ANEXO II
NORMA DE CONTROLE DE ACESSO E GESTÃO DE IDENTIDADE

Normativos relacionados:

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

Versionamento:

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

Histórico de mudanças:

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

1. INTRODUÇÃO

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

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

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

2. OBJETIVOS

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

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

3. DIRETRIZES

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

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

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

4. CONTROLE DE ACESSO

As credenciais de acesso abordadas nesta norma são pessoais e

intransferíveis. Qualquer ação realizada pelos(as) usuários(as) utilizando uma credencial específica será de responsabilidade exclusiva do mesmo(a), devendo zelar pelos princípios da segurança da informação.

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

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

a) credenciais de acesso à rede;

b) credenciais de acesso ao e-mail;

c) credenciais de acesso a sistemas administrativos;

d) credenciais de acesso a sistemas judiciais;

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

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

a) credenciais de acesso à rede;

b) credenciais de acesso a sistemas administrativos;

c) credenciais de acesso a sistemas judiciais;

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

III - unidades administrativas e/ou judiciais:

a) credenciais de acesso à rede;

b) credenciais de acesso ao e-mail.

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

autorizada pela DIA, considera quaisquer responsabilidades legais durante sua utilização.

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

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

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

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

4.1 Ativos e/ou Recursos de TIC

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

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

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

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

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

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

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

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

Mediante análise e autorização da DIA, poderá ser criado um grupo ou lista para um conjunto específico de usuários(as), conforme necessidade.

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

4.2 Sistemas de Informação

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

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

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

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

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

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

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

4.3 Acesso Remoto

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

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

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

4.4 Administrador de Redes

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

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

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

4.5 Senhas de Acesso

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

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

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

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

4.5.1 Prazo de Validade

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

I - 180 (cento e oitenta) dias para:

a) administradores(as) de redes;

b) estagiários(as);

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

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

a) magistrados(as);

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

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

d) unidades administrativas e judiciais.

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

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

4.5.2 Complexidade e Tamanho

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

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

4.5.3 Recomendações para Elaboração de Senhas

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

I - utilizar partes de sua credencial de acesso;

II - reutilizar suas senhas em diferentes credenciais de acesso;

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

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

V - aplicar partes ou variações do nome do Poder Judiciário do Estado do Maranhão (PJMA), Tribunal de Justiça do Estado do Maranhão e Corregedoria Geral da Justiça do Estado do Maranhão ou qualquer outra

variação dos itens descritos, tais como: duplicação ou escrita invertida. Exemplos: PJ, PJMA, PJMAPJMA, AMJP, TJ, TJMA, TJMATJMA, AMJT e assim sucessivamente;

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

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

4.6 Autorização de Acesso

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

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

4.7 Restrição de Acesso

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

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

4.7.1 Bloqueios

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

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

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

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

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

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

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

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

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

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

I - superior a 30 (trinta) dias para:

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

b) unidades administrativas ou judiciais;

c) estagiários(as);

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

II - superior a 60 (sessenta) dias para:

a) magistrados(as);

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

O desbloqueio das credenciais de acesso por falta de uso regular será realizado pela Diretoria de Informática e Automação (DIA) mediante solicitação formal justificada realizada pelo(a) superior imediato(a) do(a) usuário(a) ou pelo(a) gestor(a) da credencial da unidade administrativa e/ou judicial, utilizando os canais oficiais de comunicação ou solicitação do PJMA.

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

4.7.2 Exclusões

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

I - superior a 15 (quinze) dias para:

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

II - superior a 30 (trinta) dias para:

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

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

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

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

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

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

I - 15 (quinze) dias para:

a) estagiários(as).

II - 45 (quarenta e cinco) dias para:

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

III - 90 (noventa) dias para:

a) magistrados(as);

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

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

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

4.7.3 Exceções

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

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

5. PAPÉIS E RESPONSABILIDADES

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

5.1 Diretoria De Recursos Humanos

Compete à Diretoria de Recursos Humanos:

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

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

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

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

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

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

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

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

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

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

5.3 Diretoria de Informática e Automação

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

Compete à Diretoria de Informática e Automação:

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

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

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

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

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

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

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

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

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

6. INFRAÇÕES E PENALIDADES

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

7. REVISÕES

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

8. APROVAÇÃO

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