ALEXANDRE GUEDES TORRES, matrícula SIAPE nº 152****, ocupante do cargo de Professor do Magistério Superior, lotado(a) no(a) Instituto de Química, no período de 03/10/2025 a 19/10/2025, para realização de cooperação científica, participação em reuniões e conferências científicas junto à Monash University, em Melbourne, Austrália – com ônus limitado. (Processo 23079.240141/2025-11)

DESPACHO

26 de agosto de 2025

O Reitor da Universidade Federal do Rio de Janeiro, no uso da competência que lhe foi subdelegada pela Portaria nº 404/MEC de 23 de abril de 2009, resolve autorizar o afastamento do país do(s) seguinte(s)servidor(es):

LUIS EDUARDO MENEZES QUINTAS, matrícula SIAPE nº 136****, ocupante do cargo de Professor do Magistério Superior, lotado(a) no(a) ICB, no período de 12/09/2025 a 21/09/2025, para participação na 17th International Meeting on P-Type ATPases in Health & Disease, junto à International Union of Pure and Applied Biophysics, em Queensland, Austrália – com ônus limitado. (Processo 23079.236833/2025-65)

DESPACHO

26 de agosto de 2025

O Reitor da Universidade Federal do Rio de Janeiro, no uso da competência que lhe foi subdelegada pela Portaria nº 404/MEC de 23 de abril de 2009, resolve autorizar o afastamento do país do(s) seguinte(s)servidor(es):

VANESSA ESTATO DE FREITAS ALMEIDA, matrícula SIAPE nº 348****, ocupante do cargo de Professor do Magistério Superior, lotado(a) no(a) ICB, no período de 13/09/2025 a 21/09/2025, para realização de visita a laboratório, junto à Ludwig Maximilians University, e participação no 5th Day of Intravital Microscopy, junto à German BioImaging, respectivamente em Munique e Tübingen, Alemanha – com ônus limitado. (Processo 23079.242376/2025-48)

DESPACHO

26 de agosto de 2025

O Reitor da Universidade Federal do Rio de Janeiro, no uso da competência que lhe foi subdelegada pela Portaria nº 404/MEC de 23 de abril de 2009, resolve autorizar o afastamento do país do(s) seguinte(s)servidor(es):

LUCIANA FERREIRA ROMAO, matrícula SIAPE nº 173****, ocupante do cargo de Professor do Magistério Superior, lotado(a) no(a) ICB, no período de 20/09/2025 a 10/10/2025, para realização de missão de colaboração científica junto à Université Paris Cité, em Paris, França – com ônus limitado. (Processo 23079.243925/2025-00)

EXTRATO

Nº Processo: 23079.259265/2024-90

Instrumento Jurídico: 1º TERMO ADITIVO AO CONTRATO DE PRESTAÇÃO DE SERVIÇO

Contratante: SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL - CENTRO DE TECNOLOGIA DA INDÚSTRIA QUÍMICA E TÊXTIL - SENAI CETIQT, CNPJ: 03.851.105/0001-42.

Contratada: UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (UFRJ), CNPJ 33.663.683/0001-16.

Interveniente: FUNDAÇÃO COORDENAÇÃO DE PROJETOS, PESQUISAS E ESTUDOS TECNOLÓGICOS (COPPETEC), CNPJ: 72.060.999/0001-75.

Objeto: O presente Termo Aditivo tem por objeto formalizar a cessão da posição contratual do INSTITUTO SENAI DE INOVAÇÃO EM BIOSSINTÉTICOS E FIBRAS (“ISI B&F”) do SENAI CETIQT para o SENAI/DR-RJ, preservando o objeto do contrato, consistente na prestação de serviços técnicos para a realização dos serviços de consultoria processo de produção de nanofibras por eletrofiação, cuja execução será continuada pela CONTRATADA nos mesmos termos e condições originariamente avençados.

Data de Assinatura: 11/07/2025.

Fundamento Legal: Lei 10.973/2004, Art. 8º.

EXTRATO

Processo nº 23079.239538/2025-61

Espécie: Convênio Específico n° 45/2025

Objeto: Assinatura do Convênio - Projeto intitulado "I Simpósio de Sustentabilidade e Educação Regenerativa da UFRJ (SER/UFRJ)"

Valor: R$ 31.883,50 (trinta e um mil oitocentos e oitenta e três reais e cinquenta centavos)

Vigência: 26/08/2025 a 26/09/2025

Data de assinatura: 26 de agosto de 2025

Assinaram o Convênio: pela Fundação Coordenação de Projetos, Pesquisas e Estudos Tecnológicos-COPPETEC, o Diretor Superintendente Antonio MacDowell de Figueiredo e o Diretor Executivo Glaydston Mattos Ribeiro, e pela Universidade Federal do Rio de Janeiro - UFRJ, o Reitor Roberto de Andrade Medronho

PORTARIA UFRJ Nº 1194, DE 27 DE AGOSTO DE 2025

Institui a Política de Cópia de Segurança (backup) e Restauração de Dados (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, estatutária e regimental, 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 852, de 28 de março de 2023, 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 backup e restore no âmbito da Universidade Federal do Rio de Janeiro (UFRJ).

§ 1º Entende-se por cópia de segurança ou backup a cópia das informações armazenadas nos equipamentos e servidores utilizados para prover os serviços tecnológicos oferecidos pela UFRJ.

§ 2º Entende-se por restauração ou restore a recuperação da informação copiada.

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, procedimentos de configuração, execução, monitoramento, testes de backup, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas, na UFRJ é a Divisão de Serviços de TIC (DSETIC/SG-TIC);

II – Administrador do recurso: unidade responsável pela operação dos serviços ou equipamentos;

III – Tempo de retenção: tempo que permanecerá disponível o backup das informações para eventual restauração;

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

V – Backup incremental: modalidade de backup em que são salvaguardados apenas os dados novos ou modificados desde o último backup completo ou incremental efetuado;

VI – Backup diferencial: modalidade de backup em que são salvaguardados apenas dados novos ou modificados desde o último backup completo efetuado;

VII – Backup baseado em snapshot: modalidade de backup em que são salvaguardados os dados exatamente como estavam em um momento específico. Ele permite restaurar tudo rapidamente, como se fosse uma "foto" do sistema. Usa técnicas para economizar espaço, evitando guardar dados repetidos.

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

IX – Periodicidade de backup: frequência em que ocorrerá o backup;

X – Mídia: meio físico ou virtual no qual efetivamente armazenam-se os dados de um backup;

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

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

XIII – Disponibilidade: garantia de que o dado 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 pelas informações produzidas 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 ad ministração de 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 digitais;

XVIII – RTO (Recovery Time Objective): Objetivo do Tempo de Recuperação: indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após uma falha; e

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

XX – Data Center: Ambiente físico destinado à instalação e operação de servidores, ativos de rede e sistemas de TIC críticos;

XXI – Acesso autorizado: Entrada previamente permitida a pessoa identificada e acompanhada ou credenciada, conforme critérios deste procedimento;

XXII – Responsável técnico do Data Center: Servidor da DSETIC/SG-TIC com autoridade para autorizar acessos ao Data Center;

XXIII – Backup off-site: representa uma cópia dos dados guardada em um local físico diferente do local principal, como em outro data center;

XXIV – Backup em nuvem: é quando os dados são copiados e armazenados pela internet em servidores de empresas especializadas, ficando acessível de qualquer lugar com internet.

XXV – Gestor da Unidade Organizacional: dirigente máximo da unidade;

XXVI – Usuários: pessoas que utilizam os recursos de Tecnologia da Informação e Comunicação da UFRJ e que se classificam em:

a) internos: servidores, docentes e TAEs, e estudantes da UFRJ;

b) externos: os que não possuem SIAPE ou DRE e que, pela natureza de suas atividades, necessitam de cadastro prévio para uso dos recursos tecnológicos; e,

c) visitantes: os que não se enquadram na classificação prevista nas alíneas anteriores e que necessitam de acesso eventual aos recursos tecnológicos.

CAPÍTULO II
ESCOPO E ABRANGÊNCIA

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

Art. 4º Todos os serviços críticos da UFRJ deverão ser incluídos no processo de backup, conforme definido no Plano de Continuidade.

§ 1º A Política de Backup engloba como escopo todas as informações contidas em Servidores de Arquivos, de Aplicações, de Banco de Dados, de Comunicação (e-mail/mensagens) e demais Sistemas.

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

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

Art. 6º A requisição de backup de dados 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 deve especificar claramente o escopo, incluindo os dados digitais a serem salvaguardados.

§2º A requisição que trata o caput deste artigo deverá ser formalizada pelo sistema de gerenciamento de chamados utilizado pela SG-TIC e direcionada para o Administrador do Backup.

Art. 7º O Administrador de Backup deve manter o registro das requisições de backup de dados, 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 informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas nesta Portaria.

Art. 9º O serviço de backup deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de restore.

Art. 10. Todas as falhas nos procedimentos de backups deverão ser tratadas pelo administrador do backup e, em caso de falha, o administrador desse recurso deverá ser notificado.

Art. 11. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TIC ou dado salvaguardado, com prioridade para os serviços de TIC classificados como críticos.

CAPÍTULO IV
DAS RESPONSABILIDADES

Art. 12. A administração dos serviços de backup deve seguir os 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 digitais;

II – efetuar auditorias periódicas sobre as contas administrativas do ambiente de armazenamento dos dados 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 pontuais.

Art. 13. A administração dos serviços de backup 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, a configuração das janelas de backup e a periodicidade dos backups de acordo com critérios técnicos, administrativos e de disponibilidade;

II – acompanhar a execução dos backups por meio das ferramentas de monitoramento disponíveis para esse objetivo;

III – configurar as soluções de backup e o tipo (backup completo, incremental, diferencial e snapshot);

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

V – manter as unidades de armazenamento de backups preservadas, funcionais e seguras; e

VI – realizar periodicamente testes de restauração para averiguar os processos de backup e estabelecer melhorias.

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

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

II – validar, negocialmente, o resultado das restaurações eventualmente solicitadas;

III – validar, negocialmente, o resultado dos testes de restauração dos backups.

CAPÍTULO V
FREQUÊNCIA E RETENÇÃO DOS DADOS

Art. 15. Os backups dos serviços de TIC da UFRJ devem ser realizados utilizando-se os seguintes parâmetros de criticidade e frequências:

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

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

Parágrafo único. O procedimento de backup deve ser realizado preferencialmente fora do horário de expediente, não devendo interromper o serviço do qual esteja sendo extraído.

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

I – tempo de retenção padrão ou customizado da ferramenta de backup;

II – disponibilidade de armazenamento; e,

III – o que definir a legislação vigente.

CAPÍTULO VI
DOS PROCEDIMENTOS DE RESTAURAÇÃO

Art. 17. Havendo necessidade de recuperação de dados, deverá ser registrado atendimento pelo sistema de gerenciamento de chamados da SG-TIC.

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

Art. 19. Para as restaurações que apresentarem falhas, o administrador de backup deverá gerar um relatório contendo as informações pertinentes à restauração e as ações corretivas.

Parágrafo único. Em caso de perdas anteriores à conclusão da cópia de

segurança, assim como, perda de dados criados ou modificados entre execuções de cópias de segurança subsequentes, a recuperação de dados não será viabilizada e não serão protegidos por soluções de backup.

CAPÍTULO VII
DOS TESTES DE RESTAURAÇÃO

Art. 20. Os backups devem ser testados periodicamente, com o objetivo de garantir a confiabilidade e a integridade dos dados salvaguardados.

Art. 21. Os testes de restauração dos backups devem ser realizados por amostragem, em equipamentos/servidores diferentes dos equipamentos que atendem aos ambientes de produção.

Art. 22. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de backup 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 através de portaria ou instrução normativa da SG-TIC.

Parágrafo único. A execução dos testes de restauração dos backups deve obedecer o mesmo modo de operação dos procedimentos de restauração.

CAPÍTULO VIII
DAS MÍDIAS DE BACKUP

Art. 23. Os backups podem ser armazenados em:

I – disco rígido;

II – fitas magnéticas;

III – backup off-site; e,

IV – nuvem.

Art. 24. Os dados devem ser periodicamente copiados para um dispositivo de disco distinto daquele em que se encontram, de tal forma que possam ser recuperados e restaurados em caso de corrompimento, de indisponibilidade ou de perda dos dados de produção.

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

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

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

Art. 27. As unidades de armazenamento dos backups 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
POLÍTICA DE ACESSO AO DATA CENTER

Art. 28. O(A) Diretor(a) da Divisão de Serviços de TIC - DSETIC/SG-TIC, e seu substituto nas ausências previstas na legislação vigente, investido no cargo pelo(a) Reitor(a) da UFRJ, ouvido(a) Superintendente - Geral de TIC, é a autoridade responsável para a autorização de acesso ao Data Center.

§ 1º Nenhum acesso deve ocorrer sem autorização expressa, e acompanhamento, de servidores designados pelo(a) Diretor da DSETIC/SG-TIC.

§ 2º As pessoas autorizadas, serão denominadas de "visitantes", devem utilizar crachá provisório durante sua permanência no local, assinar Termo de Compromisso de Visitantes para Acesso ao Data Center (ANEXO I) e o acompanhante, de que trata o §1º deste artigo, deve verificar a validade da documentação apresentada.

§ 3º O Cadastro e Registro de Acessos (ANEXO II) é o controle em que todos os acessos devem ser registrados em forma de formulário próprio (manual ou eletrônico), contendo nome completo do visitante; matrícula ou documento de identidade; órgão, instituição ou Empresa (se aplicável); nome do responsável interno; motivo do acesso; data e horário de entrada e saída; e, o formulário deve ser arquivado por, no mínimo, 12 meses.

§ 4º A porta do Data Center deve permanecer trancada em tempo integral, com chave ou outro meio de controle disponível e registrado no Cadastro e Registro de Acessos, de que trata o §3º deste artigo, os acessos autorizados.

§ 5º A lista de servidores com acesso autorizado ao Data Center (ANEXO III) deverá ser mantida atualizada e ficar anexada em local visível na sala da DSETIC/SGTIC para controle social.

Art. 29. É vedada a permanência no Data Center de qualquer pessoa, mesmo sendo servidor da SG-TIC ou da UFRJ:

I - sem o acompanhante designado na forma do §1º do Art. 28, sendo considerada falta grave, e poderá responder administrativamente pelos seus atos;

II - fazendo uso de equipamentos pessoais (como notebooks, pendrives, celulares), sem a devida autorização de que trata o Art. 28;

III - portando mochilas, bolsas ou volumes, salvo com inspeção do acompanhante designado na forma do inciso I deste artigo;

IV- fotografando ou filmando o interior do Data Center, salvo quando previamente autorizado pelo Diretor da DSETIC/SG-TIC.

Art. 30. O controle de Chaves de Acesso ao Data Center estará sob custódia da Divisão de Serviços de TIC (DESTIC/SG-TIC).

§ 1º O uso da chave deve ser registrado com data, hora, nome do portador e motivo do acesso, no Cadastro e Registro de Acessos de que trata o §3º do Art. 28.

§ 2º Casos emergenciais, que requeiram o acesso sem o registro de que trata o §1º deste artigo, devem ser comunicados à chefia imediata ou ao(à) Superintendente Geral da TIC, imediatamente após o evento, devendo o responsável pela liberação do acesso justificar por escrito a exceção e inserir no relatório mensal de segurança física.

Art. 31. A Superintendência Geral de TIC, através de seu(sua) Superintendente Geral, é responsável por garantir o cumprimento desta portaria, pelos servidores lotados na SG-TIC, assim como fiscalizar a sua execução e garantir que os visitantes cumpram as orientações emanadas nesta norma sob pena de advertência e bloqueio de acesso futuro aos infratores.

§ 1º Os registros dos controles de acesso ao Data Center serão mantidos acessíveis para fins de auditoria interna e externa, sob responsabilidade da DSETIC/SG-TIC.

§ 2º Qualquer não conformidade será registrada e analisada no contexto do Plano de Tratamento de Riscos da SG-TIC.

§ 3º Os controles de que tratam os Anexos I, II e III deverão ser automatizados.

CAPÍTULO X
SERVIÇO DE ACESSO REMOTO

Art. 32. O acesso e o uso dos sistemas e recursos de TIC, doravante denominado de Serviço de Acesso Remoto (SAR), deve ser realizado em conformidade com as políticas de segurança da informação da UFRJ, assegurando os princípios de segurança da informação – confidencialidade, integridade, disponibilidade e autenticidade, e visando à preservação do patrimônio institucional.

Paragrafo único. A Política de Segurança da Informação e Comunicações (POSIC) é o documento que tem o objetivo de fornecer diretrizes, critérios e suporte administrativo à implementação da segurança da informação e comunicações e, após aprovação pelo Comitê de Governança Digital da UFRJ, será o instrumento normativo na UFRJ.

Art. 33. O Serviço de Acesso Remoto (SAR) será disponibilizado para:

I - utilização de serviços, sistemas e outros recursos institucionais; e,

II - suporte e manutenção de serviços, recursos e sistemas computacionais, sendo esta última modalidade restrita, exclusivamente, às equipes de tecnologia da informação e comunicação

Art. 34. A solicitação para a utilização do SAR deverá ser encaminhada à SG-TIC, através da Central de Serviços - servicos.tic.ufrj.br, com abertura de chamado eletrônico e especificando a necessidade institucional.

§ 1º Para a autorização de acesso ao SAR serão aplicados critérios específicos, podendo ser deferida ou indeferida.

§ 2º O Gestor da Unidade Organizacional de lotação do usuário solicitante do serviço, será notificado quanto à concessão ou suspensão do acesso.

Art. 35. As credenciais de acesso serão disponibilizadas exclusivamente ao usuário que utilizará o serviço, sendo vedado ao usuário o compartilhamento de suas credenciais de acesso.

§ 1º Não será autorizada a concessão de credenciais adicionais ao usuário que já tenha efetuado a solicitação, salvo quando este possuir atribuições específicas da área de tecnologia da informação e comunicação na UFRJ, a ser autorizado pelo COGTIC.

§ 2º Excepcionalmente, poderá ser concedido acesso ao serviço a usuário visitante, em caráter temporário, mediante apreciação da SG-TIC.

§ 3º A revogação da permissão para utilização do serviço poderá ser solicitada pelo usuário ou pelo gestor da unidade organizacional, sendo facultativa a apresentação de justificativa.

§ 4º No caso de inatividade do usuário superior a 180 (cento e oitenta) dias consecutivos, será suspenso o acesso concedido ao serviço solicitado, sem aviso prévio, pela DSETIC/SGTIC.

Art. 36. O usuário deverá utilizar o serviço exclusivamente para atividades relacionadas às suas atividades institucionais na UFRJ, sendo de responsabilidade do usuário do serviço zelar pela utilização adequada de seus equipamentos computacionais, assegurando que sejam periodicamente mantidos com sistemas atualizados e em conformidade com as normas de segurança.

Paragrafo único. O usuário não deverá divulgar dados e informações confidenciais, e restritas, a terceiros sem a prévia autorização de sua chefia imediata ou do responsável legal.

Art. 37. São deveres do usuário:

a) garantir a supervisão contínua de seu dispositivo enquanto este estiver conectado à rede da UFRJ;
b) assegurar o encerramento da conexão ao término de sua utilização, de forma a garantir que não haja acesso não autorizado por terceiros;
c) abster-se de utilizar redes sem fio públicas (abertas sem proteção) para a transmissão de dados e informações com a UFRJ;
d) comunicar, de forma tempestiva, quaisquer suspeitas de uso indevido de suas credenciais por terceiros, bem como eventuais violações de segurança que possam comprometer a integridade e a segurança dos dados e informações da UFRJ; e,
e) cumprir integralmente todas as leis e regulamentos aplicáveis à proteção de dados e à privacidade, incluindo a Lei Geral de Proteção de Dados Pessoais.

Art. 38. O Serviço de Acesso Remoto será monitorado pela SG-TIC, com a finalidade de garantir a segurança e o controle por meio de ações proativas ou preventivas, além de avaliar todos os incidentes que ameacem a segurança dos usuários e ativos de TIC da UFRJ.

§ 1º O monitoramento será conduzido de maneira razoável, responsável e em estrita conformidade com as leis e regulamentos aplicáveis.

§ 2º A SG-TIC será responsável por manter um inventário dos usuários com acesso aos serviços remotos e pela gestão da relação dos sistemas atribuídos a cada um deles.

§ 3º O serviço será suspenso, sem aviso prévio, caso sejam identificados indícios de conduta inadequada, violações de segurança ou ameaças potenciais que comprometam os serviços e ativos da UFRJ e, após análise do COGTIC, se for confirmado o desvio de finalidade, será encaminhado à Divisão Administrativa das Comissões, vinculada a Coordenação de Relações Institucionais e Articulação com a Sociedade (CORIN), para apuração de responsabilidade.

CAPÍTULO XI

DAS DISPOSIÇÕES FINAIS

Art. 39. O Comitê Gestor da SG-TIG (COGTIC) deverá revisar anualmente esta Política, e encaminhar sua atualização ao CGD, em caso de alteração.

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

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

Art. 40. A Superintendente Geral de TIC, ouvido o COGTIC, deverá emitir normativos para disciplinar e orientar a execução desta Política.

Art. 41. Esta Portaria entra em vigor na data de sua Publicação, considerando a urgência para produção de seus efeitos.

Paragrafo único. Os controles de que trata o §3º do Art.31 deverão ser implantados em até 180(cento e oitenta) dias da publicação de que trata o caput deste artigo.p p

Roberto de Andrade Medronho
Reitor

ANEXO I -
TERMO DE COMPROMISSO DE VISTANTES
PARA ACESSO AO DATA CENTER

Eu, _____, portador do documento de identidade nº _____, visitante da(o) _____ _____(órgão ou instituição a que pertença), declaro que:

1. Estou ciente de que o acesso ao ambiente físico do datacenter da UFRJ é restrito e que meu ingresso está condicionado à autorização prévia e acompanhamento por profissional designado da SG-TIC.
2. Comprometo-me a:
   - Respeitar todas as regras de segurança física e lógica estabelecidas;
   - Não realizar registro de imagens (foto ou vídeo) sem autorização;
   - Não portar ou utilizar dispositivos pessoais sem permissão;
   - Zelar pelo sigilo e integridade das informações eventualmente acessadas.

Estou ciente de que qualquer violação a estas regras poderá acarretar responsabilização administrativa, civil e/ou penal.pPor estar de acordo, firmo o presente termo.

Local: _____

Data:____/___/_____

Assinatura do Visitante: _____

Assinatura do Responsável da DESTIC/SGTIC: _____

ANEXO II -
CADASTRO E REGISTRO DE ACESSO

Data	Hora Entrada	Hora Saída	Nome Completo	Documento de Identificação (RG/CPF/SIAPE)	Órgão/ Instituição/ Empresa	Responsável da DESTIC/ SG-TIC	Motivo do Acesso	Nome do Acompanhante	Assinatura do Visitante

Observações: Este formulário deve ser preenchido antes da entrada no ambiente e deve ser arquivado pela SG-TIC por no mínimo 12 meses.

ANEXO III -
LISTA DE SERVIDORES COM ACESSO AUTORIZADO PERMANENTE AO DATA CENTER

Nome Completo	Matrícula SIAPE	Divisão/Unidade	Nível de Acesso	Justificativa para acesso	Aprovado por (Coordenação)	Data de Inclusão

PORTARIA Nº 7688, DE 28 DE JULHO DE 2025

O Reitor da Universidade Federal do Rio de Janeiro, no uso de suas atribuições conferidas pelo Decreto de 27 de Junho de 2023, publicada no Diário Oficial da União nº 121 de 28 de Junho de 2023, resolve:

Dispensar, a pedido, ADRIANA DE RESENDE BARRETO VIANNA, Matrícula Siape nº 1487494, Professor do Magistério Superior, da Função Gratificada de Coordenador de Pós-Graduação do Curso de Antropologia Social, do(a) Museu Nacional - MN, FUC-1, processo nº 23079.225546/25-20.

PORTARIA Nº 7689, DE 28 DE JULHO DE 2025

O Reitor da Universidade Federal do Rio de Janeiro, no uso de suas atribuições conferidas pelo Decreto de 27 de Junho de 2023, publicada no Diário Oficial da União nº 121 de 28 de Junho de 2023, resolve:

Designar MARIA ELVIRA DIAZ BENITEZ, Matrícula Siape nº 1998743, Professor do Magistério Superior, para exercer a Função Gratificada de Coordenador de Pós-Graduação do Curso de Antropologia Social, do(a) Museu Nacional - MN, FUC-1, processo nº 23079.225546/25-20.