



CONSELHO FEDERAL DE BIOLOGIA – CFBio

PORTARIA CFBIO Nº 693, DE 10 DE JULHO DE 2026

Institui a Política de Backup e Recuperação de Dados do Conselho Federal de Biologia – CFBio.

A DIRETORIA DO CONSELHO FEDERAL DE BIOLOGIA – CFBio, no uso de suas atribuições legais e regimentais,

RESOLVE:

Art. 1º Fica instituída a Política de Backup e Recuperação de Dados do Conselho Federal de Biologia – CFBio, com a finalidade de estabelecer diretrizes, responsabilidades e controles relacionados à realização de cópias de segurança e à recuperação de dados, sistemas e serviços institucionais.

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 2º Esta Política aplica-se:

I – aos sistemas, serviços, bancos de dados, repositórios documentais e demais ativos digitais institucionais do CFBio;

II – aos servidores físicos e virtuais, locais ou em nuvem;

III – aos ambientes de produção, homologação, testes, suporte e contingência;

IV – aos usuários, empregados, colaboradores, prestadores de serviço e terceiros que utilizem, administrem ou tenham acesso a recursos de Tecnologia da Informação e Comunicação do CFBio.

Art. 3º Para os fins desta Política, considera-se:

I – Backup ou Cópia de Segurança: conjunto de procedimentos destinados à salvaguarda de dados, sistemas, arquivos, configurações e demais ativos digitais, visando possibilitar sua recuperação em caso de falha, perda, indisponibilidade ou incidente;

II – Restauração ou Recuperação: processo de recuperação de dados, sistemas, serviços ou configurações a partir de cópias de segurança;

III – Banco de Dados: conjunto estruturado de informações armazenadas eletronicamente e utilizadas pelos sistemas institucionais;

IV – Serviço Crítico: serviço, sistema ou infraestrutura cuja indisponibilidade possa causar impacto significativo às atividades institucionais do CFBio;

V – Retenção: período pelo qual as cópias de segurança deverão ser mantidas armazenadas;

VI – Snapshot: mecanismo de captura do estado de um sistema, máquina virtual ou armazenamento em determinado momento;



CONSELHO FEDERAL DE BIOLOGIA – CFBio

VII – Ambiente de Produção: ambiente computacional utilizado para execução dos serviços institucionais em operação;

VIII – Ambiente de Homologação: ambiente destinado à validação, testes ou simulações de sistemas e serviços;

IX – POR, ou Objetivo de Ponto de Recuperação: limite máximo tolerável de perda de dados, medido a partir do ponto mais recente possível de restauração;

X - RTO, ou Objetivo de Tempo de Recuperação: tempo máximo estimado para restabelecimento de determinado serviço, sistema ou dado após incidente ou indisponibilidade.

CAPÍTULO II

DAS DIRETRIZES GERAIS

Art. 4º As rotinas de backup e recuperação de dados deverão observar as diretrizes estabelecidas na Política de Segurança da Informação do CFBio, bem como os princípios da disponibilidade, integridade, confidencialidade, continuidade, autenticidade, rastreabilidade e proteção das informações institucionais.

Art. 5º O CFBio deverá manter mecanismos de backup compatíveis com a criticidade dos sistemas, serviços e dados institucionais, visando possibilitar sua recuperação em caso de falhas, incidentes de segurança, indisponibilidade, corrupção ou perda de informações.

Art. 6º Os mecanismos de backup deverão adotar medidas destinadas à mitigação de riscos relacionados à perda, exclusão indevida, alteração não autorizada, corrupção, indisponibilidade ou vazamento de dados institucionais.

Art. 7º As rotinas de backup deverão, sempre que possível:

- I – utilizar mecanismos automatizados;
- II – manter múltiplas cópias das informações;
- III – utilizar ambientes de armazenamento distintos do ambiente principal;
- IV – observar a criticidade dos serviços e bancos de dados institucionais;
- V – priorizar a recuperação dos serviços considerados críticos;
- VI – adotar controles de segurança, registro e monitoramento;
- VII – permitir a verificação da integridade das cópias realizadas.

Art. 8º Os backups e dados institucionais somente poderão ser armazenados em ambientes, serviços ou infraestruturas formalmente autorizados pelo CFBio.

Parágrafo único. É vedada a utilização de contas pessoais, serviços não autorizados, dispositivos particulares ou ambientes externos não aprovados institucionalmente para armazenamento de backups, cópias de bases de dados ou informações institucionais.

Art. 9º A realização de backup não substitui as regras de gestão documental, arquivamento, guarda, descarte e preservação de documentos institucionais, devendo ser observadas as normas aplicáveis.

CAPÍTULO III

DA CLASSIFICAÇÃO E CRITICIDADE



CONSELHO FEDERAL DE BIOLOGIA – CFBio

Art. 10. Os serviços e sistemas institucionais poderão ser classificados conforme sua criticidade operacional, observando, entre outros critérios:

- I – impacto institucional decorrente da indisponibilidade;
- II – dependência operacional;
- III – necessidade de continuidade dos serviços;
- IV – relevância das informações tratadas;
- V – existência de dados pessoais, dados sensíveis ou informações restritas;
- VI – requisitos legais, contratuais, administrativos ou regulatórios aplicáveis.

Art. 11. São considerados serviços críticos do CFBio, entre outros definidos pelo Setor de Tecnologia e Segurança da Informação:

- I – Sistema Eletrônico de Informações – SEI;
- II – bancos de dados associados ao SEI;
- III – repositório documental do SEI;
- IV – sistema Integrado de Gestão – SIG;

V – demais sistemas, bancos de dados ou serviços classificados como críticos em procedimento próprio.

Art. 12. Os ambientes de homologação, testes e suporte poderão possuir requisitos diferenciados de periodicidade, retenção e recuperação, observada sua criticidade, finalidade, disponibilidade técnica e existência de dados institucionais ou pessoais.

CAPÍTULO IV

DAS ROTINAS DE BACKUP E RETENÇÃO

Art. 13. As rotinas de backup deverão contemplar, conforme aplicável:

- I – bancos de dados institucionais;
- II – arquivos e repositórios documentais;
- III – máquinas virtuais;
- IV – configurações e serviços essenciais à continuidade operacional;

V – códigos-fonte, scripts, chaves de configuração, parâmetros e demais componentes necessários à continuidade operacional, quando aplicável;

VI – logs e registros necessários à recuperação, auditoria ou investigação de incidentes, observadas as normas internas.

Art. 14. O CFBio adotará retenção mínima de backups compatível com a criticidade dos serviços, a capacidade operacional disponível e os requisitos legais, contratuais ou administrativos aplicáveis.

§1º As cópias de segurança operacionais deverão possuir retenção mínima de 7 (sete) dias, sempre que tecnicamente viável.

§2º Deverão ser mantidas cópias de segurança mensais de longo prazo para os serviços críticos, observadas a capacidade técnica e a disponibilidade de armazenamento.



CONSELHO FEDERAL DE BIOLOGIA – CFBio

§3º Os períodos de retenção poderão ser ampliados conforme necessidade operacional, requisitos legais, exigências contratuais, criticidade do serviço ou disponibilidade técnica.

§4º A exclusão ou sobrescrita de cópias de segurança deverá observar os prazos de retenção definidos e os controles técnicos aplicáveis.

Art. 15. Os backups poderão ser realizados por meio de:

I – cópias lógicas de dados;

II – backups completos, incrementais ou diferenciais;

III – mecanismos automatizados de salvaguarda;

IV – soluções de backup locais ou em nuvem institucional autorizada;

V – outras soluções tecnicamente aprovadas pelo Setor de Tecnologia e Segurança da Informação.

Art. 16. Sempre que houver atualização significativa, migração, manutenção crítica, alteração estrutural, implantação de nova funcionalidade ou modificação relevante em sistemas, bancos de dados ou servidores, deverá ser avaliada a necessidade de realização de backup prévio do ambiente afetado.

CAPÍTULO V

DA SEGURANÇA DAS CÓPIAS DE BACKUP

Art. 17. As cópias de segurança deverão ser protegidas contra acesso não autorizado, alteração indevida, exclusão acidental ou maliciosa, corrupção, perda, vazamento ou indisponibilidade.

Art. 18. Sempre que tecnicamente possível, os ambientes e soluções de backup deverão utilizar:

I – controle de acesso restrito;

II – autenticação adequada aos perfis de acesso;

III – criptografia em trânsito e/ou em repouso;

IV – segregação de permissões;

V – registro de acessos e operações realizadas;

VI – mecanismos de proteção contra exclusão indevida ou sobrescrita não autorizada;

VII – armazenamento em local ou ambiente distinto do ambiente principal.

Art. 19. O acesso às cópias de backup deverá ser concedido somente a usuários autorizados e estritamente necessários para execução de atividades de administração, segurança, auditoria, suporte ou restauração.

Art. 20. Quando as cópias de segurança contiverem dados pessoais, deverão ser observados os princípios e requisitos da Lei Geral de Proteção de Dados Pessoais – LGPD, especialmente quanto à segurança, prevenção, necessidade, responsabilização e prestação de contas.

CAPÍTULO VI

DO MONITORAMENTO E DOS TESTES DE RESTAURAÇÃO

Art. 21. As rotinas de backup deverão ser monitoradas periodicamente, incluindo verificação semanal de logs, execuções, alertas, falhas e demais evidências disponíveis.



CONSELHO FEDERAL DE BIOLOGIA – CFBio

§1º A verificação das rotinas de backup deverá ocorrer, no mínimo, semanalmente, sem prejuízo de monitoramento em menor intervalo para serviços críticos.

§2º As falhas verificadas deverão ser analisadas e tratadas pelo Setor de Tecnologia e Segurança da Informação, observada a criticidade do serviço afetado.

Art. 22. Deverão ser realizados testes periódicos de restauração de backups, com o objetivo de:

I – validar a integridade das cópias de segurança;

II – verificar a efetividade dos procedimentos de recuperação;

III – avaliar o tempo necessário para restauração;

IV – reduzir riscos relacionados à indisponibilidade de dados e serviços;

V – identificar falhas, inconsistências ou necessidades de melhoria nos procedimentos adotados.

§1º A periodicidade, o escopo e os critérios dos testes de restauração poderão ser definidos em procedimentos operacionais complementares.

§2º Os testes deverão observar, sempre que possível, ambientes distintos dos ambientes de produção.

§3º Os testes de restauração deverão ser registrados, contendo, quando aplicável, data, responsável, ambiente, sistema ou base testada, resultado, falhas identificadas e providências adotadas.

Art. 23. As atividades relacionadas à execução, monitoramento, falhas, restauração e testes de backup deverão possuir registros e evidências compatíveis com os procedimentos internos estabelecidos pelo CFBio.

CAPÍTULO VII

DA RESTAURAÇÃO DE DADOS

Art. 24. A restauração de dados deverá observar a criticidade do serviço afetado, a continuidade operacional, a integridade das informações institucionais e os impactos da operação sobre o ambiente de destino.

Art. 25. A restauração de dados que envolva substituição de informações em ambiente de produção, acesso a informações sensíveis ou tratamento de dados pessoais dependerá de autorização formal da área responsável.

§1º A solicitação de restauração deverá indicar, sempre que possível, o sistema ou dado afetado, a justificativa, a data ou versão desejada, o ambiente de destino e o responsável pela validação das informações restauradas.

§2º Em situações de incidente, indisponibilidade, risco à continuidade dos serviços ou necessidade emergencial, o Setor de Tecnologia e Segurança da Informação poderá adotar medidas imediatas de recuperação operacional, devendo registrar posteriormente as ações executadas e comunicar as áreas competentes.

Art. 26. Após a recuperação, sempre que aplicável, a área responsável pelo sistema ou informação deverá validar a consistência dos dados recuperados.

CAPÍTULO VIII



CONSELHO FEDERAL DE BIOLOGIA – CFBio

DAS RESPONSABILIDADES

Art. 27. Compete ao Setor de Tecnologia e Segurança da Informação:

I – implementar e manter as rotinas de backup e recuperação;

II – definir estratégias técnicas compatíveis com os serviços institucionais;

III – monitorar a execução dos backups;

IV – analisar e tratar falhas identificadas nas rotinas de backup;

V – realizar verificações de conformidade dos serviços contratados relacionados a backup;

VI – promover testes periódicos de restauração;

VII – manter registros relacionados às atividades de backup e recuperação;

VIII – revisar periodicamente as estratégias e mecanismos de backup adotados;

IX – propor normas complementares, procedimentos operacionais e melhorias técnicas relacionadas à proteção e recuperação de dados.

Art. 28. Compete aos gestores e responsáveis pelos sistemas institucionais:

I – informar ao Setor de Tecnologia e Segurança da Informação sobre sistemas, dados ou serviços considerados críticos;

II – indicar requisitos específicos de continuidade, recuperação ou retenção, quando existentes;

III – validar, quando necessário, os dados restaurados;

IV – comunicar alterações relevantes que possam impactar as rotinas de backup e recuperação.

Art. 29. Compete aos usuários:

I – armazenar informações institucionais apenas em ambientes autorizados pelo CFBio;

II – evitar manter documentos institucionais relevantes exclusivamente em equipamentos locais, dispositivos removíveis ou contas pessoais;

III – comunicar incidentes, falhas, perdas, exclusões acidentais ou inconsistências identificadas;

IV – observar as diretrizes estabelecidas nesta Política e na Política de Segurança da Informação do CFBio.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS

Art. 30. Normas complementares e procedimentos operacionais poderão ser elaborados pelo Setor de Tecnologia e Segurança da Informação para detalhamento técnico das rotinas de backup e recuperação, incluindo periodicidade, retenção, RPO, RTO, prioridades de restauração e responsabilidades operacionais.

Art. 31. O descumprimento desta Política poderá sujeitar o infrator às sanções administrativas, civis e penais cabíveis, nos termos da legislação vigente, dos instrumentos contratuais aplicáveis e da Política de Segurança da Informação do CFBio.



CONSELHO FEDERAL DE BIOLOGIA – CFBio

Art. 32. Esta Política deverá ser revisada bienalmente ou sempre que houver mudanças relevantes no ambiente tecnológico, operacional, contratual ou normativo do CFBio.

Art. 33. Os casos omissos serão resolvidos pela Diretoria do CFBio, com apoio do Setor de Tecnologia e Segurança da Informação.

Art. 34. Esta Portaria entra em vigor na data de sua publicação.

Brasília/DF, 10 de julho de 2026.


Bióloga Alcione Ribeiro de Azevedo
Presidente do CFBio
CRBio 016349/06-D


Biólogo Santiago Valentim de Souza
Conselheiro Tesoureiro do CFBio
CRBio 042048/02-D


Biólogo José Roberto Feitosa Silva
Vice-Presidente do CFBio
CRBio 004995/05-D


Bióloga Andréa Graciano dos Santos Figueiredo
Conselheira Secretária do CFBio
CRBio 025228/07-D