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 utilizar 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.