UNIVERSIDADE FEDERAL DO MARANHÃO
Av. dos Portugueses, 1966, - Bairro Vila Bacanga, São Luís/MA, CEP 65080-805
Telefone: (98) 3272-8000 - https://www.ufma.br

Portaria nº 341/2025/FUMA/OEC/REITORIA/GR

Aprova a Política de Gestão de Identidade – PoGI, da Universidade Federal do Maranhão – UFMA.

O REITOR DA UNIVERSIDADE FEDERAL DO MARANHÃO, o uso de suas atribuições legais, estatutárias e regimentais,

CONSIDERANDO o Decreto nº 12.198, de 24 de setembro de 2024, que institui a estratégia de Governo Digital para o período de 2024 a 2027, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;

CONSIDERANDO a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

CONSIDERANDO a Lei n° 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

CONSIDERANDO a Resolução nº 280-CONSAD, 04 de outubro de 2022 que aprova a Política de Segurança da Informação e Comunicação (PoSIC) da UFMA;

CONSIDERANDO a necessidade de estabelecer o escopo, princípios, diretrizes, competências e responsabilidades para orientar os usuários de serviços digitais oferecidos pela UFMA acerca do processo de comprovação de identidade;

CONSIDERANDO a necessidade de orientar os usuários acerca do procedimento de identificação das pessoas físicas, jurídicas ou unidades organizacionais que têm direito a acesso a serviços digitais oferecidos pela UFMA; e

CONSIDERANDO o constante dos autos do processo nº 23115.011779/2025-63,

R E S O L V E:

Art. 1º Aprovar a Política de Gestão de Identidade (PoGI) da Universidade Federal do Maranhão (UFMA), nos termos do Anexo Único, parte integrante desta Portaria.

Art. 2º A PoGI deverá ser revisada sempre que houver necessidade de adequações às políticas institucionais.

Parágrafo único. Fica a Comissão de Governança Digital e Segurança da Informação (CGDSI), em colaboração com a STI, responsável pela propositura ao Pleno do Comitê de Governança, Integridade e Transparência (CGIT) das eventuais alterações futuras ao texto desta Política.

Art. 3º Esta Portaria entra em vigor a partir da data de sua publicação.

Documento assinado eletronicamente por **FERNANDO CARVALHO SILVA**, **Reitor(a)**, em 05/05/2025, às 14:28, conforme horário oficial de Brasília, com fundamento na Lei nº14.063, de 23 de setembro de 2020.

ANEXO ÚNICO DA PORTARIA 341/2025/FUMA/OEC/REITORIA/GR, DE 05 DE MAIO DE 2025.

POLÍTICA DE GESTÃO DE IDENTIDADE DA UNIVERSIDADE FEDERAL DO MARANHÃO

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Seção I
Do Objetivo

Art. 1º A Política de Gestão de Identidade (PoGI) da Universidade Federal do Maranhão (UFMA) tem como finalidade estabelecer o escopo, princípios, diretrizes, competências e responsabilidades para orientar como as pessoas que se relacionam com a UFMA possam comprovar sua identidade.

Seção II
Do Escopo

Art. 2º A PoGI tem por escopo orientar como deve ocorrer a identificação das pessoas físicas, jurídicas ou unidades organizacionais que têm o direito de utilizar algum serviço digital oferecido pela UFMA.

§ 1º As pessoas que necessitarem se identificar para acessar algum serviço digital da instituição serão denominados usuários.

§ 2º Para efeitos desta Política, os usuários se classificam como:

I - internos: pessoas que possuem algum relacionamento direto com a instituição ou unidades organizacionais que pertencem ao organograma da instituição;

II - externos: pessoas que não possuem relacionamento com a instituição, mas necessitam acessar serviços digitais oferecidos por ela.

§ 3º Todos os usuários precisam ter uma identidade digital única que deve ser salvaguardada pela instituição.

CAPÍTULO II
DAS DEFINIÇÕES

Art. 3º Para efeitos desta Política, considera-se:

I - autenticação: ato pelo qual um usuário comprove sua identidade;

II - autorização: ato pelo qual um usuário após comprovar sua identidade recebe a permissão para executar alguma ação ou ter acesso a determinado serviço;

III - identidade digital: meio oficial utilizado para que usuários possam se identificar para acessar serviços digitais na UFMA;

IV - credencial: é um meio digital ou físico, provisório ou definitivo, vinculado à Identidade digital do usuário, utilizado em conjunto com esta, para acessar serviços na UFMA;

V - prenome: corresponde ao primeiro nome da pessoa;

VI - provedor de identidade: entidade que armazena e gerencia as identidades digitais dos usuários;

VII - relacionamento direto: discente com direito a diploma, servidor concursado da instituição ou pessoa que dê apoio às atividades institucionais que necessite ter acesso aos sistemas corporativos;

VIII - relacionamento indireto: pessoa que não possua relacionamento direto e queira usufruir dos serviços possíveis oferecidos pela instituição;

IX - sobrenome: corresponde a todos os nomes posteriores ao prenome desconsiderando as preposições;

X - serviço digital: qualquer serviço oferecido pela UFMA que ofereça a possibilidade de ser solicitado de forma eletrônica;

XI - unidade de tecnologia da informação: unidade da UFMA responsável pela gestão da tecnologia da informação.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 4º São princípios da PoGI:

I - disponibilizar uma única forma de acesso para todos os serviços digitais;

II - respeitar o acesso seguro e confiável à informação quando couber;

III - manter as informações mínimas necessárias para identificar o proprietário da Identidade digital;

IV - garantir a privacidade dos dados de todos os proprietário de identidades digitais;

V - estar alinhada com a política de segurança da informação e com a norma de controle de acesso vigentes.

CAPÍTULO IV
DAS DIRETRIZES

Art. 5º As diretrizes gerais da PoGI:

I - assegurar a proteção aos dados e eficiência na infraestrutura de Tecnologia da Informação;

II - centralizar a gestão de identidade;

III - permitir integração com outros provedores de identidade e/ou modelos federados;

IV - facilitar a auditoria dos acessos; e

V - possibilitar a criação de perfis de acesso usando grupo de usuários;

CAPÍTULO V
DA IDENTIDADE DIGITAL

Art. 6º Uma identidade digital deve ser composta de informações que identifiquem o usuário e o seu(s) relacionamento(s) com a instituição.

Parágrafo único. Só poderá haver uma identidade digital por pessoa física/jurídica.

Art. 7º Qualquer cidadão, que possua as informações mínimas exigidas, pode obter uma identidade digital na UFMA.

Seção I
Das Informações da Identidade

Art. 8º As informações minimamente exigidas para identificar um usuário são:

I - identificador: dado utilizado para identificar exclusivamente um usuário, ou seja, não pode haver dois

usuários com o mesmo identificador;

II - dado(s) pessoal(is): composto minimamente do Cadastro de Pessoa Física (CPF) ou Cadastro Nacional de Pessoa Jurídica (CNPJ), nome civil, nome social (se houver), data de nascimento, *e-mail*, telefone de contato e sexo; e

III - credencial(is): dado utilizado para que um usuário comprove sua identidade, por exemplo, senha, certificado digital e dados biométricos.

§ 1º O identificador poderá ser classificado como:

I - primário: Identificador institucional gerado pela unidade de tecnologia da informação; e

II - secundário: Identificador pessoal gerado por outros, tais como CPF, CNPJ, *e-mail*.

§ 2º A identidade digital deverá possuir obrigatoriamente um identificador primário e pelo menos um secundário, com exceção de alguns serviços digitais conforme o art. 26º.

§ 3º Outros dados pessoais poderão ser exigidos para atender algumas das seguintes situações:

I - por exigência legal;

II - por necessidade para realização do serviço; ou

III - mediante autorização do Comitê de Governança, Integridade e Transparência (CGIT).

§ 4º Quando o usuário for uma unidade organizacional, a conta estará vinculada aos dados pessoais da chefia imediata no exercício.

Art. 9º As informações minimamente necessárias para identificar o relacionamento do usuário com a instituição serão estipuladas com base no tipo de vínculo que o usuário irá assumir.

Seção II

Dos Relacionamentos da Identidade Digital

Art. 10. Os relacionamentos que um usuário pode assumir na instituição para ser considerado usuário interno são:

I - discente: pessoa que mediante processo seletivo adentra a um dos cursos regulares oferecidos pela instituição e que tenha direito a diploma mediante a integralização de carga horária proposta no currículo vigente do curso ou a certificado no caso de cursos *lato-sensu*;

II - Técnico Administrativo em Educação (TAE): servidor público concursado para exercer atividades de cunho administrativo;

III - docente: servidor público concursado para exercer atividades relacionadas a ensino, pesquisa e extensão;

IV - colaborador: prestador de serviço para auxiliar em atividades administrativas ou acadêmicas;

V - Técnico Administrativo em Educação externo: colaborador que assume papel temporário para auxiliar em atividades administrativas;

VI - docente externo: colaborador que assume papel temporário para auxiliar subunidades acadêmicos em atividades de ensino, pesquisa e extensão;

VII - docente substituto: professor contratado por tempo determinado, por meio de processo seletivo, para atender necessidade temporária das subunidades acadêmicas, regido pela Lei nº 8.745/93;

VIII - docente visitante: professor contratado temporariamente com o intuito de possibilitar intercâmbio científico e tecnológico, regido pela Lei nº 8.745/1993, e colaborar em programas de pós-graduação; e

IX - unidade organizacional: unidade pertencente ao organograma da UFMA.

Art. 11. Os relacionamentos que um usuário pode assumir na instituição para ser considerado usuário externo são:

I - credor: pessoa física ou representante de pessoa jurídica que forneça bens ou serviços;

II - concedente de estágio: representante de pessoa jurídica responsável por disponibilizar vagas de estágio não-obrigatório para discentes regularmente matriculados nos cursos de graduação da instituição;

III - aluno especial: pessoa física que tem direito de realizar um quantitativo de carga horária limitada em disciplinas oferecidas, mediante disponibilidade de vagas em um semestre letivo;

IV - auditor externo: pessoa física representante de órgãos de controle que necessite de acesso para realizar auditoria;

V - instituição externa - diploma: representante de instituições de ensino superior privada que necessitam registrar o diploma de seus discentes;

VI - participante de eventos: pessoa física que participa de eventos ou seletivos oferecidos pela comunidade universitária;

VII - responsáveis: responsável legal de discente matriculado em cursos do nível fundamental e médio;

VIII - aluno egresso: aluno que tenha satisfeito todas as exigências para recebimento do diploma ou certificado de conclusão do curso que lhe é devido; e

IX - membro externo: participante de colegiados e outras funções exercidas na instituição.

Art. 12. A identidade digital de um usuário permitirá obter todas as informações dos relacionamentos internos do usuário com a instituição.

Seção III

Do Identificador Institucional

Art. 13. O identificador primário institucional será formado com base no nome civil ou no nome social do usuário, e será denominado *login*.

§ 1° Usuários com relacionamento de unidade organizacional terão seu identificador formado em função da sigla da unidade, seguida de ponto (.) e sigla da sua unidade máxima.

§ 2° Para salvaguardar a comunicação com outras áreas ou órgãos durante a transição, as unidades que estiverem fora do padrão adotado terão o identificador anterior mantido pelo período máximo de três anos como alternativo, para que as unidades tenham tempo para realizar a atualização cadastral onde for necessária.

§ 3º O nome social será utilizado somente se respeitar a legislação vigente.

Art. 14. As opções de *login* oferecidas para o usuário, que não se enquadrem como unidades organizacionais, serão feitas com base nas seguintes regras:

I - prenome seguido de ponto (.) e um dos sobrenomes;

II - um dos sobrenomes seguido de ponto (.) e do prenome;

III - prenome seguido de ponto (.) e das iniciais dos sobrenomes; ou

IV - iniciais do prenome e dos sobrenomes até o penúltimo, seguidos de ponto (.) e do último sobrenome;

§ 1º Somente deverá ser exibido para o usuário as opções disponíveis.

§ 2º As preposições não devem ser consideradas como sobrenomes.

§ 3º Caso nenhuma das opções esteja disponível, o usuário deverá ter o *login* escolhido acrescido do sequencial de maior valor existente mais um.

§ 4º Os serviços digitais que se enquadram no art. 26º podem utilizar regras para compor *login* diversas as definidas no *caput*.

Art. 15. O *login* deve ser composto somente de letras minúsculas, número inteiros e ponto (.) e não deve conter acentos ou outros caracteres especiais.

Art. 16. O *login* poderá ser alterado somente nas seguintes condições:

I - mudança oficial no nome civil;

II - decisão judicial; e

III - criação de nome social respeitando a legislação vigente.

§ 1º Reativação de identidade digital ou novo vínculo não dá direito de alterar identificador de identidade digital existente.

§ 2º A alteração que trata os incisos I e II do *caput* deverá ser realizada conforme as opções definidas no art. 14º.

Seção IV

Da Credencial de Acesso

Art. 17. A credencial padrão do usuário será por meio de senha.

Parágrafo único. Outras credenciais poderão ser utilizadas dependendo do tipo do serviço e do nível de segurança exigido.

Art. 18. A senha é intransferível, não compartilhável e de responsabilidade única e exclusiva do usuário.

Art. 19. A senha será considerada segura, obedecendo-se os seguintes critérios:

I - mínimo de 8 (oito) caracteres;

II - letras maiúsculas e minúsculas;

III - números inteiros;

IV - caracteres especiais;

V - Não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações; e

VI - Não utilizar termos óbvios, tais como: Brasil, senha, usuário, *password ou system*.

Parágrafo único. Senhas dos usuários de unidades organizacionais serão criadas pela unidade de tecnologia da informação com qualquer padrão, para que posteriormente possam ser atualizadas pelo usuário responsável pelo identificador.

Art. 20. A senha deve ser atualizada usando a seguinte periodicidade:

I - a cada seis meses em caso de usuários internos; e

II - a cada doze meses em caso de usuários externos;

Parágrafo único. No ato da atualização, o usuário deverá definir uma senha diferente da anterior.

Seção V

Do Acesso aos Serviços

Art. 21. Um serviço digital oferecido pela instituição deverá ser acessado por um usuário mediante processo de autenticação utilizando identificador e credencial definidos na identidade digital.

§ 1º A autorização de acesso aos serviços é determinada pelo relacionamento que foi atribuído ao usuário

no ato da criação da sua identidade digital.

§ 2º O acesso ao serviço continuará disponível enquanto o(s) relacionamento(s) existir(em) ou conforme normativo de cada serviço;

Seção VI

Da Exclusão/Inativação/Reativação da Identidade Digital

Art. 22. A exclusão da identidade digital corresponde à remoção dos dados da identidade digital do provedor de identidade, e somente poderá ocorrer mediante decisão judicial ou por interesse da instituição após transcorrido o tempo definido em tabela de temporalidade.

Art. 23. A inativação da identidade digital corresponde à permanência dos dados no provedor de identidade, mas sem a possibilidade do usuário utilizá-la.

§ 1º A inativação ocorrerá nas seguintes situações:

I - a pedido do usuário;

II - quando houver desrespeito do usuário a esta política;

III - para cumprimento de decisões de cunho administrativo;

IV - para servidor (Docente e TAE) que perderam o vínculo; e

V - por inatividade do usuário em caso de colaboradores e docentes externos.

§ 2º É vedada a criação de uma nova identidade digital para um usuário que possua uma identidade digital inativada.

§ 3º Semestralmente as chefias imediatas deverão validar a identidade digital de colaboradores e docentes externos de sua unidade organizacional para evitar a inativação delas.

Art. 24. A reativação de uma identidade digital ocorrerá sempre que o usuário possuir uma identidade digital inativada e quando ocorrer uma das seguintes hipóteses:

I - o usuário obteve direito de reativar sua identidade após análise; e

II - o usuário obteve um novo vínculo com a instituição.

CAPÍTULO VI

DO PROVEDOR DE IDENTIDADE

Art. 25. A unidade de tecnologia da informação é a unidade responsável por gerir as questões relacionadas ao provimento de identidade.

§ 1º A unidade de tecnologia da informação, quando for oportuno, pode compartilhar com outras unidades da instituição a responsabilidade de gerenciar o provimento de identidade com vistas a dar celeridade ao processo.

§ 2º Todas unidades que estão envolvidas na emissão de identidades digitais devem buscar meios de garantir a autenticidade das informações prestadas pelo usuário e definir procedimentos para gestão destas identidades.

Art. 26. Para evitar que o serviço de provimento de identidade armazene identidades digitais desnecessárias, é facultada a utilização da identidade digital para os serviços digitais que:

I - atinjam um grande número de pessoas com relacionamento indireto, por exemplo, inscrição em processos seletivos ou em eventos ofertados pela instituição; e

II - a natureza do serviço de alguma maneira não exija que o usuário utilize a identidade digital com determinada frequência.

Parágrafo único. A forma de identificação para os serviços definidos nos incisos I e II do *caput* deverá ser definida pela unidade de tecnologia da informação.

CAPÍTULO VII
DAS COMPETÊNCIAS

Art. 27. Compete à unidade de tecnologia da informação:

I - definir a(s) tecnologia(s) que será(ão) usada(s) para fornecer o serviço de provimento de identidade digital;

II - realizar a gestão (emissão, alteração e inativação) de todas as identidades digitais ou das unidades que compartilham esta responsabilidade;

III - oferecer suporte de integração com a Federação CAFe;

IV - definir processos para evitar fraudes no ato da emissão de identidades digitais;

V - fazer a ativação de uma identidade digital inativada;

VI - alterar os dados pessoais do identificador de usuários com relacionamento de unidade organizacional sempre que houver mudança de chefia;

VII - permitir que outros serviços possam se autenticar utilizando a tecnologia de provimento de identidade adotada;

VIII - avisar ao interessado todas as vezes que a instituição for notificada de possíveis vazamentos de seus dados;

IX - salvaguardar o registro das operações realizadas sobre as identidade digitais para garantir possíveis auditorias; e

X - garantir que o tratamento e transparência das identidades digitais sigam a legislação vigente de modo particular Lei nº 12.527, de 18 de novembro de 2011, e a Lei nº 13.709, de 14 de agosto de 2018;

§ 1º A base de dados oficial para salvaguardar as identidades digitais será a base utilizada pelos sistemas corporativos vigentes na instituição.

§ 2º A unidade de tecnologia da informação, mediante autorização do CGIT, poderá armazenar em outras bases de dados internas as informações referentes às identidades digitais.

Art. 28. Compete ao usuário:

I - solicitar a emissão de sua identidade digital;

II - manter as credenciais de sua identidade em sigilo e não compartilhar sua identidade digital com outras pessoas;

III - manter as informações de sua identidade digital atualizadas;

IV - notificar a unidade de tecnologia da informação caso identifique que sua identidade foi violada; e

V - solicitar formalmente a inativação da sua identidade digital.

CAPÍTULO VIII
DA RESPONSABILIZAÇÃO

Art. 29. Os usuários que não manterem observância ao disposto nos artigos desta política estarão sujeitos às sanções administrativas cabíveis nos termos da lei, podendo haver cominações nas esferas cível e penal.

§ 1º A infração ao disposto no *caput* ocasionará a inativação imediata do acesso do usuário até que os fatos sejam apurados.

§ 2º O processamento administrativo para apuração de infrações aos ditames deste Regulamento, quanto aos servidores públicos, se dará nos termos do Título V - Do Processo Administrativo Disciplinar - da Lei 8.112, de 11

de dezembro de 1990, no que couber.

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS

Art. 30. Os casos omissos durante a aplicação desta política serão tratados pelo CGIT.

Art. 31. A unidade de tecnologia da informação terá até 12 (doze) meses, a partir da publicação, para operacionalizar essa política.