SERVIÇO PÚBLICO FEDERAL

MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG

PROITI - PRÓ-REITORIA DE INOVAÇÃO E TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA PROITI/FURG N° 1, DE 10 DE JULHO DE 2023

Dispõe sobre os procedimentos de execução dos Backups, testes e recuperações dos dados armazenados pelo Centro de Gestão de Tecnologia da Informação.

O PRÓ-REITOR DE INOVAÇÃO E TECNOLOGIA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG, no uso das atribuições que lhe confere o art. 32 do Regimento Geral da Universidade e a Política de Segurança da Informação (PSI), considerando:

a. o Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER);

b. o Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC);

c. o Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI);

d. as Guias Operacionais SGD;

e. a Instrução Normativa 01/GSI/PR;

f. a Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021;

g. a Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados;

h. a Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI);

i. a Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos; e

j. a Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES INICIAIS

Art. 1º Instituir a Instrução Normativa de Backup, que tem como foco prover diretrizes para atender à necessidade de implementar os controles previstos na Política de Segurança da Informação (PSI) da Universidade Federal do Rio Grande- FURG, instituindo diretrizes, responsabilidades, competências e estabelecendo mecanismos que permitam a guarda dos dados, visando à segurança dos dados digitais custodiados pelo Centro de Gestão de Tecnologia da Informação (CGTI).

Parágrafo Único. O presente documento apresenta a Instrução Normativa de Backup, onde se estabelece o modo, a periodicidade de cópia e testes de recuperação dos dados armazenados pelos sistemas computacionais, uso da rede, correto acondicionamento, transporte e descarte das mídias de

armazenamento e os responsáveis pela administração do serviço de Backup.

CAPÍTULO II
DO ESCOPO

Art. 2º Esta política se aplica:

I - aos dados armazenados no Data Center do CGTI/FURG;

II - aos dados armazenados em soluções de nuvem contratadas ou mantidas pelo CGTI/FURG, desde que sua aplicação esteja garantida nos acordos ou contratos que formalizam a relação contratual;

III - aos sistemas que utilizarão os serviços de Backup, estes devem ser formalmente homologados pelo CGTI/FURG, mediante análise de viabilidade técnica;

IV - aos membros da comunidade acadêmica, que podem ser criadores e/ou usuários de tais dados; e

V - às situações de perda desastrosa de dados, onde o sistema ou serviço fica parcial ou integralmente indisponível.

Art. 3º Esta política não deve ser aplicada:

I - em serviços em nuvem não contratados ou não mantidos pelo CGTI/FURG e

II - dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora do Data Center do CGTI/FURG ou fora de soluções em nuvem contratadas ou mantidas pelo CGTI/FURG.

CAPÍTULO III
DOS PRINCÍPOS GERAIS

Art. 4º As rotinas de Backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando há indisponibilidade de sistemas ou serviços.

Art. 5º As rotinas de Backup devem utilizar soluções especializadas para este fim, preferencialmente de forma automatizada.

Art. 6º As rotinas de Backup podem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado de acordo com a sua criticidade.

Art. 7º As rotinas de Backup devem garantir, pelo menos uma cópia do Backup, em um local distinto da infraestrutura crítica.

Art. 8º O CGTI/FURG especificará formalmente uma reserva mínima de mídias de armazenamento, para substituição em caso de falhas.

Art. 9º A FURG deverá manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de testes de restauração de Backups.

Art 10. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas por criptografia.

Art 11. Deve ser nomeada uma Equipe de Administração do Backup responsável pela administração e gerência do serviço de Backup composta por no mínimo 2 membros e substitutos integrantes do CGTI/FURG.

CAPÍTULO IV
DA FREQUÊNCIA E RETENÇÃO DOS DADOS

Art 12. É recomendado, que osBackupsdos serviços críticos de TI do CGTI/FURG, sejamrealizados diariamente, semanalmente, mensalmente e semestralmente.

Art 13. Preferencialmente, os serviços críticos de TI do CGTI/FURG, devem ser resguardados/retidossob um padrão mínimo, o qual deve observar a correlação frequência/retenção mínima de dados estabelecida a seguir:

I - diária, com retenção de uma semana;

II - semanal, com retenção de um mês;

III - mensal, com retenção de três meses; e

IV - semestral, com retenção de um ano.

Art 14. Os ativos envolvidos no processo de Backup são considerados ativos críticos para a organização.

Art 15. Para o caso de servidores em sistema de *colocation*, a salvaguarda dos dados, referentes aos serviços de TI críticos, deve ser solicitada ao CGTI/FURG, através do sistema de solicitações, refletindo os requisitos de negócio da organização, bem comoos requisitos de segurança da informação e proteção de dados e dados pessoais envolvidos, e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos: Escopo (dados digitais a serem salvaguardados):

I - escopo (dados digitais a serem salvaguardados);

II - tipo de Backup (completo, incremental, diferencial);

III - frequência temporal de realização do Backup (diária, semanal, mensal, semestral);

IV - retenção;

V - POR: *Recovery Point Objective*; e

VI - RTO: *Recovery Time Objective*.

Art 16. A alteração das frequências e tempos de retenção definidos nesta seção deve serprecedida de solicitação e justificativa formais encaminhadas ao CGTI/FURG, mediante análise de viabilidade técnica. A aprovação para execução da alteração depende da anuência do setor.

Art 17. Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e a Equipe de Administração de Backup deverá zelar pelo cumprimento das diretrizes estabelecidas.

Art 18. Os Backups deverão ser realizados, preferencialmente, como disposto a seguir:

I - os Backups diários serão executados de segunda-feira à sexta-feira, em modo incremental; e

II - os Backups semanais serão executados no sábado e domingo, em modo completo.

Parágrafo único. Em caso de incidentes de segurança, ou falha no sistema de Backup, cópias completas podem ser executas durante a semana, sendo essas documentadas.

Art 19. A execução do Backup deve concentrar-se, preferencialmente, no período da noite, para não degradar o uso da rede.

Art 20. O período de janela de Backup deve ser determinado e documentado pela Equipe de Administração do Backup para que se obtenha o máximo de desempenho e o mínimo de impacto na qualidade da rede de dados.

CAPÍTULO V

DO TRANSPORTE E ARMAZENAMENTO

Art 21. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devemconsiderar as seguintes características dos dados resguardados:

I - a criticidade do dado salvaguardado;

II - o tempo de retenção do dado;

III - a probabilidade de necessidade de restauração;

IV - o tempo esperado para restauração;

V - o custo de aquisição da unidade de armazenamento de Backup; e

VI - a vida útil da unidade de armazenamento de Backup.

Art 22. A Equipe de Administração do Backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Art 23. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimono tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.

Art 24. A execução das rotinas de Backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art 25. As unidades de armazenamento dos Backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura e poeira, e com acesso restrito a pessoas autorizadas pela Equipe de Administração do Backup.

Parágrafo único. As condições de temperatura, umidade e pressão devem ser preferencialmente aquelas descritas pelo fabricante das unidades de armazenamento.

CAPÍTULO VI

DOS TESTES DE BACKUP

Art 26. Os logs dos Backups serão verificados diariamente pela Equipe de Administração em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do Backup.

Art 27. Ações corretivas serão tomadas quando os problemas de Backup forem identificados, a fim de reduzir os riscos associados a Backups com falha.

Art 28. O CGTI/FURG manterá registros de Backups e testes de restauração para demonstrar conformidade com esta Instrução Normativa, contendo, no mínimo, a identificação do sistema, serviço ou servidor, a data da realização do teste, o tempo gasto para o retorno do Backup e se o procedimento foi concluído com sucesso.

Art 29. Os testes de restauração dos Backups devem ser realizados, por amostragem, trimestralmente, a fim de verificar se os Backups foram bem-sucedidos.

CAPÍTULO VII

PROCEDIMENTOS RESTAURAÇÃO DE BACKUP

Art 30. A restauração do Backup fica restrita aos casos de testes ou de perda desastrosa de dados, sistemas ou serviços, onde estes ficam parcial ou totalmente indisponíveis.

Art 31. No caso de servidores em sistema de *colocation*, o atendimento de solicitações de restauração de arquivos e demais formas de dados deverão obedecer às seguintes orientações:

I - a solicitação de restauração de Backups deverá sempre ser feita do responsável pelo servidor através do sistema de solicitações do sistemas FURG;

II - a solicitação deve conter, ao menos, o nome e setor do usuário, o objeto a ser recuperado, localização em que se encontra, a data da versão que deseja recuperar (se houver), local alternativo para o armazenamento do objeto recuperado e a justificativa para recuperação;

III - a restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de Backup;

IV - a solicitação de restauração de dados que tenham sido salvaguardados dependede prévia e formal autorização dos respectivos gestores das informações; e

V - a Equipe de Administração do Backup,terá a prerrogativa de negar a restauração dedados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestorda unidade do demandante.

Art 32. No caso de servidores em sistema de *colocation*, o cronograma de restauração de dados deve levar em conta que o tempo de recuperação:

I - é proporcional ao volume de dados necessários para a restauração; e

II - será definido em Acordo de Nível de Serviço entre as áreas de negócio e de TI.

CAPÍTULO VIII

DO DESCARTE DA MÍDIA

Art 33. Para o caso das mídias de armazenamento de Backup:

I - o CGTI/FURG garantirá que a mídia não contenha imagens de Backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados;

II - o CGTI/FURG garantirá a destruição física da mídia antes do descarte; e

III - o descarte das mídias de Backup inservíveis ou inutilizáveis deverá ser feito pela Divisão de Segurança da Informação do CGTI/FURG mediante solicitação da Equipe de Administração do Backup.

CAPÍTULO IX

DAS RESPONSABILIDADES

Art 34. A Equipe de Administração do Backup deve ser capacitada para as tecnologias, procedimentos e soluções utilizadas nas rotinas de Backup.

Art 35. São atribuições da Equipe de Administração do Backup:

I - propor soluções de cópia de segurança das informações digitais corporativas produzidasou custodiadas pela organização;

II - providenciar a criação e manutenção dos Backups;

III - configurar as soluções de Backup;

IV - manter as unidades de armazenamento de Backups preservadas, funcionais e seguras;

V - definir os procedimentos de restauração e neles auxiliar;

VI - comunicar ao Diretor do CGTI/FURG os erros e ocorrências nos Backups;

VII - fazer o armazenamento das mídias de Backup em cofre apropriado (se houver); e

VIII - verificar periodicamente os relatórios gerados pela ferramenta de Backup.

CAPÍTULO X

DAS DISPOSIÇÕES FINAIS

Art 36. Quaisquer exceções a esta Instrução Normativa serão totalmente documentadas e aprovadas pela Equipe de Administração do Backup e pela Direção do CGTI/FURG.

Art 37. Esta Instrução Normativa pode ser revisada a qualquer momento pela Equipe de Administração do Backup juntamente com a Direção do CGTI/FURG.

Diogo Paludo de Oliveira

Pró-Reitor de Inovação e Tecnologia da Informação em exercício

Documento assinado eletronicamente por **Diogo Paludo de Oliveira**, **Pró-Reitor, Substituto**, em 19/07/2023, às 18:24, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

ANEXO N° 1 - TERMOS E DEFINIÇÕES

(INSTRUÇÃO NORMATIVA PROITI/FURG N° 1, DE 10 DE JULHO DE 2023)

BACKUP OU CÓPIA DE SEGURANÇA - Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

BACKUP COMPLETO (FULL) - Modalidade de Backup na qual os dados são copiados em sua totalidade;

BACKUP INCREMENTAL - Modalidade de Backup na qual somente os arquivos novos ou modificados desde o último Backup - seja ele completo, diferencial ou incremental - são copiados;

COLOCATION - *Co-location* ou *housing* é o aluguel ou empréstimo de espaço físico e infra-estrutura para servidores de sistemas ou serviços oferecidos por outras unidades ou setores da Universidade ou até mesmo empresas externas e alocados no Datacenter do CGTI/FURG.

MÍDIA - Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

OBJETO - Qualquer dado passível de Backup e restauração;

RETENÇÃO - Período de tempo em que o conteúdo da mídia de Backup deve ser preservado;

INFRAESTRUTURA CRÍTICA – instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

RECOVERY POINT OBJECTIVE (RPO): ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente; e

RECOVERY TIME OBJECTIVE (RTO): tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente.

Documento assinado eletronicamente por **Diogo Paludo de Oliveira**, **Pró-Reitor, Substituto**, em 19/07/2023, às 18:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade do documento pode ser conferida no site https://sei.furg.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0 informando o código verificador **0087729** e o código CRC **04204540**.

Referência: Caso responda este documento Anexo, indicar o Processo nº 23116.012810/2023-10 SEI nº 0087729