NSTI 0001/2022

NORMA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS

Brasília, 28 de julho de 2022

Secretário de TI

Prof. Dr. Jacir Luiz Bordim

Coordenadoria de Gestão e Planejamento – CGESP

Francisco Jackson Alves de Freitas

Divisão de Contratações e Aquisições de TIC

Wellington Ferreira

Divisão de Apoio à Governança de TIC

André de Lanna Sette Fiuza Lima

Núcleo de Capacitação

Henrique de Almeida Ramos

Diretoria de Operações e Serviços - DOS

Domingos Pereira Costa

Coordenadoria de Redes e Infraestrutura

Alex Anderson Dantas Fidelis

Coordenadoria de Serviços Especializados

Marcus Vinicius da Silva Jorge

Coordenadoria de Segurança da Informação

Juvenal dos Santos Barreto

Divisão de Atendimento ao Usuário

Rister Abadio Barbosa

Divisão de Data Center

Rodrigo Coelho Guidotti

Diretoria de Sistemas da Informação

Consuelo Martins Galo

Coordenadoria de Sistemas Administrativos

Eduardo Chagas Lustoza

Coordenadoria de Sistemas Acadêmicos

Felipe Evangelista dos Santos

Coordenadoria de Sistemas de Pessoal

Andrei Lima Queiroz

Coordenadoria de Estratégia de Dados

Tiago Medina Chagas

Coordenadoria de Sites Corporativos

Elaine Teixeira dos Santos

Equipe Técnica de Elaboração

Cristiano Magno de Moraes

Joaquim Aquiles Gonsalves Castanheira

Maicon Mesquita Cunha

Pedro Serra Carvalho Portes

Equipe de Revisão

Marcus Vinicius Da Silva Jorge

Juvenal dos Santos Barreto

Histórico de Revisões

Data	Versão	Descrição	Autor
02/07/2019	1.0	Política de Backup e restauração de Dados Digitais	Equipe Técnica de Elaboração
05/02/2020	2.0	Atualização da Política	Equipe Técnica de Elaboração
01/11/2021	3.0	Atualização da Política	Equipe Técnica de Elaboração
13/06/2022	4.0	Atualização da Política e Adequação ao Modelo de Política de Backup lançado pelo Governo Federal do Brasil em Março de 2022	Equipe Técnica de Elaboração
22/07/2022	4.1	Revisão e readequação da Norma conforme diretivas do SISP.BR e da STI	Revisores

Das Responsabilidades

Responsável	Coordenadoria De Serviços Especializados – CSE/DOS/STI.
Aprovado por:	Jacir Luiz Bordim
Políticas Relacionadas	Política de Segurança da Informação e Comunicação da Universidade de Brasília – PoSIC/UnB
Localização de armazenamento	Sala Cofre (padrão ISO 9001) localizada nas dependências físicas do prédio da STI/UnB no Campus Darcy Ribeiro (Asa Norte – DF).
Data da Aprovação	27 de julho de 2022
Data de revisão	Anual, sempre no mês subsequente a aprovação desta Norma

Sumário

INTRODUÇÃO 5
Propósito 6
Escopo (conforme resolução CPLAD nº 004/2018, Art. 2º da PoSIC/UnB) 6
Não Escopo 7
Não fazem parte do Sistema de Backup administrado pela STI/UnB: 7
Termos e Definições (Conforme PORTARIA GSI/PR Nº 93, DE 18/10/2021) 7
Declarações da Norma 8
Dos Princípios Gerais 8
Da frequência e retenção dos dados 8
Dos tipos de backup 10
Do Plano de Contingência 10
Do Uso da Rede de Dados 10
Do transporte e armazenamento 10
Dos testes de backup 11
Dos procedimentos para inclusão de JOBS no Sistema de Backup 12
Dos procedimentos para restauração de JOBS do Sistema de Backup 12
Do cronograma de restauração dos dados de backup 13
Do Descarte da Mídia de Backup 13
Das Responsabilidades 13
Procedimentos Relevantes 16
Não conformidade 16
Concordância 16
Referência legal e boas práticas 17

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 Federal 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, onde a STI/UnB se enquadra, 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 a sociedade como um todo.

A Universidade de Brasília, atualmente fornece diversos tipos de serviços informatizados a sua comunidade acadêmica e a toda sociedade civil em geral, sempre pautada nos três pilares essenciais que são o ensino, a pesquisa e a extensão, em prol do alcance da missão e visão institucionais, pautados nos valores da Universidade.

A Secretaria de Tecnologia da Informação – STI/UnB é o órgão da UnB responsável em planejar e administrar a execução dos serviços relacionados com o tratamento eletrônico das informações digitais, tais como desenvolver, implantar e manter sistemas de dados acadêmicos e administrativos; serviços de emissões de guias, certificados e diplomas; fornecimento de serviços em nuvem; manter a integridade, confiabilidade, confidencialidade e a segurança dos dados digitais; desenvolver meios de facilitar a comunicação dos dados digitais através das comunicações via rede de dados cabeada, rede wireless e/ou via satélite.

A proteção dos dados digitais pelo Governo Federal, 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 instancia, impedir a geração de valor público para o cidadão.

Propósito

A Norma de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos ativos de dados digitais custodiados pela Secretaria de Tecnologia da Informação (STI/UnB) e formalmente definidos como de necessária salvaguarda na Universidade de Brasília, para se manter a continuidade do negócio. No sentido de assegurar sua missão, é fundamental estabelecer mecanismos que permitam a guarda dos dados digitais e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças. O presente documento apresenta a Norma de Backup e Restauração de Dados Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados digitais armazenados pelos sistemas computacionais acadêmicos e administrativos da Universidade de Brasília.

Escopo (conforme resolução CPLAD nº 004/2018, Art. 2º da PoSIC/UnB)

Entende-se por Serviço de Backup, os procedimentos, métodos, equipamentos e softwares que, integrados ou não, oferecem uma garantia de imunidade ao parque computacional da STI/UnB a eventuais perdas, parciais ou totais, de dados e arquivos digitais, bem como dos procedimentos formais para a solicitação de recuperação desses dados salvaguardados.

- Esta norma se aplica a todos os dados digitais no âmbito da Universidade de Brasília, incluindo dados fora da Instituição armazenados em serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem: Banco de dados relacional dos sistemas acadêmicos, administrativos e de pessoal da UnB; dados e arquivos digitais armazenados na estrutura física do serviço de armazenamento e compartilhamento de arquivos do Controlador de Domínio Institucional da UnB administrado pela STI; conteúdo web armazenado nas máquinas servidoras de sites administradas pela STI onde se encontram o Portal da UnB e demais sítios das unidades acadêmicas e administrativas da UnB lá armazenados; dados digitais das demais máquinas servidoras alocadas fisicamente no parque computacional da STI e por ela administradas.
- A definição de dados críticos e o escopo desta norma de backup serão revisados sempre que necessário ou anualmente, após a data de aniversário da publicação desta Norma.
- Os serviços de TI críticos da Universidade de Brasília devem ser formalmente elencados pelo Comitê de Governança Digital da UnB ou seu órgão equivalente.
- Esta norma se aplica as áreas de TIC da STI/UnB que podem ser agentes criadores e/ou usuários de tais dados. A norma também se aplica a terceiros que acessam e usam na UnB os sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade da instituição.
- Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores e demais equipamentos de TIC dos usuários ou em quaisquer outros dispositivos fora do parque computacional da STI pelas unidades de TI, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s) a salvaguarda destes dados. A salvaguarda dos dados em formato digital pertencentes aos serviços de TIC da Universidade de Brasília, 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 as partes envolvidas.

Não Escopo

Não fazem parte do Sistema de Backup administrado pela STI/UnB:

- Os discos locais das estações de trabalho de front end das áreas administrativas e acadêmicas da Universidade de Brasília;
- As máquinas servidoras externas ao Data Center da Secretaria de Tecnologia da Informação da UnB; e
- As máquinas servidoras alocadas fisicamente no Data Center da STI/UnB que não são administradas e da responsabilidade da equipe técnica da STI/UnB.

Termos e Definições (Conforme PORTARIA GSI/PR Nº 93, DE 18/10/2021)

- **Administrador do Servidor** - Usuário responsável pela administração da máquina servidora;
- **Backup ou cópia de segurança** - É o ato de copiar arquivos, pastas ou discos inteiros (físicos ou virtuais) para sistemas de armazenamento secundários, buscando a preservação dos dados em caso de qualquer problema técnico, físico ou atemporal;
- **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;
- **Deleção ou Eliminação** - Exclusão de dado digital ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- **Restore** - é a recuperação dos dados que foram copiados para os sistemas de armazenamento secundários, restaurando-os para o seu formato e local original;
- **Mídia** - Mecanismos onde os dados digitais são armazenados; possuem diversos formatos e tecnologias distintas para sua comunicação - inclui discos ópticos e magnéticos, CDs, fitas cartuchos e papel, entre outros;
- **Tape Library** - dispositivo físico que contém uma ou mais unidades de mídias magnéticas, certa quantidade de nichos para guardar cartuchos de mídias magnéticas, um leitor de código de barras para identificar os cartuchos de mídias e um método automatizado para inserir as mídias nas unidades de leitura/gravação de dados (robô mecânico);
- **Storage** - Meio físico (equipamento) onde são armazenados todos os dados digitais contidos no backup;
- **RPO (Recovery Point Objective)** - Ponto no tempo em que os dados dos serviços de TIC 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;
- **RTO (Recovery Time Objective)** - Tempo estimado para restaurar os dados e tornar os serviços de TIC novamente operacionais, correspondendo ao prazo máximo em que se

admite manter os serviços inoperantes até a restauração de seus dados, após um incidente ou solicitação de restore;

- **Scratch** – Mídia magnética que ainda não possui dados gravados;
- **TIC** – Tecnologia da Informação e Comunicação;
- **JOB** – Rotina de execução do backup;
- **Disaster Recovery** – Rotina de recuperação emergencial de backup.

Declarações da Norma

Dos Princípios Gerais

1. A Norma de Backup e Restauração de Dados está alinhada com a Política de Segurança da Informação – POSIC/UnB, aprovada pela CPLAD/UnB em 08/11/2018, aos princípios, diretrizes e legislações pertinentes que regem a administração pública federal, bem como aos normativos internos da Universidade de Brasília.
2. A Norma de Backup e Restauração de Dados está alinhada com a gestão de continuidade do negócio em nível organizacional.
3. As rotinas de backup são orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade dos serviços críticos de TIC.
4. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
5. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com a especificidade do serviço de TIC ou dado salvaguardado, dando prioridade aos serviços de TIC críticos da UnB.
6. O armazenamento das mídias magnéticas dos backups críticos já gravados, sempre que possível, é realizado em local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede da instituição para armazenar cópias extras dos principais backups, a exemplo dos backups de dados dos serviços críticos.
7. A infraestrutura de redes do serviço de backup encontra-se apartada, lógica e fisicamente, dos sistemas críticos da organização.
8. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
9. Em situações em que a confidencialidade é importante, cópias de segurança são protegidas através de encriptação.

Da frequência e retenção dos dados

10. Os backups dos serviços de TIC críticos da STI/UnB devem ser realizados utilizando-se as seguintes frequências temporais:

    I – Diário;

    II – Mensal;

    III – Semestral;

    IV – Anual.

NOTA TÉCNICA: Como todos os backups são feitos diariamente, o que diferencia o backup diário do mensal, semestral e anual será sempre o seu prazo de retenção, pois devido à metodologia de cópia da atual ferramenta de backup adotada pela STI, os dados copiados serão sempre de forma incremental (full).

11. Os serviços de TI críticos da STI/UnB e os não críticos devem ser resguardados sob um padrão mínimo temporal, o qual deve observar a correlação frequência/retenção dos dados de acordo com a sua criticidade.

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

13. Define-se que os arquivos críticos salvaguardadados com retenção igual ou superior a 01(um) ano serão executados para mídias magnéticas do tipo cartucho LTO.

14. Define-se a criticidade do dado/arquivo salvaguardado sendo do menor para o maior onde a criticidade 0 (zero) possui a maior criticidade e a 3 (três) com a menor criticidade, conforme demonstrado na tabela a seguir:

Criticidade	Tempo de retenção	Execução do backup	Armazenamento físico
0	Prazo não definido	Diário	Mídia Magnética
1	Até 01 ano	Diário	STORAGE de Backup
2	Até 06 meses	Diário	STORAGE de Backup
3	Até 30 dias	Diário	STORAGE de Backup

15. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

16. A solicitação de salvaguarda dos dados referentes aos serviços de TIC críticos e aos serviços de TIC não críticos deve ser realizada pelo responsável técnico do serviço crítico, banco de dados ou sistema/servidor com a anuência prévia e formal do gerente da área, refletindo os requisitos do 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 do backup (diária, semanal, mensal, anual);

IV – Retenção;

V – RPO;

VI – RTO.

17. A alteração da frequência e tempo de retenção do backup definida nesta seção deve ser precedida de solicitação e justificativa técnica formal encaminhada a Coordenadoria de Serviços Especializados da DOS/STI através de ticket aberto no Portal de Serviços da STI. A aprovação ou não dessa mudança será avaliada pela equipe responsável em administrar o Sistema de Backup (CSE/DOS/STI).

18. Os responsáveis pelos dados/arquivos deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores do Sistema de Backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

Dos tipos de backup

I – Completo (***full***)

II – Incremental

III – Diferencial

19. Salvo indicação em contrário, o backup dos dados do sistema será feito de acordo com a seguinte programação padrão:

20. A atual rotina de backup implementada na STI/UnB encontra-se definida para executar uma cópia FULL inicial do dado/arquivo/sistema copiado e as demais cópias serão do tipo FOREVER INCREMENTAL. Desta forma a janela de backup é reduzida, pois não há a necessidade de executar backups FULL novamente.

21. Com a utilização dos atuais STORAGES alocados na STI onde todos possuem a tecnologia de deduplicação do dado/arquivo, é possível realizar backups do tipo DIFERENCIAL de forma diária (Syntetic Full), o que reduz consideravelmente os tempos de RTO (Recovery Time Objective) e RPO (Recovery Point Objetive).

22. **Backup Diário** - Realizado diariamente de forma incremental e armazenado em equipamentos próprios (STORAGES de backup).

23. **Backup Extra por Solicitação ou Excepcionalidade** - Realizado sempre que necessário ou requisitado, sendo armazenado em storages de backup e depois em duas cópias (original e de segurança) para unidades de mídias magnéticas com a retenção de acordo com a criticidade do dado/arquivo ou do sistema copiado. Esse tipo de backup geralmente é requisitado quando algum sistema ou máquina servidora é desativada e requer um tempo maior de retenção destes dados para possíveis auditorias que venham a ser solicitadas pelos órgãos de controle.

Do Plano de Contingência

24. Se por algum impedimento técnico ou de falha/erro de software/hardware, as rotinas de backup não puderem ser executadas pela equipe técnica da STI/UnB, os responsáveis pelos sistemas deverão ser informados e orientados (através de comunicado interno, via SEI e ou e-mail) como proceder para manter seus dados e arquivos institucionais de forma segura através de cópias manuais diretamente em suas estações de trabalho ou em área disponibilizada para este fim remotamente pela Secretaria de Tecnologia da Informação.

Do Uso da Rede de Dados

25. A equipe responsável pelo Sistema de Backup deve estudar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do parque computacional da STI, garantindo que a performance da rede necessária às suas atividades não ocasione indisponibilidade dos demais serviços de TI da Universidade de Brasília.

26. A execução das rotinas de backup deve concentrar-se, preferencialmente, no período da janela de backup previamente definido, minimizando o impacto na rede e possível indisponibilidade de algum ativo necessário para execução de backup específico.

27. O período de janela de backup deve ser definido pela equipe responsável pelo Sistema de Backup em conjunto com a área técnica responsável pela administração da rede de dados da STI/UnB.

Do transporte e armazenamento

28. 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 do dado salvaguardado;

IV. O tempo esperado para restauração do dado salvaguardado;

V. O custo de aquisição da unidade de armazenamento de backup e do próprio Sistema de Backup (*software*);

VI. A vida útil das unidades de armazenamento de backup, das mídias magnéticas e da garantia e licença do *software* de backup.

29. Periodicamente, a equipe responsável pela administração do Sistema de Backup deve pesquisar e identificar a viabilidade da utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso, trazendo ganhos de produtividade e melhor custo benefício.

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

31. As unidades de armazenamento e demais hardwares (UFM´s, robô de backup, discos, etc.) do Sistema de Backup estão acondicionadas dentro do Data Center da STI/UnB, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador do sistema. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

32. Quando da necessidade de descarte das unidades de armazenamento e demais equipamentos desgastados e/ou obsoletos do Sistema de Backup, tais recursos serão inutilizados fisicamente, atentando-se para o descarte sustentável e ambientalmente correto, conforme as leis ambientais do País.

33. As fitas magnéticas de backup serão transportadas e armazenadas conforme descrito a seguir:

I. A mídia magnética (cartucho) será claramente identificada e armazenada em área segura e acessível apenas pelas equipes de administração e operação do sistema de backup;

II. O transporte das mídias magnéticas entre a sala cofre da STI e a fitoteca de segurança externa será executado sob a supervisão continua de no mínimo um dos membros colaboradores da equipe de operação ou administração do Sistema de Backup;

III. As mídias magnéticas armazenadas na fitoteca de segurança externa ao Data Center da STI serão transportadas de volta a STI somente após o término do seu prazo de retenção para reuso ou descarte seguro ou então quando houver alguma solicitação de restore dos dados salvaguardados;

IV. O armazenamento das mídias magnéticas em fitoteca de segurança externa ao Data Center da STI estará sujeito as mesmas condições físicas e ambientais daquelas contidas no Data Center da STI/UnB supracitadas no item 31 desta Norma.

Dos testes de backup

34. Os backups serão verificados periodicamente, seguindo as diretivas:

I. Diariamente, os logs de execução dos backups são avaliados pela equipe técnica em busca de falhas, durações anormais e em busca de oportunidades para melhorarias no desempenho dos processos;

II. Ações corretivas serão tomadas sempre que necessárias, a fim de reduzir os riscos associados a perda de dados salvaguardados;

III. A equipe de operação do Sistema de Backup manterá registros de logs e testes de restauração para demonstrar conformidade com esta norma de backup;

IV. Os testes serão realizados de forma aleatória, atendendo todos os processos, independente do ambiente de execução do backup;

V. Os testes de restore dos backups são realizados por amostragem e no mínimo uma vez por semana, dependendo da disponibilidade dos equipamentos do Sistema de Backup e dos recursos humanos de TIC, a fim de verificar a idoneidade, segurança eficiência do sistema.

VI. Verificar se os *JOBS* de backups estão atendendo os níveis de serviço pactuados, tais como os tempos de *RTO* e *RPO*.

VII. As métricas dos testes de backups deverão conter 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.

Dos procedimentos para inclusão de JOBS no Sistema de Backup

35. O atendimento das solicitações de inclusão de máquinas servidoras, arquivos, banco de dados, sistemas ou demais processos dentro do Sistema de Backup da STI/UnB obedecerão às seguintes orientações:

35.1. Somente o responsável pelo ativo a ser incluído no Sistema de Backup ou seu gestor técnico pode solicitar a inclusão do dado/arquivo/servidor no Sistema de Backup da STI/UnB. Esta solicitação deve ser feita através da abertura de chamado no Portal de Serviços TIC da STI/UnB.

35.2. O ticket aberto no Portal da STI deverá conter os seguintes parâmetros:

I. Nome da máquina servidora e o seu endereçamento IP dentro da rede interna do Data Center da STI/UnB;

II. A área (tamanho) e o(s) diretório(s) a ser(em) copiados;

III. A periodicidade do backup (diário, semanal, mensal e anual);

IV. Tempo de retenção do backup;

V. Nome, ramal, e-mail do servidor requisitante responsável pelos ativos que serão copiados.

Dos procedimentos para restauração de JOBS do Sistema de Backup

36. O atendimento das solicitações de restauração de arquivos, banco de dados, sistemas ou demais processos dos JOBS de backup obedecerão às seguintes orientações:

36.1. Somente o responsável pelo ativo a ser restaurado ou seu gestor técnico pode solicitar o restore do backup através da abertura de chamado no Portal de Serviços TIC da STI/UnB.

36.2. O ticket aberto no Portal da STI deverá conter os seguintes parâmetros:

I. Nome da máquina servidora e o seu endereçamento IP dentro da rede interna do Data Center da STI/UnB;

II. A área (tamanho) e o(s) diretório(s) a ser restaurados;

III. A data da gravação do backup a ser restaurado;

IV. Informar o local (máquina servidora e diretório) onde os dados restaurados deverão ser disponibilizados e por quanto tempo deverão ficar armazenados neste local.

36.3. A restauração dos ativos de backup somente será possível nos casos em que o *JOB* esteja inserido no sistema de backup.

36.4. A equipe de administração do Sistema de Backup terá a prerrogativa de negar a restauração dos dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade demandante.

Do cronograma de restauração dos dados de backup

37. O tempo de restauração, preferencialmente definido em Acordo de Nível de Serviço entre as áreas de negócio e de TIC da STI, é proporcional ao volume de dados necessários para o restore.

38. A restauração de backup é realizada pela equipe de Operação do Backup. A solicitação de restore deve ser registrado pelo responsável/gestor do sistema por meio do portal de atendimento da STI.

Do Descarte da Mídia de Backup

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

I. A equipe de operação do Sistema de Backup será a responsável em efetuar o descarte seguro de toda mídia de backup destinada a este fim. Ela garantirá que a mídia não contém mais imagens e arquivos válidos passíveis de serem recuperados por terceiros em hipótese alguma.

II. A equipe de operação do Sistema de Backup garantirá a destruição física da mídia antes do seu descarte em definitivo.

III. Após a inutilização física da mídia de backup e a certeza de que não há mais a possibilidade de conserto ou recuperação dos dados, a equipe de operação entregará todo o equipamento inutilizado a área administrativa da STI responsável pelo descarte seguro sem agredir o meio ambiente e as leis ambientais do nosso País.

Das Responsabilidades

40. Os administradores e a equipe de operação do Sistema de Backup da STI devem ser devidamente capacitados para uso das tecnologias, procedimentos e soluções utilizadas em todo o sistema e rotinas de backup implementadas pela STI/UnB.

41. São atribuições e responsabilidades da equipe de administração do Sistema de Backup da STI/UnB:

I. Configurar e administrar as ferramentas (sistema/software) de backup;

II. Definir os procedimentos de criação e restore das rotinas de backup, a criticidade, escalabilidade e prioridade dos JOBS de backup;

III. Pesquisar e propor novas soluções de sistemas de backups com tecnologia de ponta e que atendam melhor os objetivos da instituição;

IV. Propor a Direção da STI/UnB ou ao seu Conselho Consultivo, alterações, correções ou anulações, na sua totalidade ou em parte, da Norma de Backup vigente na Instituição.

V. Solicitar a Direção da STI, sempre que necessário, treinamentos e atualizações técnicas para a equipe de operação do Sistema de Backup da STI.

VI. Responder, de forma institucional as instâncias superiores da UnB, sobre o serviço de backup além de manter a Direção da Secretaria de Tecnologia da Informação informada sobre o andamento do serviço e das futuras necessidades de expansão do mesmo a fim de que os serviços de backup sejam mantidos de forma ininterrupta e que atenda a toda a Comunidade Universitária da UnB.

42. São atribuições e responsabilidades da equipe de operação do Sistema de Backup da STI/UnB:

I. Criar, testar e implantar os scripts (JOBS) de backups;

II. Efetuar periodicamente rotinas de testes de todo o sistema de backup com o objetivo de manter todo o sistema e seus periféricos em perfeito funcionamento;

III. Criar, etiquetar, gerenciar e manter a guarda das mídias magnéticas em local próprio e seguro, seguindo as condições físicas e ambientais explicitadas pelo fabricante dos equipamentos, tanto para a fitoteca local quanto para a fitoteca de segurança externa;

IV. Fazer a troca das mídias de backup no robô de backup retirando as mídias com armazenamento cheio por outras scratchs;

V. Quando identificado, fazer a troca das mídias defeituosas ou inservíveis por novas dentro do sistema;

VI. Mídias magnéticas inservíveis ou defeituosas devem ser inutilizadas em definitivo e descartadas após a certeza de que os dados inseridos não são possíveis de ser recuperados por terceiros;

VII. Executar, programar a execução (data/hora) e restaurar as rotinas e os *JOBS* de backups;

VIII. Verificar diariamente os relatórios e arquivos de logs de execução dos backups gerados pelas ferramentas (softwares) de backups;

IX. Executar rotinas de testes do sistema de backup e de restore dos backups em disco e mídias magnéticas. Estas rotinas são executadas semanalmente ou quando se fizerem necessárias com o objetivo de validar que o backup realizado foi feito com sucesso e que sua recuperação/restore foi realizada para garantir que o processo obteve êxito.

43. Dos responsáveis técnicos pelas máquinas e sistemas administrados pela STI/UnB:

I. Abrir chamado técnico no Portal de Serviços da STI/UnB solicitando a equipe de operação do sistema de backup a inclusão ou remoção de alguma máquina, sistema, banco de dados, disco rígido ou arquivos dentro das rotinas do Sistema de Backup da STI/UnB;

II. Informar a volumetria da atual massa de dados a ser incluída nas rotinas de backup, a periodicidade de execução do backup e o tempo de retenção que esses dados devem ser salvaguardados dentro do Sistema de Backup;

III. Informar a equipe de backup sobre uma previsão periódica (em média de até 05 anos) do aumento da volumetria das massas de dados das rotinas de backups dos sistemas e serviços por ele administrado.

44. Dos responsáveis técnicos pelas máquinas e sistemas externos não administrados pela STI/UnB:

I. A Secretaria de Tecnologia da Informação não fornece o serviço de backup para as máquinas externas alocadas no Data Center da STI que não são administradas pelo seu corpo técnico;

II. Os colaboradores técnicos e administradores das máquinas servidoras externas alocadas no Data Center da STI/UnB são os únicos responsáveis em administrar e criar as rotinas de backup dos seus sistemas. Estas rotinas não fazem parte e não são controladas pelo Sistema de Backup da STI/UnB;

III. A Secretaria de Tecnologia da Informação possui um sistema de recuperação das máquinas servidoras externas do tipo "*disaster recovery*". Este backup será restaurado, desde que seja comprovado que a falha ou o mau funcionamento de uma máquina servidora externa tenha sido causado por erro de hardware ou algum agente interno da própria STI/UnB.

45. Dos usuários do Servidor de Arquivos Institucional da UnB (Controlador de Domínio):

I. É de inteira e única responsabilidade do usuário local, armazenar todo o conteúdo de informação digital de trabalho institucional nas unidades de armazenamento remotas mapeadas virtualmente nas estações de trabalho, não cabendo a STI/UnB a gestão das pastas e arquivos nos discos rígidos das estações de trabalho locais, pois somente os dados contidos nas unidades remotas serão incluídos nas rotinas do sistema de backup administrado pela STI/UnB.

II. O usuário responsável pela estação de trabalho local é o único responsável pela salvaguarda dos arquivos e dados digitais contidos no disco rígido local e, portanto, a STI/UnB se exime da responsabilidade sobre a salvaguarda destes dados, os quais não são abarcados no Sistema de Backup administrado pela STI/UnB.

46. Da Secretaria de Tecnologia da Informação e seu Conselho Consultivo

I. Cabe a STI/UnB deliberar sobre a aprovação, alteração ou anulação, em parte ou na sua totalidade, da norma de backup aqui descrita.

II. É função da STI/UnB alertar sobre a necessidade de recursos financeiros para a aquisição e manutenção dos equipamentos do sistema de backup, assim como promover a capacitação da equipe técnica responsável sempre que for identificada a necessidade de atualização do sistema de backup e do seu corpo técnico.

47. Da Responsabilidade Geral

I. A Coordenadoria de Serviços Especializados, juntamente com a Diretoria de Operações e Serviços da STI, respondem de forma institucional as instâncias superiores da UnB sobre o serviço de backup, além de manter a Direção da Secretaria de Tecnologia da Informação informada sobre o andamento do serviço e das futuras necessidades de expansão do mesmo, a fim de que os serviços de backup sejam mantidos de forma ininterrupta e que atenda a toda a Comunidade Universitária da UnB.

Procedimentos Relevantes

48. O documento interno de responsabilidade e guarda da CSE/DOS/STI chamado de "Rotina de Backup da STI/UnB" versa pela descrição da arquitetura do Sistema de Backup e dos procedimentos técnicos para a realização das cópias de produção, segurança externa e restaurações das máquinas servidoras e dados digitais alocados no Data Center da STI/UnB. Este documento tem por finalidade complementar a atual Norma de Backup da STI/UnB.

Não conformidade

49. Em caso de violação desta Norma de Backup poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis aos agentes públicos aqui responsabilizados.

50. As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes itens:

I. Processo Administrativo Disciplinar de acordo com a legislação aplicável;

II. Passível de exoneração do servidor ou terceiro ao final do processo;

III. Ação judicial de acordo com as leis aplicáveis e acordos contratuais;

IV. Rescisão contratual para o bem do serviço público.

Concordância

51. Todos os agentes públicos aqui descritos nesta Norma de Backup declaram estar cientes e de acordo com todo o teor deste documento e afirmam que, ao violarem as diretrizes estabelecidas neste documento, poderão enfrentar ações legais e disciplinares de acordo com as leis aplicáveis e as normas internas da Universidade de Brasília e do Governo Federal do Brasil.

Referência legal e boas práticas

Orientação	Seção
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 aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	Gestão da Segurança da Informação
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	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