



MINISTÉRIO DA EDUCAÇÃO

Universidade Federal de Alfenas - UNIFAL-MG

Rua Gabriel Monteiro da Silva, 700 - Alfenas/MG - CEP 37130-001

Fone: (35) 3701-9000



UNIVERSIDADE FEDERAL DE ALFENAS - UNIFAL-MG
COMITÊ GESTOR DE TECNOLOGIA DE INFORMAÇÃO (CGTI)
RESOLUÇÃO Nº 4, DE 19 DE MAIO DE 2017

Estabelece as normas de uso de credenciais de acesso no âmbito da UNIFAL-MG.

O Comitê Gestor de Tecnologia de Informação (CGTI) da Universidade Federal de Alfenas – UNIFAL-MG, no uso de suas atribuições regimentais e considerando:

A necessidade do estabelecimento de regras e definição de responsabilidades relacionados à guarda e uso de dispositivos de identificação e credenciais de acesso (identificação do usuário e senha) por todos os usuários no âmbito da Universidade Federal de Alfenas - UNIFAL-MG, de forma a preservar a segurança das informações quando do acesso ou uso dos diversos ativos de Tecnologia da Informação e Comunicação - TIC, e;

A Norma ABNT NBR ISO/IEC 27002 e a RFC 1244,

Resolve estabelecer as normas de uso de credenciais de acesso no âmbito da UNIFAL-MG, nos seguintes termos:

Art. 1º Para os fins desta Resolução, entende-se por:

I – Usuário: qualquer pessoa (servidores, alunos, visitantes, estagiários, empregados temporários, prestadores de serviços, colaboradores, terceirizados, etc) que possua ou não vínculo com a UNIFAL-MG, e que necessite de credenciais de acesso para utilização de recursos de TIC da instituição;

II – Dispositivo de Identificação: **login**, número de registro do usuário, crachá, identificação de usuário para acesso aos sistemas (nome de usuário, matrícula etc.), certificados e assinaturas digitais (**Token/SmartCard/etc.**), características biométricas e qualquer outro dispositivo, físico ou lógico, com ou sem o uso de senha, que possa identificar univocamente um usuário;

III – Credencial de Acesso: conjunto de informações que pertencem a um usuário e que são usadas para, de forma unívoca, identificar e validar o acesso a qualquer recurso de TIC da instituição;

IV – Serviço de TIC: qualquer meio eletrônico utilizado pelo usuário para acesso, envio, recebimento e armazenamento da informação, inclusive qualquer **software**, desenvolvido ou não no âmbito da UNIFAL-MG, que acesse e manipule informações relacionadas às atividades da instituição;

V – **Login** Institucional – Juntamente com a senha pessoal: é a credencial de acesso aos serviços de TIC internos da UNIFAL-MG. Para os discentes, é o seu número de matrícula, inclusive com os pontos. Para os demais usuários, é composto pelo nome e sobrenome, separados por um ponto, no formato “nome.sobrenome”.

Art. 2º No âmbito da utilização de serviços de TIC da UNIFAL-MG, os usuários devem ser univocamente identificados, sejam eles pessoas físicas ou jurídicas, a fim de proteger a identidade do usuário, evitando e prevenindo que qualquer pessoa física ou jurídica se faça passar por outra perante a UNIFAL-MG ou a terceiros.

Parágrafo único. A identificação dos usuários internos da UNIFAL-MG perante os sistemas internos da instituição será feita através do **login** institucional.

Art. 3º A credencial de acesso é pessoal e intransferível e, portanto, não poderá ser compartilhada com outras pessoas em hipótese alguma, sob pena de responsabilização pelos atos decorrentes do uso indevido da credencial.

Art. 4º Todos os dispositivos de identificação utilizados na UNIFAL-MG devem estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

§ 1º Os Dispositivos de Identificação que se referem às unidades da UNIFAL-MG devem estar associados ao dirigente responsável pela unidade.

§ 2º É responsabilidade do dirigente da unidade o controle formal dos usuários com acesso aos dispositivos de identificação que se refiram às unidades da UNIFAL-MG.

Art. 5º O usuário vinculado a um dispositivo de identificação, enquanto titular da credencial de acesso, será responsável pela sua guarda e pelo seu uso correto perante a instituição e a legislação brasileira, tendo ainda como responsabilidades:

I. zelar pela confidencialidade da sua senha, sendo esta de uso pessoal e intransferível e garantir que ela não seja divulgada para quaisquer outras partes;

II – manter e memorizar sua senha;

III – alterar a senha sempre que existir qualquer indicação de possível comprometimento dos dados de qualquer serviço de TIC ou da própria senha;

IV – utilizar suas credenciais somente para fins designados e para os quais estiver devidamente autorizado, de acordo com as suas funções e responsabilidades;

V – substituir a senha inicial gerada pelo sistema assim que recebê-la;

VI – reportar imediatamente à Gerência de Segurança da Informação do Núcleo de Tecnologia de Informação (NTI), os casos de violação das credenciais de acesso, acidental ou não, e providenciar a troca da senha imediatamente e, se necessário, a troca do dispositivo de identificação;

VII – solicitar o cancelamento das credenciais de acesso, suas ou de seus subordinados, quando elas não forem mais necessárias; e

VII – manter e guardar as credenciais de acesso a sistemas ou serviços de informação externos que faça uso para o desempenho de suas funções na UNIFAL-MG, devendo observar e seguir o disposto nesta norma, sempre que possível.

Art. 6º São responsabilidades do NTI da UNIFAL-MG:

I – administrar as credenciais de acesso dos usuários que necessitem utilizar um serviço de TIC da UNIFAL-MG;

II – prover e manter um sistema de administração das credenciais de acesso de todos os usuários para criação, guarda e alteração das mesmas conforme o disposto nesta norma;

III – efetuar verificações periódicas a fim de detectar fragilidades que possam comprometer a segurança das informações, nos termos e procedimentos desta norma;

IV – manter as credenciais de acesso em sistema seguro e criptografado.

V – automatizar, dentro do possível, a remoção e desabilitação da credencial de acesso assim que o usuário deixar de possuir vínculo com a UNIFAL-MG; e

VI – bloquear ou desabilitar as Credenciais de Acesso em casos de determinação administrativa, judicial ou utilização indevida dos serviços de TIC da UNIFAL-MG no âmbito das normas existentes.

Art. 7º A senha é um meio de verificação da identidade do usuário para obtenção de acesso a um serviço de TIC, devendo possuir obrigatoriamente no mínimo 8 (oito) caracteres, sendo preferencialmente de fácil memorização, para que não tenha que ser anotada. Deve conter ainda, no mínimo, uma letra, um algarismo numérico e um caractere especial (!, @, #, \$, %, * etc.).

§ 1º No ato da criação de senhas, o usuário deverá observar as boas práticas contidas no Anexo I desta resolução, bem como outras que vierem a ser divulgadas pelo NTI.

§ 2º No momento do cadastro do usuário na UNIFAL-MG, serão fornecidas senhas iniciais seguras, geradas automaticamente, de forma aleatória, satisfazendo as condições descritas nesta norma, individualizadas e temporárias e que deverão ser obrigatoriamente trocadas pelo usuário no primeiro acesso. As senhas iniciais serão enviadas para o e-mail pessoal do usuário cadastrado no sistema da Pró-Reitoria de Gestão de Pessoas;

§ 3º Nos casos de esquecimento de senha, somente serão fornecidas senhas temporárias através da opção “Recuperar Senha” presente nos Serviços de TIC da UNIFAL-MG, sendo vedado o fornecimento de senhas temporárias através de contatos telefônicos ou por e-mail. Caso necessário, o usuário poderá requerer pessoalmente uma senha temporária dirigindo-se à unidade de TI de seu campus, munido de documento de identificação com foto.

§ 4º A recuperação de senha das credenciais de acesso que se referem às unidades da UNIFAL-MG só será feita mediante solicitação direta ao NTI via Ordem de Serviço pelo dirigente da unidade.

§ 5º No caso de ocorrerem cinco tentativas de autenticação malsucedidas consecutivas, a credencial de acesso será bloqueada por 15 (quinze) minutos.

§ 6º A qualquer momento poderá ser solicitada pelo NTI a troca imediata da senha de qualquer usuário caso seja detectada alguma vulnerabilidade ou irregularidade na sua criação.

Art. 8º O gerenciamento das senhas utilizadas pelos usuários no exercício de suas atribuições na UNIFAL-MG em dispositivos de identificação do tipo **Token/SmartCard** (PIN/PUK e revogação), bem como em sistemas ou serviços de informação externos, como sites, instituições financeiras e de outros órgãos será de responsabilidade exclusiva de seus titulares, devendo os mesmos observarem que a criação das senhas deve seguir o disposto nesta norma, sempre que possível.

Art. 9º O NTI fará verificações periódicas quanto ao nível de segurança das senhas a fim de detectar fragilidades que possam comprometer a segurança das informações e, assim, caso seja necessário, solicitar que o usuário realize a troca da sua senha por uma com nível de segurança maior.

§ 1º As verificações serão feitas de forma automatizada, através de **softwares** que submetem senhas a ataques de dicionário e força bruta, sendo que o usuário apenas será informado caso seja detectado que sua senha tem um nível de segurança baixo.

§ 2º As verificações serão feitas apenas no âmbito da UNIFAL-MG, em ambiente interno e controlado, de maneira que não haja vazamento de nenhuma informação que identifique o usuário e a sua respectiva senha ou que possa ferir a sua privacidade.

Art. 10. Todas as senhas que não atendam ao disposto nessa resolução serão automaticamente expiradas a partir de sua publicação, sendo exigida a troca por parte do usuário.

Art. 11. O NTI deverá dar ampla divulgação desta Resolução junto aos usuários da Universidade.

Art. 12. Os casos omissos nessa norma serão resolvidos pelo Comitê Gestor de Tecnologia da Informação - CGTI.

Art. 13. Esta Resolução entra em vigor na data de sua publicação no quadro de avisos da Reitoria.

Prof. Paulo Márcio de Faria e Silva

Presidente do CGTI

ANEXO I – BOAS PRÁTICAS PARA CRIAÇÃO DE SENHAS

I – A senha não deve ser baseada em qualquer informação pessoal como nomes de familiares, de animais de estimação, sobrenomes, datas de nascimento ou casamento, números de telefones, placas de veículos, times preferidos, bandas, etc;

II – A senha nunca deve ser igual ao nome de usuário;

III – A senha não deve ser vulnerável a ataque de dicionário, não contendo caracteres idênticos consecutivos (por exemplo: aaa, aaabbb, cckk), subsequentes (por exemplo: 123, 12321, abcde) ou sequências do teclado (asdfg, qwert, poiuy), sejam eles em ordem crescente ou decrescente;

IV – Não devem ser usadas palavras que possam ser encontradas em um dicionário de qualquer idioma;

V – Não devem ser criadas senhas parecidas com senhas anteriores;

VI – Não deve ser utilizada na instituição a mesma senha utilizada em outros serviços externos de uso pessoal.