SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DO PARÁ
CONSELHO SUPERIOR DE ADMINISTRAÇÃO

RESOLUÇÃO N. 1.529, DE 18 DE NOVEMBRO DE 2021

Aprova a Política de *Backup* e Restauração de Dados Institucionais, no âmbito da Universidade Federal do Pará (UFPA).

O REITOR DA UNIVERSIDADE FEDERAL DO PARÁ, no uso das atribuições que lhe conferem o Estatuto e o Regimento Geral, em cumprimento à decisão da Colenda Câmara de Assuntos Administrativos e do Egrégio Conselho Superior de Administração, em Reunião Ordinária realizada no dia 18.11.2021, e em conformidade com os autos do Processo n. 041936/2021 – UFPA, procedentes do Centro de Tecnologia da Informação e Comunicação (CTIC), e, ainda,

CONSIDERANDO a Norma Técnica ABNT NBR ISO/IEC 27001:2013;

CONSIDERANDO a Norma Técnica ABNT NBR ISO/IEC 27002:2013;

CONSIDERANDO a Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso às informações;

CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) e a Política de Segurança da Informação e Comunicação da Universidade Federal do Pará.

Promulga a seguinte

R E S O L U Ç Ã O :

CAPÍTULO I

DOS OBJETIVOS

Art. 1º Esta Política tem por finalidade estabelecer normas, responsabilidades e diretrizes para realizar a criação, manutenção e restauração de cópias de segurança (*backup*) de ativos de informação, concernentes às atividades da Universidade Federal do Pará (UFPA), visando à garantia da continuidade dos serviços à comunidade acadêmica.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 2º Para efeitos desta política considera-se:

I – Data Center: Ambiente destinado aos equipamentos de *hardwares*, *softwares* e núcleo da rede da UFPA, que dão suporte às atividades de ensino, pesquisa, extensão e gestão administrativa;

II – TIC: Tecnologia da Informação e Comunicação;

III – CTIC: Centro de Tecnologia da Informação e Comunicação;

IV – SIG-UFPA: Sistema Integrado de Gestão da UFPA;

V – Computação em Nuvem: "modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou de interação com o provedor de serviços" (Glossário de Segurança da Informação, GSI/PR - 2019);

VI – Terminal: computador, *notebook*, *tablet*, *smartphone*, servidores de rede ou qualquer dispositivo com capacidade de se conectar e trocar informações através da rede da UFPA;

VII – Aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet;

VIII – Cópia de Segurança (*backup*): cópia de segurança de ativos de informação, tais como: documentos, informações administrativas e acadêmicas, dados de sistemas de informação da UFPA, entre outros;

IX – Sistemas de Informação: *software* computacional que manipula dados e gera informações;

X – Rede Institucional: Infraestrutura de comunicação de dados e voz da UFPA que abrange todos os *campi*, polos e unidades na região metropolitana;

XI – Dados pessoais: são informações relacionadas à pessoa natural identificada ou identificável. Pessoa natural é qualquer tipo de pessoa física, o que inclui alunos, servidores, colaboradores terceirizados, participantes de projetos de pesquisa, extensão e sociedade em geral. Dentre o rol de dados pessoais: estão CPF, RG, endereço, estado civil, fotos, vídeos, etc.;

XII – Dados pessoais sensíveis: é um tipo de dado pessoal relacionado à origem racial ou étnica, convicção religiosa, opinião política, biométrico, gênero, dado genético, amostra de DNA, orientação sexual, etc.;

XIII – Ativos de Informação: genericamente, informação primária compreende:

a) Informação vital para o cumprimento da missão de uma organização ou para o desempenho de seu negócio;

b) Informação estratégica necessária para o alcance dos objetivos determinados pelo direcionamento estratégico;

c) Informação de alto custo, cuja coleta, armazenamento, processamento e transmissão demandam um longo tempo ou incorrem em um alto custo de aquisição;

XIV – Natureza da Informação: considerar para esta política, a classificação das informações quanto a sua natureza, conforme disposto a seguir:

a) Dados de sistemas de informação*:* banco de dados, arquivos de configuração de servidores e serviços de TIC, sítio web, documentação, manual de usuário, material de treinamento, procedimentos de suporte ou operacional;

b) Dados administrativos: contratos, convênios, acordos, portarias, ofícios, normas, etc.;

c) Dados pessoais: nome, endereço, matrícula, cargo e quaisquer atributos de informação relevantes a respeito dos usuários que compõem o Sistema Integrado de Gestão da UFPA.

XV – Logs: dados gerados a partir de registro de eventos em sistemas de informação, na rede institucional e nos terminais da UFPA, tais como:

a) Registro de conexão: conjunto de informações referentes à data e hora de início de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

b) Registro de acesso a aplicações de TIC: conjunto de informações referentes à data e hora de uso de uma determinada aplicação de TIC a partir de um determinado endereço IP (*Internet Protocol*)*;*

c) Registro de eventos relacionados ao funcionamento de software: conjunto de informações que guardam data e hora de eventos de um determinado software;

d) Registro de eventos relacionados ao funcionamento de ativos de rede: conjunto de informações que guardam data e hora de eventos de um ativo de rede*;*

e) Registro de acesso dos usuários aos terminais: conjunto de informações referentes à data e hora de início e fim do acesso do usuário aos terminais da Instituição.

XVI – Classificação da informação: A informação deve ser classificada levando-se em consideração seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada. Os proprietários de ativos de informação devem ser os responsáveis por sua classificação. Os ativos de informação podem ser classificados de acordo com:

a) nível de importância;

b) nível de confidencialidade;

c) controle de acesso.

XVII – Retenção: é o período em que os dados devem estar salvaguardados. A retenção pode variar, de acordo com:

a) Legislação vigente: deve levar em consideração, leis, normas, decretos e instruções normativas do governo federal;

b) Natureza e classificação da informação;

c) Proporção de dados: deve levar em consideração o volume de dados produzidos e os recursos de TIC disponíveis para *backup* e sua retenção.

XVIII – Atores: São estabelecidos como atores no processo de *backup* e restauração:

a) proprietário da informação: pessoa ou unidade responsável pela informação, ainda que produzida por uma equipe de pessoas, sistema ou unidade externa. É a pessoa ou unidade autorizada a solicitar a recuperação do *backup* dos dados. Também é o responsável pela validação da classificação da informação;

b) custo diante da informação: pessoa ou unidade que zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

c) administrador de *backup*: responsável pela criação e/ou implantação do plano de backup, além de ser o responsável pela administração das atividades relacionadas aos procedimentos do backup;

d) solicitante de *backup*: pessoa que pode solicitar a restauração de dados de *backup*, ainda que não seja o proprietário dos dados, mas que seja autorizado por ele;

e) operador de *backup*: pessoa que atua junto à equipe de administração do *backup*, realizando procedimentos relacionados às rotinas de *backup*.

XIX – Janela de *backup*: é o período definido para realização do *backup*. Deve-se escolher, preferencialmente, para ser realizado em horário não comercial;

XX – Tipos de *backup*:

a) completo: realiza a cópia integral dos dados;

b) incremental: realiza a cópia das alterações ocorridas em relação ao último *backup*;

c) diferencial: realiza a cópia, cumulativamente, das alterações ocorridas desde o último *backup* completo;

d) pontual: Realiza a cópia de informações em horário dispare. As informações contidas no *backup* Pontual podem ser completas ou de informações selecionadas.

XXI – Modos de *backup*:

a) o*n-line*: ocorre sem a paralisação de atualização dos dados. O sistema provedor dos dados para *backup* continua em produção;

b) o*ff-line*: ocorre com a paralisação de atualização dos dados. O sistema provedor dos dados para *backup* fica indisponível enquanto estiver ocorrendo o *backup*.

XXII – Locais para o armazenamento do *backup*:

a) data center da UFPA: Localizado nas dependências do CTIC, responsável por armazenamento lógico em servidor dedicado para *backup* de dados;

b) nuvem computacional: armazenamento lógico em conta institucional criada em provedores de serviços de computação em nuvem utilizados pela UFPA;

c) mídias digitais: dispositivos de armazenamento que deverão ficar armazenados em cofre corta-fogo, ou em localidade diferente da origem dos dados.

XXIII – IP: "Internet Protocol" - é um número que identifica um dispositivo em uma rede (um computador, impressora, roteador, etc.);

XXIV – LGPD: Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018).

CAPÍTULO III

DO PLANO DE *BACKUP*

Art. 3º Estabelece os requisitos necessários para a manutenção do serviço de *backup*. O plano de *backup* deve atender, no mínimo, aos seguintes requisitos:

I – classificação dos dados que serão salvaguardados, levando-se em consideração o nível de importância, nível de confidencialidade e controle de acesso;

II – definição do administrador e operador(es) de *backup*;

III – definição da janela de *backup*;

IV – definição do período de retenção do *backup*;

V – definição do tipo (completo, diferencial e incremental) e modo (on-line ou off-line) de *backup*;

VI – definição de *softwares*, *scripts* e comandos para execução, restauração e monitoramento do *backup*;

VII – documentação sobre procedimentos de operação do serviço de *backup*, tais como agendamento do *backup*, restauração do *backup*, entre outros;

VIII – definição das mídias utilizadas para *backup* de acordo com requisitos de velocidade de *backup*/restauração, escalabilidade, preservação e custos;

IX – proprietário da informação e solicitante do *backup*;

X – definição e execução de testes de restauração do *backup.*

CAPÍTULO IV

DAS DIRETRIZES PARA IMPLEMENTAÇÃO DO PLANO DE *BACKUP*

Art. 4º As diretrizes desta política devem considerar, prioritariamente, os requisitos legais, os objetivos estratégicos, a estrutura e a finalidade da instituição.

Art. 5º É necessário disponibilizar o nível apropriado de proteção física e ambiental às informações de *backup* contidas nas mídias de armazenamento.

Art. 6º É necessário haver uma redundância das mídias de *backup* e que elas estejam fisicamente separadas a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal.

Art. 7º As mídias de *backup* devem ser testadas regulamente para garantir que elas sejam confiáveis.

Art. 8º As cópias de *backup* devem ser testadas regularmente para garantir que as ferramentas de backup estejam funcionando adequadamente e que os dados salvaguardados estejam íntegros.

Art. 9º A realização do *backup* ocorrerá diariamente ou agendada, preferencialmente, fora do horário comercial, para não ocasionar problemas de acesso e atualização dos dados.

Art. 10. A solicitação de restauração de dados está sujeita à verificação das permissões de proprietário e de solicitante do *backup*.

Art. 11. A restauração do *backup* está sujeita à disponibilidade do dado dentro do período de retenção determinado no plano de *backup*.

Art. 12. O *backup* de dados confidenciais e sensíveis será criptografado.

CAPÍTULO V

DAS RESPONSABILIDADES PARA O *BACKUP* DOS DADOS INSTITUCIONAIS

Art. 13. Ao CTIC, enquanto órgão central de TIC na UFPA, compete a salvaguarda dos dados de serviços de TIC desenvolvidos, mantidos ou gerenciados, por suas subunidades tais como:

I – SIG-UFPA (SIGAA, SIPAC, SIGRH, SIGED, SIGEleição, SIGADMIN, SAGITTA, PTA E COC);

II – Sistemas de internet como e-mail, servidores web, DNS, DHCP, LDAP, VPN, NTP, CAFe, bancos de dados, etc.;

III – sites web institucionais vinculados à Administração Superior e hospedados nos servidores do CTIC: Portal da UFPA, SEGE, Pró-Reitorias, Procuradoria, Prefeitura, *Campi* do interior e órgãos suplementares;

IV – regras e configuração dos *firewalls* de borda e perímetro da UFPA;

V – configurações do roteador de borda e núcleo da rede institucional;

VI – configurações do serviço de rede sem fio institucional;

VII – arquivos de configurações dos serviços de TIC gerenciados pelo CTIC;

VIII – configurações da rede de telefonia institucional;

IX – Logs:

a) de sistemas de informação mantidos e gerenciados pelo CTIC;

b) de conexão à internet a partir de ou para os terminais da Instituição;

c) de acesso aos sistemas de internet gerenciados pelo CTIC;

d) de ativos de rede gerenciados pelo CTIC.

Art. 14. As unidades/subunidades acadêmicas ou administrativas são as responsáveis pela elaboração e execução dos seus planos de *backup*, como também, pela salvaguarda dos dados sob sua responsabilidade, tais como:

I – dados institucionais de suas contas dos serviços de e-mail e armazenamento em nuvem computacional;

II – repositórios e acervos digitais de arquivos (documentos, imagens ou multimídia);

III – arquivos de configuração de servidores (físicos ou virtuais) e sistemas de informação sob sua responsabilidade;

IV – banco de dados desenvolvidos, implantados ou gerenciados sob sua responsabilidade;

V – arquivos de configuração e base de dados dos seus sites institucionais;

VI – arquivos de configuração e código fonte das soluções de *softwares* desenvolvidas, implantadas ou gerenciadas sob sua responsabilidade;

VII – é de responsabilidade das unidades e subunidades a classificação das informações de acordo com esta política ou orientação do CTIC;

VIII – a classificação das informações é uma etapa que antecede o plano de *backup* e visa identificar o valor e criticidade dos dados para a Instituição;

IX – quando uma unidade/subunidade realizar por conta própria a coleta de dados pessoais, através de formulários eletrônicos, aplicações, planilhas, documentos, etc., é sua a responsabilidade pela guarda e proteção dos dados. Portanto, deverá tratar e zelar pela segurança dos dados coletados de acordo com os princípios e diretrizes da LGPD.

Art. 15. Aos usuários que utilizam os terminais, redes e sistemas de informações institucionais, compete:

I – não armazenar documentos, *softwares*, fotos, vídeos, áudios, informações sigilosas e pessoais nos terminais da UFPA, pois a salvaguarda de quaisquer dados digitais nos

equipamentos e servidores de arquivos destina-se, prioritariamente, a manter e a proteger informações de interesse da instituição;

II – a UFPA não é responsável pela salvaguarda dos arquivos, dados sigilosos e pessoais dos usuários, armazenados em seus terminais.

Art. 16. Os dados pessoais e dados sensíveis dos usuários, de acordo com o art. 7º, inciso II e III e art. 11º, inciso II, "a" e "b", da LGPD, contidos nos serviços de TIC inclusos no plano de *backup* do CTIC, serão processados e armazenados seguindo procedimentos de controle de acesso e segurança da informação para garantir ao máximo o não vazamento das informações.

Art. 17. Os dados pessoais e dados sensíveis dos usuários coletados pelo Sistema Integrado de Gestão da UFPA (SIG-UFPA) são tratados, armazenados e salvaguardados conforme plano de *backup* do CTIC, seguindo a natureza e classificação da informação definidas nesta política.

Art. 18. As unidades e subunidades que não dispõem de infraestrutura ou pessoal para implementação de seu plano de backup, devem solicitar apoio ao CTIC, que avaliará a execução do plano de *backup* bem como a salvaguarda dos dados de acordo com a classificação da informação, infraestrutura de recursos de TIC e corpo técnico disponíveis.

CAPÍTULO VI

DAS CONSIDERAÇÕES FINAIS

Art. 19. Compete ao Comitê de Segurança da Informação (CSI) a elaboração de normas técnicas que visem a atender a esta política.

Art. 20. Os casos omissos ou não previstos nesta Resolução serão tratados pelo Comitê de Governança Digital.

Art. 21. Esta Resolução se aplica a todos os usuários, às unidades e às subunidades da UFPA.

Art. 22. Esta Resolução entra em vigor na data de sua aprovação.

Reitoria da Universidade Federal do Pará, em 18 de novembro de 2021.

EMMANUEL ZAGURY TOURINHO

R e i t o r

Presidente do Conselho Superior de Administração