Boletim de Serviço Eletrônico em 18/08/2022

INSTITUTO FEDERAL
Rondônia

MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Rondônia

INSTRUÇÃO NORMATIVA 2/2022/REIT - CGAB/REIT

PROCESSO SEI Nº 23243.010912/2021-75

DOCUMENTO SEI Nº 1689967

Estabelece as instruções para procedimento de backup no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – IFRO.

O REITOR PRO TEMPORE DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RONDÔNIA – IFRO, nomeado pelo Decreto Presidencial de 4 de agosto de 2022, publicado no DOU nº 148, de 5 de agosto de 2022, Seção 2, pág. 1, no uso de suas atribuições legais e regimentais conferidas pela Lei nº 11.892, de 29 de dezembro de 2008, publicada no D.O.U. de 30 de dezembro de 2009 e estabelecidas pelo art. 67 do Regimento Geral do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – IFRO, aprovado pela Resolução nº 65/CONSUP/IFRO, de 29 de dezembro de 2015, e posteriores; resolve:

CAPÍTULO I

DO OBJETIVO

Art. 1º Esta Instrução Normativa tem por objetivo definir as diretrizes dos procedimentos de *backup*, testes e restauração das informações eletrônicas corporativas do IFRO, visando garantir a sua integridade e disponibilidade, bem como evitar que informações sejam permanentemente perdidas em caso de algum incidente físico, lógico ou ambiental.

Art. 2º As regras gerais para o serviço de *backup* do IFRO obedecem ao disposto nesta Instrução Normativa e estão alinhadas com os princípios e diretrizes da Política de Segurança da Informação e Comunicação deste Instituto Federal.

Art. 3º Esta Instrução Normativa está em consonância com a Resolução nº 18/2010/CONSUP/IFRO (SEI nº 1134645), de 31/5/2010, que dispõe sobre a normativa de uso dos Recursos de Tecnologia da Informação e Comunicação no Instituto Federal de Educação, Ciência e Tecnologia de Rondônia.

CAPÍTULO II

DAS DEFINIÇÕES

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

I - Acesso: permissão, privilégio ou capacidade de ler, registrar, atualizar, gerenciar ou administrar a consulta e/ou a manipulação do acervo de dados e informações do IFRO;

II - Administrador de *Backup*: técnico responsável e qualificado para as tarefas de configuração dos serviços de *backup* e também da restauração em casos de desastre ou solicitação de responsáveis pelos dados ou administradores de serviço;

III - Administrador de Ativo: administrador de ativos de TIC utilizados pelo IFRO, que também podem requisitar a restauração de *backup* dos ativos por eles gerenciados em caso de desastre;

IV - Agente: qualquer pessoa ou conjunto de pessoas autorizadas pelo IFRO para o acesso e/ou tratamento dos dados corporativos: docentes, funcionários, discentes e terceirizados;

V - Ativo: qualquer bem, tangível ou intangível, que tenha valor para a Instituição;

VI - Ativo Institucional: ativos que são utilizados por toda a instituição sob gerenciamento da DGTI;

VII - *Backup*: Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação em caso de perda das originais. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

VIII - *Backup* Diferencial: *backup* apenas dos arquivos alterados, em sua primeira execução. É executado após o último *backup FULL* e realiza na segunda execução, o *backup* dos arquivos que foram alterados após o último *backup FULL*, mais os arquivos que foram alterados depois do primeiro *backup* Diferencial e assim sucessivamente;

IX - *Backup* Incremental: realiza *backup* apenas dos últimos arquivos alterados;

X - *Backup Full*: é uma cópia completa de todos os arquivos "marcados" para *backup* ele pode também ser chamado de *backup* completo;

XI - Código Fonte: conjunto de palavras ou símbolos escritos de forma ordenada, contendo instruções em uma das linguagens de programação existentes, de maneira lógica;

XII - Criticidade: grau de importância da informação para a continuidade das atividades e serviços;

XIII - Custódia: consiste na responsabilidade de se guardar um ativo para terceiros. A custódia não permite automaticamente o acesso ao ativo e nem o direito de conceder acesso a outros;

XIV - Dado: Qualquer elemento identificado em sua forma bruta e que, por si só, não conduz a uma compreensão de um fato ou situação;

XV - Descarte: Eliminação correta dos dados, unidades de armazenamento e acervos digitais;

XVI - Disponibilidade: Garantia de que o dado esteja acessível e utilizável sob demanda ou entidade devidamente autorizada;

XVII - Dado de Uso Corporativo ou Institucional: todos os dados capturados e utilizados nas operações de serviço e administrativas do IFRO;

XVIII - *Log* ou Registro de Auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional, para posterior análise, podendo ser gerado por sistemas operacionais, aplicações, entre outros;

XIX - IEC: *International Electrotechnical Commission*;

XX - Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXI - ISO: *International Organization for Standardization*;

XXII - Janela de *Backup*: intervalo de tempo durante o qual as cópias de segurança sob execução agendada ou manual, poderão ser executadas;

XXIII - Mídias: Meios difundidos de cópias de segurança incluem CD-ROM, DVD, disco rígido externo, fitas magnéticas, *flash* de memória, entre outros que porventura surjam com o avanço tecnológico;

XXIV - NBR: normatização técnica brasileira elaborada pela ABNT;

XXV - Restore: Restauração dos *backups* realizados;

XXVI - Retenção: significa o tempo até que os arquivos de *backup* sejam sobrescritos ou apagados do sistema de *backup*;

XXVII - Rotina de *Backup*: procedimento de realização de cópias de segurança;

XXVIII - RPO: *Recovery Point Objective*, é o período de tempo máximo durante o qual as alterações feitas aos dados podem ser perdidas com o processo de recuperação de dados;

XXIX - RTO: *Recovery Time Objective*, é a quantidade de tempo que as operações levam para voltar ao normal, após uma parada; e

XXX - *Snapshot*: ponto de restauração de máquinas virtuais que permite o retorno a um estado anterior.

CAPÍTULO III

DAS DIRETRIZES

Art. 5º Assegurar o acesso contínuo às informações definidas por esta normativa, através de procedimentos para *backup* e restauração que observem criteriosamente o modo e a periodicidade de cada cópia dos dados.

Art. 6º Definir e informar aos usuários do IFRO quais tipos de informação são relevantes e pertinentes de salvamento em dispositivos secundários.

Art. 7º Definir os procedimentos formais de solicitação por parte do agente acerca da restauração de arquivos ou informações eventualmente perdidas.

Art. 8º Definir os procedimentos de armazenamento e descarte da mídia utilizada no processo de *backup*, bem como o período de tempo em que essas mídias permanecerão guardadas até serem reutilizadas.

Art. 9º Definir a periodicidade e os procedimentos para realização de testes de *restore* e validação dos *backups* gerados, inclusive gerando evidências, status e documentação. Garantindo assim a confiabilidade do *backup*.

Art. 10. Orientar as as rotinas de *backup* para a restauração dos dados no menor tempo possível, principalmente quando um incidente ocasionar indisponibilidade de serviços de TI.

Art. 11. Realizar levantamento de ativos com a designação do respectivo administrador do ativo e sua classificação quanto a criticidade (críticos e não críticos).

Art. 12. A coordenação responsável por gerenciar os ativos de TIC deve definir um plano de *backup* a ser elaborado pelo respectivo gestor de TIC, onde deverá ser mapeado os ativos, as criticidades, periodicidade e tempo de retenção do *backup*.

§ 1º Para cada plano de *backup* deverá haver um plano de Contingência deverá ser definido no caso do não funcionamento do esquema de *backup* definido nesta instrução Normativa.

§ 2º O plano de *backup* institucional deverá ser submetido ao comitê gestor de TI para aprovação.

CAPÍTULO IV

DO ESCOPO

Art. 13. Os dados de máquinas locais e individuais não estão cobertos por esta normativa, sendo que a proteção e cópia de segurança (*backup*) dos dados são de responsabilidade do seu usuário.

Art. 14. Todo e qualquer ativo de TI que esteja armazenando dados e que esteja sob responsabilidade da DGTI deverá ser considerado para avaliação de inclusão no processo de *backup*.

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 15. São atribuições do Administrador de *Backup*:

I - propor modificações visando o aperfeiçoamento da política de *backup*;

II - criar e manter as tarefas de *backup*;

III - configurar a ferramenta de *backup* e os clientes;

IV - criar e manter mídias;

V - testar o *backup* e a restauração;

VI - criar notificações e relatórios;

VII - verificar periodicamente os relatórios gerados pela ferramenta de *backup*;

VIII - restaurar os *backups* em caso de necessidade;

IX - gerenciar mensagens e *logs* diários dos *backups*, fazendo o tratamento dos erros de forma que o procedimento de *backup* tenha sequência e os erros na sua execução sejam eliminados;

X - fazer manutenções periódicas dos dispositivos de *backup*; e

XI - comunicar ao Administrador do Serviço os erros e ocorrências nos *backups*.

Art. 16. São atribuições do Administrador de Ativo:

§ 1º O responsável por cada ativo deverá definir quais diretórios e arquivos serão incluídos no *backup*, tendo como prioridade:

a) arquivos de configurações de sistemas operacionais e aplicativos instalados em servidores;

b) arquivos de *log* dos aplicativos, inclusive *log* da ferramenta de *backup* e restauração;

c) informações e configurações de banco de dados;

d) conteúdo de repositórios de dados associados a sistemas;

e) arquivos institucionais (documentos); e

f) arquivos de aplicações desenvolvidas pelo IFRO ou quaisquer outros não descritos neste, mas que a perda de suas informações gere prejuízo ao Instituto.

§ 2º O Administrador de *Backup* ou o Administrador de ativo que pleiteia a inclusão de um Cliente de *Backup* deverá definir quais diretórios e arquivos não serão incluídos na rotina, tendo como referência:

a) arquivos do sistema operacional ou de aplicações que podem ser recolocados através de uma nova instalação; e

b) arquivos temporários.

§ 3º Para os aplicativos e/ou bancos de dados devem ser seguidas as recomendações sugeridas pelo desenvolvedor e/ou fabricante.

§ 4º Para a especificação de um *backup*, o Administrador do Serviço deverá formalizar chamado técnico através da ferramenta de controle de atendimentos (SUAP). O chamado deverá conter as informações relativas ao *backup*, tais como: identificação do servidor e dados a serem incluídos.

Art. 17. A solicitação de restauração de dados que tenham sido salvaguardados deve ser realizada por meio das ferramentas institucionais de comunicação, e depende de prévia e formal autorização do respectivo gestor da informação.

Art. 18. A Reitora deverá prover a tecnologia e recursos adequados para o bom andamento do serviço de *backup* dos ativos institucionais.

Parágrafo único. É de responsabilidade da coordenação de TI da unidade, prover a tecnologia e recursos para a realização de *backup* dos serviços/ativos disponibilizados localmente.

CAPÍTULO VI

DAS FERRAMENTAS DE *BACKUP*

Art. 19. As rotinas de *backup* devem utilizar soluções especializadas para este fim, preferencialmente de forma automatizada.

Art. 20. Os ativos envolvidos no plano de *backup* são considerados ativos críticos para a organização.

Parágrafo único. Compete à área de TI, solicitar com as justificativas pertinentes, os recursos necessários para a plena execução do plano de *backup*.

CAPÍTULO VII

DA FREQUÊNCIA E RETENÇÃO DOS *BACKUPS*

Art. 21. Recomenda-se que os *backups* dos serviços de TI sejam realizados utilizando-se as seguintes frequências temporais:

I - diária;

II- semanal;

II - mensal; e

III - anual.

Art. 22. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados, que devem estar devidamente registrados no plano de *backup* do sistema, base de dados e repositório de arquivos.

Art. 23. Quaisquer procedimentos programados nos equipamentos computacionais físicos ou virtuais e que impliquem riscos de funcionamento com interrupção dos sistemas e serviços essenciais do IFRO, somente deverão ser executados após a realização do *backup* dos seus dados.

Parágrafo único. Em casos excepcionais em que a urgência justifique, desde que autorizados pelo Diretor de Gestão de Tecnologia da Informação, os procedimentos mencionados no caput deste artigo poderão ser executados sem a realização do *backup*.

Art. 24. As áreas finalísticas deverão contribuir com o plano de *backup*, no que compete ao prazo de retenção, avaliando a necessidade × custo benefício de sua execução.

CAPÍTULO VIII

DOS TESTES DE *BACKUP*

Art. 25. Os *backups* devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

Art. 26. Os testes de restauração dos *backups* devem ser realizados em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.

Art. 27. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de *backup* devem ser devidamente registradas no plano de *backup*.

CAPÍTULO IX

DOS DESCARTES DAS MÍDIAS

Art. 28. As mídias defeituosas ou inservíveis deverão ser encaminhadas para, procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados por terceiros e devem ter sua data de descarte registrada em controles sempre que possível para se manter uma trilha de auditoria.

Art. 29. As mídias de *backup* deverão ser substituídas de acordo com os padrões e prazos definidos pelo fabricante.

CAPÍTULO X

DAS DISPOSIÇÕES FINAIS

Art. 30. Esta Instrução Normativa deverá ser amplamente divulgada, em especial nas suas respectivas áreas de TI.

Art. 31. Esta Instrução Normativa poderá ser revisada pela DGTI a qualquer tempo, para fins de eventual atualização, quando identificada a necessidade de alteração em qualquer de seus dispositivos.

Art. 32. Os casos omissos serão dirimidos pela Diretoria de Gestão de Tecnologia da Informação – DGTI e/ou setores responsáveis em sua respectiva Unidade.

Art. 33. Esta Instrução Normativa entra em vigor na data de sua assinatura.

EDSLEI RODRIGUES DE ALMEIDA

Documento assinado eletronicamente por **Edslei Rodrigues de Almeida**, **Reitor pro tempore**, em 18/08/2022, às 09:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ifro.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1689967** e o código CRC **0DE77AEE**.

Referência: Processo nº 23243.010912/2021-75 SEI nº 1689967