



Ministério Público Federal

## INSTRUÇÃO NORMATIVA Nº 11, DE 7 DE AGOSTO DE 2014

Alterada pela [PORTARIA SG/MPF Nº 1210, DE 7 DE OUTUBRO DE 2014](#)

Dispõe sobre os critérios mínimos de segurança de senhas de contas de usuários, de equipamentos e de aplicações no âmbito do Ministério Público Federal.

O SECRETÁRIO-GERAL DO MINISTÉRIO PÚBLICO FEDERAL, no uso da atribuição que lhe confere o art. 23, incisos I e XV, da Portaria PGR/MPF nº 591, de 20/11/2008, e tendo em vista o que consta no Processo Administrativo PGR/MPF nº 1.00.000.007128/2014-52, resolve:

Art. 1º Os critérios mínimos de segurança de senhas utilizados nos sistemas do Ministério Público Federal, a responsabilidade das áreas de informática pelo armazenamento, pela guarda, pela manutenção e pela auditoria das senhas institucionais e a responsabilidade dos usuários pela guarda e pelo sigilo das senhas de contas que lhes são disponibilizadas serão disciplinados por esta Instrução Normativa.

### CAPÍTULO I

#### DAS DISPOSIÇÕES GERAIS

Art. 2º As senhas de contas de usuários utilizadas no âmbito do Ministério Público Federal, com disponibilização pessoal e individualizada, são de responsabilidade exclusiva do usuário ao qual se destinam, e permitem o acesso a sistemas compatíveis com a natureza das atividades regularmente desempenhadas.

Art. 3º É vedado ao usuário o compartilhamento de sua senha com terceiros, bem como a utilização de senha de terceiros para acesso a qualquer sistema do Ministério Público Federal.

Art. 4º A concessão de credenciais de acesso ao usuário observará o critério do privilégio mínimo, segundo o qual o usuário não possuirá acesso a sistema cuja abrangência seja maior do que aquela necessária à consecução de suas atividades.



## Ministério Público Federal

§ 1º A autenticação dos sistemas utilizados no âmbito do Ministério Público Federal ocorrerá, preferencialmente, por meio do uso da senha armazenada no Serviço Nacional de Diretório.

§ 2º Sempre que possível, utilizar-se-á autenticação de pelo menos dois fatores, com vistas a se garantir maior segurança ao sistema.

### CAPÍTULO II

#### DAS FALHAS NA UTILIZAÇÃO DE SENHA

Art. 5º Caso ocorram falhas de ordem técnica na inclusão, na alteração ou no desbloqueio de senha, o usuário deverá contactar a Coordenadoria de Atendimento e Relacionamento da Secretaria de Tecnologia da Informação e Comunicação da Secretaria Geral do Ministério Público Federal ou a área responsável pelos serviços de Tecnologia da Informação na respectiva unidade.

Art. 6º Na hipótese de esquecimento de senha, a Secretaria de Tecnologia da Informação e Comunicação responsabilizar-se-á pela disponibilização de mecanismo seguro para que o próprio usuário, mediante êxito em respostas a questionário a ele previamente submetido, possa gerar nova senha de acesso ao sistema.

### CAPÍTULO III

#### DOS CRITÉRIOS MÍNIMOS DE SEGURANÇA DE SENHAS

Art. 7º As senhas serão compostas pelo mínimo de 8 (oito) caracteres e conterá, ao menos, uma letra maiúscula, uma letra minúscula e um numeral.

Parágrafo único. A exigência de composição mínima das senhas, nos termos do caput deste artigo, não impede que outros requisitos sejam determinados pela área de Tecnologia da Informação da unidade, com vistas a se assegurar maior grau de segurança das informações.

Art. 8º A substituição das senhas deverá ocorrer, ao menos, uma vez a cada 180 (cento e oitenta) dias, vedada a reutilização das 5 (cinco) últimas senhas registradas pelo usuário.

§ 1º Atingido o prazo previsto no caput deste artigo, o usuário será comunicado para que promova a substituição de sua senha dentro de, no mínimo, 2 (dois) dias úteis.

§ 2º As contas de usuários que permitem acesso em nível de administrador deverão ser substituídas, ao menos, uma vez a cada 90 (noventa) dias.

§ 3º As contas privilegiadas de acesso aos equipamentos somente poderão ser utilizadas por meio de console ou de Internet Protocols (IP's) restritos e previamente cadastrados,



Ministério Público Federal

possuirão tamanho mínimo de 20 (vinte) caracteres e serão substituídas, ao menos, uma vez a cada 1 (um) ano.

Art. 9º É vedada a utilização, por usuários anônimos, de aplicações ou serviços que acessem métodos de autenticação, como o sistema Single Sign-On (SSO) ou o protocolo Lightweight Directory Access Protocol (LDAP).

§ 1º As contas a que se referem o caput deste artigo possuirão unicidade de usuário e de senha por aplicação ou sistema, tamanho mínimo de 20 (vinte) caracteres e serão substituídas, ao menos, uma vez a cada 1 (um) ano.

§ 2º Os sistemas legados, qualificados por mecanismo próprio de autenticação, que possuam limitação de tamanho, deverão ser informados para a Divisão de Segurança da Informação da Secretaria de Tecnologia da Informação e Comunicação da Secretaria Geral do Ministério Público Federal, para fins de análise de risco.

Art. 10. Quando verificadas 5 (cinco) tentativas incorretas de acesso ao sistema, a senha deverá ser bloqueada por um intervalo mínimo de 30 (trinta) minutos, findo o qual ocorrerá o desbloqueio automático da conta e se possibilitará novo acesso sem necessidade de intervenção da área de Tecnologia da Informação.

Parágrafo único. As tentativas incorretas de acesso deverão ser armazenadas de forma segura, para posterior auditoria, por um período mínimo de 1 (um) ano.

Art. 11. As senhas de acesso ao sistema não poderão apresentar identidade com o login do usuário, ser formadas por padrões de letras ou números sequenciais e de fácil dedução, ou pelos seguintes critérios:

I - somente palavras de dicionário ou siglas das unidades e dos órgãos do Ministério Público Federal;

II - somente datas ou números de telefone;

III - somente nomes próprios ou nomes escritos inversamente;

IV - somente identificadores pessoais do usuário, como o número de matrícula, do Registro de Identidade Civil (RIC) ou do Cadastro de Pessoa Física (CPF).

Art. 12. Para cadastramento da senha de acesso, o usuário deverá seguir as seguintes orientações:

I - cadastrar senhas, nos sistemas institucionais, diversas daquelas utilizadas em acessos particulares, como em sistemas bancários, provedores de internet e contas de e-mail pessoal;

~~II - sempre que possível, cadastrar senhas diferentes para sistemas distintos;~~



Ministério Público Federal

II - sempre que possível, cadastrar senhas diferentes para sistemas distintos, ressalvados os sistemas institucionais habilitados com autenticação única (Single Sign-On – SSO);

**(Redação dada pela Portaria SG/MPF nº 1210, de 7 de outubro de 2014)**

III - não transcrever a senha em qualquer meio ou armazená-la on-line sem prévia criptografia;

IV - não compartilhar ou revelar a senha a terceiros, o que abrange, inclusive, servidores da área de Tecnologia da Informação, assessores e secretários;

V - não fazer uso de ferramentas de gerenciamento de contas e senhas;

VI - não revelar a senha por qualquer meio de comunicação eletrônica;

VII - desabilitar a opção de armazenamento de senha nas aplicações, como navegadores, e programas de bate papo;

Parágrafo único. Todas as senhas devem ser tratadas como informação confidencial, cabendo aos servidores guardarem sigilo e protegerem as senhas que lhes são destinadas, observadas sua disponibilidade, autenticidade, integridade e eventual restrição de acesso, nos termos da legislação vigente.

~~Art. 13. A Secretaria de Tecnologia da Informação e Comunicação realizará auditoria das senhas cadastradas no âmbito do Ministério Público Federal, para fins de averiguação do atendimento aos requisitos mínimos de segurança.~~

~~Parágrafo único. Na realização da auditoria prevista no caput deste artigo, observar-se-ão as melhores práticas de segurança da informação, vedada qualquer revelação de senhas, ressalvada a hipótese de notificação ao próprio usuário, caso em que se manterá a senha segura de acesso por terceiros não envolvidos no processo de auditoria.~~

Art. 13. A Secretaria de Tecnologia da Informação e Comunicação deverá habilitar mecanismo automatizado de auditoria de senhas cadastradas no âmbito do Ministério Público Federal para fins de averiguação do atendimento aos requisitos mínimos de segurança. **(Redação dada pela Portaria SG/MPF nº 1210, de 7 de outubro de 2014)**

§ 1º Na realização da auditoria prevista no caput deste artigo, observar-se-ão as melhores práticas de segurança da informação, vedados o armazenamento, o acesso textual e a reversibilidade das senhas cadastradas pelos usuários. **(Redação dada pela Portaria SG/MPF nº 1210, de 7 de outubro de 2014)**

§ 2º Em caso de identificação de senha fraca, decorrente do processo de auditoria automatizada, caberá à Secretaria de Tecnologia da Informação e Comunicação notificar o usuário



Ministério Público Federal

para que providencie sua imediata alteração, em consonância com os critérios estabelecidos nesta Instrução Normativa. **(Redação dada pela Portaria SG/MPF nº 1210, de 7 de outubro de 2014)**

#### CAPÍTULO IV

##### DOS PADRÕES NO DESENVOLVIMENTO DE APLICAÇÕES

Art. 14. Os servidores responsáveis pelo desenvolvimento de sistemas devem se certificar de que os programas possuam os seguintes aspectos de segurança:

I - existência de sistema de autenticação institucionalizado;

II - suporte à autenticação de indivíduos, vedada a utilização de senha coletiva;

III - não armazenamento de senhas em texto em claro ou em qualquer forma de fácil reversão;

IV - utilização de salt, caso aplicada a função hash para o armazenamento de senha;

V - utilização do algoritmo de hash SHA-256, ou versão superior;

VI - alternativas de gerenciamento de usuários que permitam a assunção das funções sem que se tenha acesso à senha do usuário.

Parágrafo único. Na hipótese do inciso V, possibilita-se a utilização de versões inferiores do algoritmo, como MD5 e SHA-1, mediante análise prévia de risco e autorização específica por parte da Divisão de Segurança da Informação da Secretaria de Tecnologia da Informação e Comunicação.

Art. 15. A autenticação entre o sistema e o usuário deverá ser objeto de criptografia, mediante utilização de algoritmos seguros e reconhecidos pela área de Tecnologia de Informação e Comunicação.

#### CAPÍTULO V

##### DAS DISPOSIÇÕES FINAIS

Art. 16. Havendo necessidade de cadastro de senha com requisitos maiores de segurança que aqueles estabelecidos nesta Instrução Normativa, facultar-se-á ao custo diante do sistema a aplicação dos critérios adequados e necessários à qualificação da senha.

Art. 17. No caso de perda, furto, roubo, acesso indevido ou comprometimento da senha, o usuário deverá comunicar a Coordenadoria de Atendimento e Relacionamento da Secretaria de Tecnologia da Informação e Comunicação ou a área responsável pelos serviços de Tecnologia da Informação na respectiva unidade, para fins de bloqueio imediato da conta até a disponibilização de nova senha.



Ministério Público Federal

Parágrafo único. Nos casos de dispensa ou exoneração de usuários terceirizados, fornecedores e sem vínculo direto com o Ministério Público Federal, desprovidos de conta de e-mail e que possuam conta no diretório e acesso a sistemas institucionais, caberá à Secretaria de Administração da Secretaria Geral, na Procuradoria Geral da República, e aos Gestores Cadastrais, nas demais unidades, a comunicação ao órgão de informática, o qual promoverá o cancelamento da conta do usuário.

Art. 18. Esta Instrução Normativa entrará em vigor após decorridos noventa dias de sua publicação, ressalvado o Capítulo IV, cujas disposições entrarão em vigor após decorridos cento e oitenta dias de sua publicação.

**LAURO PINTO CARDOSO NETO**

*Publicado no Caderno Administrativo do DMPF-e nº 143/2014, de 08/08/2014, p. 9.*

**M P F**  
**Ministério Público Federal**