CONSELHO REGIONAL DE BIOLOGIA – 1ª REGIÃO (SP, MT, MS) – CRBio-01
Rua Manoel da Nóbrega nº 595, conjunto 111 - CEP 04001-083 – Paraíso, São Paulo, SP
Telefone: (11) 3884-1489 – Fax (11) 3887-0163
www.crbio01.gov.br

PORTARIA CRBio-01 Nº 409, DE 22 DE JANEIRO DE 2026

Institui a política de credenciais de acesso no âmbito do CRBio-01.

A Presidente em exercício do Conselho Regional de Biologia - 1ª Região (SP, MT, MS) - CRBio-01, autarquia federal com sede nesta capital, no uso de suas atribuições legais e regimentais conferidas pelo disposto na Lei nº 6.684/79, de 3 de setembro de 1979,

CONSIDERANDO a necessidade de assegurar a confidencialidade, a integridade e a disponibilidade das informações sob a responsabilidade do CRBio-01;

CONSIDERANDO a importância de estabelecer diretrizes formais para a autenticação e o controle de acesso aos sistemas de informação;

RESOLVE:

Art. 1º - Fica instituída, no âmbito do CRBio-01, a **Política de Credenciais de Acesso**, na forma do **Anexo Único** desta Portaria.

Art. 2º - Compete à unidade responsável pela Tecnologia da Informação assegurar a implementação, a atualização e a divulgação da Política instituída por esta Portaria.

Art. 3º - O descumprimento do disposto na Política sujeitará o infrator às sanções administrativas cabíveis, nos termos da legislação vigente.

Art. 4º - Esta Portaria entra em vigor na data de sua publicação.

São Paulo, 22 de janeiro de 2026

Neiva Maria Robaldo Guedes

Presidente em Exercício

CRBio 006476/01-D

Anexo Único

Política de Credenciais de Acesso

Versão 1.0

Versionamento

Versão	Data	Autores	Detalhes
1.0	16/12/2025	Leonardo Gil Andrade de Almeida	Versão inicial

Aprovação

Versão	Data	Nome	Cargo
1.0	18/12/2025	Cátia Cristina Soares Costa	Superintendente

Revisão

Periodicidade	Última revisão	Próxima revisão
Anual	- - -	janeiro/2027

Sumário

1. Objetivo

Esta política estabelece os requisitos obrigatórios para a criação, uso, proteção e gestão de credenciais utilizadas para acesso aos sistemas de informação institucionais. Seu objetivo é mitigar riscos de acesso não autorizado, vazamento de dados e interrupção de serviços decorrentes do uso de credenciais fracas, reutilizadas ou comprometidas.

2. Escopo

Esta política aplica-se a todos os funcionários que possuam acesso aos sistemas de informação da entidade. Abrange todos os sistemas e serviços que utilizem autenticação baseada em senha, incluindo, mas não se limitando a, estações de trabalho, servidores, dispositivos de rede, serviços em nuvem, plataformas SaaS, aplicações internas e soluções de acesso remoto.

3. Definições

· **Conta de usuário padrão:** Conta atribuída a um indivíduo para a execução de atividades rotineiras de trabalho.

· **Conta privilegiada:** Conta com permissões elevadas, incluindo acesso administrativo, de sistema ou de nível raiz.

· **Conta de serviços comuns:** Contas utilizadas por múltiplos usuários ou sistemas para acesso a serviços compartilhados, aplicações legadas, dispositivos, integrações técnicas ou processos operacionais que não suportem autenticação individualizada.

· **Autenticação multifator (MFA):** Método de autenticação que requer dois ou mais fatores independentes de verificação.

4. Princípios Gerais

As senhas devem ser tratadas como informações confidenciais e protegidas de forma adequada. A entidade adota uma abordagem baseada em risco, priorizando o comprimento, a exclusividade e a resistência à quebra de senhas em detrimento de trocas frequentes e previsíveis. Sempre que tecnicamente viável, as senhas devem ser complementadas por MFA.

5. Requisitos

5.1. Contas de usuário padrão

· Comprimento mínimo: 10 caracteres.

· Comprimento recomendado: 16 caracteres ou mais.

· As senhas podem conter letras maiúsculas, letras minúsculas, números e caracteres especiais.

· O uso de frases-senha longas, compostas por palavras não relacionadas entre si, é fortemente recomendado.

As senhas de contas padrão não devem expirar de forma periódica. A alteração será exigida apenas quando:

· Houver evidência ou suspeita razoável de comprometimento;

· O usuário divulgar sua senha a terceiros;

· A conta estiver envolvida em incidente de segurança;

· A equipe de TI solicitar formalmente a troca.

5.2. Contas privilegiadas

· Comprimento mínimo: 22 caracteres.

· As senhas podem conter letras maiúsculas, letras minúsculas, números e caracteres especiais.

· Contas privilegiadas não devem ser utilizadas para atividades rotineiras, como navegação web ou e-mail.

· O uso de contas privilegiadas compartilhadas deve ser evitado. Quando inevitável, as credenciais devem ser armazenadas em gerenciador de senhas.

· Rotação a cada 180 dias.

· Senhas de contas de contingência (*break-glass*) devem ser revisadas e rotacionadas após qualquer

utilização.

5.3. Contas de serviços comuns

· Comprimento mínimo: 16 caracteres.

· Deve ser gerada aleatoriamente ou criada por meio de gerenciador de senhas.

· Deve ser armazenada exclusivamente em um gerenciador de senhas em ambientes de operação comum, podendo ser armazenadas em texto puro somente em ambientes de acesso privilegiado.

· Rotação imediata após desligamento de usuário com acesso.

O compartilhamento de senhas é permitido apenas para contas de serviços comuns, desde que:

· A conta seja formalmente classificada com conta de serviço comum;

· A unidade responsável justifique a necessidade;

· Não exista alternativa viável de autenticação individual, federada ou baseada em certificados.

5.4. Senhas iniciais ou temporárias

Senhas iniciais ou temporárias devem ser geradas aleatoriamente e obrigatoriamente alteradas no primeiro acesso.

5.5. Conteúdo proibido

As senhas não devem:

· Conter nome do usuário, nome de login, endereço de e-mail, matrícula ou outras informações pessoais.

· Conter o nome da entidade, nomes de sistemas ou projetos internos.

· Ser baseadas em senhas comuns, previamente comprometidas, palavras isoladas de dicionário, padrões de teclado, sequências alfanuméricas ou caracteres repetidos.

· Ser reutilizadas a partir de senhas anteriores ou de serviços pessoais externos.

Sempre que suportado tecnicamente, as senhas devem ser verificadas contra listas de credenciais conhecidamente comprometidas.

6. Reutilização e Histórico de Senhas

· A reutilização de senhas é estritamente proibida.

· Quando for tecnicamente possível, os sistemas de autenticação devem manter histórico mínimo de 10 senhas anteriores.

· Cada sistema que não utilize autenticação centralizada deve possuir uma senha exclusiva.

7. Autenticação Multifator

O uso de autenticação multifator é recomendável sempre que disponível, e obrigatório para:

· Contas privilegiadas;

· Serviços em nuvem.

São considerados métodos de MFA aprovados: aplicativos autenticadores, chaves de segurança físicas e aprovações por *push*. O uso de MFA via SMS e e-mail deve ser evitado sempre que existirem alternativas.

8. Armazenamento e Manuseio de Senhas

É proibido o compartilhamento de senhas individualizadas com qualquer pessoa, inclusive com a equipe de TI. As senhas não devem ser anotadas em papel ou armazenadas em arquivos não protegidos. Recomenda-se o uso de um gerenciador de senhas, em específico do aplicativo KeePass (https://keepass.info/download.html), aprovado pela equipe de TI.

9. Gestão do Ciclo de Vida de Contas

· O provisionamento de novas contas de usuário deve ocorrer mediante autorização formal.

· A equipe de TI deve ser comunicada de desligamentos, términos de contrato ou encerramentos de vínculo para que as contas de usuário correspondentes sejam desativadas imediatamente.

· Alterações de cargo/função devem resultar em revisão dos privilégios de acesso.

10. Exceções

Exceções a esta política devem ser formalmente documentadas, conter justificativa de risco e possuir aprovação da gestão.

11. Conformidade

A adesão a esta política é obrigatória para todos os funcionários do CRBio-01. O descumprimento desta política, seja por negligência, inação ou interferência deliberada, pode resultar em restrições de acesso e aplicação de medidas disciplinares.

12. Revisão

Esta política deve ser revisada anualmente, ou antes, caso haja alterações significativas no ambiente tecnológico, regulatório ou no cenário de ameaças. Quaisquer revisões desta política devem ser formalmente aprovadas pelo gestor de TI e pela liderança executiva antes da implementação.

Documento assinado eletronicamente por **Neiva Maria Robaldo Guedes**, **Presidente em Exercício**, em 11/02/2026, às 19:06, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://cfbio.gov.br/validar-assinatura/ informando o código verificador **0107265** e o código CRC **BC6486A2**.