ATA-GabDesJMGN - 32023
Código de validação: BF78A7E158

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

Ata da 4ª Reunião de 2023 (12/06/2023)

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

Como membros(as), registraram-se as presenças do desembargador JAMIL DE MIRANDA GEDEON NETO (TJMA - presidente do CGSI e CGPD), do juiz JOSÉ JORGE FIGUEIREDO DOS ANJOS JÚNIOR (CGJ - Membro do CGSI e CGPD), do diretor CLÁUDIO HENRIQUE CARNEIRO SAMPAIO (Diretoria de Informática e Automação - Membro do CGSI e CGPD), do diretor LAÉRCIO LEÃO AMARAL (Diretoria Judiciária - Membro do CGPD), da diretora JUREMA MAMEDE DE PAIVA SANTOS (Diretoria de Auditoria Interna - Membra do CGPD), da diretora MILENA VIEIRA DE OLIVEIRA (Diretoria de Recursos Humanos - Membra do CGSI e CGPD), do diretor ANDRÉ MENEZES MENDES (Diretoria do FERJ - Membro do CGPD), do diretor MAYCO MURILO PINHEIRO (Diretoria de Engenharia - Membro do CGPD), substituindo o LUIZ CLÁUDIO PATRÍCIO DE LIMA e da assessora ISABELLA CAROLINA SILVA E SILVA (Assessoria de Comunicação da Presidência - Membra do CGSI).

Estavam ausentes os(as) membros(as): - o juiz FRANCISCO SOARES REIS JÚNIOR (TJMA - Coordenador do CGPD e membro do CGSI), substituído por PAULA GARDÊNIA COSTA SERRA, o juiz JOSÉ NILO RIBEIRO FILHO (TJMA - Coordenador do CGSI e membro do CGPD), o diretor ALEXANDRE MAGNO DE SOUSA NUNES (Diretoria de Segurança Institucional e Gabinete Militar - Membro do CGSI e CGPD), a diretora CÉLIA REGINA PEREIRA DA SILVA (Diretoria Financeira - Membra do

CGPD), substituída por CRISTIANO DE JESUS SOUSA DE ABREU, a diretora KEILA FONSECA DA SILVA (Diretoria Administrativa - Membra do CGSI e CGPD) e o diretor CARLOS ANDERSON DOS SANTOS FERREIRA (Diretoria Geral - Membro do CGSI).

Como convidados, registraram-se as presenças do Sr. GIVANILDO MARQUES (Coordenadoria de Atendimento ao Usuário), PATRYCKSON MARINHO SANTOS (Divisão de Obras e Serviços), HALLYSON CARLOS (INTEROP) e MARCELO (FAC Tecnologia).

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

- Ações da ENSEC-PJ - Relatório de progresso;
- Nova Política de Segurança da Informação (PSI) - Minuta de Resolução;
- Normas da PSI (ANEXOS) - Minutas;
- Autenticação em duas etapas (2FA) - Cronograma;
- Ações da LGPD - Relatório de progresso;
- Ações futuras.

O Sr. Jairo Rocha saudou a todos(as) e apresentou o relatório de progresso da ENSEC-PJ demonstrando sua evolução durante as reuniões do CGSI. O progresso, focado na conclusão, evoluiu de 10,6% (31.01.2023) para 26,6% (20.03.2023) e seguiu para 36,2% (09.06.2023).

Apresentou o andamento do processo do DIGIDOC nº 25553/2023 (Requisição nº: 894457), que dispõe sobre a nova Política de Segurança da Informação no âmbito do Poder Judiciário do Estado do Maranhão, relatando que o processo estava pendente de assinatura do presidente do Tribunal de Justiça do Estado do Maranhão para seguir para publicação.

Pontuou a adição de alguns parágrafos no item 4.4 (página 10) da norma de uso aceitável de ativos disciplinando a criação e o uso do drive compartilhado.

Falou resumidamente sobre as normas de Controle de Acesso e Gestão de Identidade, Classificação e Tratamento da Informação, Segurança Física no Ambiente de TIC, Gestão de Ativos, Uso Aceitável de Ativos, Proteção Contra Códigos Maliciosos,

Gestão de Vulnerabilidades Técnicas e Registro de Eventos, anexas a esta ata. Posteriormente, as mesmas foram colocadas em votação pelos membros do CGSI e todas foram aprovadas.

Relatou sobre o andamento das demais normas e da previsão de finalização das mesmas.

Demonstrou a baixa adesão da ativação do 2FA no ambiente colaborativo do TJMA e apresentou um cronograma para acelerar e fortalecer esta ativação. O cronograma findaria no mês de dezembro de 2024. Após sugestão do juiz José Jorge Figueiredo dos Anjos Júnior e deliberação dos membros do CGSI, o mesmo foi ajustado para ser finalizado em fevereiro de 2024.

Foi passada a palavra para o Sr. Marcelo, da empresa FAC Tecnologia, que discorreu sobre o andamento das ações da LGPD de forma sucinta.

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

PALÁCIO DA JUSTIÇA "CLÓVIS BEVILÁCQUA" DO ESTADO DO MARANHÃO

São Luís, 12 de junho de 2023.

ANEXO II

NORMA DE CONTROLE DE ACESSO E GESTÃO DE IDENTIDADE

Normativos relacionados:

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

Versionamento:

Versão:	1.0
Data:	03/04/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	12/06/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

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

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

Esta norma obedece ao escopo definido na Política de Segurança da Informação. No que se refere ao controle de acesso físico, as diretrizes serão detalhadas na norma de segurança física no ambiente de TIC.

2. OBJETIVOS

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

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

3. DIRETRIZES

Disponibilizar credencial de acesso ao(à) usuário(a) autorizado(a) para utilização de ativos e/ou recursos de TIC do PJMA, de acordo com seu cargo, função, necessidade ou atribuições, para execução de atividades administrativas, funcionais e/ou judiciais (atividades laborais).

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

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

4. CONTROLE DE ACESSO

Todas as credenciais de acesso tratadas nesta norma são pessoais e intransferíveis e qualquer ação executada pelo(a) usuário(a) utilizando uma

determinada credencial de acesso será de responsabilidade exclusiva do(a) mesmo(a), devendo este(a) zelar pelos princípios da segurança da informação.

Os(As) usuários(as) que serão tratados(as) nesta norma e as respectivas credenciais de acesso permitidas:

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

a) credencial de acesso de rede;

b) credencial de acesso ao e-mail;

c) credencial de acesso a sistemas administrativos;

d) credencial de acesso a sistemas judiciais;

e) credencial de acesso remoto, exceto unidades administrativas e/ou judiciais e estagiários(as).

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

a) credencial de acesso de rede;

b) credencial de acesso a sistemas administrativos;

c) credencial de acesso a sistemas judiciais;

d) credencial de acesso remoto, apenas com autorização da DIA.

Excepcionalmente, observando os princípios do privilégio mínimo, poderá ser concedida credencial de acesso aos(as) prestadores(as) de serviço, agentes públicos externos(as), visitantes e outras pessoas não previstas, em caráter temporário, para execução de atividades laborais relacionadas ao PJMA. A concessão, autorizada pela DIA, levará em consideração quaisquer responsabilidades legais durante o uso da credencial.

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

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

O controle de acesso e a gestão de identidade dispostos nesta norma aplicam-se às seguintes categorias:

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

4.1 Ativos e/ou Recursos de TIC

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

O(A) usuário(a) poderá acessar os ativos e/ou recursos de TIC através de:

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

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

Cada usuário(a), de acordo com a necessidade de suas atividades laborais, terá acesso a uma caixa de correio eletrônico corporativo, única e exclusiva, que será acessada através da credencial de acesso ao e-mail para utilização do serviço de correio eletrônico.

As unidades administrativas e judiciais poderão ter uma ou mais caixas de correio eletrônico corporativo, de acordo com as necessidades de seus organogramas, e deverão ser acessadas regularmente pelo(a) superior imediato(a) ou pelos(as) usuários(as) daquela unidade, devidamente autorizado(a) pelo(a) superior imediato(a).

Poderá ser criada caixa de correio eletrônico de serviço para sistemas ou

serviços, através de credencial de acesso ao e-mail, relacionados a uma atividade específica, exercida no âmbito de uma unidade administrativa e/ou judicial após aprovação da DIA.

Na necessidade de criação de endereços eletrônicos de e-mail para eventos ou projetos no âmbito do PJMA, os endereços poderão ser criados na forma de grupo ou lista, com a devida atribuição de membros participantes e responsáveis.

Poderá ser criado grupo ou lista para um conjunto específico de usuários(as), conforme necessidade, após autorização da DIA.

A utilização de Múltiplo Fator de Autenticação (MFA) será obrigatória para todas as credenciais de acessos na utilização dos serviços de correio eletrônico (e-mail) e de ambiente colaborativo, caso exista suporte para esta tecnologia.

4.2 Sistemas de Informação

A identificação dos(as) usuários(as) ao acessar os sistemas de informação (administrativos ou judiciais) do PJMA, para execução de atividades laborais, será realizado através de credencial de acesso aos sistemas ou mediante utilização de certificado digital, quando aplicável.

O(A) usuário(a) poderá utilizar os sistemas de informação através de:

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

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

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

No caso de sistemas de informação acessados mediante uso de certificado digital, a mesma será fornecida aos(às) usuários(as) observando-se as regras da Resolução nº 27/2013-TJ ou posterior que a substitua.

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

4.3 Acesso Remoto

O acesso remoto à rede de dados corporativa, quando essencial ao desenvolvimento das atividades do PJMA, dar-se-á mediante Rede Privada Virtual (Virtual Private Network – VPN), após requisição efetuada pelo(a) superior imediato(a) do(a) usuário(a) via DIGIDOC, cabendo à DIA autorizar e implementar o acesso.

O acesso remoto do(a) usuário(a) à rede de dados corporativa do PJMA será realizado mediante credencial de acesso remoto com permissões definidas de acordo com as suas responsabilidades e atribuições.

O Múltiplo Fator de Autenticação (MFA) deverá ser utilizado, obrigatoriamente, em todas as credenciais de acesso remoto à rede de dados corporativa do PJMA, caso o recurso esteja disponível.

4.4 Perfil de Administrador

Somente os(as) servidores(as) lotados(as) na DIA, devidamente identificados(as) e autorizados(as), terão credencial de acesso com perfil de administrador para acessar ativos e/ou recursos de TIC do PJMA, incluindo os críticos.

Os(As) usuários(as) que possuem credencial de acesso com perfil de administrador deverão utilizá-la somente para a execução de atividades administrativas que requeiram esse nível de acesso**.**

O Múltiplo Fator de Autenticação (MFA) deverá ser utilizado, obrigatoriamente, para todas as credenciais de acesso de administrador do PJMA, caso o recurso esteja disponível.

4.5 Senha de Acesso

As senhas associadas às credenciais de acesso aos ativos e/ou recursos de TIC do PJMA são de uso pessoal e intransferível. O(A) usuário(a) deverá zelar pela sua guarda e sigilo, garantindo assim o princípio da confidencialidade.

A Diretoria de Informática e Automação será responsável por fornecer senha de acesso inicial ao(à) usuário(a), que deverá proceder com a troca imediata da mesma no momento que efetuar o primeiro acesso. Após a efetivação da troca da senha, os(as) servidores(as) da DIA não terão mais conhecimento da mesma.

Os(as) usuários(as) serão incentivados(as) a utilizar ferramenta de gerenciamento de senhas, para armazenar e gerir suas credenciais de acesso.

O(A) usuário(a) deverá alterar a senha imediatamente e notificar o(a) superior imediato(a) e a DIA se houver indicação para acreditar que alguma de suas credenciais de acesso foi vazada, acessada e/ou utilizada indevidamente por pessoa não autorizada, para que a DIA tome as providências cabíveis.

4.5.1 Prazos

A senha da credencial de acesso de rede possuirá prazo de validade de:

I - 90 (noventa) dias para:

a) colaboradores(as);

b) terceirizados(as);

c) perfil de administradores(as).

A senha da credencial de acesso de rede e ao e-mail possuirá prazo de validade de:

I - 90 (noventa) dias para:

a) estagiários(as).

II - 180 (cento e oitenta) dias para:

a) magistrados(as);

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

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

d) unidades administrativas e judiciais.

As senhas das credenciais de acesso aos sistemas administrativos e judiciais do PJMA possuirão prazo de validade de 180 (cento e oitenta) dias para todos(as) usuários(as) habilitados(as) definidos no item 4 desta norma.

No caso da senha da credencial de acesso, quando autorizada pela DIA, de prestador(a) de serviço, agente público externo(a), visitante e outras pessoas não previstas, o prazo de validade será flexível conforme quantidade de dias de execução

do serviço ou de duração da visita.

Caso o serviço e/ou visita ultrapasse a quantidade de dias informados inicialmente, o prazo de validade poderá ser prorrogado após nova análise e definição da DIA, verificando cada caso em particular.

Decorrido o prazo de validade da senha, será gerada automaticamente uma notificação para o(a) usuário(a) realizar a troca da mesma. A senha ainda poderá ser trocada, a qualquer tempo, caso o(a) usuário(a) ache conveniente.

4.5.2 Complexidade e Tamanho

A senha associada à credencial de acesso será composta por uma quantidade mínima de 10 (dez) caracteres, combinando letras maiúsculas, minúsculas, números e caracteres especiais ($, %, &, #, !, …).

A senha associada à credencial de acesso com perfil de administrador será composta por uma quantidade mínima de 14 (quatorze) caracteres, combinando letras maiúsculas, minúsculas, números e caracteres especiais $, %, &, #, !, …).

4.5.3 Recomendações para Definição de Senha

Na criação da senha da credencial de acesso, o(a) usuário(a) não deverá utilizar:

I - partes de sua credencial de acesso;

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

III - informações pessoais, tais como: o próprio nome, sobrenome ou de familiares, placa de carro, data de aniversário, endereço, número de telefone, nome de time de futebol, animal de estimação, dentre outros;

IV - partes ou variações do nome do Poder Judiciário do Estado do Maranhão, Tribunal de Justiça do Estado do Maranhão e Corregedoria Geral da Justiça do Estado do Maranhão ou qualquer outra variação dos itens descritos, tais como: duplicação ou escrita invertida. Exemplos: PJ, PJMA, TJ, TJMA, CGJ, CGJMA, PJMAPJMA, TJMATJMA, CGJMACGJMA e AMJT.

4.6 Autorização de Acesso

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

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

4.7 Restrição de Acesso

A DIA estabelece e segue um processo, para revogar ou restringir o acesso aos ativos e/ou recursos de TIC do PJMA, por meio da redefinição da credencial de acesso do(a) usuário(a).

As credenciais de acessos deverão ser bloqueadas, preferencialmente, em vez de excluídas, para preservação das trilhas de auditoria.

O gerenciador de identidade de usuários(as) não permitirá a reutilização das últimas 03 senhas utilizadas pelo(a) usuário(a).

A credencial de acesso do(a) usuário(a) será bloqueada nos seguintes casos:

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

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

III - pela falta de uso regular ou decorrente de aposentadoria, desligamento ou falecimento;

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

O desbloqueio da credencial de acesso, por tentativas de acesso com senhas

inválidas, será solicitado para a DIA pelo(a) usuário(a) ou por seu(sua) superior imediato(a). Já o desbloqueio da unidade administrativa ou judicial, será solicitado pelo(a) superior imediato(a) ou gestor(a) detentor(a) da credencial de acesso da unidade para a DIA, ambas formalizadas através dos canais oficiais de comunicação ou solicitação do PJMA.

4.7.1 Bloqueio

Determina-se que, caso não seja identificado o uso regular da credencial de acesso de rede e ao e-mail pelo(a) usuário(a), as respectivas credenciais serão bloqueadas por motivos de segurança, conforme prazos abaixos:

I - superior a 30 (trinta) dias:

a) estagiário(a);

b) unidade administrativa ou judicial;

c) colaborador(a) e terceirizado(a), apenas credencial de acesso de rede.

II - superior a 60 (sessenta) dias:

a) magistrado(a);

b) servidor(a) efetivo(a) ou requisitado(a);

c) servidor(a) ocupante de cargo em comissão sem vínculo efetivo.

O desbloqueio da credencial de acesso do(a) usuário(a) ou da unidade administrativa e/ou judicial, por falta de uso regular, será realizado pela DIA, após solicitação formal, devidamente justificada, pelo(a) superior imediato(a) do(a) usuário(a) ou pelo(a) superior imediato(a) detentor(a) da credencial da unidade, através do DIGIDOC.

4.7.2 Exclusão

Caso não seja identificado o uso regular da credencial de acesso ao e-mail pelo(a) usuário(a), a respectiva credencial poderá ser excluída, a contar da data do bloqueio da mesma, segundo os prazos abaixos:

I - superior a 30 (trinta) dias:

a) estagiário(a);

b) unidade administrativa ou judicial.

II - superior a 120 (cento e vinte) dias:

a) magistrado(a);

b) servidor(a) efetivo(a) ou requisitado(a);

c) servidor(a) ocupante de cargo em comissão sem vínculo efetivo.

A exclusão da credencial de acesso ao e-mail do(a) usuário(a) observará as diretrizes da norma de cópias de segurança da informação.

4.7.3 Exceções de Bloqueio e Exclusão

Em casos de afastamento superiores a 180 (cento e oitenta) dias, a Diretoria de Recursos Humanos (DRH) deverá notificar formalmente a DIA para não haver a possibilidade de exclusão da credencial de acesso ao e-mail do(a) usuário(a), devendo a mesma permanecer bloqueada por motivos de segurança, caso não esteja sendo utilizada regularmente.

Em caso de desligamento, aposentadoria ou falecimento do(a) usuário(a), a credencial de acesso será bloqueada.

O(A) usuário(a) poderá solicitar cópia de segurança das mensagens eletrônicas contidas na sua caixa de correio eletrônico, em até 180 (cento e oitenta) dias, a contar da data de bloqueio da credencial, nos casos de desligamento ou aposentadoria. Decorrido esse prazo a credencial de acesso ao e-mail será excluída.

Caso ocorra extinção da unidade administrativa e/ou judicial a qual a credencial de acesso ao e-mail esteja relacionada, caberá ao CGSI decidir que ações serão tomadas com relação à credencial e às mensagens eletrônicas da caixa de correio eletrônico vinculadas a ela.

5. PAPÉIS E RESPONSABILIDADES

O(A) usuário(a), deverá observar as responsabilidades e deveres desta norma, podendo vir a ser responsabilizado(a) por quaisquer danos, diretos ou indiretos, que venha causar ao PJMA ou a terceiros(as), podendo ser apurados em processo

administrativo disciplinar, sem prejuízo das ações cíveis e penais cabíveis.

5.1 Diretoria De Recursos Humanos

Compete à Diretoria de Recursos Humanos:

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

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

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

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

I - solicitar à DIA a concessão de acesso a novo(a) usuário(a) a ativos e/ou recursos de TIC para execução de atividades laborais, observando cargo ou funções exercidas;

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

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

IV - requisitar à DIA a concessão de acesso a colaborador(a), terceirizado(a), estagiário(a), prestador(a) de serviço, agente público externo(a), visitante ou outra pessoa não prevista sob sua supervisão justificando a necessidade de acesso a ativos e/ou recursos de TIC, observando as definições, exceções e prazos constante nos itens 4 e 4.5.1 desta norma;

V - informar à DIA quando do encerramento do contrato com colaborador(a), terceirizado(a) e/ou estagiário(a) que fazem uso de ativos e/ou recursos de TIC do PJMA para a devida revogação da credencial de acesso;

VI - solicitar à DIA, com a devida justificativa, a concessão do(a) usuário(a) ao acesso remoto, anexando a portaria que colocou o(a) mesmo(a) à disposição do

trabalho remoto.

5.3 Diretoria de Informática e Automação

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

Compete à Diretoria de Informática e Automação:

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

II - bloquear, quando solicitado e justificado, as credenciais de acesso ou permissões do usuário(a) ou da unidade judicial e/ou administrativa do PJMA;

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

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

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

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

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

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

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

6. INFRAÇÕES E PENALIDADES

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

7. REVISÕES

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

8. APROVAÇÃO

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

ANEXO III
NORMA DE CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

Normativos relacionados:

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

Versionamento:

Versão:	1.0
Data:	03/04/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	12/06/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

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

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

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

2. OBJETIVO

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

3. DIRETRIZES

Orientações da norma de classificação e tratamento da informação.

3.1 Classificação da Informação

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

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

I - pública: informação disponibilizada pelo Poder Judiciário do Estado do Maranhão para o público geral. A divulgação deste tipo de informação causará danos mínimos ou nenhum ao PJMA. Podendo ser compartilhada livremente sem restrições, desde que mantida sua integridade e respeitada as regras de direitos autorais;

II - de uso interno: informação disponibilizada para usuários(as) e unidades administrativas e/ou judiciais do Poder Judiciário do Estado do Maranhão, empresas contratadas e órgãos parceiros. A qual não deverá ser compartilhada com o público em geral, exceto com autorização expressa do gestor da

informação. A divulgação deste tipo de informação poderá causar pequenos danos e prejuízos à reputação e às operações do PJMA;

III - de uso restrito: informação limitada a um grupo restrito de usuários(as) do Poder Judiciário do Estado do Maranhão, que necessitem dessas informações para a realização de suas atividades administrativas e/ou judiciais, independentemente do cargo ocupado. Esta informação deverá ser protegida adequadamente contra acessos internos e externos não autorizados. A divulgação deste tipo de informação poderá trazer sérios danos de privacidade, de reputação e de operações ao PJMA;

IV - confidencial: informação de caráter sigiloso, devendo ser comunicada exclusivamente a usuários(as) autorizados(as) pelo Poder Judiciário do Estado do Maranhão que necessitem conhecê-las para o desempenho de suas atividades administrativas e/ou judiciais. A divulgação ou alteração não autorizada deste tipo de informação poderá causar graves danos e prejuízos para o PJMA e a sociedade. Portanto, seu compartilhamento deverá ser restrito e feito de maneira controlada.

3.2 Rotulagem da Informação

Os rótulos (tags) observarão o modelo descrito no ANEXO A – MODELO PARA ROTULAGEM DE INFORMAÇÕES e também obedecerão as regras abaixo:

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

II - para a informação de uso interno, de uso restrito ou confidencial, deverá constar a classificação no rótulo de cada uma individualmente, seguido da unidade administrativa e/ou judicial específica criadora da informação, quando for o caso.

3.2.1 Em mensagens eletrônicas

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

3.2.2 Em documentos eletrônicos

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

3.3 Manuseio da Informação

Os documentos de uso interno, de uso restrito ou confidenciais em formato físico deverão ser guardados em gavetas ou armários trancados de forma a impedir o acesso de pessoas não autorizadas.

Em períodos de ausência da estação de trabalho, documentos em formato físico deverão ser retirados das mesas e de outras áreas de superfície e guardados em gavetas ou armários trancados de forma a impedir o acesso de pessoas não autorizadas.

Os documentos de uso interno, de uso restrito ou confidenciais em formato eletrônico ou digital deverão ser armazenados em ambientes com acesso controlado através de credencial de acesso que utilize senha e Múltiplo Fator de Autenticação (MFA), caso o recurso esteja disponível.

3.4 Guarda da Informação

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

3.5 Descarte da Informação

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

3.6 Transferência da Informação

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

4. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

4.1 Gestor da Informação

É responsabilidade do gestor da informação, classificar as informações

considerando os requisitos de confidencialidade, integridade e disponibilidade, seguindo a categorias abaixo:

I - pública;

II - de uso interno;

III - de uso restrito;

IV - confidencial.

5. INFRAÇÕES E PENALIDADES

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

6. REVISÕES

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

7. APROVAÇÃO

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

ANEXO A – MODELO PARA ROTULAGEM DE INFORMAÇÕES

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

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

INFORMAÇÃO	RÓTULO	FONTE (HEX)	FUNDO (HEX)
PÚBLICA	PÚBLICA	#FFFFFF	#4D4D4D
DE USO INTERNO	INTERNA	#FFFFFF	#38761D
DE USO RESTRITO	RESTRITA	#000000	#F1C232
CONFIDENCIAL	CONFIDENCIAL	#FFFFFF	#CC0000

2. RODAPÉ

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

EXEMPLOS:

TJMA – PÚBLICA
TJMA – INTERNA / Diretoria de Recursos Humanos
CGJMA – RESTRITA / Coordenadoria das Serventias

ANEXO IV
NORMA DE SEGURANÇA FÍSICA NO AMBIENTE DE TIC

Normativos relacionados:

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

Versionamento:

Versão:	1.0
Data:	03/04/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	12/06/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

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

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

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

2. OBJETIVO

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

3. DIRETRIZES

Orientações da norma de segurança física no ambiente de TIC.

3.1 Segurança física

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

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

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

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

I - todo acesso às áreas restritas de TIC deverá, obrigatoriamente, ser autorizado pela DIA, registrando a data e horário de início e fim do acesso para posteriores averiguações em caso de ocorrências;

II - os(as) servidores(as) do PJMA autorizados(as) pela DIA a acessarem as áreas restritas de TIC, deverão portar seus crachás funcionais, fixados em local de fácil visualização;

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

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

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

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

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

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

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

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

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

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

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

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

5. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

5.1 Diretoria de Informática e Automação

É responsabilidade da Diretoria de Informática e Automação:

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

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

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

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

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

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

pelo PJMA.

5.2 Diretoria de Segurança Institucional e Gabinete Militar

É competência da Diretoria de Segurança Institucional e Gabinete Militar:

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

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

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

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

5.3 Diretoria Administrativa

Compete à Diretoria Administrativa:

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

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

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

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

II - solicitar formalmente à DIA, através dos canais oficiais de comunicação ou solicitação do PJMA, a liberação de usuários(as) que necessitam de acesso às

áreas restritas de TIC com a devida justificativa.

6. INFRAÇÕES E PENALIDADES

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

7. REVISÕES

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

8. APROVAÇÃO

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

ANEXO V
NORMA DE GESTÃO DE ATIVOS

Normativos relacionados:

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

Versionamento:

Versão:	1.0
Data:	02/05/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	12/06/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

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

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

As diretrizes que se referem a utilização dos ativos e recursos de TIC serão detalhadas na norma de uso aceitável de ativos.

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

2. OBJETIVO

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

3. DIRETRIZ

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

4. INVENTÁRIO

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

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

II - computadores de mesa, dispositivos de armazenamento removíveis, dispositivos móveis, periféricos ou hardwares e demais equipamentos de TIC que compõem o patrimônio do TJMA;

III - sistemas de gerenciamento de banco de dados;

IV - níveis de permissões;

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

VI - sistemas desenvolvidos ou softwares adquiridos;

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

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

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

I - a identificação e a descrição;

II - a categoria e subcategoria;

III - o responsável (gestor);

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

V - a localização.

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

I - requisitos legais;

II - valor financeiro;

III - seu potencial de agregar valor ao negócio;

IV - sua vida útil.

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

5. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

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

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

I - identificar ativos de TIC sob sua responsabilidade;

II - identificar potenciais ameaças e vulnerabilidades relacionadas aos ativos;

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

IV - avaliar os riscos dos ativos de TIC;

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

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

5.2 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação:

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

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

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

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

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

VI - assegurar que softwares não autorizados sejam retirados de uso em ativos de TIC do PJMA;

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

6. INFRAÇÕES E PENALIDADES

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

7. REVISÕES

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

8. APROVAÇÃO

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

ANEXO VI

NORMA DE USO ACEITÁVEL DE ATIVOS

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
Resolução nº 27/2013-TJ	
Resolução nº 5/2017-GP	

Versionamento:

Versão:	1.0
Data:	03/04/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	12/06/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

Esta norma complementa a Política de Segurança da Informação (PSI) e define diretrizes para os(as) usuários(as) devidamente autorizados(as) para a utilização aceitável de 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 da 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 pelo(a) usuário(a).

4. USO DE ATIVOS E/OU RECURSOS DE TIC

O(A) usuário(a) do PJMA deverá utilizar os ativos e/ou recursos de TIC, de propriedade do 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 poderá, a seu critério, ceder aos(às) usuários(as) ativos de TIC (dispositivo móvel, certificado digital ou dispositivo de armazenamento removível, etc.) para execução de suas atividades laborais, que poderão ser utilizados fora das dependências do PJMA.

Além de observar as disposições definidas na Resolução nº 5/2017-GP ou posterior que a substitua, o(a) usuário(a) deverá:

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

II - desligar computadores de mesa (desktops) ou notebooks no final do expediente ou sempre que ausentar-se por um período prolongado de seu local de execução de atividades laborais;

III - fechar ou bloquear programas ou sistemas, desconectar da rede (logoff) ou bloquear a tela do computador de mesa (desktop) ou do notebook quando não estiver mais utilizando ou sempre que ausentar-se de seu local de execução de atividades laborais;

IV - utilizar o serviço de ambiente colaborativo, serviço de correio eletrônico, o acesso à internet e o acesso remoto em conformidade ao estabelecido nesta norma e na Política de Segurança da Informação do PJMA.

O bloqueio de tela, protegido por senha, será ativado automaticamente sempre que o computador de mesa (desktop) ou notebook do(a) usuário(a) ficar inativo por mais de 05 (cinco) minutos.

Qualquer dano aos ativos de TIC do PJMA, sob guarda do(a) usuário(a), será devidamente analisado pela DIA. Havendo a constatação de que tal dano decorreu pela falta de zelo, negligência ou imprudência do(a) usuário(a), caberá ao(a) mesmo(a) exercer o direito de reparação ao prejuízo, através da tomada de ações cabíveis.

Além de observar as disposições definidas na Resolução nº 5/2017-GP ou posterior que a substitua, o(a) usuário(a) não deverá:

I - conectar equipamentos particulares na rede de dados corporativa do PJMA, seja em segmentos cabeados ou sem fio, sem avaliação e autorização formal pela 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 programa 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 ativos e/ou recursos de TIC, disponibilizados pelo PJMA, para fins particulares, diversão pessoal ou qualquer outra atividade não relacionada com o serviço público ou que não seja pertinente ao cargo que exerça;

V - copiar materiais originais ou qualquer material protegido por copyright, sem que possua licença ou autorização para tal, 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 tecnologia de propriedade particular, quando utilizados nas dependências do Poder Judiciário,

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:

- Uso de Dispositivo Móvel Corporativo;
- Acesso Remoto (Conexão Remota);
- Dispositivo de Armazenamento Removível;
- Armazenamento de Arquivos;
- Certificado Digital;
- Equipamentos de Impressão e Fotocópia;
- Política de Mesa Limpa e de Tela Limpa;
- Uso do Acesso à Internet;
- Uso do Serviço de Correio Eletrônico;
- Uso do Serviço de Ambiente Colaborativo;
- Uso dos Sistemas de Informação;
- Direito de Propriedade Intelectual;
- Uso de Aplicativos de Mensagens, Redes Sociais e Serviço de Correio Eletrônico Pessoal.

4.1 Uso de Dispositivo Móvel Corporativo

O PJMA poderá, a seu critério exclusivo, fornecer aos seus(suas) usuários(as) dispositivos móveis corporativos (notebooks, celulares, smartphones, tablets, smartwatches, etc.) para execução de atividades laborais.

O(A) usuário(a) ao fazer uso do dispositivo móvel corporativo, deverá:

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

II - habilitar o bloqueio de segurança pessoal no dispositivo, utilizando, preferencialmente, recursos biométricos;

III - manter o sistema operacional e os aplicativos atualizados;

IV - estar atento à segurança do dispositivo sob sua responsabilidade, principalmente ao utilizar veículos automotores, dando preferência para a guarda do mesmo em compartimentos de armazenamento resistentes e não chamativos, durante trajetos de deslocamento;

V - levar o dispositivo junto de si para que o mesmo não fique desacompanhado em caso de necessidade de ausentar-se do interior do veículo automotor.

Os dispositivos móveis corporativos deverão estar em conformidade com a norma de proteção contra códigos maliciosos, norma de gestão de vulnerabilidades técnicas e com níveis adequados de proteção.

Os(As) usuários(as) poderão utilizar seus dispositivos móveis pessoais, exceto notebooks que serão avaliados e autorizados pela DIA, para fins laborais e fazer uso do mesmo durante o expediente, desde que, não atrapalhe a própria concentração ou dos(as) demais usuários(as) em suas atividades, não violem a legislação, políticas e normas vigentes ou gerem riscos ao PJMA.

Em caso de perda, roubo ou furto de dispositivo móvel corporativo ou pessoal utilizado para fins laborais, o(a) usuário(a) deverá procurar a ajuda das autoridades policiais registrando boletim de ocorrência e em seguida comunicar, via DIGIDOC, as Diretorias Administrativa e de Informática e Automação para que possam ser tomadas as medidas cabíveis.

4.2 Acesso Remoto (Conexão Remota)

O acesso remoto à rede de dados corporativa do PJMA será disponibilizado por meio de Virtual Private Network (VPN) e é restrito aos(às) usuários(as) do PJMA para execução de suas atividades laborais fora de seu local de trabalho presencial e será atribuído com as permissões mínimas necessárias para execução de suas atividades laborais, podendo ser realizado através de computadores de mesa (desktops) e/ou notebooks corporativos/pessoais.

Os computadores de mesa (desktops) ou notebooks corporativos deverão possuir recursos em conformidade com as normas vigentes, em especial as de proteção contra códigos maliciosos e de gestão de vulnerabilidades técnicas.

O(A) usuário(a), ao utilizar o computador de mesa ou notebook pessoal, inspecionado e autorizado pela DIA, para realizar o acesso remoto à rede de dados corporativa, deverá seguir recomendações de boas práticas de segurança, tais como:

I - utilizar programas e sistemas operacionais originais e licenciados, exceto os baseados em softwares livres;

II - manter o sistema operacional e programas atualizados;

III - obter aplicativos de fontes confiáveis e lojas oficiais;

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

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

VI - proteger suas credenciais de acesso;

VII - criar uma conta padrão e usá-la em tarefas rotineiras, utilizando a conta de administrador somente quando necessário e pelo menor tempo possível;

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

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

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.

Caso o computador de mesa ou notebook pessoal não esteja em conformidade com os itens I, II, III, IV e IX das recomendações de boas práticas de proteção e segurança, o acesso remoto do(a) usuário(a), já devidamente autorizado(a), poderá ser bloqueado, sempre dando ciência ao(à) superior imediato(a) do(a) usuário(a).

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

4.3 Dispositivo de Armazenamento Removível

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

O(A) usuário(a) ao fazer uso de dispositivo de armazenamento removível, deverá:

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, de modo a minimizar o impacto 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 sua utilização.

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

É estritamente proibido que o(a) usuário(a) cancele 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.

4.4 Armazenamento de Arquivos

O Poder Judiciário do Estado do Maranhão disponibilizará 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.

O(A) usuário(a) deverá armazenar os arquivos nas áreas:

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

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

O(A) usuário(a) ao fazer uso das áreas de armazenamento de arquivos, não deverá:

I - criar, manipular, armazenar, acessar, copiar, distribuir, divulgar, disponibilizar ou transmitir qualquer material protegido por copyright, sem que possua licença ou autorização para tal, incluindo músicas, filmes, jogos,

emuladores de jogos, vídeos, sistemas operacionais, aplicativos e arquivos com conteúdo ofensivo, agressivo, preconceituoso, discriminatório, terrorista, subversivo, injurioso, calunioso, difamatório, infamante, vexatório, de práticas de aborto, de drogas ilícitas ou não, de pornografia, de pirataria, com credenciais de acesso, informações protegidas por segredo de estado ou outro estatuto legal, assim como qualquer outra 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.

Os arquivos não deverão ser armazenados localmente nos computadores de mesa (desktops) ou notebooks, pois a cópia de segurança (backup) desses arquivos não serão realizadas pela DIA, sendo esse procedimento de única e exclusiva responsabilidade do(a) usuário(a).

O PJMA tem propriedade legal sobre todos os arquivos criados ou produzidos em seus ativos de TIC e/ou locais 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, respeitará os tamanhos a seguir:

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

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

O espaço de armazenamento de arquivos disponibilizado remotamente, no Google Drive, seguirá os tamanhos abaixo:

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

II - magistrados(as) e unidades administrativas e/ou judiciais: ilimitado.

O espaço de armazenamento de arquivos disponibilizado remotamente (Google Drive) é compartilhado com a caixa de correio eletrônico corporativo do ambiente colaborativo (Gmail).

Apenas as credenciais de acesso de magistrados(as) e unidades administrativas e judiciais poderão:

I - criar drives compartilhados;

II - disponibilizar arquivos eletrônicos ou áreas de armazenamento do drive compartilhado com qualquer pessoa que não faça parte do domínio do PJMA, desde que seja para atender as atividades judiciais ou administrativas do PJMA e não cause danos à segurança da informação do PJMA, bem como não contrarie as políticas e normas vigentes.

Os drives compartilhados criados terão 01 TeraByte (01 TB) de limite de espaço disponibilizado para uso, exceto em situação que necessite de mais espaço, desde que devidamente justificada pelo(a) solicitante e autorizada pela DIA**.**

Os(As) magistrados(as) e gestores(as) das unidades administrativas e/ou judiciais serão responsáveis pela:

I - gestão do acesso (permissões, compartilhamento, etc.) aos drives compartilhados criados;

II - pelo mau uso que o acesso indevido possa ocasionar ao PJMA.

4.5 Certificado Digital

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

Para emissão e uso do certificado digital, os(as) usuários(as) do PJMA deverão observar a PORTARIA-GP - 972019 ou portaria posterior que a substitua e a Resolução nº 272013-GP ou posterior que a substitua.

4.6 Equipamentos de Impressão e Fotocópia

O(A) usuário(a) deverá 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.

4.7 Política de Mesa Limpa e de Tela Limpa

Todas as informações classificadas como de uso interno, de uso restrito e confidenciais especificadas na norma de classificação e tratamento da informação são consideradas sensíveis neste item.

O(A) usuário(a) deverá:

I - manter as mesas de trabalho (mobília), outros móveis e os ativos de TIC (impressoras, digitalizadores, fotocopiadoras, etc.) limpos de papéis (documentos físicos) e de dispositivos de armazenamento removíveis (mídias de CD's, DVD's e/ou BLU-RAY, pendrives e discos rígidos externos) que contenham informações sensíveis;

II - guardar em mobília segura (cofres, armários e gaveteiros com chave) os papéis, dispositivos de armazenamento removíveis e outros ativos de TIC sob sua responsabilidade que contenham informações sensíveis;

III - utilizar procedimentos de descarte seguro para papéis e dispositivos de armazenamento removíveis (mídias de CD's, DVD's e/ou BLU-RAY, pendrives e discos rígidos externos) conforme classificação das informações neles contidas;

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

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

4.8 Uso do Acesso à Internet

O acesso à internet será disponibilizado através da rede corporativa do PJMA para os(as) usuários(as) observando a necessidade de uso responsável para o desenvolvimento das atividades administrativas, funcionais e/ou judiciais.

O(A) usuário(a) deverá:

I - acessar à internet através de sua credencial de acesso identificada,

registrada e devidamente autorizada;

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

III - comunicar à DIA 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 DIA. Os registros de acessos à internet serão preservados em conformidade com a legislação e normas vigentes.

O(A) usuário(a) durante uso do acesso à internet não deverá acessar arquivos ou sítios eletrônicos com conteúdos relacionados, expressa ou subjetivamente, direta ou indiretamente, a(ao):

I - qualquer espécie de exploração: infantil, ambiental, sexual, laboral, financeira, racial ou étnica, etc.;

II - qualquer forma de conteúdo adulto, erótico, pornográfico e de relacionamentos íntimos;

III - qualquer forma de ameaça, chantagem e assédio moral ou sexual;

IV - qualquer ato ofensivo, agressivo, terrorista, subversivo, injurioso, calunioso, difamatório, infamante, vexatório, de práticas de aborto, atentatório à moral e aos bons costumes da sociedade, assim como qualquer outra que possa infringir as legislações, políticas e/ou normas vigentes;

V - quaisquer espécies de preconceito ou discriminação, especialmente os baseados em: cor, sexo, idade, orientação sexual, raça, origem, condição social, crença ou religião, deficiências e necessidades especiais;

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

VII - compra e/ou uso de armas de fogo;

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

IX - práticas de quaisquer atividades comerciais desleais e anúncios;

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

XI - softwares peer-to-peer (P2P), tais como: kazaa, bittorrent, emule, ares e afins;

XII - atividades relacionadas a jogos eletrônicos e/ou jogos de azar;

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

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

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

XVI - quaisquer redes sociais, excetuando 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 programas de acesso remoto;

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

XIX - desrespeito a imagem institucional do PJMA.

Na constatação do acesso a sítios eletrônicos com os conteúdos relacionados acima por parte do(a) usuário(a), a Diretoria de Informática e Automação poderá comunicar o fato para o Comitê de Governança de Segurança da Informação (CGSI) para as providências cabíveis, dando ciência ao(à) superior imediato(a) do(a) usuário(a).

O CGSI poderá autorizar, após parecer técnico da Diretoria de Informática e Automação, 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.

4.9 Uso do Serviço de Correio Eletrônico

O Poder Judiciário do Estado do Maranhão fornece o serviço de correio eletrônico (e-mail) para seus(suas) usuários(as) e unidades administrativas e/ou judiciais para desempenho de suas atividades laborais, não sendo permitido o uso de qualquer serviço de correio eletrônico que não seja o oficialmente oferecido ou contratado pelo PJMA. O uso do serviço de correio eletrônico pessoal será permitido e disciplinado no item 4.13.

As caixas de correio eletrônico corporativo das unidades administrativas e judiciais deverão ser utilizadas preferencialmente para as comunicações oficiais entre as unidades.

No caso de afastamento temporário ou provisório do(a) usuário(a) autorizado(a) a acessar a caixa de correio eletrônico corporativo da unidade administrativa ou judicial, caberá ao(à) superior imediato(a) garantir, através de requerimento formal à Diretoria de Informática e Automação, que o(a) usuário(a) substituto(a) mantenha o acesso regular à caixa de correio eletrônico corporativo.

São deveres do(a) usuário(a) do serviço de correio eletrônico:

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 (conta de correio eletrônico corporativo);

III - acessar sua caixa de correio eletrônico corporativo regularmente, observando os prazos de bloqueio e exclusão definidos na norma de controle de acesso e gestão de identidade;

IV - acessar o serviço de correio eletrônico 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 levando ao conhecimento da 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.

As contas de correio eletrônico corporativas das unidades administrativas e judiciais poderão ser divulgadas através da intranet e internet, de acordo com a conveniência dessas.

Quando o(a) usuário(a) fizer uso do serviço de correio eletrônico do Poder Judiciário do Estado do Maranhão, 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 informação classificada 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, ressalvadas as atividades que exijam esse 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 pela autoridade competente;

VII - enviar mensagem eletrônica não solicitada, indesejada ou ilícita ao serviço de correio eletrônico do PJMA ou de 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 de 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 pornográficas, ofensivas, agressivas, preconceituosas, discriminatórias, terroristas, subversivas, injuriosas, caluniosas, difamatórias, infamantes, vexatórias, de práticas de aborto, que incentive o uso de drogas ilícitas ou não, assim como qualquer outra que possa infringir as legislações, políticas e/ou normas vigentes;

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 DIA e tem objetivo de proteger a organização de ameaças virtuais, tais como phishing, spam e outras ameaças existentes, bem como produzir evidências relativas à eventual

violação das normas e/ou da legislação em vigor.

Durante o monitoramento, a DIA, dentro dos limites legais, se resguarda no direito de, sem qualquer notificação ou aviso, tratar as mensagens eletrônicas enviadas ou recebidas pelo(a) usuário(a) através do serviço de correio eletrônico para atender finalidades administrativas, judiciais e extrajudiciais, incluindo investigações cíveis ou criminais.

As caixas de correio eletrônico 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:

"*Esta mensagem, juntamente com qualquer outra informação anexada, é confidencial e protegida por lei, e somente os(as) seus(suas) destinatários(as) são autorizados(as) a usá-la. Caso a tenha recebido por engano, por favor, informe o remetente e em seguida apague a mensagem, observando que não há autorização para armazenar, encaminhar, imprimir, usar ou copiar o seu conteúdo.*"

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

4.10 Uso do Serviço de Ambiente Colaborativo

O PJMA fornece o serviço de ambiente colaborativo (armazenamento remoto, agenda/calendário, videoconferência, bate-papo e suíte de escritório), através do Google Workspace (GW), para seus(suas) usuários(as) e/ou unidades administrativas e judiciais, exclusivamente, para o desempenho de suas atividades laborais, não sendo permitido o uso de qualquer serviço de ambiente colaborativo, que não seja o oficialmente fornecido ou contratado pelo Poder Judiciário do Estado do Maranhão.

No serviço de ambiente colaborativo estão 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: 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 liberados pelo Google Workspace e adicionados à lista acima, depois de avaliados e autorizados pela DIA serão disponibilizados aos(às) usuários(as) do PJMA para execução de atividades laborais.

São responsabilidades do(a) usuário(a) do serviço de ambiente colaborativo:

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 o(a) usuário(a) fizer 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 Uso dos Sistemas de Informação

O acesso aos sistemas de informação do PJMA será disponibilizado aos(às) usuários(as) para o desenvolvimento de suas atividades laborais.

Para acesso aos sistemas de informação que utilize certificado digital, o(a) usuário(a) necessitará obtê-lo observando-se as disposições da Resolução nº 27/2013-TJ ou posterior que a substitua.

O(A) usuário(a) poderá acessar os sistemas de informação através de:

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

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

Os registros de acessos aos sistemas de informação serão preservados em conformidade com a legislação e normas vigentes e estarão sujeitos a monitoramento pela 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), ao fazer uso dos sistemas de informação:

I - manter o sigilo das senhas das credenciais de acesso;

II - ser cauteloso(a) na utilização dos sistemas do PJMA;

III - guardar sigilo sobre fato ou informação de qualquer natureza de que tiver

conhecimento, por força de suas atribuições, ressalvadas aquelas de acesso público, não podendo alegar a quebra e/ou divulgação, em qualquer hipótese, pelo uso indevido de sua credencial de acesso;

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

4.12 Direito de Propriedade Intelectual

O PJMA não autoriza fazer uso de qualquer tipo de ativo ou recurso de TIC não contratado, não licenciado ou não homologado pela Diretoria de Informática e Automação.

4.13 Uso de Aplicativos de Mensagens, Redes Sociais e Serviço de Correio Eletrônico Pessoal

O uso de aplicativos de mensagens, especificamente whatsapp e telegram, e serviço de correio eletrônico pessoal (hotmail, google, yahoo, protonmail, etc.), pelo(a) usuário(a), nas dependências do PJMA, será permitido.

Já o uso de redes sociais (facebook, instagram, etc.) pelo(a) usuário(a), nas dependências do PJMA, será permitido apenas para realização de atividades laborais, desde que devidamente justificado pelo(a) superior imediato(a) e autorizado pela DIA.

O(A) usuário(a) será responsável pelo uso e guarda de suas senhas de acesso a redes sociais, aplicativos de mensagens e serviço de correio eletrônico pessoal.

4.13.1 Aplicativos de Mensagens

O(A) usuário(a) ao utilizar aplicativos de mensagens nas dependências do PJMA não deverá:

I - divulgar, enviar ou publicar qualquer dado, arquivo ou informação sensível do ambiente interno, exceto aquele que seja de interesse do PJMA;

II - prejudicar o exercício de suas atividades laborais ou de qualquer outro(a) usuário(a) do PJMA;

III - compartilhar, postar, divulgar ou expor qualquer imagem, foto, vídeo ou som captado nas dependências internas, exceto aquele que seja de interesse do PJMA;

IV - compartilhar, postar, divulgar ou expor qualquer comentário ou texto que revele ou induza terceiros(as) a crerem que se trata de uma opinião ou posicionamento do PJMA.

4.13.2 Redes Sociais

O(A) usuário(a), devidamente autorizado(a), ao utilizar redes sociais nas dependências do PJMA não deverá:

I - divulgar, enviar ou publicar qualquer dado, arquivo ou informação sensível do ambiente interno do PJMA;

II - prejudicar o exercício de suas atividades laborais ou de qualquer outro(a) usuário(a) do PJMA;

III - compartilhar, postar, divulgar ou expor qualquer imagem, foto, vídeo ou som captado nas dependências internas do PJMA;

IV - compartilhar, postar, divulgar ou expor qualquer comentário ou texto que revele ou induza terceiros(as) a crerem que se trata de uma opinião ou posicionamento do PJMA.

4.13.3 Serviço de Correio Eletrônico Pessoal

O(A) usuário(a) ao usar o serviço de correio eletrônico pessoal nas dependências do PJMA não deverá:

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

II - enviar mensagem eletrônica contendo arquivo ou código malicioso, qualquer forma de rotinas ou códigos de programação prejudiciais e danosas aos computadores de mesa (desktops), dispositivos móveis (notebooks, celulares, smartphones, tablets, smartwatches, etc.), rede de dados corporativa ou ao serviço de correio eletrônico do PJMA ou de domínios externos;

III - disseminar ou transmitir mensagens eletrônicas pornográficas, ofensivas, agressivas, preconceituosas, discriminatórias, terroristas, subversivas, injuriosas, caluniosas, difamatórias, infamantes, vexatórias, de práticas de aborto, que incentive o uso de drogas ilícitas ou não, assim como qualquer outra que possa infringir as legislações, políticas e/ou normas vigentes.

O uso de redes sociais, aplicativos de mensagens e serviço de correio eletrônico pessoal através da rede corporativa do PJMA, poderá ser monitorado pela DIA a fim de garantir a segurança da informação, respeitando a privacidade e confidencialidade dos conteúdos na comunicação do(a) usuário(a).

A DIA poderá realizar perícias e auditorias para finalidades administrativas, judiciais e extrajudiciais, incluindo investigações cíveis ou criminais de toda informação registrada ao utilizar de redes sociais, aplicativos de mensagens e serviço de correio eletrônico pessoal através da rede corporativa do PJMA.

5. PAPÉIS E RESPONSABILIDADES

O(A) usuário(a), deverá observar as responsabilidades e deveres desta norma, podendo vir a ser responsabilizado(a) por quaisquer danos, diretos ou indiretos, que venha causar ao PJMA ou a terceiros(as), podendo ser apurados em processo administrativo disciplinar, sem prejuízo das ações cíveis e penais cabíveis, assegurados o contraditório e a ampla defesa.

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 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 pelo(a) usuário(a), principalmente, em relação às categorias tratadas nesta norma, tais como: acesso remoto, armazenamento de arquivos, acesso à internet, serviço de correio eletrônico, serviço de ambiente colaborativo, sistemas de informação, dentre outros;

II - realizar a guarda dos ativos de TIC disponibilizados pelo PJMA;

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

5.2 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação:

I - 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, o serviço de ambiente colaborativo, os sistemas de informação e demais 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, em caso de necessidade e observando o disposto nesta norma, os limites, regulações e controles estabelecidos, quando solicitado pelo(a) superior imediato(a) do(a) usuário(a), com a 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 críticos do PJMA para determinados países, caso necessário.

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 ao(à) usuário(a), 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

Compete à Assessoria de Comunicação:

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 e a Escola Superior da Magistratura do Estado do Maranhão, observando sempre o disposto nesta norma.

5.6 Escola Superior da Magistratura do Estado do Maranhão (ESMAM)

Compete à ESMAM:

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

6. INFRAÇÕES E PENALIDADES

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

7. REVISÕES

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

8. APROVAÇÃO

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

ANEXO X
NORMA DE PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo

Versionamento:

Versão:	1.0
Data:	03/04/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	12/06/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A norma de proteção contra códigos maliciosos complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para proteção dos ativos e/ou recursos de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário do Estado do Maranhão (PJMA) contra códigos maliciosos de qualquer natureza.

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

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

2. OBJETIVO

Assegurar que informações, ativos de TIC e recursos de processamento da informação estejam protegidos contra códigos maliciosos.

3. DIRETRIZES

Orientações da norma de proteção contra códigos maliciosos.

3.1 Ferramenta de proteção contra códigos maliciosos

O Poder Judiciário do Estado do Maranhão disponibilizará nos seus ativos de TIC uma ferramenta de proteção contra códigos maliciosos. A ferramenta deverá realizar a proteção contra diversos tipos de malwares, tais como: vírus, ransomware, cavalo de tróia (trojan), backdoor, verme (worm), Remote Access Trojan - RAT, spyware (screenlogger, keylogger e adware), rootkit e similares, devendo ser instalada nos seguintes ativos de TIC:

I - computadores de mesa (desktop);

II - dispositivos móveis corporativos (notebooks, celulares, smartphones e tablets);

III - servidores de rede (arquivos, aplicações, etc.).

A ferramenta de proteção contra códigos maliciosos do Poder Judiciário do Estado do Maranhão adotará as seguintes regras de uso:

I - atualização diária, em tempo real, do arquivo de assinaturas de códigos

maliciosos;

II - realização de verificações automáticas, agendadas e manuais conforme a necessidade nos ativos de TIC suportados (computadores de mesa, dispositivos móveis corporativos e servidores de rede) do PJMA;

III - as verificações automáticas deverão analisar todos os arquivos em cada uma das unidades de armazenamento locais, inclusive as originadas a partir de dispositivos de armazenamento removíveis (mídias de CD's, DVD's e/ou BLU-RAY, pendrives e discos rígidos externos), conectados aos computadores de mesa e dispositivos móveis corporativos;

IV - as verificações automáticas nos servidores de rede serão limitadas a pastas ou arquivos específicos, previamente definidas pela DIA, de modo a evitar o comprometimento do desempenho do seus recursos computacionais (alto consumo do uso de CPU, memória, disco rígido, etc.);

V - as funções de proteção em tempo real e detecção com base no comportamento da ameaça, deverão estar habilitadas para todos os ativos de TIC suportados;

VI - sítios eletrônicos, serviços e arquivos acessados, baixados ou executados da internet, bem como softwares não autorizados ou não licenciados detectados serão automaticamente bloqueados nos ativos de TIC suportados.

Caso um servidor de rede esteja infectado ou com suspeita de infecção de código malicioso, serão adotadas medidas para garantir o isolamento do mesmo da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor, bem como preservar as informações necessárias para posterior auditoria.

3.2 Prevenção dos(as) usuários(as) contra códigos maliciosos

Mesmo com a presença da ferramenta para proteção contra códigos maliciosos nos ativos de TIC do PJMA, os(as) usuários(as) deverão adotar um comportamento cauteloso, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos.

Os(As) usuários(as) deverão notificar imediatamente a DIA, utilizando os canais oficiais de comunicação ou solicitação do PJMA, de qualquer infecção ou suspeita de infecção por código malicioso nos ativos de TIC suportados que tomem ciência.

É vedado aos(às) usuários(as):

I - instalar outra ferramenta de proteção contra códigos maliciosos de ativos de TIC que não seja a disponibilizada pelo PJMA;

II - remover/desinstalar ou desativar a ferramenta oficial de proteção contra códigos maliciosos de ativos de TIC do PJMA;

III - tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;

IV - desenvolver, testar ou armazenar partes de códigos de qualquer tipo, a menos que expressamente autorizado;

V - impedir, através de qualquer meio, a verificação automática da ferramenta de proteção contra códigos maliciosos, principalmente ao fazer uso dos dispositivos de armazenamento removíveis;

VI - habilitar MACROS para arquivos provenientes de fontes suspeitas, baixados ou recebidos da internet. Caso necessário, deverá ser solicitado o apoio da DIA para validar se o arquivo representa ou não uma ameaça.

4. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

4.1 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação:

I - instalar e gerir a ferramenta de proteção e controle contra códigos maliciosos nos ativos de TIC suportados;

II - tratar os casos de infecção ou suspeita de infecção por códigos maliciosos;

III - garantir que novas modalidades de códigos maliciosos sejam adequadamente investigadas e tratadas e os ativos de TIC protegidos pela ferramenta adotada pelo PJMA;

IV - garantir a divulgação, por meio de treinamentos e informativos periódicos, de informações de ameaças, códigos maliciosos e medidas de proteção para os(as) usuários(as) do PJMA.

5. INFRAÇÕES E PENALIDADES

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

6. REVISÕES

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

7. APROVAÇÃO

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

ANEXO XI
NORMA DE GESTÃO DE VULNERABILIDADES TÉCNICAS

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo

Versionamento:

Versão:	1.0
Data:	02/05/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	12/06/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A norma de gestão de vulnerabilidades técnicas complementa a Política de Segurança da Informação, definindo diretrizes para execução de processos de monitoramento e tratamento de vulnerabilidades técnicas em todos os ativos de TIC do Poder Judiciário do Estado do Maranhão (PJMA).

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

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

2. OBJETIVO

Assegurar a integridade dos sistemas operacionais e mitigar a exploração de vulnerabilidades técnicas conhecidas.

3. DIRETRIZES

Estabelecer um processo contínuo e proativo visando tratar riscos, realizar monitoramento, corrigir falhas e adotar ações de proteção contra ameaças cibernéticas e violação de dados. Dessa forma, reduz-se a exposição do PJMA a riscos existentes, com a mitigação de um número maior de vulnerabilidades.

As ações de proteção deverão ser sempre acompanhadas por ações de detecção e de tomada de decisão sobre o ativo de TIC vulnerável.

A DIA deverá, no mínimo, por meio do inventário de ativos de TIC:

I - observar a classificação dos ativos definidas na norma de gestão de ativos;

II - classificar e tratar continuamente as vulnerabilidades neles existentes;

III - priorizar as ações de correção e de mitigação por meio da avaliação do nível de ameaça e de criticidade da vulnerabilidade.

A fim de operacionalizar as atividades supracitadas, a DIA deverá:

I - acompanhar as notificações, os alertas e as recomendações emitidas, por CVE ou registro similar, para execução de ações necessárias;

II - estabelecer o gerenciamento de patches e atualizações;

III - estabelecer o gerenciamento de configuração e de correção de vulnerabilidades.

As orientações sobre correção ou mitigação, bem como o procedimento para aplicação de medidas corretivas, deverão ser estabelecidas em normativo interno.

3.1 Gerenciamento de Vulnerabilidades

O gerenciamento de vulnerabilidades deverá ser criado, implementado, mantido e aplicado no PJMA e contemplará:

I - estabelecer mecanismos para obter informações sobre vulnerabilidades técnicas dos sistemas e ativos de TIC, avaliação da exposição do PJMA a tais vulnerabilidades e a implementação de controles apropriados para tratamento do risco associado;

II - gerenciar os diversos ativos de TIC que sustentam os serviços do PJMA;

III - estabelecer funções e responsabilidades das equipes para realizar todas as atividades de maneira oportuna e eficaz para o PJMA;

IV - realizar atualizações de softwares, notificadas pelo fabricante ou fornecedor homologado, utilizando recursos autorizados, tais como: sítio eletrônicos de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

3.2 Inventário de Ativos

O inventário de ativos de TIC, conforme a norma de gestão de ativos, deverá constar no escopo do gerenciamento de vulnerabilidades e patches, necessitando ser atualizado periodicamente ou sempre que ocorrerem alterações significativas, para garantir que os recursos informacionais estejam cobertos pelo gerenciamento de vulnerabilidades no PJMA.

3.3 Detecção de Vulnerabilidades

As ferramentas precisarão de configurações e ajustes adequados, conforme o escopo avaliado. Assim como, os tipos de detecções e os tipos de testes terão que ser avaliados e ajustados, concordando com o escopo definido.

A frequência dos testes de segurança levará em consideração os requisitos legais, regulamentares e contratuais, como também, os riscos associados aos ativos de TIC do Poder Judiciário do Estado do Maranhão.

Os testes de segurança utilizarão o feed de vulnerabilidade mais recente, de forma a evitar que determinadas vulnerabilidades não sejam detectadas.

Os testes de segurança na rede corporativa deverão ser realizados pela DIA ou empresa especializada em períodos que não causem impactos no uso dos recursos e sistemas disponibilizados pelo PJMA.

Para cada teste, verificar-se-á a integridade da ferramenta utilizada, se ela analisou corretamente as vulnerabilidades dos ativos de TIC verificados e se existem exceções a serem tratadas.

As ferramentas utilizadas serão ajustadas continuamente, de forma a evitar que detecções feitas por ferramentas distintas gerem resultados diferentes.

O teste de invasão ou de penetração (pentest) será realizado, periodicamente ou conforme necessidade do PJMA, incluindo o escopo da avaliação, os métodos de uso e os requisitos operacionais, a fim de fornecer as informações mais precisas e relevantes sobre as vulnerabilidades atuais, sem afetar as atividades do PJMA.

A integridade do resultado sobre as detecções de vulnerabilidades será avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos. A detecção manual de vulnerabilidades será considerada como complemento às detecções automáticas.

Poderão ser realizados novos testes de segurança para certificação do saneamento das vulnerabilidades encontradas.

3.4 Elaboração e Manutenção dos Relatórios de Vulnerabilidades

A DIA deverá elaborar relatórios após cada ciclo de detecção para entender e mensurar as vulnerabilidades existentes. Deverá ainda adotar métricas padronizadas internacionalmente ou amplamente utilizadas para os relatórios de vulnerabilidades e determinar o valor percentual dos ativos de TIC vulneráveis por gravidade.

Novas vulnerabilidades deverão ser monitoradas por: severidade, tipo de ambiente, tipo de sistema, autoridade de numeração CVE e tipo de vulnerabilidade.

O relatório deverá ser classificado de acordo com a criticidade das informações nele contidas.

Todas as versões do relatório serão encaminhadas ao Comitê de Governança da Segurança da Informação para as ações necessárias.

3.5 Banco de Dados de Vulnerabilidades

Deverá ser mantido um banco de dados de vulnerabilidades coletadas de várias fontes que precisam ser aplicadas aos sistemas e ativos de TIC do Poder Judiciário do Estado do Maranhão.

O banco de dados poderá incluir informações, análise para priorização e plano de correção da vulnerabilidade.

3.6 Priorização e Correção de Vulnerabilidades

O tratamento de vulnerabilidades deverá ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, impacto em caso de exploração e no valor que o ativo de TIC tem para o Poder Judiciário do Estado do Maranhão.

As vulnerabilidades deverão ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados abaixo:

Nível de severidade	Prazo de correção	Descrição do risco
Muito Crítico (6)	Até 2 dias	Condição totalmente inaceitável quando medidas deverão ser tomadas imediatamente para eliminar a materialização do risco e mitigar perigos e impactos.
Crítico (5)	Até 15 dias	Pessoas mal-intencionadas poderão facilmente obter o controle do ativo de TIC, o que poderá comprometer toda a rede de dados corporativa do PJMA. As vulnerabilidades incluem acesso de leitura e gravação a arquivos, execução remota de comandos e backdoors.
Alto (4)	Até 30 dias	Pessoas mal-intencionadas poderão obter o controle do ativo de TIC ou coletar informações altamente confidenciais, incluindo acesso de "leitura" ao arquivo, backdoors em potencial ou uma lista de todas as contas de usuários(as) no ativo.

Médio (3)	Até 45 dias	Pessoas mal-intencionadas poderão obter acesso às configurações de segurança no ativo de TIC, o que poderá levar ao acesso a arquivos e à divulgação de conteúdo de arquivos, navegação em diretórios, ataques de negação de serviço e uso não autorizado de serviços.
Baixo (2)	Até 60 dias	Pessoas mal-intencionadas poderão coletar informações confidenciais do ativo de TIC, como versões de software instaladas, que poderão revelar vulnerabilidades conhecidas.
Muito baixo (1)	Até 90 dias	Pessoas mal-intencionadas poderão coletar informações sobre o ativo de TIC por meio de portas ou serviços abertos, o que poderá levar à divulgação de outras vulnerabilidades.

Os testes que forem concluídos com falha deverão ser examinados novamente até que sua execução seja concluída com êxito. Caso não seja possível, deverá ser avaliado se a vulnerabilidade será incluída na lista de exceções pela DIA, com base no processo de aceitação de risco.

Deverão ser estabelecidos mecanismos para obtenção regular de atualizações de software quando emitidas pelo fabricante ou fornecedor oficial, utilizando recursos autorizados, tais como sítios eletrônicos de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

Os alertas de vulnerabilidades, os patches de correções, as aplicações de atualizações e as ameaças emergentes que correspondam aos recursos informacionais relacionados no inventário de sistema e ativos de TIC deverão ser monitorados.

3.7 Das Exceções de Vulnerabilidades

Para os ativos de TIC do Poder Judiciário do Estado do Maranhão não contemplados por esta norma em função de dificuldades técnicas ou obrigações contratuais e normativas ou quaisquer exceções a esta norma, deverão ser documentadas e aprovadas.

3.8 Das Correções de Vulnerabilidades

As correções bem-sucedidas de vulnerabilidades poderão ser testadas por meio

de detecção de vulnerabilidades de rede e de host, verificação de logs de patches, testes de invasão/penetração (pentest) e verificação das definições de configuração.

3.9 Implementação e Verificação das Correções de Vulnerabilidades

Somente correções de vulnerabilidades que foram efetivamente testadas e aprovadas deverão ser implantadas em produção. Atividades de correção de vulnerabilidades geralmente incluem, mas não se limitam à instalação de patches de segurança, aplicações de atualizações, bem como a ajustes de configuração e/ou remoção de software.

Quando instalações de patches de segurança e ajustes de configuração são recomendadas para mitigar as vulnerabilidades, elas deverão seguir procedimento interno, devidamente documentado.

4. INFRAÇÕES E PENALIDADES

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

5. REVISÕES

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

6. APROVAÇÃO

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

ANEXO XIV
NORMA DE REGISTROS DE EVENTOS

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo

Versionamento:

Versão:	1.0
Data:	03/04/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	12/06/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A norma de registros de eventos complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para gerenciar registros de eventos 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 da PSI.

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

2. OBJETIVOS

Registrar eventos, gerar evidências, assegurar a integridade das informações de registro, prevenir contra acesso não autorizado, identificar eventos de segurança da informação que possam levar a um incidente de segurança e apoiar investigações.

Utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de TIC e de ações dos(as) usuários(as), permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança.

3. DIRETRIZES

A atividade de auditoria de registros de eventos de TIC é de competência da Diretoria de Informática e Automação (DIA). Os arquivos de registro de eventos deverão ser protegidos contra exclusão, alteração, inclusão indevida ou acesso não autorizado.

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

Os ativos de TIC, principalmente os ativos de TIC críticos, deverão estar obrigatoriamente com as informações de data e hora sincronizadas via protocolo NTP (Network Time Protocol), caso haja suporte.

Ações de restabelecimento de serviços e sistemas afetados por incidentes de segurança, não deverão impossibilitar a coleta, a preservação e a disponibilidade de

evidências em suas formas íntegras.

Os registros de eventos de ativos de TIC deverão ser criados e retidos na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades suspeitas ou não autorizadas. Os registros de eventos serão armazenados em pelo menos um repositório central.

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

Caso exista disponibilidade nos ativos de TIC, deverão ser registrados os eventos de:

I - tentativas de acesso (sistemas de informação, serviço de diretório e outros recursos) bem-sucedidas e fracassadas;

II - alterações na configuração do sistema;

III - uso de privilégios;

IV - arquivos acessados e tipo de acesso, incluindo a exclusão de arquivos importantes, a exemplo os arquivos de log de auditoria;

V - alarmes críticos ou importantes disparados pelo serviço de diretório;

VI - gerenciamento: criação, modificação ou exclusão de identidades;

VII - uso de programas e aplicações utilitários;

VIII - operações executadas pelos usuários em aplicações/sistemas, limitando-se ao que é exigido por lei;

IX - ativação e desativação de sistemas de segurança, como ferramenta de proteção contra códigos maliciosos (antivírus), sistemas de detecção de intrusão, etc.

Entradas de trilha de auditoria para componentes de sistema de informação podem ser registradas de forma classificada e personalizada, devendo ser registrados os eventos de:

I - identificação do usuário;

II - origem ou tipo do evento;

III - data e hora;

IV - indicação de sucesso ou falha;

V - endereços IP e portas de origem e destino, para eventos de rede;

VI - a identidade ou o nome dos dados afetados, componentes ou recursos do sistema.

Ativos de TIC críticos ou que contenham dados sensíveis deverão ser registrados os eventos de:

I - identificação do usuário;

II - origem ou tipo do evento;

III - data e hora;

IV - indicação de sucesso ou falha;

V - endereços IP e portas de origem e destino, para eventos de rede.

Uma ferramenta de gerenciamento de eventos de segurança da informação, tipo SIEM ou serviço equivalente, deverá ser utilizada para armazenar, correlacionar, normalizar e analisar informações de eventos e gerar alertas.

Quando não forem mais necessários para requisitos legais, regulatórios ou de negócios do PJMA, os registros dos eventos deverão ser removidos observando diretrizes de descarte seguro.

5. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

5.1 Diretoria de Informática e Automação

É responsabilidade da Diretoria de Informática e Automação, devendo a mesma:

I - possuir acesso irrestrito às informações necessárias ao bom desempenho de

suas funções, ao executar as atividades de auditoria;

II - selecionar os registros de eventos e observar os respectivos tempos de guarda, bem como as demais características para utilização dos mesmos;

III - coletar e preservar os registros de eventos e as mídias de armazenamento dos ativos de TIC afetados, pelo tempo necessário para realizar as atividades de auditoria;

IV - configurar e manter a estrutura original dos registros de eventos, principalmente de ativos de TIC críticos ou de ativos que contenham dados sensíveis para o PJMA;

V - justificar formalmente, a impossibilidade de preservar as evidências dos registros de evento de segurança da informação;

VI - realizar análises de auditoria, periódicas e quando forem necessárias, para detectar anomalias ou eventos inusitados que possam indicar uma ameaça potencial;

VII - coletar e armazenar registros de eventos de rede de provedores de serviço, caso haja viabilidade técnica;

VIII - fornecer e gerir serviço de NTP para sincronização dos ativos de TIC do PJMA.

6. INFRAÇÕES E PENALIDADES

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

7. REVISÕES

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

8. APROVAÇÃO

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

Desembargador JAMIL DE MIRANDA GEDEON NETO
Matrícula 53991

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

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

LAÉRCIO LEÃO AMARAL
Diretor Judiciário
Diretoria Judiciária
Matrícula 128835

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

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

ANDRE MENEZES MENDES
Diretor do FERJ
Diretoria do FERJ
Matrícula 114819

MAYCO MURILO PINHEIRO
Diretor de Engenharia
Diretoria de Engenharia
Matrícula 114389

ISABELLA CAROLINA SILVA E SILVA

Assessora Chefa da Assessoria de Comunicação da Presidência
Assessoria de Comunicação da Presidência
Matrícula 198986

Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 16/06/2023 16:32 (LAÉRCIO LEÃO AMARAL)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 16/06/2023 17:10 (CLÁUDIO HENRIQUE CARNEIRO SAMPAIO)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 16/06/2023 17:22 (ANDRE MENEZES MENDES)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 19/06/2023 09:18 (ISABELLA CAROLINA SILVA E SILVA)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 19/06/2023 12:06 (MILENA VIEIRA DE OLIVEIRA)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 19/06/2023 14:27 (JOSÉ JORGE FIGUEIREDO DOS ANJOS JUNIOR)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 19/06/2023 16:53 (JUREMA MAMEDE DE PAIVA SANTOS)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 21/06/2023 15:10 (MAYCO MURILO PINHEIRO)
Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 22/06/2023 09:25 (JAMIL DE MIRANDA GEDEON NETO)