MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RORAIMA
REITORIA
Conselho Superior
Rua Fernão Dias Paes Leme, 11, Calungá, Boa Vista - RR, CEP 69303220 ,
www.ifrr.edu.br

Resolução CONSUP/IFRR N° 812, de 29 de novembro de 2024.

A Política de Backup e Restauração de Dados Digitais visa instituir diretrizes, responsabilidades e competências que garantem à segurança, proteção e disponibilidade dos dados digitais custodiados pela área de Tecnologia da Informação.

A presidente em exercício do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia de Roraima, no uso de suas atribuições legais, tendo em vista o que consta no Processo nº 23231.000916.2024-27 - Política de Backup e Restauração, e a decisão do colegiado tomada na 94ª sessão plenária, realizada em 11 de outubro de 2024,

RESOLVE:

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Backup e Restauração de Dados Digitais (PBRD) visa instituir diretrizes, responsabilidades e competências para garantir a segurança, a proteção e a disponibilidade dos dados digitais custodiados pela área de Tecnologia da Informação e formalmente definidos como de necessária salvaguarda no IFRR, para se manter a continuidade do negócio.

Art. 2º No sentido de assegurar sua missão é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças. O presente documento apresenta a Política de Backup e Restauração de Dados Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais, visando garantir a segurança, integridade e disponibilidade, conforme a Política de Segurança da informação e Comunicação - PoSIC – IFRR.

Art. 3° Se faz necessário estabeles o escopo da PBRD:

I. Esta política se aplica a todos os servidores e sistemas on premisse gerenciados pelo IFRR. O escopo desta política de backup será revisado a cada 2 anos.

II. Todas as aplicações em produção hospedadas no *Datacenter* deverão estar cobertas pelo backup, como:

a. Sistema Unificado de Administração Pública (SUAP);

b. Portal Institucional (Site);

c. Sistema de Gerenciamento de Certames (SGC);

d. Servidor de Autenticação do IFRR (*Active Directory - AD*);

e. Repositório de Publicações Cientificas;

f. Sistema de Biblioteca - Pergamum;

g. Sistema Acadêmico Q-acadêmico;

h. Arquivos dos setores;

i. Configuração de ativos de rede;

j. Ambientes Virtuais de Aprendizagem - AVA/Moodle;

k. Terminais de Ponto Eletrônico;

l. Sistema de Folha de Pagamento - Sippag;

III. Executar o backup das máquinas virtuais, dos bancos de dados das aplicações, e dos arquivos de configuração dos servidores, visando facilitar a restauração do serviço dependendo do incidente ocorrido;

IV. Esta política se aplica a todos os colaboradores que podem ser criadores e/ou usuários de tais dados;

V. A política também se aplica a dados de terceiros que acessam e usam sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade do IFRR;

VI. Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s);

VII. A salvaguarda dos dados em formato digital pertencentes a serviços de TI do IFRR, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

Art. 4º Para os fins desta politica devem ser adotadas as seguintes definições:

I. 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;

II. Custodiante da Informação: qualquer indivíduo ou estrutura de órgão, ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança conforme as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

III. Eliminação: exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

IV. 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;

V. Infraestrutura Primária: 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;

VI. 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;

VII. 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;

VIII. Backup Completo (Full): modalidade de backup na qual os dados são copiados em sua totalidade;

IX. Backup Diferencial: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup completo são copiados;

X. Backup Incremental: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup - seja completo, diferencial ou incremental - são copiados;

XI. Clientes de backup: todo equipamento servidor no qual é instalado o agente de backup;

XII. Recuperação de Desastre: estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;

XIII. Formatação de baixo nível: tipo de método de limpeza de HD que apaga todos os vestígios de arquivos do disco por meio de ação mecânica.

CAPÍTULO II - DECLARAÇÕES DA POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS

Art. 5º Dos princípios gerais:

I. Esta Política de Backup e Restauração de Dados deve estar alinhada com as Políticas de Segurança da Informação do - PoSIC do IFRR;

II. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI;

III. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada;

IV. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização, relacionado no Manual de Procedimentos de Restore de Backup;

V. O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um site de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos;

VI. Recomenda-se que a infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização;

VII. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup;

VIII. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Art. 6º Da frequência e retenção dos dados:

I. Os backups dos serviços de TI primários e secundários do IFRR devem ser realizados utilizando-se as seguintes frequências temporais, que estarão definidas no MI – Backup e Restore:

a. Diária;

b. Semanal;

c. Mensal;

d. Anual.

II. Especificidades dos serviços de primários e dos serviços de TI secundários podem demandar frequência e tempo de retenção diferenciados e estão estabelecidos no MI – Restore de Backup;

III. Os ativos envolvidos no processo de backup são considerados ativos primários para a organização;

IV. A solicitação de salvaguarda dos dados referentes aos serviços de TI primários e aos serviços de TI secundários, deve ser realizada pelos responsáveis, com a anuência prévia e formal da gestão, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização;

V. Mais especificamente, a aprovação dos itens de backup com a sua devida classificação é feita pelo diretor sistêmico de tecnologia da informação, toda a solução de backup é gerenciada e acessada somente por administradores e operadores de backup previamente designados, em que se utilizam credenciais especificas para este fim como forma de segurança;

VI. Deve explicitar, no mínimo, os seguintes requisitos técnicos abaixo descritos:

a. Escopo conforme definido no item 2 desta Política;

b. Tipo de backup (completo, incremental, diferencial);

c. Frequência temporal de realização do backup (diária, semanal, mensal, anual);

d. Retenção;

e. RPO;

f. RTO.

VII. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas à equipe de infraestrutura de tecnologia da informação, denominados operadores de backup. A aprovação para execução da alteração depende da Gestão de Tecnologia;

VIII. Os responsáveis pelos dados devem ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup devem zelar pelas diretrizes estabelecidas.

Art. 7º Do uso da rede:

I. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do IFRR, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI;

II. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup definido e preferencialmente ser executado fora do horário comercial;

III. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a área técnica responsável com a validação e aprovação do diretor de tecnologia da informação.

Art. 8º Do transporte e armazenamento

I. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

a. a criticidade do dado salvaguardado;

b. o tempo de retenção do dado;

c. a probabilidade de necessidade de restauração;

d. o tempo esperado para restauração;

e. o custo de aquisição da unidade de armazenamento de backup;

f. A vida útil da unidade de armazenamento de backup.

II. O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso;

III. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações;

IV. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento;

V. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento;

VI. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

Art. 9º Dos testes de backup e testes de restore:

I. Os backups serão verificados periodicamente:

a. Semanalmente, os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup;

b. Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha;

c. A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política;

d. Os testes devem ser realizados em todos os backups produzidos independente do ambiente;

II. Os testes de restauração dos backups devem ser realizados, por amostragem mensalmente em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos;

III. Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs;

IV. Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso;

VI. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas e serem encaminhadas/comunicadas ao Comitê de Governança Digital (CGD) ou Comitê Gestor de Segurança da Informação (CGSI)Para a execução dos testes de restore, que deve ser mensal, todas as evidências devem ser armazenadas.

Art. 10. Do Descarte da Mídia – Validar com o IF se é aplicável:

I. A mídia de backup será retirada e descartada conforme descrito neste documento:

a. A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados;

b. A TI garantirá a destruição física da mídia antes do descarte;

c. O uso de terceiros para descarte e certificação segura de descarte é recomendado.

II. Para a formatação é recomendado o uso dos métodos:

a. NIST Clear: O método limpa os dados em todos os locais endereçáveis por meio de técnicas lógicas. Ele é geralmente aplicado por meio de comandos padrão do tipo “Leitura” e “Escrita” no dispositivo de armazenamento;

b. NIST Purge: O método Purge (Purgar) de sanitização de mídia oferece um nível mais alto de segurança para dados confidenciais, tornando a recuperação de dados inviável por meio de tais técnicas como sobrescrita, apagamento de blocos e criptografia;

c. NIST Destroy: O método Destroy (Destruir) de sanitização de mídia envolve a destruição física da mídia de armazenamento, proporcionando o mais alto nível de proteção de dados para informações altamente sensíveis ou dispositivos irreparáveis;

Art. 11. Das Responsabilidades:

I. O(s) administrador(es) e o(s) operador(es) de backup, assim como as suas atribuições, deverão ser indicados mediante portaria pelo diretor de TI. O(s) administrador(es) e o(s) operador(es) de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

Art. 12. Os procedimentos relacionados a esta Políticas estão descritos no MI – Manual de Instruções de Restore de Backup.

Art. 13. Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

Art. 14. Está resolução entra em vigor na data de sua publicação.

Dê-se ciência, publique-se e cumpra-se.

Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia de Roraima, em Boa Vista-RR, 29 denovembro de 2024.

Aline Cavalcante Ferreira
Presidente em exercício do CONSUP

ANEXO I - Referência legal e de boas práticas quando aplicável

Orientação	**Seção**
Acórdão 1.109/2021-TCU-Plenário	Em sua íntegra
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI;	v4.1: DS11: Gerenciar Dados v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
Guia do Framework de Privacidade e Segurança da Informação	Controle 11
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	Gestão da Segurança da Informação
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea g, h
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo IV
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;	A.12.3 Cópias de segurança
Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;	12.3 Cópias de segurança
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra

ANEXO II - Termo de Concordância

Eu li e entendi a Política de Backup e Restauração de Dados Digitais do _____. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais e/ou disciplinares conforme as leis aplicáveis e as normas internas.

Local, ____ de _____ de 20 ___

_____

Nome do Servidor

Cargo

Documento assinado eletronicamente por:

- **Aline Cavalcante Ferreira**, **REITOR(A) - SUB-CHEFIA - GAB**, em 29/11/2024 10:58:18.

Este documento foi emitido pelo SUAP em 25/11/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrr.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 315395
Código de Autenticação: e4bd6831cc