MINISTÉRIO DA EDUCAÇÃO

Instituto Federal de Educação, Ciência e Tecnologia de Brasília

PORTARIA 15/2024 - RIFB/IFBRASILIA, DE 20 de agosto de 2024

Estabelece as normas e procedimentos técnicos para o backup e restauração de arquivos no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Brasília - IFB.

A REITORA DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE BRASÍLIA, nomeada pelo Decreto de 02 de Agosto de 2023, publicado no Diário Oficial da União em 03 de agosto de 2023, no uso de suas atribuições legais e regimentais, e

CONSIDERANDO as seguintes orientações de referência legal e de boas práticas:

Orientação	**Seção**
Acórdão 1.109/2021-TCU-Plenário - Auditoria sobre a Efetividade dos Procedimentos de Backup das Organizações Públicas Federais	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, de 27 de maio de 2020 - Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.	Art.12, Inciso IV, alínea g, h
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021 - Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal	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	A.12.3 Cópias de segurança

- Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;	
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 - Aprova o Glossário de Segurança da Informação	Em sua íntegra

Resolve:

Art. 1º Estabelecer normas e procedimentos técnicos para o backup e restauração de arquivos no âmbito do Instituto Federal de Brasília - IFB, de acordo com as diretrizes desta Portaria Normativa.

CAPÍTULO I
DAS DEFINIÇÕES

Art. 2º Para efeitos desta Portaria Normativa foram 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 em conformidade com 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 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;

VI. Backup Completo (*FULL*) - Uma cópia de todos os dados de um sistema, independente dos backups anteriores. É a forma mais abrangente de backup e serve como a base para outros tipos de backups;

VII. Backup Incremental - Copia apenas os dados que foram alterados ou adicionados desde o último backup (seja ele completo ou incremental). Isso economiza espaço e tempo, mas requer todos os backups incrementais anteriores para uma restauração completa;

VIII. Backup Diferencial - Copia todos os dados que foram alterados ou adicionados desde o último backup completo. Cada backup diferencial contém todas as mudanças feitas desde o último backup completo, tornando a restauração mais rápida que o incremental, mas consumindo mais espaço;

IX. Administradores de Backup - São os responsáveis pela configuração e execução dos procedimentos de backup na instituição;

X. Operador de Backup - O Operador de Backup monitora e verifica os processos de backup, assegura a integridade e segurança dos dados, responde a solicitações de restauração, e documenta todas as operações, garantindo a conformidade com normas e requisitos regulatórios;

XI. 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;

XII. 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.

CAPÍTULO II
DO PROPÓSITO E DO ESCOPO

Art. 3º Esta portaria normativa objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela Direção de Tecnologia da Informação e Comunicação - DTIC, e formalmente definidos como de necessária salvaguarda no IFB, para se manter a continuidade do negócio. No sentido de assegurar sua missão é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades, ataques, catástrofes naturais, outras ameaças ou outras excepcionalidades que causem impacto significativo à instituição. O presente documento apresenta as Normas e Procedimentos Técnicos de B*ackups* e Restauração de Dados Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

Art. 4º Esta normativa se aplica a todos os dados advindos de sistemas no âmbito do IFB, armazenados e mantidos pela DTIC.

I. Os dados de sistemas, neste contexto, incluem: códigos fonte, bancos de dados, arquivos de configuração, diretórios de arquivos usados pelo sistema, logs, dentre outros dados considerados essenciais pelo setor responsável por um sistema. A definição de dados e o escopo desta portaria normativa serão revisados sempre que houver necessidade.

II. Os dados de sistemas de terceiros hospedados nos servidores do IFB deverão ser definidos através do documento de detalhes técnicos (Anexo 2).

Art. 5º Estas normas se aplicam a agentes públicos que podem ser criadores e/ou usuários de tais dados. As normas também se aplicam a terceiros que acessam e usam no IFB sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade do IFB.

Art. 6º Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora do centro de processamento de dados mantido pela DTIC, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).

Parágrafo único. A salvaguarda dos dados em formato digital pertencentes a serviços de TI do IFB, 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.

CAPÍTULO III
DOS PRINCÍPIOS GERAIS

Art. 7º As normas e procedimentos técnicos descritos neste documento devem estar alinhadas com a Política de Segurança da Informação do IFB.

Art. 8º As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

Art. 09º As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 10. O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto para armazenar cópias extras dos principais backups.

Art. 11. A infraestrutura de rede de backup deve ser logicamente apartada dos sistemas da organização.

Art. 12. Deve-se manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.

Art. 13. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

CAPÍTULO IV
DA FREQUÊNCIA E RETENÇÃO DOS DADOS

Art. 14. Os backups dos serviços de TI do IFB devem ser realizados utilizando-se as seguintes frequências temporais:

I - Diária;

II - Semanal;

III - Mensal;

IV - Anual.

Art. 15. Os serviços de TI do IFB devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I – Diária: 1 mês;

II – Semanal: 2 meses;

III – Mensal: 1 ano;

IV – Anual: 5 anos.

Art. 16. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

Art. 17. Os sistemas de TI do IFB a terem seus dados salvaguardados devem ser formalmente elencados pelo setor responsável pelo sistema através de um requerimento (Anexo I) contendo informações de temporalidades e retenção dos dados e também através de um documento contendo detalhes técnicos do sistema (Anexo II) a ser realizado em conjunto com o custodiante da informação e com anuência da direção da DTIC.

Art. 18. A alteração das frequências e tempos de retenção definidos nesta portaria deve ser precedida de solicitação e justificativa formais encaminhadas à DTIC. A aprovação para execução da alteração depende da anuência do Diretor da DTIC e do Setor responsável pelo sistema.

Art. 19. Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

CAPÍTULO V
DO TIPO DE BACKUP E USO DA REDE

Art. 20. Os tipos de backup a serem adotados na instituição serão os backups completos (*full),* backups incrementais.

Parágrafo único: A depender das características dos dados e de sua frequência de alteração, poderá ser substituído o backup incremental para o backup diferencial, ficando a cargo dos administradores do backup essa decisão.

Art. 21. Os administradores de backup devem considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do IFB, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da instituição.

Art. 22. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.

§ 1° O período de janela de backup deve ser determinado pelos administradores de backup em conjunto com a área técnica responsável pela administração da rede de dados da instituição.

§ 2° Os horários de realização de backup serão definidos no documento de detalhes técnicos de cada sistema (Anexo II).

CAPÍTULO VI
DO TRANSPORTE E ARMAZENAMENTO

Art. 23. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar 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;
VI – A vida útil da unidade de armazenamento de backup.

Art. 24. Os administradores de backup devem identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Art. 25. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos administradores do backup.

Art. 26. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art. 27. 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 pelos administradores de backup.

Art. 28. Pelo menos uma vez ao mês, de forma a prevenir perda de dados em casos de desastres naturais ou acontecimentos adversos, os últimos backups completos de cada sistema serão armazenados em unidades de armazenamento que deverão ser retiradas do data center e armazenadas em um outro local que contenha um cofre à prova de água, umidade e fogo, possuindo também blindagem eletromagnética e proteção contra poeira.

§ 1° A mídia será claramente identificada e armazenada em uma área segura acessível apenas para pessoa(s) autorizada(s) pela DTIC.

§ 2° A mídia não será deixada sem supervisão durante o transporte para área segura.

§ 3° Backups de sistemas já não mais utilizados devem possuir uma cópia de segurança também armazenadas nas unidades de armazenamento remotas.

§ 4° A mídia deverá ser mantida no cofre por 1 ano, no caso dos backups mensais, e por 5 anos, no caso dos backups anuais.

Art. 29. 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.

§ 1° A administração do backup 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.

CAPÍTULO VII
DOS TESTES DE BACKUP

Art. 30. Os backups serão verificados periodicamente:

§ 1º Semanalmente, os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.

§ 2° Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.

§ 3° A DTIC manterá registros de backups e testes de restauração para demonstrar conformidade com esta norma.

Art. 31. Os testes de restauração dos backups devem ser realizados, por amostragem, uma vez por semestre, 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.

Art. 32. 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.

CAPÍTULO VIII
DOS PROCEDIMENTOS DE RESTAURAÇÃO DE BACKUP

Art. 33. O atendimento de solicitações de restauração de dados de sistemas deverá obedecer às seguintes orientações:

§ 1º A solicitação de restauração de objetos deverá sempre partir do responsável pelo sistema, através de Ofício.

§ 2º A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

§ 3º A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.

§ 4º O operador de backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

CAPÍTULO IX
DAS RESPONSABILIDADES

Art. 34. O administrador de backup e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

§ 1º O administrador e o operador de backup do IFB serão indicados pelo diretor de Tecnologia da Informação e Comunicação (DTIC), entre os servidores lotados na Coordenação de Infraestrutura em Tecnologia da Informação (CITIC).

§ 2º Caso não seja possível a indicação de servidores distintos, o mesmo servidor poderá exercer os papéis de administrador e operador de backup.

Art. 35. São atribuições dos administradores de backup:

I - Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou 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 - reportar imediatamente ao setor a que está subordinado os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de backups;

IX - gerenciar mensagens e registros de auditoria (LOGs) dos backups;

X - disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos backups;

XI - propor modificações visando ao aperfeiçoamento das normas e procedimentos de Backup e Recuperação de Dados Digitais, objeto desta Portaria.

Art. 36. São atribuições dos operadores de backup:

I – Monitorar a execução dos processos de backup, garantindo que todas as cópias de segurança sejam realizadas conforme programado;

II – Verificar a integridade e a validade dos backups realizados, realizando testes periódicos de restauração para assegurar a funcionalidade;

III – Registrar e documentar todas as operações de backup, incluindo falhas e ações corretivas tomadas;

IV – Realizar a rotação e o armazenamento adequado dos dispositivos de backup, assegurando que estejam em locais seguros e protegidos contra danos físicos e acessos não autorizados;

V – Responder as solicitações de restauração de dados, colaborando com as equipes de TI e usuários finais para recuperar informações conforme necessário;

VI – Garantir a conformidade com as normas e procedimentos de backup da organização e com os requisitos legais e regulatórios relacionados à retenção e proteção de dados;

VII – Colaborar com o administrador de backup para resolver problemas técnicos e otimizar processos de backup e recuperação;

VIII – Fornecer suporte técnico em relação aos sistemas de backup utilizados, identificando e resolvendo problemas operacionais;

IX – Acompanhar a utilização e a capacidade de armazenamento dos dispositivos de backup, planejando a aquisição de novos equipamentos quando necessário.

Art. 37. São atribuições dos setores responsáveis pelos sistemas:

I - solicitar restaurações de dados, com anuência da chefia do setor;

II - sanar dúvidas técnicas do administrador de backup acerca das informações salvaguardadas;

III - validar, tecnicamente, o resultado das restaurações eventualmente solicitadas;

IV - validar, tecnicamente, o resultado dos testes de restauração dos backups.

CAPÍTULO XI
DAS DISPOSIÇÕES FINAIS

Art. 38. Esta portaria poderá ser alterada sempre que necessário, haja vista das mudanças tecnológicas e soluções de TI, além de possíveis mudanças na legislação vigente.

Art. 39. Casos omissos serão apreciados pela DTIC.

Art. 40. Esta Portaria entra em vigor na data de sua assinatura.

(documento assinado eletronicamente)
VERUSKA RIBEIRO MACHADO

ANEXOS

Os anexos I e II desta portaria podem ser encontrados como modelos de documentos no SUAP. Para acessa-los deve-se criar novo documento com o seguinte passo a passo.

Anexo I: Solicitação de Backup em Sistemas de Informação

Adicionar novo documento no link: https://suap.ifb.edu.br/admin/documento_eletronico/documentotexto/add/
Tipo: Requerimento - Documento
Modelo: Tecnologia da Informação - Solicitação de Backup em Sistemas de Informação
Assunto: Solicitação de Backup em Sistemas de Informação - (Colocar o nome do sistema)
Nível de Acesso: Restrito
Hipótese Legal: Proteção da Propriedade Intelectual de Software (Art. 2o da Lei no 9.609/1998)

Anexo II: Documentação Técnica de Sistema para Backup

Adicionar novo documento no link: https://suap.ifb.edu.br/admin/documento_eletronico/documentotexto/add/
Tipo: Relatório Técnico;
Modelo: Tecnologia da Informação - Documentação Técnica de Sistema para Backup.
Assunto: Documentação Técnica de Sistema para Backup - (Colocar o nome do sistema)
Nível de Acesso: Restrito
Hipótese Legal: Proteção da Propriedade Intelectual de Software (Art. 2o da Lei no 9.609/1998)

Documento assinado eletronicamente por:

- **Veruska Ribeiro Machado**, **REITOR(A) - CD1 - IFBRASILIA**, em 20/08/2024 10:27:20.

Este documento foi emitido pelo SUAP em 05/06/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifb.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 544231
Código de Autenticação: eed20a3fb2