NOME	LOTAÇÃO
DAYVID SILVA MONTEIRO	Vitória da Conquista - 15ª Promotoria de Justiça
LUCCA NASCIMENTO E NASCIMENTO	Salvador - 39ª Promotoria de Justiça de Assistência
HAECKEL RODRIGO BULCÃO DA SILVA	Salvador - 01ª Promotoria de Justiça de Família - 08º Promotor de Justiça

Salvador, 12 de janeiro de 2021.

NORMA ANGÉLICA REIS CARDOSO CAVALCANTI
Procuradora-Geral de Justiça

ATO NORMATIVO Nº 001, DE 12 DE JANEIRO DE 2021
Disciplina o gerenciamento e utilização das credenciais de acesso à rede e sistemas institucionais do Ministério Público do Estado da Bahia.

A PROCURADORA-GERAL DE JUSTIÇA DO ESTADO DA BAHIA, no uso de suas atribuições, nos termos da Lei Complementar nº 11/1996;

CONSIDERANDO o disposto no Ato Normativo 002/2015 que instituiu a Política de Segurança da Informação do Ministério Público do Estado da Bahia;

CONSIDERANDO a necessidade de estabelecer mecanismos que garantam o acesso adequado à rede e sistemas institucionais disponibilizados no âmbito do Ministério Público do Estado da Bahia;

CONSIDERANDO a importância de reduzir os riscos a que estão expostos os ativos de Tecnologia da Informação (TI) do Ministério Público do Estado da Bahia;

CONSIDERANDO a necessidade de implementar procedimento de gerenciamento e utilização de credenciais de acesso no Ministério Público do Estado da Bahia com intuito de reduzir riscos de incidentes de segurança da informação;

RESOLVE

Art. 1º Disciplinar e estabelecer os procedimentos de segurança para gerenciamento e utilização das credenciais de acesso à rede e sistemas institucionais disponibilizados aos órgãos e unidades do Ministério Público do Estado da Bahia (MPBA), em conformidade com as diretrizes de política de segurança da informação e com os interesses institucionais.

Parágrafo único. Para efeito do disposto neste Ato Normativo considera-se:

I - credencial de acesso: conta de usuário e senha utilizados para acesso à rede institucional do Ministério Público do Estado da Bahia;

II - serviços de internet: recursos computacionais disponibilizados na rede institucional do Ministério Público do Estado da Bahia, visando prover o acesso e os serviços da rede mundial de computadores e demais redes públicas externas de comunicação de dados;

III - rede institucional do Ministério Público: ambiente computacional disponibilizado, gerenciado e mantido pelo Ministério Público do Estado da Bahia, composto pelo conjunto de redes locais, softwares, sistemas de informação, áreas de armazenamento de dados, bases de dados e demais recursos de informática;

IV - rede pública externa de comunicação de dados: rede de dados externa compartilhada, que permite a conexão de seus usuários;

V - rede local: ambiente de rede interna, composto pelo conjunto dos recursos de informática, assim como meios físicos e lógicos de conexão, de modo a permitir o compartilhamento de programas, dados e arquivos;

VI - rede mundial de computadores (internet): conjunto de redes de computadores interligados, de âmbito mundial, descentralizado e de acesso público;

VII - confidencialidade: qualidade da informação que não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

VIII - criptografia: ciência de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de decriptografia específica. A criptografia de dados pode ser aplicada a um dado específico (como uma senha) ou, mais amplamente, a todos os dados de um arquivo, ou ainda a todos os dados da Instituição;

IX - ativo: tudo aquilo que tem valor para a empresa, podendo ser tangível ou intangível - instalações, computadores, informações etc;

X - ativos de TI: ativos de tecnologia da informação, tais como softwares, dispositivos de rede, computadores etc;

XI - ativos de TI críticos: ativos de tecnologia da informação que dão suporte, direta ou indiretamente, aos principais processos do MPBA, cuja indisponibilidade ou o mau funcionamento afeta os serviços desta Instituição, trazendo prejuízos com alta possibilidade de afetar a sociedade;

XII - senha com complexidade média: aquela composta por letras e números não consecutivos;

XIII - senha com complexidade alta: aquela composta por letras, números e símbolos especiais não consecutivos;

XIV - usuários: Procuradores de Justiça, Promotores de Justiça, servidores efetivos, servidores comissionados, servidores cedidos de outros órgãos, estagiários, voluntários, menores aprendizes, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações do MPBA.

Art. 2º O disposto neste Ato Normativo será aplicado ao uso, em caráter permanente ou temporário, ao acesso aos sistemas e serviços de tecnologia da informação disponibilizados através da rede institucional deste Ministério Público.

Art. 3º A administração, o acompanhamento, o controle e avaliação dos acessos aos serviços de internet, a outras redes públicas de comunicação de dados e aos sistemas providos pela rede institucional do Ministério Público serão de responsabilidade da Superintendência de Gestão Administrativa, por meio da Diretoria de Tecnologia da Informação (DTI).

Art. 4º O acesso à rede institucional e a todos os sistemas e serviços disponibilizados através dela dar-se-á mediante credencial de acesso individual do usuário – login e senha –fornecida pela DTI.

§ 1º As credenciais de acesso (login e senha) atribuídas a cada usuário, são de caráter pessoal e intransferível, serão definidas de acordo com o interesse e a disponibilidade da Administração e sua utilização será de responsabilidade exclusiva do respectivo usuário, que zelará pela sua confidencialidade.

§ 2º No primeiro acesso à rede institucional a senha temporária disponibilizada será obrigatoriamente trocada.

Art. 5º Todas as senhas terão tamanho mínimo de 8 caracteres sendo pelo menos uma letra maiúscula, uma letra minúscula, um número e um caractere especial, caracterizando a criação de senha com complexidade alta.

Art. 6º As senhas deverão ser alteradas pelos usuários a cada 360 (trezentos e sessenta) dias com o intuito de aumentar a segurança dos acessos.

Parágrafo único. Este procedimento será viabilizado pela Superintendência de Gestão Administrativa através de solução tecnológica provida pela Diretoria de Tecnologia da Informação.

Art. 7º Não será permitida a repetição das últimas 03 (três) senhas utilizadas.

Art. 8º Após 03 (três) tentativas erradas de digitação de uma senha, a conta do usuário será bloqueada.

Parágrafo único. As solicitações de desbloqueio devem ser realizadas através da Central de Serviços de TI, que seguirá um procedimento de validação de informações do usuário para efetuar o desbloqueio.

Art. 9º O sistema de gerenciamento de senhas institucionais deve, na medida do possível, possibilitar as seguintes ações:

I - permitir que o usuário selecione e modifique suas próprias senhas a qualquer momento;

II - possuir um procedimento de visualização na criação e modificação de senhas visando evitar erros de digitação;

III - obrigar a escolha de senhas com complexidade alta, atendendo os requisitos mínimos elencados no Art. 5º deste ato;

IV - obrigar a troca de senhas iniciais e temporárias no primeiro acesso;

V - manter o registro das 03 (três) últimas senhas utilizadas e 03 (três) últimas tentativas mal sucedidas, conforme especificado no Art. 5º

VI - ocultar as senhas na tela quando forem digitadas, substituindo por símbolos quando digitado cada caractere;

Art. 10. A DTI será responsável por operacionalizar a customização da complexidade das senhas a serem criadas pelo usuário, mediante as instruções definidas.

§ 1º Sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha, mediante sinalização da DTI, a senha deverá ser alterada, independente da periodicidade de sua substituição.

§ 2º Na hipótese do parágrafo anterior, a DTI deverá manter contato com o titular da senha e, caso não obtenha sucesso, efetuará a sua troca por outra temporária, evitando o risco à segurança da informação do MPBA.

Art. 11. Em caso de esquecimento, perda ou comprometimento da senha de acesso, a nova credencial temporária será gerada pela DTI e deverá ser trocada obrigatoriamente no primeiro acesso, através de solução tecnológica disponibilizada.

Art. 12. As contas e senhas padrões de fabricante de equipamentos e aplicações devem ser trocadas imediatamente após a instalação, observando as regras elencadas no Art. 5º deste Ato Normativo.

Art. 13. Os administradores de rede e/ou serviços de rede institucionais devem possuir contas e senhas individualizadas com privilégios administrativos, que deverão ser utilizadas, exclusivamente, para o desempenho de suas atividades.

Art. 14. As credenciais de acesso de administração de ativos de TI e de TI críticos, tais como root, administrador e administrator devem ser guardadas com identificação do ativo, em local adequado, seguro, com acesso apenas às pessoas autorizadas pelo responsável do recurso.

Parágrafo único. A gestão dessas credenciais deve fazer parte de um procedimento visando controlar e documentar, com justificativa, data, e todas informações necessárias para possível auditória.

Art. 15. São responsabilidades da DTI:

I - monitorar, acompanhar e fazer cumprir as determinações e disposições estabelecidas para o gerenciamento das senhas de acesso à rede;

II - comunicar à Superintendência de Gestão Administrativa e ao Comitê Estratégico de TI a constatação de qualquer ocorrência de fatos relacionados ao estabelecido neste Ato Normativo.

Art. 16. O acesso à rede institucional será fornecido apenas aos integrantes com vínculos formalizados e ativos com a Instituição, excetuando-se os acessos necessários para obtenção de informações pessoais por integrantes aposentados.

§ 1º O desligamento ou exoneração de um usuário, para que a credencial de acesso seja revogada, deverá ser comunicado formal e imediatamente à DTI:

a) pela Diretoria de Gestão de Pessoas, em caso de membro e servidores;
b) pelo Centro de Estudos e Aperfeiçoamento Funcional, em caso de estagiários e voluntários;
c) pela Diretoria de Contratos, Convênios e Licitação, em caso de terceirizados;
d) pela Assistência Militar, em caso de policiais militares;
e) pelo setor responsável, nos demais casos não especificados acima.

§ 2º Caso o usuário que esteja sendo desligado da instituição tenha conhecimento de credenciais de acesso que permanecem ativas, as senhas destas devem ser alteradas após encerramento do vínculo com a instituição.

Art. 17. Os sistemas institucionais desenvolvidos pelas equipes técnicas do MPBA ou adquiridos de fornecedores externos devem, preferencialmente, utilizar autenticação integrada com a rede institucional.

Art. 18. A DTI poderá implementar fatores adicionais de autenticação, desde que aprovado previamente pelo Comitê Estratégico de TI e divulgado amplamente através dos canais oficiais da instituição.

Art. 19. O descumprimento do disposto neste Ato Normativo sujeitará seu responsável às penalidades cabíveis, previstas no âmbito administrativo, cível e criminal.

Art. 20. Os casos omissos deverão ser dirimidos pelo Gabinete da Procuradoria Geral de Justiça, com apoio técnico da Superintendência de Gestão Administrativa.

Art. 21. Este Ato Normativo entrará em vigor na data de sua publicação, revogando-se as disposições em contrário.

Salvador, 12 de janeiro de 2021

NORMA ANGÉLICA REIS CARDOSO CAVALCANTI
Procuradora-Geral de Justiça