Ministério da Educação
Universidade Federal do Cariri
Comitê de Governança

ATO DECISÓRIO CG N.o 02, DE 05 DE MARÇO DE 2024

Aprova a Política de Backup da UFCA.

O PRESIDENTE DO COMITÊ DE GOVERNANÇA DA UNIVERSIDADE FEDERAL DO CARIRI - UFCA, no uso da competência que lhe confere o Decreto Presidencial de 1º de junho de 2023, publicado no Diário Oficial da União, no dia 02 de junho de 2023, seção 2, página 1, e tendo em vista o que deliberou o Comitê de Governança - CG em sua Reunião Ordinária, em 05 de março de 2024, na forma do que dispõe o art. 8 do Regimento Interno do Comitê de Governança, resolve:

Art. 1º Aprovar a Política de Backup da UFCA nos termos do anexo a este Ato decisório.

Art. 2º Este Ato Decisório entra em vigor em 05 de março de 2024.

Documento assinado digitalmente
SILVÉRIO DE PAIVA FREITAS JÚNIOR
Presidente do Comitê de Governança

UNIVERSIDADE FEDERAL DO CARIRI
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

POLÍTICA DE BACKUP

JUAZEIRO DO NORTE (CE) - MARÇO / 2024

SUMÁRIO

ESCLARECIMENTOS

O objetivo deste documento é fornecer aos responsáveis pela proteção de dados, arquivos e gestão da Segurança da Informação da Universidade Federal do Cariri (UFCA), orientações para mitigação de possíveis riscos ligados às temáticas de privacidade e segurança da informação relativos aos seus sistemas informacionais e processos de trabalho da instituição.

INTRODUÇÃO

No contexto da transformação digital do Estado brasileiro, o Governo Federal publicou em 29 de abril de 2020, por meio do Decreto nº 10.332, a Estratégia de Governo Digital, iniciativa que se encontra em plena execução. Ela norteia as ações de todos os órgãos federais, com o objetivo de transformar o governo pelo digital, oferecendo políticas públicas e serviços de melhor qualidade, mais simples, acessíveis de qualquer lugar e a um custo menor para o cidadão.

Hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.

Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no Art.46. da Lei Geral de Proteção de Dados, sancionada em 14 de agosto de 2018 – "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

A sua não observância pode impactar diretamente a capacidade do governo federal de cumprir suas missões precípuas de promover uma gestão pública eficiente, ampliar o acesso à cidadania, estimular uma economia brasileira crescentemente digitalizada, dinâmica, produtiva e competitiva, e em última instância, impedir a geração de valor público para o cidadão.

POLÍTICA DE BACKUP

A Política de Backup da UFCA tem como objetivo atender a necessidade de implementar os controles previstos na Política de Segurança da Informação - PSI, considerando as diretrizes gerais estabelecidas para implementação da PSI, conforme prevê o Art.12, Inciso IV da Instrução Normativa Nº 01/GSI/PR, bem como os Capítulos III e IV da Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021, a qual dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

Responsável	DDC - Lucas Emanuel Dantas Barbosa DSI - Francisco Henrique Balbino de Godoy DTI - Taciano Pinheiro de Almeida Alcântara
Aprovado por:	Comitê de Governança da UFCA
Políticas Relacionadas	Política de Segurança da Informação - PSI
Data da Aprovação	05 / 03 / 2024
Data de Revisão	Revisão Anual (após a data da aprovação)

PROPÓSITO

A Política de Backup objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela Diretoria de Tecnologia da Informação (DTI) e formalmente definidos como de necessária salvaguarda na UFCA, para manutenção e 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 ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças.

O presente documento apresenta a Política de Backup, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

ESCOPO

- Esta política se aplica aos dados armazenados nos Data Centers da UFCA.
- Esta política se aplica aos dados armazenados em soluções de nuvem mantidas pela UFCA, desde que sua aplicação esteja garantida nos acordos ou contratos que formalizam a relação contratual.
- Os sistemas a serem backupeados, devem ser formalmente homologados pela DTI, mediante análise de viabilidade técnica;
- Esta política se aplica aos membros da comunidade acadêmica, que podem ser criadores e/ou usuários de tais dados.

NÃO ESCOPO

- Serviços em nuvem mantidos por terceiros;
- Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos Data Centers da UFCA ou fora de soluções em nuvem mantidas pela UFCA;
- Esta política não se aplica aos ambientes de testes e homologações.

TERMOS E DEFINIÇÕES

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 DIFERENCIAL - Modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup completo (full) são copiados;

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;

SNAPSHOT - Conhecido também como "cópia instantânea" é o registro do estado de um arquivo, aplicação ou sistema em um certo ponto no tempo. Dessa forma, é criada uma "fotografia" do status dos dados em um determinado momento, permitindo definir o ponto correto de restauração em casos de erros e falhas;

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;

ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

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;

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

OBJETO - Qualquer dado passível de backup e restauração;

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;

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;

SOLUÇÃO MANTIDA PELA UFCA: Aquilo que resolve, soluciona (problema, dificuldade etc.) com operação e sustentação realizada pela Universidade.

SOLUÇÃO MANTIDA POR TERCEIROS: Aquilo que resolve, soluciona (problema, dificuldade etc.) com operação e sustentação realizada por outras companhias sem vínculo com a Universidade.

REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Orientação	Secção
Acórdão 1.889/2020-TCU-Plenário	Relatório de Levantamento de Auditoria Páginas 30-32
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
Framework de segurança cibernética do CIS 8	Salvaguardas do controle 11 (Data Recovery Capabilities)
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem	Gestão da Segurança da Informação

aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	
Guias Operacionais SGD	Todos
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea g, h
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	1. 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

DECLARAÇÕES DA POLÍTICA

Dos princípios gerais

1. A Política de Backup deve estar alinhada com a Política de Segurança da Informação da UFCA.
2. A Política de Backup deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
3. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.
4. As rotinas de backup devem utilizar soluções especializadas para este fim, preferencialmente de forma automatizada.
5. 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.
6. As rotinas de backup devem garantir, se possível, pelo menos uma cópia de segurança do backup, em um local distinto da infraestrutura crítica.
7. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.

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

Das Responsabilidades

9. O administrador e o operador de backup devem ser, necessariamente, servidores da Diretoria de Tecnologia da Informação - DTI, designados para tais funções;
10. O administrador e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup;
11. São atribuições do administrador e o operador de backup:

I – Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;
II – Providenciar a criação e manutenção das rotinas de 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 Gestor da DTI os erros e ocorrências nos backups;
VII – Fazer o armazenamento das mídias de backup em cofre apropriado(se houver);
VIII – Verificar periodicamente os relatórios gerados pela ferramenta de backup;

Da frequência e retenção dos dados

12. A solicitação de backups dos dados deverá partir do responsável pelo sistema;
13. É recomendado que os backups dos serviços de TI críticos da UFCA sejam realizados, utilizando-se as seguintes frequências temporais:

    I – Diária;

    II – Semanal;

    III – Mensal;

    IV – Semestral.

14. Preferencialmente, os serviços de TI críticos da UFCA devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

Frequência	Retenção
Diária	15 dias
Semanal	1 mês
Mensal	12 meses
Semestral	3 anos
Snapshot	3 dias úteis

15. A solicitação de salvaguarda dos dados referentes aos serviços de TI deve ser realizada à DTI, 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, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

    I – Escopo (dados digitais a serem salvaguardados);

    II – Tipo de *backup* (completo, incremental, diferencial);

    III – Frequência temporal de realização dos backups (diária, semanal, mensal, semestral);

    IV – Retenção;

    V – RPO;

    VI – RTO.

16. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas à DTI, mediante análise de viabilidade técnica. A aprovação para execução da alteração depende da anuência da DTI.

17. Os responsáveis pelos dados deverão ter ciência das rotinas de backup estabelecidas para cada tipo de informação e o administrador de backup deverá zelar pelo cumprimento das diretrizes estabelecidas.

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

    I - Os backups diários serão executados de domingo à sexta-feira, em modo incremental;

    II - Os backups semanais serão executados nos finais de semana, iniciando aos sábados, em modo completo;

    III - Os backups mensais serão executados no 1º domingo de cada mês, em modo completo;

    IV - Os backups semestral serão executados no 2º domingo de cada mês, em modo completo.

    V - As solicitações de Snapshot de máquinas virtuais deverão ser realizadas através do sistema de help desk.

Do uso da rede

19. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da UFCA, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da UFCA.
20. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.
21. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a área técnica responsável pela administração da rede de dados da UFCA.

Do transporte e armazenamento

22. 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 dos dados;

    III – A viabilidade da restauração dos dados;

    IV – O tempo esperado para restauração;

    V – O custo de aquisição da unidade de armazenamento de backup.
23. 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.
24. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelo administrador de Backups.
25. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.
26. 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.
27. 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;
28. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

Verificações dos backups

29. Os backups serão verificados periodicamente:
    - Diariamente os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.
    - Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.
    - A TI manterá registros de backups para demonstrar conformidade com esta política.

Testes de restauração dos backups

30. A TI manterá registros dos testes de restauração para demonstrar conformidade com esta política.
31. Os testes de restauração dos backups devem ser realizados, por amostragem, mensalmente, exceto por indisponibilidade do operador de backup e do responsável técnico pelo sistema, a fim de verificar se os backups foram bem-sucedidos.
32. Os registros devem conter, no mínimo, a identificação do sistema que teve o seu backup restaurado e testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso.
33. O ambiente restaurado deve ser testado e aprovado pelo responsável do sistema.
34. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pela DTI.

Procedimento de restauração de backup

35. O atendimento de solicitações de restauração de arquivos e demais formas de dados deverá obedecer às seguintes orientações:

    a. A solicitação de restauração de objetos deverá sempre partir do responsável pelo sistema, através de chamado técnico, utilizando a ferramenta de controle de atendimentos.

    b. O chamado técnico deve conter, ao menos, o nome e setor do usuário, o(s) objeto(s) a ser(em) recuperado(s), localização em que se encontra(m), a data da versão que deseja recuperar, local alternativo para o armazenamento do(s) objeto(s) recuperado(s) e a justificativa para recuperação.

    c. Somente será possível a restauração de objetos que foram contemplados em alguma rotina de backup.

d. A restauração de snapshot's, só será possível, nos casos em que tenha ocorrido prévia solicitação e confirmação da realização da criação do snapshot através do sistema de help desk.

e. A aprovação da solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização do respectivo administrador de backup.

f. O administrador 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.

36. O cronograma de restauração de dados:

a. O tempo de recuperação é proporcional ao volume de dados necessários para o restore.

b. O tempo de restauração, preferencialmente, definido em Acordo de Nível de Serviço entre as áreas de negócio e de TI, o tempo de restauração, quando tecnicamente viável é de, no máximo, 15 dias úteis.

Do Descarte da Mídia

37. 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 descarte das mídias de backup inservíveis ou inutilizáveis deverá ser feito pelo Responsável da Segurança da Informação mediante solicitação do administrador de backup.

ANEXO I

TERMO DE VALIDAÇÃO DE TESTE DE RESTAURAÇÃO DE BACKUP

IDENTIFICAÇÃO DO RESPONSÁVEL	
Nome:	
E-mail:	Telefone:

DETALHAMENTO TÉCNICO DA RESTAURAÇÃO
Máquina(s) restaurada(s):
Tipo de restauração: ☐ 1. Máquina virtual completa ☐ 2. Arquivo ou diretório específico ☐ 3. Sistema restaurado Caso o tipo seja 2 ou 3, especifique o item abaixo:

Criticidade da máquina: ☐ 1. Alta ☐ 2. Média ☐ 3. Baixa	Storage policy usada no backup: ☐ 1. Policy_Diário ☐ 2. Policy_Semanal ☐ 3. Policy_Mensal ☐ 4. Policy_Semestral	Tipo de backup a ser restaurado: ☐ 1. Full ☐ 2. Incremental ☐ 3. Diferencial
Data da realização:		
Horário de início:	Horário de término:	Duração da restauração:

OBSERVAÇÕES

_____
Assinatura do responsável pela restauração

_____
Assinatura da chefia imediata

_____
Assinatura do responsável pelo teste

ANEXO II
TERMO DE SOLICITAÇÃO DE RESTAURAÇÃO

IDENTIFICAÇÃO DO RESPONSÁVEL	
Nome:	
E-mail:	Telefone:
Setor:	

DETALHAMENTO TÉCNICO DO ARQUIVO/PASTA A SER RESTAURADO

Nome do arquivo/pasta que será restaurado:
Data do arquivo arquivo/pasta que será restaurado:
Local para armazenar o arquivo/pasta restaurado:

OBSERVAÇÕES SOBRE O OBJETO DE RESTAURAÇÃO

_____

Assinatura do solicitante

OBSERVAÇÕES:
Após verificação da viabilidade de restauração, o arquivo/pasta solicitado(a) será disponibilizado(a) no local indicado no formulário acima acima em até XX dias conforme a Política de Backup da Universidade Federal do Cariri - UFCA.