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.