INSTRUÇÃO NORMATIVA Nº 33 – GR/UFOPA, DE 10 DE FEVEREIRO DE 2023

Dispõe sobre as normas para realização, gestão, manutenção e armazenamento de cópias de segurança (backup) de informações e documentos digitais no âmbito da Universidade Federal do Oeste do Pará (Ufopa).

A **REITORA DA UNIVERSIDADE FEDERAL DO OESTE DO PARÁ**, no uso de suas atribuições conferidas pelo Decreto Presidencial de 20 de abril de 2022, publicado no Diário Oficial da União n° 75-A, Seção 2 - Edição Extra, pág. 1, em 20 de abril de 2022, e consoante as disposições legais e estatutárias vigentes;

Considerando a Resolução Consad nº 102, de 26 de setembro de 2022, que aprova a Política de Segurança da Informação e Comunicação da Universidade Federal do Oeste do Pará e dispõe, em seu art. 6º, que a política de segurança deverá conter normas complementares que contemplem a implementação de controles de segurança da informação de maneira estruturada para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos;

Considerando que o art. 15, inciso II, da Resolução Consad nº 102/2022, prevê a regulamentação, via norma complementar, do uso, processamento, armazenamento e divulgação de dados pessoais em posse da Ufopa, sob a responsabilidade do encarregado de dados ou de pessoa indicada pela Reitoria para essa função;

Considerando a Portaria Normativa nº 8/GR/UFOPA, de 5 de dezembro de 2022, que aprova o Regimento Interno do Comitê de Governança Digital da Universidade Federal do Oeste do Pará, resolve:

CAPÍTULO I
DO OBJETIVO E DO ESCOPO

Art. 1º Estabelecer normas para realização, gestão, manutenção e armazenamento de cópias de segurança (backup) de informações e documentos digitais no âmbito da Universidade Federal do Oeste do Pará (Ufopa), visando à proteção dos recursos de Tecnologia da Informação (TI) com base em boas práticas de segurança da informação.

Art. 2º A norma complementar para cópia e restauração de dados digitais deve ser utilizada como referência para todos os procedimentos relativos à cópia e recuperação de dados armazenados em meio digital.

Art. 3º Esta norma se aplica a todos os dados no âmbito da Ufopa, incluindo dados fora da Instituição, armazenados em nuvem pública ou privada.

Art. 4º Esta norma se aplica a todos os membros da comunidade acadêmica que possam ser criadores e/ou usuários de dados, a terceiros que acessam e usam na Ufopa sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade da Instituição.

Art. 5º Esta norma está alinhada com a Política de Segurança da Informação da Ufopa, com os Planos de Continuidade do Negócio (PCNs) e com as demais normas e procedimentos vigentes que façam parte do Sistema Gestor de Segurança da Informação (SGSI).

Art. 6º São incluídos em dados críticos, para os fins desta norma complementar:

I – os Sistemas de Gestão Acadêmica – SIGs (SIGRH, SIGAA, Sipac, SIGEventos, SIGAdmin, SIGEleição, seu banco de dados com todas as bases e os servidores que hospedam a aplicação);

II – os Sistemas de Processo Seletivo Regular e Especial;

III – o Sistema de Habilitação dos Processos Seletivos;

IV – o serviço de armazenamento e sincronização de arquivos (nuvem Ufopa);

V – o sistema de e-mail institucional;

VI – os sites institucionais (homepage da Ufopa, pró-reitorias, campi e institutos e diretorias);

VII – o sistema de abertura de chamados técnicos (GLPI);

VIII – o gerenciador de repositório de software (GitLab);

IX – o servidor de Web conferência e a sala de aula virtual (Big Blue Button);

X – o sistema da Comissão de Ética no Uso de Animais (CEUA);

XI – o Repositório Institucional de Produção Científica Poraquê;

XII – o Sistema de Acompanhamento de Atividades Docentes (SAAD);

XIII – Sistema Acadêmico de Apoio à Pesquisa e Extensão (SAAPE);

XIV – o Sistema Gerenciador de Projetos Redmine;

XV – o Sistema Gerenciador de Projetos OpenProject;

XVI – os servidores dos campi (PfSense/Zabbix);

XVII – O Sistema de Certificado Digital ;

XVIII – o sistema de monitoramento de redes, servidores e serviços Zabbix;

XIX – a base de dados institucional de *logins* e senhas de acesso (LDAP).

Parágrafo único. A definição dos dados críticos e o escopo desta norma complementar devem ser revisados no período máximo de 4 (quatro) anos ou, em prazo mais curto, de acordo com as necessidades definidas pelo Comitê de Governança Digital (CGD).

CAPÍTULO II
DAS RESPONSABILIDADES

Art. 7º Cabe ao Centro de Tecnologia da Informação e Comunicação (CTIC) a responsabilidade pela elaboração dos procedimentos relativos aos serviços de cópia e restauração das informações e arquivos em formato digital, bem como pelo armazenamento e transporte das mídias móveis, ficando ainda responsável por assegurar o cumprimento desta norma e de seus procedimentos.

Parágrafo único. Os analistas responsáveis pelas operações de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

Art. 8º Cabe ao CGD aprovar e manter esta norma atualizada, bem como garantir seu cumprimento mediante auditorias e verificações de conformidade.

CAPÍTULO III

DOS PRINCÍPIOS GERAIS

Art. 9° 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. 10. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 11. 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.

Art. 12. O armazenamento de backup deve ser realizado em um local distinto da infraestrutura crítica, sendo desejável que se tenha um sítio de backup em um local remoto da sede da organização para armazenar cópias, extras dos principais backups, a exemplo dos backups de dados de serviços críticos.

Art. 13. A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

Art. 14. A infraestrutura de T.I. destinada à realização de backups deve possuir uma reserva de recursos (físicos e lógicos) para realização de teste de restauração.

Art. 15. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas por meio de encriptação.

Art. 16. Os dados críticos da Ufopa, elencados no art. 6º desta norma devem ser obrigatoriamente resguardados sob um padrão mínimo de rotina de backup, o qual deve observar a correlação frequência/retenção de dados e ser estabelecido pelo CTIC em procedimento formal, de maneira a atender às especificidades de cada informação ou sistema a ser resguardado.

Parágrafo único. A inclusão de novos itens na lista de dados críticos da Ufopa será feita mediante avaliação e aprovação pelo CGD, devendo sua inserção na rotina de backup ser realizada em até 30 (trinta) dias após a publicação da norma complementar revisada.

Art. 17. Os dados não críticos da Ufopa devem ser resguardados sob um padrão mínimo a ser estabelecido pelo CTIC em procedimento formal, de maneira a atender às especificidades de cada informação ou sistema a ser resguardado.

Parágrafo único. A solicitação de salvaguarda dos dados não críticos deve ser realizada pelo responsável pelos dados, por meio de procedimento definido pelo CTIC, 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, devendo explicitar, no mínimo, os requisitos técnicos, o escopo, o tipo de backup, a frequência e a retenção.

Art. 18. Os ativos envolvidos no processo de backup são considerados críticos para a organização.

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

Art. 20. Os responsáveis pelas operações de backup devem considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI.

Art. 21. Será estipulado pelo CTIC um período de janela de backup, devendo a execução das cópias de segurança concentrar-se, preferencialmente, no período de janela de backup.

CAPÍTULO IV
DO TRANSPORTE, DO ARMAZENAMENTO E DO DESCARTE

Art. 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 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. 23. 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 concedido a pessoas autorizadas pelo CTIC.

Art. 24. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

Art. 25. A mídia de backup será retirada e descartada, garantindo que não contenha mais imagens ativas de backup, que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados e que seja fisicamente destruída antes do descarte.

CAPÍTULO V
DOS TESTES E DA RESTAURAÇÃO DOS BACKUPS

Art. 26. Os backups devem ser verificados periodicamente para a correção de erros, aplicação de melhorias nos processos e redução de riscos.

Art. 27. Os testes de restauração dos backups devem ser realizados por amostragem, em equipamentos e locais distintos dos ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.

Art. 28. O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados deverá obedecer às seguintes orientações:

I - a solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, por meio de procedimento formal;

II - a restauração de objetos somente será possível nos casos em que estes tenham sido atingidos pela estratégia de backup;

III - a solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações;
IV - o CTIC tem a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao solicitante.

Art. 29. Esta norma passa a vigorar a partir de 1° de março de 2023.

ALDENIZE RUELA XAVIER:67350020244

Assinado de forma digital por ALDENIZE RUELA XAVIER:67350020244
Dados: 2023.02.13 09:09:36 -03'00'

ALDENIZE RUELA XAVIER
Presidente do Comitê de Governança Digital
Reitora da Universidade Federal do Oeste do Pará