UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

Reitoria
Gabinete da Reitoria
Chefia de Gabinete do Reitor
Secretaria Administrativa

PORTARIA UFRJ Nº 1448, DE 16 DE OUTUBRO DE 2026

Institui a Política de Cópias de Segurança (backup) e de Restauração de Dados e Informações (restore) no âmbito da Universidade Federal do Rio de Janeiro.

O REITOR DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO, ad referendum do Comitê de Governança Digital (CGD), nomeado pelo Decreto de 27 de junho de 2023, publicado no Diário Oficial da União nº 121, de 28 de junho de 2023, na qualidade de Presidente do Comitê no uso de suas atribuições legais, estatutárias e regimentais, com fulcro na Lei nº 13.709/2018, que versa sobre a Lei Geral de Proteção de Dados Pessoais; no Decreto nº 12.572, de 04 de agosto de 2025, que instituiu a Política Nacional de Segurança da Informação e dispõe sobre a governança da informação no âmbito da administração pública federal; a Portaria SGD/MGI Nº 9.511, de 28 de outubro de 2025, que dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI; nas recomendações constantes no Relatório de Avaliação da Auditoria Interna - exercício 2024; e, através do processo nº 23079.254468/2024-90, resolve:

CAPÍTULO I

DOS CONCEITOS E DEFINIÇÕES

Art. 1º Instituir a Política de cópias de segurança (backup) e de restauração de dados e informações (restore) no âmbito da Universidade Federal do Rio de Janeiro (UFRJ).

§ 1º Entende-se por cópia de segurança, ou backup, a cópia dos dados e informações armazenados nos equipamentos e servidores utilizados para prover os serviços tecnológicos de informação e comunicação oferecidos pela UFRJ.

§ 2º Entende-se por restauração de dados, ou restore, a recuperação dos dados ou informações armazenados em cópia de segurança para os equipamentos e servidores utilizados para prover os serviços tecnológicos de informação e comunicação oferecidos pela UFRJ.

Art. 2º Para os fins desta Portaria, considera-se:

I – Administrador do backup: unidade responsável pelos serviços de backup, pelo planejamento de soluções de backup, pelos procedimentos de configuração, execução, monitoramento e testes de backup, pela definição de padrões, pelas configurações e pelo atendimento avançado na resolução de incidentes e problemas relacionados à cópia e restauração de dados. A Divisão de Serviços de TIC (DSETIC/SG-TIC) é a responsável por estas atividades na UFRJ;

II – Administrador do recurso: unidade responsável pela operação dos equipamentos e servidores utilizados para prover os serviços tecnológicos de informação e comunicação oferecidos pela UFRJ;

III – Tempo de retenção: tempo que os dados e informações permanecerão disponíveis em cópia de

segurança para eventual restauração;

IV – Backup completo: modalidade de cópia de segurança em que todos os dados e informações a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde a última cópia de segurança realizada;

V – Backup incremental: modalidade de cópia de segurança em que são salvaguardados apenas os dados e informações novos ou modificados desde a última cópia de segurança realizada de forma completa ou incremental;

VI – Backup diferencial: modalidade de cópia de segurança em que são salvaguardados apenas dados e informações novos ou modificados desde a última cópia de segurança completa realizada;

VII – Backup baseado em snapshot: modalidade de cópia de segurança em que os dados e informações são salvaguardados exatamente como estavam em um momento específico. Este tipo de cópia de segurança permite restaurar tudo rapidamente, como se fosse uma "foto" do sistema. Usa técnicas para economizar espaço, evitando o armazenamento de dados duplicados.

VIII – Ferramenta de backup: É um software ou sistema desenvolvido para realizar cópias de segurança de dados, com o objetivo de garantir que dados e informações importantes possam ser recuperados em caso de perda, falha, exclusão acidental, ataque cibernético ou desastre;

IX – Periodicidade de backup: frequência em que ocorrerá a cópia de segurança;

X – Mídia: meio físico no qual efetivamente se armazenam os dados de uma cópia de segurança;

XI – Criticidade: grau de importância dos dados e informações para a continuidade das atividades e serviços da organização;

XII – Descarte: eliminação correta de dados e informações, documentos, unidades de armazenamento e acervos digitais;

XIII – Disponibilidade: garantia de que o dado ou informação esteja acessível e utilizável sob demanda de pessoa física ou determinado serviço de TIC da SG-TIC ou unidade devidamente autorizada;

XIV – Janela de backup: período durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

XV – Gestor da Informação: agente público formalmente responsável pelos dados e informações produzidos no processo de trabalho que está sob sua gestão técnica (unidade organizacional que demanda sistemas, banco de dados etc.);

XVI – Gestor de TIC: agente público formalmente responsável pela administração dos serviços de TIC. Na UFRJ são os servidores lotados na SG-TIC;

XVII – Unidade de armazenamento de backup: unidade de armazenamento com características específicas para retenção de cópia de segurança de dados e informações digitais;

XVIII – Objetivo do Tempo de Recuperação (RTO - Recovery Time Objective) : indicador utilizado para medir o tempo máximo em que um sistema, um dado ou uma informação pode ficar indisponível após uma falha;

XIX – Ponto Objetivo de Recuperação (RPO - Recovery Point Objective): indicador utilizado para apurar a quantidade de recursos mínimos a serem recuperados em caso de falhas ou perda de dados;

XX– Backup off-site: representa uma cópia de segurança dos dados e informações guardada em um local físico diferente do local principal, como, por exemplo, em outro Data Center;

XXI – Backup em nuvem: representa uma cópia de segurança dos dados e informações armazenada na internet, em servidores de empresas especializadas, ficando acessível de qualquer lugar com acesso à internet.

CAPÍTULO II

ESCOPO E ABRANGÊNCIA

Art. 3º Esta Política de Cópias de Segurança define diretrizes, responsabilidades e competências que visam à segurança, à proteção e à disponibilidade dos dados e informações digitais custodiados pelos administradores de backup e de recursos, com o objetivo de manter a continuidade institucional da UFRJ.

Art. 4º Todos os serviços tecnológicos de informação e comunicação oferecidos pela UFRJ deverão ser incluídos no processo de cópias de segurança, conforme definido no Plano de Continuidade.

§ 1º A Política de Cópias de Segurança abrange todos os dados e informações contidos nos Servidores de Arquivos, de Aplicações, de Banco de Dados, de Comunicação (e mail/mensagens) e nos demais Sistemas da Administração Central da UFRJ.

§ 2º Informações armazenadas localmente nas estações de trabalho não farão parte do escopo das cópias de segurança.

Art. 5º Na ausência de Plano de Continuidade, os serviços que estão inclusos no processo de cópias de segurança serão definidos pelo Comitê de Governança Digital da Universidade Federal do Rio de Janeiro (CGD-UFRJ)

Art. 6º A requisição de cópia de segurança de dados e informações pode ser solicitada pelo Gestor da Informação ou por responsáveis técnicos dos serviços sob gestão da SG-TIC.

§ 1º A solicitação deve refletir os requisitos operacionais da DSETIC/SG-TIC, considerar os aspectos de segurança da informação envolvidos, levar em conta a criticidade dos dados para a continuidade das operações e especificar claramente o escopo, incluindo os dados e as informações digitais a serem salvaguardados.

§ 2º A requisição de que trata o caput deste artigo deverá ser formalizada no sistema de gerenciamento de chamados utilizado pela SG-TIC e direcionada ao Administrador de Backup.

Art. 7º O Administrador de Backup deve manter o registro das requisições de cópias de segurança de dados e informações, bem como das solicitações de restauração e dos testes de restauração, além de emitir pareceres técnicos.

CAPÍTULO III

DISPOSIÇÕES PRELIMINARES

Art. 8º Os gestores da informação e de TIC deverão ter ciência do tempo de retenção estabelecido para cada tipo de dado e de informação, e o Administrador de Backup deverá zelar pelo cumprimento das diretrizes estabelecidas nesta Portaria.

Art. 9º O serviço de cópia de segurança deve ser orientado para possibilitar a restauração dos dados e informações no menor tempo possível, principalmente em caso de indisponibilidade de serviços que dependam da operação de restauração dos dados e informações.

Art. 10. Todas as falhas nos procedimentos de cópia de segurança deverão ser tratadas pelo Administrador de Backup e notificadas ao Administrador do Recurso.

Art. 11. As rotinas de cópia de segurança devem possuir requisitos mínimos diferenciados, de acordo com o tipo de serviço de TIC ou de dados e informações salvaguardados, com prioridade para os serviços de TIC classificados como críticos.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 12. A administração dos serviços de cópia de segurança deve atender aos requisitos de segurança definidos pela Divisão de Segurança da Informação - DIVSEG/SG-TIC/UFRJ.

Parágrafo único. Caberá à Divisão de Segurança da Informação (DIVSEG/SG-TIC/UFRJ):

I – definir os requisitos de segurança para o armazenamento dos dados e informações digitais;

II – efetuar auditorias periódicas sobre as contas administrativas do ambiente de armazenamento dos dados e informações digitais;

III – definir critérios de segurança para processos de geração da cópia de segurança dos bancos de dados; e

IV – definir requisitos de segurança para recuperação de dados e informações pontuais.

Art. 13. A administração dos serviços de cópia de segurança é atribuição da Divisão de Serviços de TIC - DSETIC da SG-TIC/UFRJ. Parágrafo único. Caberá à Divisão de Serviços de TIC (DSETIC/SG-TIC/UFRJ):

I – definir o tempo de retenção de dados e informações, a configuração das janelas e a periodicidade das cópias de segurança de acordo com critérios técnicos, administrativos e de disponibilidade;

II – acompanhar a execução das cópias de segurança por meio das Ferramentas de Backup disponíveis para esse objetivo;

III – configurar as soluções de cópia de segurança e o tipo (completo, incremental, diferencial ou baseado em snapshot);

IV – definir, manter e atualizar as informações de RTO e RPO para fins de documentação e melhorias;

V – manter as unidades de armazenamento das cópias de segurança reservadas, funcionais e seguras; e

VI – realizar periodicamente testes de restauração para avaliar os processos de cópia de segurança e identificar oportunidades de melhoria.

Art. 14. São atribuições dos Gestores da Informação junto ao gestor de TIC:

I – solicitar, formalmente, a salvaguarda dos dados e informações geridas e dar anuência à solicitação feita pela área técnica para recuperação de dados;

II – validar, negocialmente, o resultado das restaurações de dados e informações eventualmente solicitadas;

III – validar, negocialmente, o resultado dos testes de restauração de dados e informações.

CAPÍTULO V

FREQUÊNCIA E RETENÇÃO DOS DADOS E INFORMAÇÕES

Art. 15. As cópias de segurança dos serviços de TIC da UFRJ devem ser realizadas utilizando se, de forma inicial e sem prejuízo da realização de um backup completo, os seguintes parâmetros de criticidade e frequências:

I – Os dados e informações classificados como críticos serão submetidos a backup incremental ou diferencial três vezes ao dia, ou mais, conforme critérios técnicos e a disponibilidade de recursos definidos pelo Administrador de Backup.

II – Os dados e informações classificados como não críticos serão submetidos a backup diferencial uma vez ao dia ou mais, conforme critérios técnicos e a disponibilidade de recursos definidos pelo Administrador de Backup, ou, de forma pontual, quando necessário.

Parágrafo único. O procedimento de cópia de segurança deve ser realizado preferencialmente fora do horário de expediente, sem interromper o serviço a partir do qual os dados e informações são copiados.

Art. 16. Os serviços de TIC da UFRJ devem ser resguardados observando a correlação frequência/retenção de dados e informações estabelecida a seguir:

I – tempo de retenção padrão ou configurado na Ferramenta de Backup;

II – disponibilidade de unidades de armazenamento; e,

III – o que define a legislação vigente.

CAPÍTULO VI

DOS PROCEDIMENTOS DE RESTAURAÇÃO DE DADOS E INFORMAÇÕES

Art. 17. Deverá ser registrado atendimento pelo sistema de gerenciamento de chamados da SG TIC toda vez que houver necessidade de recuperação de dados e informações.

Art. 18. Deverá ser gerado relatório contendo informações sobre a restauração de dados e informações efetuada.

Art. 19. O Administrador de Backup deverá gerar um relatório contendo um histórico de eventos pertinentes à restauração de dados e informações, bem como as ações corretivas relativas às restaurações que apresentarem falhas.

Parágrafo único. Em caso de perdas anteriores à conclusão da cópia de segurança, bem como de perdas de dados e informações criados ou modificados entre execuções subsequentes de cópias de segurança, a recuperação de tais dados e informações não será viabilizada, e tais dados e informações não serão protegidos por soluções de backup.

CAPITULO VII

DOS TESTES DE RESTAURAÇÃO DE DADOS

Art. 20. As cópias de segurança devem ser testadas periodicamente, a fim de garantir a confiabilidade e a integridade dos dados e informações salvaguardados.

Art. 21. Os testes de restauração de dados e informações das cópias de segurança devem ser realizados por amostragem, em equipamentos/servidores distintos dos que atendem aos ambientes de produção.

Art. 22. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de restauração de dados e informações serão definidos em processo específico, a ser elaborado pela Divisão de Serviços de TIC (DSETIC/SG-TIC/UFRJ), em conjunto com os Gestores da Informação e a Divisão de Segurança da Informação (DIVSEG/SG-TIC/UFRJ), apreciado pelo Comitê Gestor da SG-TIC (COGTIC) e publicado por meio de portaria ou instrução normativa da SG-TIC após apreciação pelo CGD/UFRJ.

Parágrafo único. A execução dos testes de restauração de dados e informações deve obedecer ao mesmo modo de operação dos procedimentos de restauração.

CAPÍTULO VIII

DAS MÍDIAS E LOCAIS DE ARMAZENAMENTO DAS CÓPIAS DE SEGURANÇA

Art. 23. As cópias de segurança devem ser armazenadas localmente em:

I – disco rígido;

II – unidade de estado sólido (SSD);

III – fitas magnéticas;

Parágrafo único. A localização das cópias de segurança em ambiente externo à UFRJ pode ocorrer, opcionalmente, por meio de backup off-site ou na nuvem.

Art. 24. Os dados e informações devem ser periodicamente copiados para uma unidade de armazenamento distinta daquela em que se encontram, de modo que possam ser recuperados em caso de corrupção, indisponibilidade ou perda dos dados e informações de produção.

Art. 25. De acordo com a criticidade, as cópias de segurança armazenadas localmente em disco rígido ou em unidade de estado sólido podem ser copiadas para fitas magnéticas apropriadas para esse fim, para backup off-site e/ou na nuvem.

Art. 26. O descarte das mídias de cópia de segurança inservíveis ou inutilizáveis deverá ser realizado mediante proposta apresentada pelo Administrador de Backup, dirigida ao Arquivo Central/SIARQ, conforme a política de descarte vigente.

Parágrafo único. As mídias a serem descartadas deverão ser destruídas, de modo a impedir sua reutilização ou o acesso indevido a informações por pessoas não autorizadas.

Art. 27. As unidades de armazenamento das cópias de segurança devem ser acondicionadas em

locais apropriados, com controle de fatores ambientais sensíveis como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo Administrador de Backup.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS

Art. 28. O Comitê Gestor da SG-TIG (COGTIC) deverá revisar anualmente esta Política de Cópia de Segurança e Recuperação de Dados e, em caso de alteração, encaminhar a atualização ao CGD.

§ 1º Propostas de alteração desta Política devem ser encaminhadas à SG-TIG, pelo e mail superintendencia@tic.ufrj.br.

§ 2º Os casos omissos serão tratados pela SG-TIC e encaminhados ao CGD/UFRJ.

Art. 29. A Superintendência Geral de TIC, ouvido o COGTIC, deverá emitir normativos para disciplinar e orientar a execução desta Política de Cópia de Segurança e Recuperação de Dados.

Art. 30. Fica revogada a Portaria UFRJ nº 1194, de 27 de agosto de 2025, publicada no Boletim de Serviço Eletrônico UFRJ em 27 de agosto de 2025.

Art. 31. Esta Portaria entra em vigor na data de sua publicação, considerando a urgência para a produção de seus efeitos.

ROBERTO DE ANDRADE MEDRONHO

Reitor

Documento assinado eletronicamente por **Roberto de Andrade Medronho**, **Reitor(a)**, em 16/10/2026, às 11:02, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufrj.br/autentica, informando o código verificador **7131638** e o código CRC **4802429C**.

Rua Antônio de Barros Castro, 119 - - Bairro Cidade Universitária

Rio de Janeiro - RJ - CEP 21941-853 - Telefone: (21) 3733-1985 - http://www.ufrj.br