MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO CEARA

RESOLUÇÃO Nº 05/CATI, DE 15 DE ABRIL DE 2025

Institui a Política de Definição e Uso de Senhas nos Sistemas de Informação Institucionais e Recursos Computacionais da Universidade Federal do Ceará.

O REITOR DA UNIVERSIDADE FEDERAL DO CEARÁ, no uso de suas atribuições legais e estatutárias, e em atendimento à recomendação expressa do Comitê Administrativo de Tecnologia da Informação (CATI), em sua reunião de 15 de abril de 2025, e considerando a documentação apresentada por meio do processo administrativo SEI nº 23067.002588/2026-12,

RESOLVE:

Art. 1º Aprovar a Política de Definição e Uso de Senhas de Acesso a Sistemas Institucionais e Recursos Computacionais da Universidade Federal do Ceará (UFC), a qual passa a integrar esta Resolução como Anexo.

Art. 2º Estabelecer um recadastramento geral de senhas do Sistema Integrado de Informações Institucionais (SI3) por meio de Portaria a ser publicada pela Superintendência de Tecnologia da Informação (STI).

Art. 3º Esta Resolução entra em vigor na data de sua publicação, revogadas as disposições em contrário, notadamente o Capítulo III dos Anexos da Política de Segurança da Informação e Comunicação (POSIC) da UFC, objeto da Instrução Normativa 1/2021/CISI/STI_REITORIA/REITORIA, de 08 de abril de 2021.

Reitoria da Universidade Federal do Ceará, em Fortaleza , 15 de abril de 2025.

CUSTÓDIO LUÍS SILVA DE ALMEIDA
Reitor

ANEXO À RESOLUÇÃO Nº 05/CATI, DE 15 DE ABRIL DE 2025

POLÍTICA DE DEFINIÇÃO E USO DE SENHAS DA UNIVERSIDADE FEDERAL DO CEARÁ

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Seção I
Do Objetivo

Art. 1º Estabelecer normas para sistematização do processo de definição e utilização de

senhas para acesso aos recursos institucionais, em conformidade com a Política de Segurança da Informação e Comunicações (POSIC) da UFC.

Seção II
Do Escopo

Art. 2º Esta norma se aplica aos processos de criação e uso de senhas de acesso institucional, por qualquer meio disponível, para qualquer sistema de informação institucional da UFC.

Art. 3º O usuário da rede e dos sistemas institucionais da UFC deve estar devidamente identificado para que se possa obter o acesso aos recursos institucionais, através de um identificador único de usuário (ID) e senha.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 4º Esta política é orientada pelos princípios básicos da Política de Segurança da Informação e Comunicação (POSIC) da UFC, que considera os preceitos básicos da segurança da informação, sendo os incisos VIII e IX fundamentos para todas as ações e diretrizes dessa política:

I - a confidencialidade;

II - a legalidade;

III - a autenticidade;

IV - o não-repúdio;

V - a conformidade;

VI - o controle de acesso;

VII - a auditabilidade;

VIII - a integridade;

IX - a disponibilidade.

Art. 5º No ambiente de Tecnologia da Informação, o uso de senhas provê o controle necessário para que os dados institucionais possam ser acessados apenas por aqueles que detém sua explícita autorização de guarda e uso.

CAPÍTULO III
CONCEITOS E DEFINIÇÕES

Seção I
Da Terminologia

Art. 6º São termos e definições utilizados nesta Política:

I - Senha: Conjunto de caracteres destinado a identificar o usuário ou a permitir acesso a dados, programas ou sistemas que não estão disponíveis ao público.

II - Usuário: Indivíduo devidamente identificado que possui acesso a sistemas e recursos computacionais da instituição.

III - *Login* ou ID: identificador único atribuído a um Usuário.

IV - *Logon*: Processo para acessar um sistema de informação restrito feita através da autenticação ou identificação do usuário, usando credenciais previamente cadastradas no sistema.

V - *Logoff*: Processo para saída de um sistema de informação restrito feita através da autenticação ou identificação do usuário.

Art. 7º Para os efeitos desta Política e das normas dela originadas, entende-se por:

I - Reitoria: é o órgão executivo superior, ao qual compete dirigir, administrar, planejar, coordenar, estabelecer parcerias e fiscalizar as atividades da universidade;

II - Comitê Administrativo de Tecnologia da Informação e Governança Digital (CATI): Comitê responsável por elaborar, revisar e apreciar periodicamente a POSIC e normas relacionadas, entre

outras competências; tem entre suas atribuições principais: participar e orientar o planejamento dos investimentos em Tecnologia da Informação e Comunicações de acordo com as diretrizes do Plano de Desenvolvimento Institucional (PDI) em execução; estabelecer as políticas, diretrizes e prioridades na área de Tecnologia da Informação e Comunicações (TIC); promover e estimular o desenvolvimento da Tecnologia da Informação e Comunicações no âmbito da UFC; elaborar, acompanhar e avaliar um Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) para a UFC; elaborar, acompanhar e avaliar as Políticas de Segurança da Informação e Comunicações para a UFC;

III - Superintendência de Tecnologia da Informação (STI): instância administrativa/executiva responsável pelo desenvolvimento, implantação e manutenção dos ativos de sistemas de informação;

IV - Coordenadoria de Infraestrutura e Segurança da Informação (CISI): responsável por monitorar e analisar o cumprimento das políticas, normas e procedimentos de segurança dos sistemas de informação e comunicações, além de elaborar estratégias para comunicação, publicação e divulgação das políticas, normas e procedimentos de segurança dos sistemas de informação e comunicações;

CAPÍTULO IV
COMPETÊNCIAS E RESPONSABILIDADES

Art. 8º A STI é a unidade responsável por assegurar a execução das normas de definição e uso de senhas institucionais.

CAPÍTULO V
DIRETRIZES GERAIS

Art. 9º São diretrizes gerais da Política de Senhas da UFC:

I - O procedimento de identificação e autenticação, chamado de *logon*, deve divulgar o mínimo de informações sobre o sistema, evitando fornecer, a um usuário não autorizado, informações detalhadas;

II - Informar que o serviço ou sistema só deve ser acessado por pessoas autorizadas;

III - Evitar identificar o sistema ou suas aplicações até que o processo de *logon* esteja completamente concluído;

IV - Durante o processo de *logon*, evitar o fornecimento de mensagens de ajuda que poderiam auxiliar um usuário não autorizado a completar esse procedimento;

V - Validar a informação de *logon* apenas quando todos os dados de entrada estiverem completos. Caso ocorra algum erro, o sistema não deve indicar qual parte do dado de entrada está correta ou incorreta, como por exemplo, ID ou senha;

VI - Limitar o número de tentativas de *logon* sem sucesso, por exemplo um máximo de três tentativas;

VII - Registrar as tentativas de acesso inválidas;

VIII - Definir um tempo de espera antes de permitir novas tentativas de entrada no sistema ou rejeitar qualquer tentativa posterior de acesso sem autorização específica;

IX - Encerrar as conexões com o sistema ou serviço, depois de um período de inatividade ou quando finalizado o acesso;

X - Limitar o tempo máximo para o procedimento de *logon*. Se excedido, o sistema deverá encerrar o procedimento;

XI - Mostrar as seguintes informações, quando o procedimento de *logon* no sistema finalizar com êxito, tais como data e hora do último *logon* com sucesso ou detalhes de qualquer tentativa de *logon* sem sucesso, desde o último procedimento realizado com sucesso.

XII - Observar as boas práticas e procedimentos de Segurança da Informação e Comunicações recomendados por órgãos e entidades responsáveis pelo estabelecimento de padrões, bem como o que foi disposto pela POSIC da UFC e suas normas.

Art. 10. As Diretrizes de Segurança da Informação definidas nesta política são aplicadas aos ativos de informação, de hardware, de software e intangíveis, fornecendo orientações para práticas de gestão de segurança da informação.

Seção I
Das Diretrizes para a Definição de Senhas de Acesso Institucionais

Art. 11. Os sistemas ou serviços que façam uso de controle de acesso à informação e usuários devem restringir a criação de senhas compostas de elementos facilmente identificáveis, como por exemplo:

I - nome do usuário;

II - identificador do usuário, mesmo que os caracteres estejam embaralhados;

III - nomes de pessoas ou lugares em geral;

IV - nome do sistema operacional ou da máquina que está sendo utilizada;

V - nomes próprios;

VI - palavras que constam de dicionários em qualquer idioma;

VII - letras ou números repetidos;

VIII - sequência de três números consecutivos (123, 789, 456, etc.);

IX - sequência de três letras seguidas do teclado do computador (ASD, QWE, YUI, etc.) ou do alfabeto (ABC, XYZ, etc.);

X - qualquer senha com menos de 8 (oito) caracteres;

XI - qualquer senha com mais de 64 (sessenta e quatro) caracteres.

Art. 12. As senhas definidas pelo usuário deverão possuir pelo menos uma letra maiúscula, uma letra minúscula, um número e um símbolo, totalizando, no mínimo, 8 (oito) caracteres.

Parágrafo único. O usuário não deve usar data de nascimento, número de CPF, número de SIAPE, número de RG.

Art. 13. Os sistemas, serviços e usuários que façam uso do controle de acesso à informação devem alterar a senha em intervalos regulares não superiores a 6 (seis) meses ou com base no número de acessos, vedada a reutilização das últimas 4 (quatro) senhas já utilizadas.

Parágrafo único. Caso o usuário não efetue a troca no prazo estabelecido, será bloqueado seu acesso aos sistemas institucionais até que a nova senha seja configurada.

Art. 14. Ao usuário detentor do acesso aos serviços institucional é proibido:

I - revelar a senha de acesso de sistema institucional, sendo ela pessoal e intransferível, além de que o fornecimento ou empréstimo de senha que possibilite o acesso de pessoas não autorizadas a sistemas de informações é tratado no inciso I do § 1º do art. 325 do Código penal.

II - registrar as senhas em papel, navegador ou meio que não garanta privacidade da informação;

III - divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

IV - falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

V - trocar arquivos que entrem em desacordo com leis, políticas e normas vigentes.

Art. 15. A STI poderá, a qualquer momento, motivada por suspeita de algum tipo de abuso, suspender, sem aviso prévio, qualquer conta de acesso a sistemas ou serviços institucionais, pelo tempo que julgar necessário.

Parágrafo único. Todos os usuários devem alterar a senha sempre que existir qualquer indicação de possível comprometimento do sistema, da própria senha ou quando solicitado pela STI.

Art. 16. A STI poderá modificar a Política Institucional de Definição e Uso de Senhas a qualquer momento e sem aviso prévio, de acordo com a sua necessidade técnica, recursos disponíveis e normas e legislação vigentes.

Art. 17. O usuário deve responder, em todas as instâncias, pelas consequências das ações ou omissões da própria parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de sua senha ou das transações a que tenha acesso.

CAPÍTULO VI
VIOLAÇÕES, PENALIDADES E SANÇÕES

Art. 18. A desobediência ou violação desta norma implicará em sanções administrativas nos termos da lei, normas complementares, regimentos e resoluções internas, sem prejuízo de outras previstas nas esferas cível e penal.

Parágrafo único. O procedimento para a aplicação das penalidades e/ou sanções seguirá o rito específico da legislação, norma, regimento ou resolução a que corresponder o caso concreto.

CAPÍTULO VII
FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

Art. 19. As referências legais e normativas utilizadas para a elaboração da POSIC da UFC e destas políticas estão de acordo com:

I - O disposto no artigo 5o, incisos IV e VI, da Instrução Normativa no 1, de 13/6/2008, do Gabinete de Segurança Institucional da Presidência da República, publicada na seção 1 do D.O.U. no 115, de 18/6/2008;

II - Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso da Informação;

III - Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação - PNSI, no âmbito da administração pública federal;

IV - Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais;

V - Lei nº 9.069, de 19 de fevereiro de 1998, Lei do Software;

VI - Lei nº 12.965, de 23 de abril de 2014, Marco Civil da Internet.

CAPÍTULO VIII
DISPOSIÇÕES FINAIS

Art. 20. Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Definição e Uso de Senhas deverão ser analisados e resolvidos pela STI.

Art. 21. A presente política passa a vigorar a partir da data de sua aprovação, revogando-se as disposições em contrário.

Histórico de versões

Data	Versão	Descrição	Autor
15/04/2025	1.0	Produção da versão inicial	Coordenadoria de Infraestrutura e Segurança da Informação (CISI)

Reitoria da Universidade Federal do Ceará, em 15 de abril de 2025.

CUSTÓDIO LUÍS SILVA DE ALMEIDA
Reitor

Documento assinado eletronicamente por **CUSTODIO LUIS SILVA DE ALMEIDA**, **Reitor**, em 23/02/2026, às 17:11, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufc.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6128506** e o código CRC **057D18E3**.

Av. da Universidade, 2853 - (85) 3366-7305
CEP 60020-181 - Fortaleza/CE - http://ufc.br/