de Controle de Acesso e Gestão de Identidade da PSI, o(a) administrador(a) de cópias de segurança poderá recuperar as mensagens e os arquivos eletrônicos dos(as) usuários(as) em até 20 dias a partir da data de exclusão da credencial.

## 10. DO DESCARTE DA MÍDIA

Para o descarte da mídia da cópia de segurança, dever-se-á:

I - assegurar que a mídia não contenha mais dados ativos e que o conteúdo, atual ou anterior, não possa ser lido ou recuperado por pessoas não autorizadas;

II - garantir a destruição física e lógica da mídia antes do descarte.

## 11. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

### 11.1 Diretoria de Informática e Automação

É responsabilidade da Diretoria de Informática e Automação (DIA) prover ativos e/ou recursos de TIC, a fim de sustentar a gestão das cópias de segurança da informação do PJMA.

### 11.1.1 Administradores(as) das cópias de segurança da informação

Os(As) administradores(as) das cópias de segurança da informação deverão ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de cópia de segurança. São atribuições dos(as) administradores(as):

I - gerir a(s) ferramenta(s) que realiza(m) as cópias de segurança da informação do PJMA;

II - realizar cópias de segurança da informação dos dados produzidos ou custodiados pelo PJMA;

III - gerir as cópias de segurança da informação, através da guarda, preservação, restauração e descarte seguro das mesmas;

IV - manter as unidades de armazenamento das cópias de segurança preservadas, funcionais e seguras;

V - definir procedimentos que envolvem os processos de cópias e restauração de segurança da informação;

VI - realizar testes de restauração das cópias de segurança;

VII - observar os registros de eventos (logs) das cópias de segurança da informação do PJMA.

## 12. INFRAÇÕES E PENALIDADES

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

## 13. REVISÕES

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

## 14. APROVAÇÃO

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

# ANEXO XI
# NORMA DE GESTÃO DE VULNERABILIDADES TÉCNICAS

**Normativos relacionados:**

| Ato normativo | Capítulo / Seção / Artigo |
|---|---|
| | |
| | |
| | |

**Versionamento:**

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

**Histórico de mudanças:**

| Data | Versão | Alterado por | Descrição das alterações |
|---|---|---|---|
| 12/06/2023 | 1.0 | | |
| 22/04/2024 | 2.0 | GTT do CGSI | Conforme arquivo de registro de alterações (changelog). |
| | | | |
| | | | |
| | | | |

## 1. INTRODUÇÃO

A Norma de Gestão de Vulnerabilidades Técnicas complementa a Política de Segurança da Informação, definindo diretrizes para execução de processos de monitoramento e tratamento de vulnerabilidades técnicas em todos os ativos de TIC do Poder Judiciário do Estado do Maranhão (PJMA).

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

Esta norma obedece ao escopo definido na Política de Segurança da Informação.

## 2. OBJETIVO

Assegurar a integridade dos sistemas operacionais e mitigar a exploração de vulnerabilidades técnicas conhecidas.

## 3. DIRETRIZES

Estabelecer um processo contínuo e proativo para tratar riscos, realizar monitoramento, corrigir falhas e adotar medidas de proteção contra ameaças cibernéticas e violação de dados. Dessa forma, reduz-se a exposição do PJMA a riscos existentes e mitiga-se um número maior de vulnerabilidades.

As ações de proteção deverão ser sempre acompanhadas por ações de detecção e tomada de decisão sobre os ativos de TIC vulneráveis.

### 3.1 Gerenciamento de Vulnerabilidades

O gerenciamento de vulnerabilidades deverá ser criado, implementado, mantido e aplicado no PJMA e contempla:

I - estabelecer mecanismos para obter informações sobre vulnerabilidades técnicas dos sistemas e ativos de TIC, avaliação da exposição do PJMA a tais vulnerabilidades e a implementação de controles apropriados para tratamento do risco associado;

II - gerenciar os diversos ativos de TIC que sustentam os serviços do PJMA;

III - estabelecer funções e responsabilidades das equipes para realizar todas as atividades de maneira oportuna e eficaz para o PJMA;

IV - realizar atualizações de softwares, notificadas pelo fabricante ou fornecedor homologado, utilizando recursos autorizados, tais como: sítio eletrônicos de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais

recentes.

### 3.2 Inventário de Ativos

O inventário de ativos de TIC, conforme estabelecido no ANEXO V - Norma de Gestão de Ativos da PSI, deverá ser incluído no escopo do gerenciamento de vulnerabilidades e patches. Ele deverá ser atualizado periodicamente ou sempre que ocorrerem alterações significativas, garantindo que os recursos informacionais estejam cobertos pelo gerenciamento de vulnerabilidades do PJMA.

### 3.3 Detecção de Vulnerabilidades

As ferramentas precisarão de configurações e ajustes adequados de acordo com o escopo avaliado. Da mesma forma, os tipos de detecções e testes terão que ser avaliados e ajustados para estar em conformidade com o escopo definido.

A frequência dos testes de segurança leva em consideração os requisitos legais, regulamentares e contratuais, bem como os riscos associados aos ativos de TIC do Poder Judiciário do Estado do Maranhão.

Os testes de segurança utilizarão o feed de vulnerabilidade mais recente para garantir a detecção abrangente de vulnerabilidades. Esses testes deverão ser realizados pela Diretoria de Informática e Automação (DIA) ou por uma empresa especializada, em horários que não impactem o uso dos recursos e sistemas disponibilizados pelo PJMA.

Para cada teste, deverá ser verificada a integridade da ferramenta utilizada, sua capacidade de analisar adequadamente as vulnerabilidades dos ativos de TIC, bem como identificar e tratar exceções.

As ferramentas utilizadas serão ajustadas continuamente para evitar discrepâncias nos resultados gerados por ferramentas distintas.

O teste de invasão ou de penetração (pentest) deverá ser realizado, periodicamente ou conforme necessidade do PJMA, incluindo o escopo da avaliação, os métodos de uso e os requisitos operacionais, a fim de fornecer as informações mais precisas e relevantes sobre as vulnerabilidades atuais, sem afetar as atividades do PJMA.

A integridade do resultado sobre as detecções de vulnerabilidades deverá ser avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos. A detecção manual de vulnerabilidades será considerada como complemento às detecções automáticas. E, poderão ainda ser realizados novos testes de segurança para certificação do saneamento das vulnerabilidades encontradas.

### 3.4 Elaboração e Manutenção dos Relatórios de Vulnerabilidades

A Diretoria de Informática e Automação (DIA) deverá elaborar relatórios após cada ciclo de detecção para entender e mensurar as vulnerabilidades existentes. É essencial adotar métricas padronizadas internacionalmente ou amplamente utilizadas para os relatórios de vulnerabilidades, determinando o valor percentual dos ativos de TIC vulneráveis por gravidade.

Novas vulnerabilidades serão monitoradas levando em consideração sua severidade, tipo de ambiente, tipo de sistema, autoridade de numeração e tipo de vulnerabilidade.

O relatório resultante será classificado de acordo com a criticidade das informações contidas e poderá ser encaminhado ao Comitê de Governança da Segurança da Informação para avaliação e definição das ações necessárias.

### 3.5 Banco de Dados de Vulnerabilidades

Deverá ser mantido um banco de dados de vulnerabilidades, atualizado regularmente com informações coletadas de várias fontes, para ser aplicado aos sistemas e ativos de TIC do Poder Judiciário do Estado do Maranhão. Este banco de dados poderá incluir detalhes sobre as vulnerabilidades, análises para priorização e planos de correção, proporcionando uma visão abrangente das medidas necessárias para mitigar os riscos de segurança.

### 3.6 Priorização e Correção de Vulnerabilidades

O tratamento de vulnerabilidades deverá ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, impacto em caso de exploração e no valor que o ativo de TIC tem para o Poder Judiciário do Estado do Maranhão.

As vulnerabilidades deverão ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados no quadro abaixo:

| Nível de severidade | Prazo de correção | Descrição do risco |
|---|---|---|
| Muito Crítico (6) | Até 02 dias | Situação inaceitável. Ações imediatas serão necessárias para eliminar o risco e reduzir os potenciais perigos e impactos. |
| Crítico (5) | Até 15 dias | Indivíduos mal-intencionados poderão facilmente assumir o controle dos ativos de TIC, colocando em risco toda a rede de dados do PJMA. As vulnerabilidades incluem acesso não autorizado a arquivos, execução remota de comandos e backdoors. |

| | | |
|---|---|---|
| Alto (4) | Até 30 dias | Existe o risco de indivíduos mal-intencionados adquirirem controle dos ativos de TIC ou coletarem informações altamente confidenciais, como acesso de "leitura" a arquivos, backdoors ou lista de contas de usuários(as). |
| Médio (3) | Até 45 dias | Indivíduos mal-intencionados poderão obter acesso às configurações de segurança nos ativos de TIC, permitindo o acesso não autorizado a arquivos, navegação em diretórios e ataques de negação de serviço. |
| Baixo (2) | Até 60 dias | Há o risco de coleta de informações sobre os ativos de TIC, revelando vulnerabilidades conhecidas, como versões de software instaladas. |
| Muito baixo (1) | Até 90 dias | Existe a possibilidade de coletar informações sobre os ativos de TIC por meio de serviços ou portas de conexão de rede abertas, resultando na descoberta de outras vulnerabilidades. |

Quadro 1: Nível de severidade e prazos de correção

Os testes que forem concluídos com falha deverão ser revisados até que sua execução seja concluída com êxito. Caso não seja possível, deverá ser avaliado se a vulnerabilidade será incluída na lista de exceções, conforme o processo de aceitação de risco.

Deverão ser estabelecidos mecanismos para obtenção regular de atualizações de software quando emitidas pelo fabricante ou fornecedor oficial, utilizando recursos autorizados, tais como sítios eletrônicos de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

Os alertas de vulnerabilidades, os patches de correções, as aplicações de atualizações e as ameaças emergentes que correspondam aos recursos informacionais relacionados no inventário de sistema e ativos de TIC deverão ser monitorados.

### 3.7 Das Exceções de Vulnerabilidades

Para os ativos de TIC do Poder Judiciário do Estado do Maranhão não contemplados por esta norma em função de dificuldades técnicas ou obrigações contratuais e normativas ou quaisquer exceções a esta norma, deverão ser documentadas e aprovadas.

### 3.8 Das Correções de Vulnerabilidades

As correções bem-sucedidas de vulnerabilidades poderão ser testadas por meio de detecção de vulnerabilidades de rede e de host, verificação de logs de patches, testes de invasão/penetração (pentest) e verificação das definições de configuração.

### 3.9 Implementação e Verificação das Correções de Vulnerabilidades

Somente correções de vulnerabilidades que foram efetivamente testadas e aprovadas deverão ser implantadas em produção. Atividades de correção de vulnerabilidades geralmente incluem, mas não se limitam à instalação de patches de segurança, aplicações de atualizações, bem como a ajustes de configuração e/ou remoção de software.

Quando instalações de patches de segurança e ajustes de configuração forem recomendadas para mitigar as vulnerabilidades, elas deverão seguir procedimento interno, devidamente documentado.

## 4. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

### 4.1 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação:

I - observar o inventário de ativos de TIC definidos no ANEXO V - Norma de Gestão de Ativos da PSI;

II - classificar e tratar continuamente as vulnerabilidades existentes nos ativos;

III - priorizar as ações de correção e mitigação, avaliando o nível de ameaça e criticidade das vulnerabilidades;

IV - acompanhar notificações, alertas e recomendações emitidas, como Common Vulnerabilities and Exposures (CVE) ou registros similares, para executar ações necessárias;

V - estabelecer o gerenciamento de patches, atualizações, configurações e correções de vulnerabilidades.

As diretrizes para correção ou mitigação, assim como os procedimentos para aplicação de medidas corretivas, deverão ser definidos em normativo interno.

## 5. INFRAÇÕES E PENALIDADES

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 XII
# NORMA DE DESENVOLVIMENTO SEGURO

**Normativos relacionados:**

| Ato normativo | Capítulo / Seção / Artigo |
|---|---|
| Resolução-GP nº 5/2017 | |
| Portaria nº 3/2021-DIA | |
| | |

**Versionamento:**

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

**Histórico de mudanças:**

| Data | Versão | Alterado por | Descrição das alterações |
|---|---|---|---|
| 25/07/2023 | 1.0 | | |
| 22/04/2024 | 2.0 | GTT do CGSI | Conforme arquivo de registro de alterações (changelog). |
| | | | |
| | | | |
| | | | |

## 1. INTRODUÇÃO

A Norma de Desenvolvimento Seguro complementa a Política de Segurança da Informação (PSI) e estabelece diretrizes para desenvolvimento e manutenção de softwares e sistemas que fazem parte do Poder Judiciário do Estado do Maranhão (PJMA).

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

A equipe da Coordenadoria de Sistema de Informação (CSI) será representada por servidores(as), terceirizados(as), prestadores(as) de serviço e estagiários(as) lotados(as) na própria Coordenadoria subordinada à Diretoria de Informática e Automação (DIA) do Poder Judiciário do Estado do Maranhão.

Esta norma obedecerá ao escopo definido na Política de Segurança da Informação e às diretrizes detalhadas na Resolução-GP nº 5/2017 - TJMA ou posterior que a substitua, estendendo-se a outras unidades judiciais ou administrativas que estejam envolvidas no desenvolvimento de sistemas ou aplicações no PJMA.

## 2. OBJETIVOS

Garantir que a segurança da informação seja implementada em todo ciclo de vida de desenvolvimento dos sistemas de informação.

Atender aos princípios e requisitos de segurança da informação para sistemas de informação adquiridos pelo TJMA.

Atender aos princípios e requisitos de segurança da informação para sistemas de informação mantidos e/ou desenvolvidos pela equipe de sistemas do TJMA ou por terceirizados e/ou contratados supervisionados pela equipe de sistemas do TJMA.

Adotar práticas e requisitos de segurança cibernética no desenvolvimento de projetos novos ou em desenvolvimento, tais como ativação do Múltiplo Fator de Autenticação (MFA).

## 3. DIRETRIZES

Orientações da Norma de Desenvolvimento Seguro.

### 3.1 Requisitos de Segurança da Aplicação

Ao desenvolver, ou adquirir novos sistemas de informação ou alterar os existentes, a CSI deverá identificar e especificar os requisitos de software por meio de uma avaliação de risco. Nesse processo, deverão ser avaliados, no mínimo, os seguintes itens:

I - riscos relacionados ao acesso não autorizado ao ambiente de desenvolvimento;

II - riscos relacionados a mudanças não autorizadas no ambiente de desenvolvimento;

III - vulnerabilidades técnicas dos sistemas de TIC utilizados no PJMA, incluindo relatórios e um processo de entrada, atribuição, correção e teste da correção das vulnerabilidades;

IV - riscos que uma nova tecnologia pode trazer caso seja utilizada no PJMA.

### 3.2 Requisitos de Segurança Relacionados às Redes Públicas

A Diretoria de Informática e Automação (DIA) será responsável pela definição dos controles de segurança relacionados às informações em serviços de aplicativos que trafegam pelas redes públicas, incluindo:

I - a descrição dos sistemas de autenticação a serem utilizados;

II - a descrição de como assegurar a confidencialidade e integridade das informações;

III - a descrição de como garantir o não repúdio das ações.

### 3.3 Princípios de Desenvolvimento Seguro

A Diretoria de Informática e Automação (DIA) deverá garantir a proteção integral de todos os componentes dos softwares contra adulteração e/ou acesso não autorizado, gerenciando adequadamente o controle de acesso para proteger os arquivos relacionados ao desenvolvimento. Tal medida inclui a atribuição de permissões específicas a usuários(as) ou grupos de usuários(as), restringindo o acesso apenas a desenvolvedores(as) autorizados(as). Além disso, é fundamental aplicar o princípio do menor privilégio, garantindo que cada desenvolvedor(a) tenha apenas as permissões necessárias para desempenhar suas atividades laborais.

A Coordenadoria de Sistema de Informação (CSI) será responsável por produzir software seguro que tenha vulnerabilidades de segurança mínimas em suas aplicações ou sistemas, considerando as boas práticas de desenvolvimento seguro, tais como a possibilidade de ativação do Múltiplo Fator de Autenticação (MFA) e utilização de Single Sign-On (SSO).

Para análise de segurança do código fonte, a CSI poderá utilizar ferramentas de análise estática para verificar automaticamente o código em busca de vulnerabilidades e conformidade com os padrões de codificação segura. Essas ferramentas deverão ser utilizadas para corrigir práticas de software inseguras documentadas e verificadas continuamente.

A CSI poderá, quando necessário, utilizar bibliotecas e/ou componentes de software de terceiros atualizados e confiáveis, selecionando obrigatoriamente frameworks estabelecidos no mercado e comprovadamente seguros.

A Coordenadoria de Sistema de Informação (CSI) deverá aplicar os princípios de design seguro em arquiteturas de aplicativos, seguindo as melhores práticas do mercado, como o projeto OWASP (Open Web Application Security Project).

A CSI deverá elaborar a modelagem de ameaças, sendo conduzido por pessoas especializadas que avaliam o design da aplicação e medem os riscos de segurança para cada ponto de entrada e nível de acesso.

### 3.4 Ambiente de Desenvolvimento

As aplicações desenvolvidas pelo PJMA, deverão possuir separação adequada quanto aos sistemas de desenvolvimento, homologação e produção e operação deles em diferentes domínios (por exemplo, em ambientes virtuais ou físicos separados).

As informações sensíveis, como dados pessoais, utilizadas nos ambientes de desenvolvimento e de homologação dos sistemas de informação deverão ser evitadas, substituindo-os, sempre que possível, por dados fictícios ou anonimizados.

### 3.5 Ambiente de Homologação

As alterações nas aplicações deverão ser validadas formalmente pelos(as) usuários(as) final(is) e pela equipe técnica no ambiente de homologação antes de serem aplicadas no ambiente de produção.

Dados confidenciais, bem como dados que possam estar relacionados a informações pessoais e protegidos pela Lei Geral de Proteção de Dados Pessoais (LGPD), não deverão ser utilizados nos ambientes de desenvolvimento e homologação. As exceções serão aprovadas pelo Comitê Gestor de Proteção de Dados Pessoais (CGPD), cabendo à DIA definir como esses dados serão protegidos.

A DIA é responsável por definir a metodologia, as responsabilidades e o prazo para verificar se todos os requisitos de segurança da informação foram cumpridos e se o sistema é aceitável para entrar em produção.

### 3.6 Treinamentos

A Diretoria de Informática e Automação (DIA) deverá:

I - certificar-se de que todo o pessoal de desenvolvimento de software receba treinamento para escrever código seguro, incluindo princípios gerais de segurança e práticas padrão de segurança de aplicativos;

II - garantir treinamentos que promovam a segurança dentro da equipe de desenvolvimento e construam uma cultura de segurança entre os desenvolvedores.

A Coordenadoria de Sistema de Informação (CSI) é responsável por definir as habilidades e conhecimentos necessários para o processo de desenvolvimento seguro dos treinamentos propostos.

A CSI deverá editar procedimentos baseados em boas práticas de desenvolvimento seguro para os sistemas de informações, tanto para a elaboração de novos sistemas quanto para a manutenção dos sistemas existentes, bem como definirá as normas mínimas de segurança que deverão ser cumpridas.

Os mesmos princípios de desenvolvimento seguro serão aplicados para sistemas de informação mantidos e/ou desenvolvidos por terceirizados(as) e/ou contratados(as) supervisionados(as) pela Coordenadoria de Sistema de Informação (CSI).

## 3.7 Repositórios

Os códigos-fonte deverão ser hospedados em repositórios internos cedidos pelo PJMA. Os repositórios remotos, como GitHub, GitLab ou Bitbucket só deverão ser utilizados caso sejam devidamente autorizados pela Diretoria de Informática e Automação (DIA).

O acesso aos repositórios deverá ser protegido por autenticação de dois fatores (2FA) e outras medidas de segurança, como utilização de senhas fortes.

Dependendo da sensibilidade do código ou de outros arquivos relacionados ao desenvolvimento, a CSI poderá criptografá-los para impedir o acesso não autorizado, que poderá ser alcançado por meio de criptografia de disco, criptografia de arquivo ou criptografia de transporte, seguindo as diretrizes do ANEXO IX - Norma de Gestão de Criptografia e Gerenciamento de Chaves da PSI.

## 3.8 Controle de Versão (Versionamento)

A Coordenadoria de Sistema de Informação (CSI) poderá utilizar o sistema de controle de versão (numeração, datas, etc.) e aplicar nos ambientes de desenvolvimento, homologação e/ou produção. Este sistema permite que várias pessoas trabalhem em conjunto, rastreiem as alterações feitas no código ao longo do tempo e revertam para versões anteriores, caso seja necessário.

Todos os sistemas de informação próprios e de terceiros, terão suas diversas versões disponibilizadas em ciclos de desenvolvimento, homologação e/ou produção, denominados de lançamentos (releases). Os lançamentos serão disponibilizados em intervalos fixos mínimos de 30 (trinta) dias na maioria dos casos, podendo ocorrer em intervalos menores caso haja necessidade expressa da administração.

Toda e qualquer alteração não emergencial nos sistemas de informação deverá ser incluída no próximo lançamento, de acordo com a capacidade operacional da DIA e seguindo ordem de priorização definida pela CSI.

A cada ciclo de desenvolvimento, a Diretoria de Informática e Automação informará sua capacidade operacional, a fim de suportar a priorização de suas demandas e determinada pelos seguintes fatores:

I - número de homem/horas disponíveis para cada lançamento;

II - demandas emergenciais impostas por alterações legais ou normativas, pelo Conselho Nacional de Justiça (CNJ) ou pela equipe técnica da DIA;

III - projetos definidos no Planejamento Estratégico do TJMA;

IV - correção emergencial de erros críticos dos sistemas de informação em uso;

V - projetos definidos como prioritários pela DIA ou pela Presidência do Tribunal de Justiça do Maranhão.

A Diretoria de Informática e Automação (DIA) categoriza os sistemas de informação em uso no Poder Judiciário do Estado do Maranhão (PJMA) em:

I – operacionais;

II – táticos;

III – estratégicos.

## 3.9 Cópias de Segurança

Os sistemas de informações do PJMA deverão possuir cópias de segurança (backup) regulares dos arquivos relacionados ao desenvolvimento para prevenir perdas de dados em casos de incidentes de segurança da informação, tais como, falhas de hardware, desastres naturais ou ataques cibernéticos. As cópias de segurança deverão ser armazenadas em locais seguros e testadas regularmente para garantir sua integridade e capacidade de recuperação, seguindo as diretrizes do ANEXO VIII - Norma de Cópias de Segurança da Informação da PSI.

## 3.10 Controle de Alterações

As alterações no desenvolvimento e nas manutenções dos sistemas de informação do PJMA deverão ser realizadas em conformidade com o disposto na PORTARIA-DIA nº 3/2021 ou em posterior que a substitua.

O Diretor de Informática e Automação poderá, a seu critério, autorizar alterações

emergenciais no desenvolvimento e na manutenção dos sistemas de informação do PJMA.

### 3.10.1 Alterações Emergenciais

Considera-se como “erro emergencial” qualquer comportamento anômalo ou díspar 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 de informação ou no setor que possa mitigar o erro em questão, este não será considerado emergencial.

Quando necessário, poderão ser criadas versões intermediárias dos sistemas antes da resolução do problema emergencial.

### 3.11 Propriedade Intelectual

O uso não autorizado de software ou sistema de informação de propriedade intelectual do PJMA, como reprodução, modificação, distribuição ou qualquer outra forma de uso das aplicações sem permissão expressa da Diretoria de Informática e Automação (DIA), é proibido.

## 4. NOVOS SISTEMAS DE INFORMAÇÃO

A implementação de novos sistemas de informação, seja por aquisição, doação ou desenvolvimento interno, estará condicionada à análise prévia de viabilidade técnica, realizada por 02 (dois) servidores efetivos da Diretoria de Informática e Automação (DIA).

A análise deverá resultar em um Relatório de Diagnóstico de Sistema, elaborado e assinado pelos 02 (dois) servidores efetivos da DIA. O relatório analisará a adequação do sistema proposto ao ambiente computacional do PJMA, recomendando a continuidade ou cancelamento do processo de implementação, considerando questões relacionadas à segurança da informação e privacidade de dados pessoais.

A Coordenadoria de Sistemas de Informação deverá emitir parecer técnico sobre a aquisição ou desenvolvimento de novos sistemas, assim como para a realização de manutenções evolutivas e corretivas em sistemas já existentes, necessárias para cumprimento de atos administrativos.

## 5. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

### 5.1 Diretoria de Informática e Automação

Compete exclusivamente à Diretoria de Informática e Automação (DIA):

I – gerir os softwares e sistemas de informação do PJMA;

II – homologar sistemas de informação para uso nas atividades jurisdicionais e administrativas;

III – desenvolver ou adquirir sistemas de informação, buscando dar celeridade às atividades jurisdicionais ou administrativas;

IV – realizar atividades de perícia e auditoria das operações nos sistemas de informação;

V – estabelecer políticas de homologação de softwares e sistemas;

VI – implementar mecanismos de controle de licenças de uso e bloqueio de instalações de softwares não licenciados ou não homologados;

VII – aplicar políticas de controle de alterações das configurações dos sistemas;

VIII - definir os meses de liberação dos lançamentos (releases), seguindo os ciclos estabelecidos.

IX - divulgar amplamente informações sobre as novas versões lançadas, mantendo um histórico das alterações realizadas nos últimos de 02 (dois) anos.

### 5.2 Comitê Gestor de Proteção de Dados Pessoais

É responsabilidade do Comitê Gestor de Proteção de Dados Pessoais (CGPD):

I - aprovar o uso de dados confidenciais e dados pessoais protegidos pela Lei Geral de Proteção de Dados Pessoais (LGPD) nos ambientes de desenvolvimento e homologação.

## 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 XIII
# NORMA DE PROTEÇÃO DE DADOS PESSOAIS

**Normativos relacionados:**

| Ato normativo | Capítulo / Seção / Artigo |
|---|---|
| Resolução-GP nº 5/2024 | |
| | |
| | |

**Versionamento:**

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

**Histórico de mudanças:**

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

## 1. INTRODUÇÃO

A Norma de Proteção de Dados Pessoais complementa a Política de Segurança da Informação (PSI) estabelecendo princípios que deverão 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 titulares.

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

As orientações da Norma de Proteção de Dados Pessoais são baseadas nos princípios da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) e seguem as diretrizes que constam na Resolução-GP nº 05/2024 - TJMA ou posterior que a substitua.

## 2. OBJETIVO

Assegurar o cumprimento dos requisitos legais, estatutários, regulamentares e contratuais relacionados aos aspectos de segurança da informação e 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 Poder Judiciário do Estado do Maranhão, atendendo aos padrões de proteção de dados no âmbito institucional.

#### 3.1.1 Legalidade, Transparência e Não Discriminação

O Poder Judiciário do Estado do Maranhão (PJMA) trata 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(a), 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, voluntária, 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 dos(as) titulares e os princípios previstos na Política Geral de Privacidade e Proteção de Dados Pessoais 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 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, só 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 previstos do(a) titular 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 deverá ser limitado ao mínimo necessário para o cumprimento da finalidade específica, não podendo ser excessivo ou desproporcional. Portanto, deverão ser 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 Poder Judiciário do Estado do Maranhão (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 Poder Judiciário do Estado do Maranhão (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 Poder Judiciário do Estado do Maranhão (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 - TJMA 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, poderão ser utilizadas:

I - a anonimização;

II - a pseudonimização.

### 3.1.7 Responsabilização e Prestação de Contas

O Poder Judiciário do Estado do Maranhão (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;

II - registro de dados pessoais, incluindo:

a) registros de atividades de tratamento de dados pessoais, com a descrição dos propósitos/finalidades, os(as) destinatários(as) 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 estejam agindo em conformidade com esta norma e com a legislação e regulamentação aplicáveis;

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

## 3.2 Padrões de Segurança

O Poder Judiciário do Estado do Maranhão (PJMA) está comprometido em garantir a segurança da informação e a proteção de dados pessoais, respeitando o direito fundamental do indivíduo à autodeterminação da informação.

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

Os(As) usuários(as) deverão observar as boas práticas de proteção de dados a seguir:

I - observar as normas, políticas e orientações aplicáveis adotadas pelo PJMA, ANPD e CNJ;

II - utilizar apenas meios seguros para realizar o tratamento de dados pessoais, reduzindo o risco relacionado à segurança da informação;

III - evitar o tratamento de informações desnecessárias ou em excesso ao estrito cumprimento de sua tarefa (princípio da necessidade);

IV - atentar para e-mails contendo dados pessoais, evitando o envio de informações excessivas e destinando-os apenas às pessoas necessárias;

V - não deixar documentos que contenham dados pessoais expostos na impressora, copiadora ou na mesa de trabalho;

VI - não expor a tela do monitor do computador ao tratar dados pessoais, se não estiver em uso;

VII - certificar-se de que existam salvaguardas contratuais adequadas, caso seja necessário compartilhar dados pessoais com terceiros (pessoas ou organizações);

VIII - não fotografar, filmar ou divulgar documentos que contenham dados pessoais;

IX - assegurar o direito dos(as) titulares de revisarem seus dados e, caso detectem não-conformidades, corrigir ou permitir que o(a) usuário(a) faça os ajustes necessários;

X - armazenar os dados pessoais apenas pelo prazo necessário para a finalidade para a qual foram captados, eliminando-os da forma adequada, após decorrido esse prazo;

XI - explicar com clareza aos(às) titulares a forma de utilização e de tratamento dos dados pessoais.

### 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 Poder Judiciário do Estado do Maranhão (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 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 Poder Judiciário do Estado do Maranhão (PJMA) deverá adotar medidas para garantir a aplicação das regras de privacidade e proteção de dados durante todo o ciclo de vida do tratamento (coleta, armazenamento, uso, manutenção e descarte).

### 3.2.4 Direito dos(as) Titulares de Dados Pessoais

O Poder Judiciário do Estado do Maranhão (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 Operadores

Os operadores do Poder Judiciário do Estado do Maranhão (PJMA) estarão sujeitos às obrigações estabelecidas pela legislação e regulamentação vigentes de proteção de dados pessoais.

O PJMA deverá garantir que o contrato de prestação de serviços inclua cláusulas de privacidade e proteção de dados, exigindo que o operador implemente medidas de segurança adequadas. Além disso, deverá assegurar controles técnicos e administrativos apropriados para garantir a confidencialidade, a integridade e a segurança dos dados pessoais e especificar no contrato que o operador está autorizado a tratar dados pessoais apenas mediante solicitação formal do PJMA.

Nos casos em que o operador estiver localizado fora do país em que o dado pessoal é 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

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 Poder Judiciário do Estado do Maranhão (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 realizada em prazo razoável, conforme detalhado no ANEXO VII - Norma de Gestão de Incidentes de Segurança da Informação da Política de Segurança da Informação, 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 Poder Judiciário do Estado do Maranhão (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

São responsabilidades do Comitê Gestor de Proteção de Dados Pessoais (CGPD):

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 outras atribuições determinadas pelo PJMA ou estabelecidas em normas complementares;

IV - apoiar a implementação e a manutenção de práticas de conformidade do PJMA à legislação sobre o tratamento de dados pessoais;

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

São responsabilidades da Diretoria de Informática e Automação (DIA):

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 Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e em conformidade com a legislação vigente de proteção de dados.

### 4.4 Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação

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

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

II - apoiar o(a) Encarregado(a) pelo tratamento de dados pessoais na comunicação à Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e ao(à) titular dos dados em casos de ocorrência de incidentes de segurança que possam acarretar riscos ou danos relevantes aos(às) titulares, seguindo os procedimentos estabelecidos e os prazos determinados pela legislação e regulamentação vigentes.

### 4.5 Usuários(as)

São responsabilidades dos(as) usuários(as) do Poder Judiciário do Estado do Maranhão (PJMA):

I - encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento ao(à) Encarregado(a) pelo tratamento de dados pessoais ou, quando pertinente, ao Comitê Gestor de Proteção de Dados Pessoais (CGPD);

II - comunicar ao(à) Encarregado(a) qualquer evento que coloque em risco os dados pessoais tratados pelo PJMA, garantindo a pronta notificação de incidentes de segurança ou outras irregularidades que possam comprometer a proteção de dados pessoais;

III - responder pela inobservância das diretrizes da segurança da informação e

da proteção de dados pessoais, assegurado o contraditório e a ampla defesa.

Os(As) usuários(as) poderão ser responsabilizados(as) por condutas ilícitas relacionadas ao tratamento de dados pessoais e acesso à informação quando:

I - recusar a fornecer a informação requerida nos termos da lei, retardar deliberadamente seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa;

II - utilizar indevidamente, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenha acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;

III - agir com dolo ou má-fé na análise das solicitações de acesso à informação;

IV - divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal;

V - impuser sigilo à informação para obtenção de proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem;

VI - ocultar da revisão de autoridade superior competente informação sigilosa para beneficiar a si ou a outrem, ou em prejuízo de terceiros;

VII - destruir ou subtrair, por qualquer meio, documentos concernentes a possíveis violações de direitos humanos por parte de agentes do Estado;

VIII - agir em desacordo com disposto na Lei Geral de Proteção de Dados Pessoais (LGPD).

## 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.

# PLANO DE COMUNICAÇÃO

# PODER JUDICIÁRIO DO ESTADO DO MARANHÃO

# Sumário

# APRESENTAÇÃO

O Plano de Comunicação do Poder Judiciário do Estado do Maranhão (PJMA) representa um novo marco na jornada da instituição, levando ao conhecimento dos cidadãos os seus direitos à proteção de dados pessoais.

Como guardião da privacidade e da proteção dos dados pessoais dos cidadãos que utilizam seus serviços, o PJMA reconhece a importância de uma comunicação transparente, acessível, orientativa e educativa, por isso, criou o presente Plano de Comunicação.

## Construindo uma nova cultura de proteção de dados

Uma das premissas da atuação do PJMA é a formação de uma nova cultura: a de proteção dos dados pessoais no Tribunal. Isso exige uma comunicação eficaz, clara e de fácil acesso. Através do fortalecimento da comunicação, o PJMA busca atuar de forma estratégica com os diversos públicos que usufruem de seus serviços.

## Valores fundamentais da comunicação do PJMA

O Plano de Comunicação do PJMA tem como base os seguintes valores, que refletem a missão da instituição de promover a consciência sobre a importância da proteção de dados para garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD):

- Transparência: O PJMA se compromete a ser transparente em suas ações e decisões relacionadas à proteção de dados pessoais.
- Acessibilidade: A informação sobre proteção de dados deve ser acessível a todos, de forma clara e concisa.
- Orientação: O PJMA tem o compromisso de fornecer orientações práticas para que os cidadãos possam exercer seus direitos.
- Educação: O Tribunal promoverá ações educativas para conscientizar o público-alvo, interno e externo, sobre a importância da proteção de dados pessoais.

## Construindo um ambiente digital mais seguro e respeitoso

O PJMA está empenhado em construir uma cultura de respeito à garantia fundamental à privacidade e à proteção de dados pessoais com vistas a criar um ambiente digital mais seguro e respeitoso para todos. O Tribunal entende que a informação é a chave para dar poder aos cidadãos.

## INTRODUÇÃO

O PJMA tem como missão, promover a efetividade da Justiça servindo à sociedade na solução de conflitos, respeitando e protegendo os dados pessoais e a privacidade dos cidadãos, contribuindo para o fortalecimento do Estado Democrático de Direito.

O PJMA quer ser reconhecido nacionalmente pela prestação jurisdicional de qualidade que, também, integra a proteção de dados e da privacidade como princípios fundamentais, decorrente de práticas modernas e inovadoras de gestão.

O PJMA reconhece a importância da proteção de dados pessoais e da privacidade dos cidadãos e se compromete a:

- Tratar os dados pessoais de forma lícita, transparente e segura.
- Garantir aos cidadãos o direito de acesso, correção, exclusão e portabilidade de seus dados pessoais.
- Adotar medidas para proteger os dados pessoais contra acessos não autorizados, uso indevido, divulgação, perda ou destruição.
- Promover a cultura de proteção de dados pessoais entre seus magistrados, servidores, terceirizados e estagiários.
- Manter canais de comunicação acessíveis para que os cidadãos possam exercer seus direitos relativos à proteção de dados pessoais.

O PJMA está ciente de que a proteção de dados pessoais e da privacidade é fundamental para a construção de uma sociedade justa e democrática. Por isso, o Tribunal se compromete a implementar medidas eficazes para garantir a proteção dos dados dos cidadãos em todas as suas atividades.

O presente Plano de Comunicação visa atender aos requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD) e a Resolução-GP nº 52024, de 24 de janeiro de 2024, do Tribunal de Justiça do Estado do Maranhão - TJMA ou posterior que a substitua, no âmbito do PJMA. Ele abrange, entre outras, ações estratégicas para conscientizar e educar magistrados, servidores, terceirizados e estagiários e o público em geral sobre a importância da proteção de dados pessoais.

A adequação à LGPD é um programa que exige o engajamento de todos os membros do Tribunal de Justiça do Maranhão. O Plano de Comunicação apresentado neste documento é um instrumento fundamental para garantir que a informação sobre a LGPD chegue a todos os públicos-alvo de forma clara, objetiva e acessível.

## PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Em um mundo cada vez mais digital, onde os dados pessoais são a moeda de troca da economia global, a Lei Geral de Proteção de Dados Pessoais (LGPD) surge como um marco na defesa da privacidade e dos direitos dos cidadãos brasileiros.

Embora a discussão sobre o tema tenha se iniciado na década de 1970, com a Alemanha como pioneira na regulamentação, no Brasil a LGPD só foi promulgada em 2018, após anos de debate. Inspirada no GDPR da União Europeia, a lei brasileira entrou em vigor em 2020, consolidando o direito à proteção de dados como uma garantia fundamental na Constituição Federal.

Nesse contexto, o Plano de Comunicação do PJMA assume um papel fundamental na sensibilização da sociedade sobre a importância da LGPD e na promoção de práticas responsáveis no tratamento de dados pessoais pelo Tribunal.

O Plano de Comunicação do PJMA é um instrumento essencial para garantir que os dados pessoais dos cidadãos sejam tratados de forma ética e responsável, em consonância com os princípios da LGPD.

Principais pontos da LGPD:

- Regula o tratamento de dados pessoais no Brasil;
- Protege a privacidade dos cidadãos;
- Garante o uso transparente, responsável e seguro dos dados pessoais;
- A Autoridade Nacional de Proteção de Dados (ANPD) é a responsável pela sua aplicação e fiscalização.

## PLANO DE COMUNICAÇÃO

### 1. Objetivos

- Conscientizar: Informar sobre a LGPD, seus princípios e conceitos, e as responsabilidades do PJMA na proteção de dados pessoais.
- Educar: Capacitar magistrados, servidores, terceirizados e estagiários sobre boas práticas na gestão de dados, incluindo coleta, armazenamento, tratamento, compartilhamento e exclusão.
- Promover a cultura de proteção de dados: Incentivar a adoção de medidas para garantir a segurança e a privacidade dos dados pessoais sob responsabilidade do PJMA.
- Transparência: Divulgar de forma clara e acessível as medidas de adequação à LGPD adotadas pelo PJMA.
- Prestação de contas: Demonstrar o compromisso do PJMA com a proteção de dados pessoais.

## 2. Público-alvo

- Interno: Magistrados, servidores, terceirizados e estagiários.
- Externo: Advogados, partes em processos, imprensa e sociedade em geral.

## 3. Eixos Estratégicos

### 3.1. Informação

- Criação de um canal específico no portal do PJMA sobre a LGPD, com perguntas frequentes, cartilhas, vídeos explicativos e outros materiais informativos.
- Elaboração de um guia prático sobre a LGPD para magistrados e servidores.
- Realização de campanhas internas de conscientização sobre a LGPD, com banners, cartazes, e-mails informativos e outros materiais.
- Promoção de palestras, workshops e treinamentos sobre a LGPD para magistrados, servidores, terceirizados e estagiários.
- Criação de um canal de comunicação para dúvidas e sugestões sobre a LGPD.

### 3.2. Capacitação

- Cursos online e presenciais sobre a LGPD para magistrados, servidores, terceirizados e estagiários (Item 4.3);
- Workshops e palestras sobre temas específicos da LGPD, como o tratamento de dados sensíveis e o uso de cookies (Item 4.3);
- Treinamento sobre segurança da informação e privacidade (Anexo I).

### 3.3. Diálogo e engajamento

- Realização de consultas públicas sobre temas relacionados à LGPD.

- Promoção de eventos para discutir a LGPD com a comunidade jurídica e a sociedade civil.

## 4. Plano de Ação

### 4.1. Ações

- **Elaboração de um guia prático sobre a LGPD para magistrados e servidores:** O guia deve ser um material de fácil consulta, com linguagem clara e objetiva, que orienta os magistrados e servidores sobre como lidar com dados pessoais em suas atividades diárias.
- **Realização de campanhas internas de conscientização sobre a LGPD:** As campanhas devem utilizar diversos canais de comunicação, como banners, cartazes, e-mails informativos e outros materiais, para conscientizar os magistrados, servidores, terceirizados e estagiários sobre a importância da proteção de dados.
- **Promoção de palestras, workshops e treinamentos sobre a LGPD:** As palestras, workshops e treinamentos devem ser realizados para diferentes públicos, como magistrados, servidores, terceirizados, estagiários e público em geral, com o objetivo de aprofundar o conhecimento sobre a LGPD e suas implicações.

### 4.2. Canais de Comunicação

- Portal do PJMA: Página LGPD, com informações sobre a lei, as medidas tomadas pelo PJMA - https://www.tjma.jus.br/hotsite/lgpd
- Endomarketing: Envio de informativos periódicos sobre a LGPD para magistrados, servidores, terceirizados e estagiários.
- Redes sociais: Publicação de conteúdos informativos sobre a LGPD nas redes sociais do PJMA (Facebook, Twitter, Instagram e LinkedIn).
- Palestras e workshops: Realização de palestras e workshops sobre a LGPD para magistrados, servidores, terceirizados, estagiários e público em geral.
- Cartilhas e materiais informativos: Elaboração de cartilhas e materiais informativos sobre a LGPD em linguagem acessível.
- Canal de atendimento: Criação de um canal de atendimento específico para dúvidas e sugestões sobre a LGPD. (https://sistemas.tjma.jus.br/attende/xhtml/frmAvisoOuvidoria.jsf)

4.3. Treinamento LGPD

Mês 1-2: Fundamentos da LGPD

- Lançamento da campanha de conscientização sobre a LGPD.
- Palestra/Workshop: Introdução à LGPD

i.
  - Contexto mundial sobre a utilização de dados pessoais;
  - Explanação dos conceitos fundamentais da LGPD.

- Criação da página específica sobre a LGPD no site do TJMA.

- E-mails Informativos / Material Impresso e Digital (folhetos, cartazes, infográficos):

i.
  - Definições:

i.
  - Classificação/tipo de dados;
  - Tratamento de dados pessoais;
  - Partes envolvidas no tratamento de dados pessoais.

- Canais de Suporte Contínuo:

i.
  - Estabelecimento de um canal de suporte contínuo para recebimento e esclarecimento de dúvidas.
  - Uso de Cookies.

- Avaliação e Feedback:

i.
  - Desenvolvimento de simulações on-line para testar o conhecimento dos magistrados, servidores, terceirizados e estagiários;
  - Realização de pesquisas periódicas para avaliar a eficácia das iniciativas de conscientização.

Mês 3-4: Bases Legais da LGPD

- Palestra/Workshop: Explorando as Bases Legais da LGPD

- Explanação das bases legais para o tratamento de dados pessoais;
- Estudo de casos para compreensão prática.

- E-mails Informativos / Material Impresso e Digital (folhetos, cartazes, infográficos):

i.
  - Bases Legais:

i.
  - Exercício regular de direitos em processos;
  - Proteção da vida ou da incolumidade física do titular;
  - Tutela da Saúde;
  - Legítimo Interesse;
  - Proteção do Crédito;
  - Execução de contrato ou procedimentos preliminares;
  - Órgãos de Pesquisa;
  - Políticas Públicas;
  - Cumprimento de Obrigação Legal ou Regulatória;
  - Consentimento.

- Avaliação e Feedback:

i.
  - Desenvolvimento de simulações on-line para testar o conhecimento dos magistrados, servidores, terceirizados e estagiários;
  - Realização de pesquisas periódicas para avaliar a eficácia das iniciativas de conscientização.

Mês 5-6: Compreendendo os Direitos dos Titulares dos Dados

- Palestra/Workshop: Direito dos Titulares de Dados Pessoais

i.
  - Workshops interativos explorando os direitos dos titulares de dados;
  - Discussões de casos práticos e estudos de exemplo.

- E-mails Informativos / Material Impresso e Digital (folhetos, cartazes, infográficos):

i.
  - Direito dos Titulares:

i.
  - Confirmação da Existência de Tratamento;
  - Acesso aos Dados;
  - Correção de dados incompletos, inexatos ou desatualizados;
  - Anonimização, bloqueio ou eliminação de dados desnecessários;
  - Portabilidade de Dados;
  - Eliminação de dados pessoais tratados com o consentimento do titular;
  - Informação sobre dados compartilhados;
  - Informação da consequência do não consentimento;
  - Revogação do consentimento.

- Avaliação e Feedback:

i.
  - Desenvolvimento de simulações on-line para testar o conhecimento dos magistrados, servidores, terceirizados e estagiários;
  - Realização de pesquisas periódicas para avaliar a eficácia das iniciativas de conscientização.

Mês 7-8: Responsabilidade Institucional e Adequação de Processos

- Palestra/Workshop: Direito dos Titulares de Dados Pessoais

i.
  - Palestras detalhando as responsabilidades da instituição perante a LGPD.
  - Foco na revisão de processos internos com destaque para boas práticas na coleta e tratamento de dados, para garantir a conformidade com a LGPD.
  - Identificação de áreas de melhoria e ajustes necessários.

- Intranet: Documentação e Recursos de Adequação

i.
  - Disponibilização de documentos, modelos de políticas internas e recursos para auxiliar na adequação.

- E-mails Informativos / Material Impresso e Digital (folhetos, cartazes, infográficos):

i.
  - Campanha “Práticas Seguras, Dados Seguros”:

i.
  - Lançamento de uma campanha interna destacando comportamentos seguros.

- Avaliação e Feedback:

i.
  - Desenvolvimento de simulações on-line para testar o conhecimento dos colaboradores;
  - Realização de pesquisas periódicas para avaliar a eficácia das iniciativas de conscientização.

## 5. Medidas adotadas pelo PJMA

- Diagnóstico de Segurança da Informação e Privacidade;
- Nomeação do Encarregado de Dados Pessoais - Resolução-GP nº 05, de 24 de janeiro de 2024;
- Instituição do Comitê de Governança de Segurança da Informação (CGSI), do Comitê Gestor de Proteção de Dados Pessoais (CGPD), da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) e do Comitê de Crise Cibernética (CCCiber) no Poder Judiciário do Estado do Maranhão (Atualização de Normativo) - Resolução-GP nº 14, de 7 de março de 2024;
- Criação da página LGPD (hotsite) no portal do PJMA - https://www.tjma.jus.br/hotsite/lgpd;
- Atualização da página LGPD no portal do PJMA - https://www.tjma.jus.br/hotsite/lgpd - (Ações realizadas);
- Criação e Publicação da Política Geral de Privacidade e Proteção de Dados Pessoais – Resolução-GP nº 05, de 24 de janeiro de 2024;
- Criação e Publicação da Política de Segurança da Informação e seus Anexos – Resolução-GP nº 39, de 12 de junho de 2023 - TJMA;
- Criação e Publicação da Política de Navegação do Portal - https://www.tjma.jus.br/midia/lgpd/pagina/hotsite/505375/politica-de-navegacao-do-portal;
- Criação de um canal de acesso à informação sobre a LGPD no portal do PJMA https://www.tjma.jus.br/hotsite/lgpd;
- Curso de formação sobre LGPD para magistrados https://www.tjma.jus.br/midia/portal/noticia/511288/PJMA-promove-formacao-sobre-lgpd-no-judiciario;
- Divulgação das ações de proteção de dados do PJMA nas redes sociais e outros canais de comunicação:
    - Curso de formação sobre LGPD para magistrados https://www.tjma.jus.br/midia/portal/noticia/511288/PJMA-promove-formacao-sobre-lgpd-no-judiciario;

https://www.tjma.jus.br/midia/portal/noticia/504487/trees;

    - Curso de formação para servidores de diversas áreas do PJMA https://www.tjma.jus.br/midia/portal/noticia/509840/profissionais-do-judiciario-discutem-sobre-privacidade-e-protecao-de-dados;
- Criação do Canal de Atendimento para dúvidas e sugestões sobre a LGPD https://sistemas.tjma.jus.br/attende/xhtml/frmAvisoOuvidoria.jsf;
- Proteção de Dados Pessoais nos serviços notariais e de registro https://www.tjma.jus.br/midia/portal/noticia/507901/cgj-ma-orienta-cartorios-sobre-diretrizes-estrategicas-e-lgpd;

https://www.tjma.jus.br/midia/portal/noticia/508852/cartorios-participam-de-capacitacao-sobre-protecao-de-dados-pessoais;
https://www.tjma.jus.br/midia/esmam/noticia/504347/curso-sobre-lgpd-para-serventuarios-da-justica-do-maranhao;
https://www.tjma.jus.br/midia/portal/noticia/503911/corregedoria-promove-workshop-sobre-lei-

geral-de-protecao-de-dados-para-cartorios;

- Mapeamento de Dados Pessoais e avaliação de riscos de segurança da informação e privacidade;
- Criação do Procedimento para Violação de Dados Pessoais e simulação de respostas.
- Ações do programa de adequação realizadas e/ou em andamento (Anexo II);

## 6. Recursos Humanos

- A Assessoria de Comunicação da Presidência (ASSCOM) do PJMA será responsável pela execução do plano de comunicação.

## 7. Indicadores de Sucesso

- Nível de conhecimento sobre a LGPD entre magistrados, servidores, terceirizados e estagiários.
- Número de acessos à página específica sobre a LGPD no site do PJMA.
- Número de participantes em palestras, workshops e cursos online sobre a LGPD.
- Número de dúvidas e sugestões recebidas pelo canal de atendimento.
- Nível de adequação do PJMA à LGPD.

## 8. Documentos de referência

- https://www.planalto.gov.br/ccivil 03/ ato2015-2018/2018/lei/l13709.htm - LGPD - (Lei Geral de Proteção de Dados Pessoais)
- https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd - Perguntas Frequentes – ANPD
- Resolução-GP nº 5/2024 PJMA - Nomeação do Encarregado de Dados Pessoais
- Ato da Presidência-GP nº 39/2021 e Ato da Presidência-GP nº 862022 - Criação do Comitê Gestor de Proteção de Dados Pessoais (CGPD)
- Resolução-GP nº 5/2024 PJMA - Criação e Publicação da Política Geral de Privacidade e Proteção de Dados Pessoais
- Resolução-GP nº 39/2023 PJMA - Criação e Publicação da Política de Segurança da Informação (PSI)
- Política de Navegação do Portal https://www.tjma.

jus.br/midia/lgpd/pagina/hotsite/505375/politica-de-navegacao-do-portal

- Página LGPD no portal do PJMA https://www.tjma.jus.br/hotsite/lgpd

# ANEXO I

# PLANO DE CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE – 2023/2024

## Documento

| | |
|---|---|
| **Versão:** | 1.0 |
| **Data da versão:** | 31/01/2024 |
| **Criado por:** | Frederico Coelho, Marcelo Black e Thiago Vieira |
| **Classificação:** | Restrito |

## Histórico de Alterações

| Data | Versão | Responsável | Descrição da alteração |
|---|---|---|---|
| 31/01/2024 | 1.0 | FAC Tecnologia | Criação do documento. |
| | | | |
| | | | |

## 1. Introdução

Este documento tem como objetivo apresentar as ações propostas para o Plano de Conscientização e Treinamento em Segurança da Informação e Privacidade no ano de 2024, desenvolvido pelo Comitê Gestor de Proteção de Dados Pessoais do Poder Judiciário do Estado do Maranhão (PJMA).

O objetivo deste Plano é treinar e conscientizar usuários do PJMA sobre tópicos importantes de Segurança da Informação e Privacidade, tais como:

- Políticas e Normas;
- O valor dos dados e das informações;
- Ameaças (humanas e cibernéticas);
- Certificado Digital e senhas;
- Boas práticas para a proteção de dados pessoais;
- Recomendações para a utilização de ativos tecnológicos (dispositivos, sistemas e a internet).

Salienta-se que, nem sempre a segurança da informação está restrita a meios digitais, por isso, o Plano aborda temas cotidianos que podem favorecer o vazamento de informações e comumente são desconsiderados nas atividades diárias dos usuários.

## 2. Justificativa

Mesmo com as organizações alocando mais tempo e dinheiro para lidar com os riscos de segurança, sobretudo cibernéticos, a ocorrência de incidentes de segurança e de violações de dados não está diminuindo.

Mas por que isso? Simplificando, a maioria das organizações realiza investimentos em controles de segurança para o núcleo da sua estrutura de TI (data centers, servidores, etc) não estão fazendo o suficiente para combater as ameaças em evolução. Com os cibercriminosos usando métodos mais avançados técnicas para explorar humanos, a rota tradicional de treinamento de conscientização de segurança uma vez por ano não é suficiente para proteger as organizações da perda de informações confidenciais, danos à reputação e repercussões financeiras.

Os usuários há muito são vistos como o “elo mais fraco” na cadeia de segurança cibernética de uma organização e, com erro humano ainda sendo a causa número um de violações de dados.

## 3. Da composição do Plano

A disseminação deste Programa se dará por meio de ações de comunicação, campanhas internas, externas e institucionais, com treinamentos, cursos de capacitação, eventos e ferramentas de atualização periódica, com objetivo de concretizar sua aderência.

O PJMA fornecerá treinamento a todos os usuários e prestadores de serviço que tratam dados pessoais para ajudá-los a compreender suas responsabilidades ao manipular dados

pessoais. Também serão promovidas ações de educação para todos os usuários e fornecedores-chave, para a conscientização sobre procedimentos de segurança da informação.

Haverá amplo canal de comunicação aos usuários via informativos, nos respectivos departamentos, com o intuito de promover ações de divulgação de boas práticas sobre procedimentos de segurança da informação, englobando cuidados da proteção de dados pessoais.

Deverá ser desenvolvido canal interno para atender às dúvidas dos magistrados, servidores, terceirizados e estagiários em procedimentos de tratamento de dados pessoais, a fim de garantir a adoção das melhores práticas em todos os procedimentos e operações, facilitando a comunicação com o Comitê Gestor de Proteção de Dados Pessoais (CGPD) .

Para que o pessoal entenda a importância da gestão da segurança da informação e sua própria contribuição para proteção e a compreensão das consequências da violação das regras de segurança, os treinamentos e atividades de sensibilização poderão ser realizadas através de diferentes meios, como:

- Ações de endomarketing
- Intranet
- Newsletter
- Reuniões conjuntas
- E-learning
- Mensagens de e-mail internas
- Gravações em vídeo
- Workshops online
- Quiz, e etc.

A implementação de treinamentos e conscientização foi planejada em duas ações. Um Plano para trabalho de conscientização e outro Plano para Capacitação dos usuários, dividido por tipos e necessidade.

## 4. Plano de Conscientização

Este plano está estruturado em formato de tabela em que na primeira coluna tem-se o mês previsto da ação; na segunda, a descrição resumida da atividade; na terceira observações.

| PROGRAMAÇÃO DE TEMAS PARA TREINAMENTO RECORRENTES | | | |
|---|---|---|---|
| Mês | Assuntos / Tópicos | Detalhamento | Público Alvo |
| | Introdução à | Importância da Segurança da Informação. Conceitos básicos de | Magistrados, |

| | | | |
|---|---|---|---|
| Abril / 2024 | Segurança da Informação e Cibersegurança | cibersegurança<br>Ameaças e riscos comuns.<br>Política de Segurança da Informação. | Servidores, Estagiários e Terceirizados. |
| Abril / 2024 | Controle de Acesso e Gestão de Identidades | Orientações, responsabilidades e cuidados para uso das Credenciais de acesso (certificado digital, senhas, MFA).<br>Apresentar Norma. | Magistrados, Servidores, Estagiários e Terceirizados. |
| Maio / 2024 | Classificação e tratamento da informação | Orientar os usuários sobre as categorias de Classificação da Informação e como rotular de acordo com sua sensibilidade.<br>Apresentar Norma. | Magistrados, Servidores, Estagiários e Terceirizados. |
| Junho / 2024 | Segurança física | Aspectos e ameaças relacionadas à segurança física e controles de acesso.<br>Apresentar Norma. | Magistrados, Servidores, Estagiários e Terceirizados. |
| Julho / 2024 | Uso aceitável dos ativos | Orientações para uso adequado dos ativos de informação, como computador, pasta de rede, e-mail, internet, impressora, acesso remoto, dispositivo móvel, ambiente colaborativo, etc.<br>Apresentar Norma. | Magistrados, Servidores, Estagiários e Terceirizados. |
| Agosto / 2024 | Incidentes e violação de dados | Identificar um incidente e saber como reportar.<br>Cenários de incidentes que já aconteceram no judiciário e como prevenir.<br>Apresentar Norma. | Magistrados, Servidores, Estagiários e Terceirizados. |

| | | | |
|---|---|---|---|
| Setembro / 2024 | Cópias de segurança | Importância da salvaguarda de informações.<br>Apresentar Norma. | Magistrados, Servidores, Estagiários e Terceirizados. |
| Outubro / 2024 | Certificado Digital e criptografia | Boas práticas no uso de certificado digital e criptografia.<br>Apresentar Norma. | Magistrados, Servidores, Estagiários e Terceirizados. |
| Novembro / 2024 | Proteção de Dados Códigos maliciosos Engenharia Social | Tipos de ataques de engenharia social<br>Como identificar e evitar fraudes<br>Importância da conscientização do usuário | Magistrados, Servidores, Estagiários e Terceirizados. |
| Dezembro / 2024 | Continuidade de Negócios | Importância do planejamento para respostas em caso de desastres relacionados a TIC.<br>Apresentar Norma. | Magistrados, Servidores, Estagiários e Terceirizados. |

| TEMAS ESPECIAIS PARA TREINAMENTOS OCASIONAIS | | |
|---|---|---|
| Formato Sugerido | Assuntos / Tópicos | Detalhamento |
| Workshop (2 horas) | Proteção de Dados Pessoais | • Leis de privacidade de dados (exemplo: LGPD, GDPR)<br>• Responsabilidades individuais na proteção de dados<br>• Práticas adequadas de coleta e armazenamento de dados<br>• Responsabilidade individual na proteção de dados pessoais no ambiente corporativo |
| | | • Utilização de aplicativos desatualizados<br>• Utilização de aplicativos pirateados<br>• Backup de dados |

| | | |
|---|---|---|
| Workshop (2 horas) | Comportamentos para o uso Internet: Orientações Práticas | • Compras na internet e pagamentos eletrônicos<br>• Cuidados com a conta de e-mail e de redes sociais<br>• Senhas<br>• WhatsApp |
| Workshop (2 horas) | Golpes Digitais: como acontecem? | • Whatsapp<br>• Instagram e Redes Sociais<br>• Instituições financeiras<br>• Utilização de PIX<br>• Compras na internet<br>• Boletos falsificados |

## 5. Plano de Capacitação

Este plano está estruturado em formato de tabela em que na primeira coluna tem-se o mês previsto da ação; na segunda, a descrição resumida da atividade; na terceira observações.

| Público-alvo | Curso | Descrição | Ementa Programa do curso | Carga horária |
|---|---|---|---|---|
| CGPD | Plano de Respostas a Incidentes e Violação de Dados Pessoais | | | |
| CGPD | Data Mapping e LGPD: Como tratar dados com segurança na prática | | | |
| CGPD | Gestão de Riscos de Segurança da Informação e Privacidade | | | |
| CGPD | Políticas e Legal Design | | | |
| CGPD | Elaboração do | | | |

| | | | | |
|---|---|---|---|---|
| | Relatório de Impacto de Proteção de Dados (RIPD) | | | |
| Magistrados | Segurança da Informação prática para magistrados | | | |
| Coordenadoria de Sistemas da Informação - CSI | Desenvolvimento Seguro | | | |
| Coordenadoria de Infraestrutura e Telecomunicações - CIT / Segurança | Implementação do SGSI com a ISO/IEC 27001:2022 | | | |
| CAU | Fundamentos de Segurança da Informação e Privacidade | | | |

## 6. Da Responsabilidade da Execução

O CGPD ficará responsável pela criação de conteúdos escritos, audiovisuais ou mesmo realização de atividades presenciais como palestras e workshops.

A ESMAM ficará responsável pela viabilização dos treinamentos previstos no Plano de Treinamento.

# ANEXO II

# RELATÓRIO DE ATIVIDADES PROGRAMA DE ADEQUAÇÃO LGPD – PJMA

## 2023/2024

## Documento

| | |
|---|---|
| **Versão:** | 1.0 |
| **Data da versão:** | 05/02/2024 |
| **Criado por:** | Frederico Coelho, Marcelo Black e Thiago Vieira |
| **Classificação:** | Restrito |

## Histórico de Alterações

| Data | Versão | Responsável | Descrição da alteração |
|---|---|---|---|
| 05/02/2024 | 1.0 | FAC Tecnologia | Criação do documento. |
| | | | |
| | | | |

## 1. ATIVIDADES REALIZADAS – Abril e Maio 2023

O início das atividades do Programa (Projeto) de adequação LGPD do TJMA teve como ponto de partida a reunião de kick-off, realizada no dia 19/04/2023 de forma remota, através da plataforma Teams.
Na ocasião, foi apresentado, conforme mostra a imagem abaixo, o macro cronograma do Programa de Adequação.


Foi acordado na reunião de kick-off, que seriam realizadas, às quintas-feiras, reuniões semanais entre equipe do Projeto e Consultoria para apoio no mapeamento e ações paralelas. Todas as reuniões estão sendo gravadas.

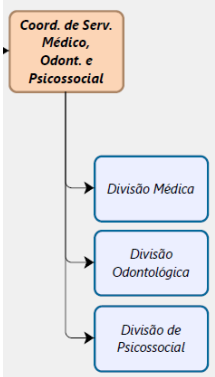
Atividades que foram realizadas até o dia 31/05/2023.

1. Definição das primeiras áreas a serem mapeadas (área médica);
2. Workshop Mapeamento de Dados Pessoais para área médica;
3. Preenchimento das planilhas pelo time do TJ-MA;
4. Reuniões semanais para tirar dúvidas e ajustes com a consultoria;
5. Apresentação da plataforma Securiti.ai com engenheiro da plataforma e fornecedor Shield;
6. Visita presencial do consultor Frederico Coelho com validação dos mapeamentos;
7. Visitas em áreas estratégicas;
8. Avaliação inicial da Política de Privacidade;
9. Avaliação inicial do fluxo de atendimento dos titulares;

Como resultado do inventário de tratamento de dados pessoais da área médica, para

atendimento do Art. 37 da LGPD, foram gerados os resultados abaixo:

- 34 Atividades de Tratamento de Dados Pessoais;
- 11 riscos identificados;
- 2 oportunidades de melhoria.




Como resultado o inventário/mapeamento de dados pessoais, foi possível identificar alguns riscos e oportunidades conforme tabela abaixo:

| RISCOS | CENÁRIOS |
|---|---|
| **Psicosocial - Whatsapp** | Uso de chip institucional em celular particular. Podem receber documentos com dados sensíveis. Pacientes entram em contato a qualquer hora do dia com o psicólogo. Criar procedimento para limpeza mensal do celular, em relação aos anexos que recebem. |
| **Psicosocial - Video Conferencia** | Em situações pontuais, as vídeos são realizadas através de Whatsapp. Sem procedimento formal definido para esta atividade. |
| **Psicosocial - Planilha de triagem** | Sem nível de permissão definido no Google Workspace. Criar restrições de acesso, para isso deve-se orientar os usuários da área. |
| **Psicosocial - Senhas** | Compartilhamento de senhas. |
| **DIVISÃO MÉDICA - Senhas** | Compartilhamento de senhas. |
| **DIVISÃO MÉDICA - Estagiária** | Estagiária não possui conta de acesso e utiliza contas de colegas. |
| **DIVISÃO MÉDICA - Descarte** | Possuem fragmentadora, porém foi identificado documentos de saúde descartados no lixo de forma imprópria. |
| **DIVISÃO MÉDICA - Arquivo** | Sala do arquivo a chave fica sempre na porta. Recomendável trancar e somente pessoas autorizadas terem acesso. |
| **DIVISÃO MÉDICA - Certificado Digital** | Pasta de rede possui uma pasta com todos os certificados dos profissionais. Determinada pessoa pode assinar por outra. |
| **Política de Privacidade** | Definições e atribuições dos agentes de tratamento não estão corretas. Art. 6 |
| **Atendimento aos Titulares** | Fluxo definido não está implementado. Recomenda-se atualizar o procedimento com validação do titular. |

| OPORTUNIDADES | CENÁRIOS |
|---|---|
| **DIVISÃO MÉDICA - Arquivo** | Oportunidade para digitalizar todo arquivo físico e seguir com arquivamento e/ou descarte. |
| **DIVISÃO MÉDICA - PROCESSOS: LICENÇA À GESTANTE (MATERNIDADE) - SERVIDORA 1º GRAU** | O questionário de acompanhamento familiar em PDF, é realizado o download para preenchimento, para depois ser digitalizado, enviado e incluindo no sistema. Pode ser melhorado, incorporando o formulário no sistema. |

Foi apresentado na reunião do dia 01/06/2023 os resultados gerados pela consultoria incluíndo os próximos passos, conforme elencados abaixo:

- Workshop de mapeamento de Dados Pessoais com RH (Contrato - Direitos e Deveres);
- Mapeamento das áreas;
- Validação do mapeamento;
- Levantamento de quantidade de conectores para ferramenta da Securiti.ai (orçamento);
- Agendar nova apresentação da Securiti.ai com módulo de Compliance/Riscos;
- Análise e atualização da Política de Privacidade;
- Análise e atualização do Fluxo de Atendimento aos Titulares;
- Definição das próximas áreas a serem mapeadas.

## 2. ATIVIDADES REALIZADAS – Junho 2023

Atividades realizadas até o dia 30/06/2023.

1. Reuniões semanais para tirar dúvidas e ajustes com a consultoria;
2. Avaliação da Política de Privacidade;
3. Avaliação do fluxo de atendimento dos titulares;
4. Reuniões com as áreas do RH para mapeamento de dados pessoais;
5. Estruturação do mapeamento de dados pessoais do RH;
6. Apresentação de riscos relacionados ao processo de atendimento aos titulares;
7. Enviado sugestão de nova versão da Política de Privacidade e Proteção de Dados;
8. Sugestões para novo fluxo de atendimento aos titulares;
9. Levantamento de propostas e fornecedores para solução de GRC.
10. Todas as reuniões estão gravadas em nosso ambiente do Teams.

## 3. ATIVIDADES REALIZADAS – Julho 2023

Atividades realizadas até o dia 31/07/2023.

1. Reuniões semanais para tirar dúvidas e ajustes com a consultoria;
2. Reuniões com todas as áreas da Diretoria de RH para mapeamento de dados pessoais;
3. Workshop sobre mapeamento para as áreas da Diretoria de RH que estavam pendentes;
4. Estruturação do mapeamento de dados pessoais de todas as áreas da Diretoria de RH;
5. Levantamento de riscos relacionados aos processos que estão sendo mapeados;
6. Reunião com grupo de trabalho do Projeto para relatar a dificuldade no avanço dos mapeamentos de dados;
7. Reunião com Dr. Francisco para tratar de melhorias no mapeamento de dados;
8. Todas as reuniões estão gravadas em nosso ambiente do Teams.

## 4. ATIVIDADES REALIZADAS – Agosto 2023

Atividades realizadas no mês de agosto de 2023.

1. Reuniões semanais para tirar dúvidas e ajustes com a consultoria;
2. Levantamento de riscos relacionados aos processos que estão sendo mapeados;
3. Reunião com Dr. Francisco para tratar de estratégias do projeto;
4. Todas as reuniões estão gravadas em nosso ambiente do Teams;
5. Workshops realizados e mapeamentos em execução, conforme áreas abaixo:

21/08 WORKSHOP
1. DIRETORIA JUDICIÁRIA
2. DIRETORIA FINANCEIRA
3. DIRETORIA DO FERJ
4. DIRETORIA DE ENGENHARIA
28/08
1. DIRETORIA DE INFORMÁTICA E AUTOMAÇÃO
2. DIRETORIA DE SEGURANÇA INSTITUCIONAL E GABINETE MILITAR

## 5. ATIVIDADES REALIZADAS – Setembro 2023

Atividades realizadas no mês de setembro de 2023.
1. Reuniões semanais para tirar dúvidas e ajustes com a consultoria;
2. Levantamento de riscos relacionados aos processos que estão sendo mapeados;
3. Reunião com Dr. Francisco para tratar de estratégias do projeto;
4. Todas as reuniões estão gravadas em nosso ambiente do Teams;
5. Workshops realizados e mapeamentos em execução, conforme áreas abaixo:

04/09 WORKSHOP - Mapeamento de Dados Pessoais
1. UNIDADE DE MONITORAMENTO CARCERÁRIO
2. COORDENADORIA ESTADUAL DA MULHER – CEMULHER

22/09 WORKSHOP - Mapeamento de Dados Pessoais
1. COORDENADORIA DE PROCESSOS ADMINISTRATIVOS, DISCIPLINARES E SINDICÂNCIA

## 6. ATIVIDADES REALIZADAS – Outubro 2023

Atividades realizadas no mês de outubro de 2023.
1. Reuniões semanais para tirar dúvidas e ajustes com a consultoria;
2. Levantamento de riscos relacionados aos processos que estão sendo mapeados;
3. Reunião com Dr. Francisco para tratar de estratégias do projeto;
4. Todas as reuniões estão gravadas em nosso ambiente do Teams;
5. Workshops realizados e mapeamentos em execução, conforme áreas abaixo:

02/10 WORKSHOP – Mapeamento de Dados Pessoais
1. Núcleo de combate à desinformação - nucode
2. Núcleo de gerenciamento de precedentes – nugepnac
3. Núcleo de solução de conflitos - nupemec

4. Núcleo socioambiental
5. Núcleo de justiça restaurativa
6. Núcleo de apoio técnico para demandas de saúde - natjus
7. Núcleo de cooperação judiciária
8. Núcleo permanente de acessibilidade da pessoa idosa e com deficiência
9. Núcleo de gestão de processos institucionais

05/10 WORKSHOP – Mapeamento de Dados Pessoais
1. Núcleo Sócio Ambiental
2. Coordenadoria de processo judicial eletrônico - pje
3. Coordenadoria da gestão da memoria e biblioteca
4. Coordenadoria de gestão estratégica

09/10 - WORKSHOP – Mapeamento de Dados Pessoais
1. Ouvidoria
2. Diretoria Geral
3. 1ª Vice-Presidência
4. 2ª Vice-Presidência
5. ASCOM – Assessoria de Comunicação

16/10 - WORKSHOP – Mapeamento de Dados Pessoais
1. Apoio no preenchimento da planilha de áreas que já tinham participado de Workshop

19/10 - WORKSHOP – Mapeamento de Dados Pessoais
1. Apoio no preenchimento da planilha de áreas que já tinham participado de Workshop

23/10 a 27/10 - WORKSHOP – Mapeamento de Dados Pessoais
1. Visita presencial a várias áreas/setores do PJMA – apoio no preenchimento da planilha de mapeamento
2. Workshop para Ouvidoria do PJMA com participação da Ouvidoria do Governo do Maranhão e alguns secretários do Estado do Maranhão
3. Workshop para assessores de desembargadores do PJMA

30/10 - WORKSHOP – Mapeamento de Dados Pessoais
1. Diretoria Financeira

31/10 - WORKSHOP – Mapeamento de Dados Pessoais
1. Coordenadoria de Arquivo e Gestão Documental

## 7. ATIVIDADES REALIZADAS – Novembro 2023

Atividades realizadas no mês de novembro de 2023.

1. Reuniões semanais para tirar dúvidas e ajustes com a consultoria;
2. Levantamento de riscos relacionados aos processos que estão sendo mapeados;
3. Workshops realizados e mapeamentos em execução, conforme áreas abaixo:
   14/11 WORKSHOP – Mapeamento de Dados Pessoais
4. Workshop on-line para assessores de desembargadores do PJMA

## 8. ATIVIDADES EM ANDAMENTO – Dezembro 2023

Atividades que estão em andamento nos meses de dezembro de 2023 e janeiro 2024.

1. Ajustes na planilha de mapeamento de dados, incluindo as bases legais
2. Levantamento de riscos relacionados aos processos que estão sendo mapeados e elaboração do relatório de riscos.

## 9. ATIVIDADES REALIZADAS – Janeiro 2024

Abaixo, serão listadas as atividades realizadas no mês de janeiro de 2024.

1. Elaboração do Plano de Comunicação do Programa de Adequação à LGPD;
2. Levantamento de riscos relacionados aos processos que estão sendo mapeados;
3. Reunião com Dr. Francisco para tratar de estratégias do projeto;
4. Todas as reuniões estão gravadas em nosso ambiente do Teams;
5. Workshops realizados e mapeamentos em execução, conforme áreas abaixo:

12/01 WORKSHOP – Mapeamento de Dados Pessoais

1. Workshop on-line de Mapeamento de Dados Pessoais para Coordenadoria de Arquivo e Gestão Documental

26/01 WORKSHOP – Mapeamento de Dados Pessoais

1. Workshop on-line de Mapeamento de Dados Pessoais e Validação para Diretoria Jurídica

6. Serão necessários Workshops para preenchimento e validação das planilhas das seguintes coordenadorias/divisões/diretorias/áreas:

1.
   a. Coordenadoria da Gestão da Memória e Biblioteca
   b. Coordenadoria de Processo Judicial Eletrônico – PJE
   c. Coordenadoria Estadual da Mulher
   d. Diretoria de Informática e Automação
   e. Diretoria de Segurança Institucional

f. Diretoria Judiciária
g. Gestão de Processos Institucionais
h. Gabinete dos Desembargadores
i. Núcleo de Cooperação Judiciária
j. Núcleo de Combate à Desinformação
k. Ouvidoria da Mulher
l. Secretaria Geral do Plenário
m. ESMAM – Escola Superior da Magistratura do Maranhão

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

BRUNO JORGE PORTELA SILVA COUTINHO
Diretor de Informática e Automação em Exercício
Coordenadoria de Infraestrutura e Telecomunicações
Matrícula 143784

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

PATRÍCIA FONSECA PEREIRA DOS SANTOS
Coordenadora de Avaliação de Controle Internos e Monitoramento
Coordenadoria de Avaliação de Controle Internos e de Monitoramento
Matrícula 139840

CRISTIANO DE JESUS SOUSA DE ABREU
Coordenador de Orçamento
Coordenadoria de Orçamento
Matrícula 120477

FABRICYO CASTRO COTRIM
Coordenador do Ferj
Coordenadoria do FERJ
Matrícula 195602

Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 24/04/2024 14:02 (PATRÍCIA FONSECA PEREIRA DOS SANTOS)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 24/04/2024 14:24 (CRISTIANO DE JESUS SOUSA DE ABREU)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 24/04/2024 14:57 (JOSÉ JORGE FIGUEIREDO DOS ANJOS JUNIOR)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 24/04/2024 15:51 (MILENA VIEIRA DE OLIVEIRA)
Documento assinado. SÃO LUÍS - ENTRÂNCIA FINAL, 24/04/2024 22:27 (FRANCISCO SOARES REIS JÚNIOR)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 25/04/2024 09:02 (FABRICYO CASTRO COTRIM)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 25/04/2024 09:23 (BRUNO JORGE PORTELA SILVA COUTINHO)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 25/04/2024 10:39 (JAMIL DE MIRANDA GEDEON NETO)