Guia de uso

Aceitável de Ativos

2024

TRIBUNAL DE JUSTIÇA DO ESTADO DO MARANHÃO

Desembargador José de Ribamar Fróz Sobrinho
Presidente

Desembargador Raimundo Moraes Bogéa
1º Vice-Presidente

Desembargador José Jorge Figueiredo dos Anjos
2º Vice-Presidente

Desembargador José Luiz Oliveira de Almeida
Corregedor-Geral

Desembargador Jamil de Miranda Gedeon Neto
Presidente do Comitê de Governança de Segurança da Informação e do Comitê Gestor de Proteção de Dados Pessoais

Juiz Auxiliar José Jorge Figueiredo dos Anjos Júnior
Tribunal de Justiça do Estado do Maranhão
Coordenador do Comitê de Governança de Segurança da Informação

Juiz Auxiliar Francisco Soares Reis Júnior
Tribunal de Justiça do Estado do Maranhão
Coordenador do Comitê Gestor de Proteção de Dados Pessoais

Juiz Auxiliar Marcelo Silva Moreira
Corregedoria Geral da Justiça

MEMBROS(AS) DO COMITÊ DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E COMITÊ GESTOR DE PROTEÇÃO DE DADOS PESSOAIS

Amudsen da Silveira Bonifácio
Célia Regina Pereira da Silva
Claridelma Barros Brasil Mesquita
Cláudio Henrique Carneiro Sampaio
Diana Bastos Ordahy
João Paulo Tobias Teixeira de Souza Cordeiro
Jurema Mamede de Paiva Santos
Mayco Murilo Pinheiro
Paulo Fernando Almeida Falcão de Oliveira
Rodrigo Ericeira Valente da Silva
MM. Ticiany Gedeon Maciel Palácio

EQUIPE TÉCNICA

Diretoria de Informática e Automação
Assessoria de Comunicação da Presidência
Grupo Técnico de Trabalho do CGSI e CGPD

SUMÁRIO

1. INTRODUÇÃO

O objetivo deste guia é orientar os(as) usuários(as): magistrados(as), servidores(as), estagiários(as) e prestadores(as) de serviço quanto ao uso dos ativos e/ou recursos de TIC disponibilizados pelo Poder Judiciário do Estado do Maranhão.

As orientações divulgadas neste material baseiam-se nas normas e na Política de Segurança da Informação (PSI) publicada pelo PJMA por meio da Resolução-GP nº 39, de 12 de junho de 2023, do Tribunal de Justiça do Estado do Maranhão - TJMA.

Para uso deste guia aplica-se a lista de termos do glossário com suas respectivas definições, conforme ANEXO I - Glossário da PSI.

O texto na íntegra pode ser consultado no tópico 4 e nos itens 4.2, 4.4, 4.5, 4.7, 4.8, 4.14.1 e 4.15 do ANEXO VI - Norma de Uso Aceitável de Ativos da Política de Segurança da Informação.

Resolução-GP nº 39/2023 - TJMA

2. ATIVOS DE TIC

Os(As) usuários(as) devem:

- **zelar pelo uso dos ativos e/ou recursos de TIC disponibilizados pelo PJMA, a fim de garantir sua preservação física e lógica;**
- **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:**
- não estiver mais utilizando o ativo de TIC;
- ausentar-se do local de trabalho por um curto período de tempo.
- **desligar computadores de mesa (desktops) ou notebooks:**
- ao final do expediente;
- ausentar-se do local de trabalho por um longo período de tempo.
- **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).**

2. ATIVOS DE TIC

Os(As) usuários(as) não devem:

- **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, equipamentos portáteis, dispositivos móveis, impressoras, câmeras, switches, roteadores, modems, etc.;**

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

- **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;**

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

- **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.;**

2. ATIVOS DE TIC

- 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.

Qualquer dano aos ativos de TIC do PJMA, sob responsabilidade do(a) usuário(a), deve ser devidamente analisado pela Diretoria de Informática e Automação. Se constatado que tal dano decorreu da falta de zelo, negligência ou imprudência, cabe a este(a) adotar as medidas necessárias para reparação do prejuízo, por meio das ações cabíveis.

3. DISPOSITIVO MÓVEL CORPORATIVO

Os(As) usuários(as) devem:

- **utilizar criptografia obrigatoriamente ao armazenar informações restritas e confidenciais, quando o dispositivo assim permitir;**
- **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;**
- **manter o sistema operacional e os aplicativos atualizados;**
- **evitar que os dados do dispositivo sejam acessados por pessoas não autorizadas;**
- **realizar cópias de segurança dos dados do dispositivo periodicamente;**
- **utilizar redes de comunicação seguras, preferencialmente criptografadas.**

3. DISPOSITIVO MÓVEL CORPORATIVO

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

- **guardá-lo de forma segura, como em mochila, maleta, case ou capa;**
- **mantê-lo sempre à vista e atento(a) à sua segurança;**
- **acomodá-lo em local seguro e fora do alcance da visão de terceiros ao transportá-lo em veículos automotores;**
- **levá-lo consigo para evitar deixá-lo desacompanhado dentro do veículo.**

4. DISPOSITIVO DE ARMAZENAMENTO REMOVÍVEL

Os(As) usuários(as) devem:

- **utilizar criptografia, obrigatoriamente, ao armazenar informações de uso restrito e confidenciais, quando o dispositivo assim permitir;**
- **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;**
- **zelar pela segurança dos ativos de TIC, certificando-se da inexistência de códigos maliciosos nos dispositivos antes de utilizá-los.**

5. ARMAZENAMENTO DE ARQUIVOS

Os(As) usuários(as) devem armazenar os arquivos em uma das seguintes áreas:

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

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

5. ARMAZENAMENTO DE ARQUIVOS

Os(As) usuários(as) não devem:

- **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;**

- **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;**

- **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.**

6. EQUIPAMENTOS DE IMPRESSÃO E FOTOCÓPIA

Os(As) usuários(as) devem:

- **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;**

- **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.**

7. MESA LIMPA E TELA LIMPA

Os(As) usuários(as) devem:

- **manter a mesa de trabalho e outros móveis, bem como os ativos de TIC, como impressoras, digitalizadores, fotocopiadoras, etc., organizados e livres de papéis com informações sensíveis;**

- **guardar em mobília segura 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;**

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

- **manter a área de trabalho do computador de mesa ou do notebook livre de arquivos que contenham informações sensíveis;**

7. MESA LIMPA E TELA LIMPA

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

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

8. APLICATIVOS DE MENSAGENS

Os(As) usuários(as) não devem:

- **divulgar, enviar ou publicar dados, arquivos ou informações sensíveis, restritas ou confidenciais do ambiente interno, exceto quando de interesse do PJMA;**
- **prejudicar o exercício de suas atividades laborais ou de outros(as) usuários(as) do PJMA;**
- **compartilhar, postar, divulgar ou expor imagens, fotos, vídeos ou sons captados nas dependências internas, exceto quando de interesse do PJMA;**
- **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;**
- **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.**

9. INTELIGÊNCIA ARTIFICIAL

Os(As) usuários(as) não devem:

- **compartilhar informações confidenciais do PJMA, como objetivos estratégicos, metas, transações financeiras e indicadores;**
- **submeter códigos-fonte de sistemas ou aplicações do PJMA;**
- **compartilhar credenciais de acesso corporativas, códigos de autenticação ou informações de acesso;**
- **divulgar informações sobre segredos comerciais e de propriedade intelectual;**
- **compartilhar detalhes médicos pessoais;**
- **fornecer dados pessoais, tais como: números de documentos de identificação, nome, endereço, etc.;**
- **submeter dados biométricos, como impressões digitais ou reconhecimento facial;**

9. INTELIGÊNCIA ARTIFICIAL

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

- **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.**

TJMA

TRIBUNAL DE JUSTIÇA DO ESTADO DO MARANHÃO

Comitê de Governança de Segurança da Informação
Comitê Gestor de Proteção de Dados Pessoais