MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO DELTA DO PARNAÍBA
CAMPUS MINISTRO REIS VELLOSO

RESOLUÇÃO CONSUNI N° 64 DE 7 DE MARÇO DE 2024

Aprova a Política de Backup e Restauração de Dados no âmbito da Universidade Federal do Delta do Parnaíba.

O REITOR DA UNIVERSIDADE FEDERAL DO DELTA DO PARNAÍBA e PRESIDENTE DO CONSELHO UNIVERSITÁRIO - CONSUNI, no uso de suas atribuições, tendo em vista decisão do mesmo Conselho em reunião de 1º de fevereiro de 2024, e considerando:

- o Processo nº 23855.007678/2023-85

RESOLVE:

Art. 1º Regulamentar a Política de Backup e Restauração de Dados da Universidade Federal do Delta do Parnaíba, conforme disposto no anexo único desta Resolução.

Art. 2º Esta Resolução entra em vigor na data de sua publicação, conforme disposto no Parágrafo Único, do art. 4º, do Decreto nº 10.139, de 28 de novembro de 2019, justificando-se a urgência na excepcionalidade operacional da atividade administrativa da PROTIC/ UFDPar e a necessidade de sua regulamentação.

João Paulo Sales Macedo
Reitor

ANEXO ÙNICO DA RESOLUÇÃO CONSUNI N° 64 DE 17 DE MARÇO DE 2024

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Seção I - Do Objetivo

Art. 1° A Política de Backup e Recuperação de Dados Digitais tem por objetivo estabelecer normas, diretrizes, responsabilidades e competências para realizar a criação, manutenção e restauração de cópias de segurança (backup) com proteção e disponibilidade dos dados digitais da UFDPar, sob governança e responsabilidade da Pró-reitora de Tecnologia da Informação e Comunicação – PROTIC da UFDPar.

Parágrafo único. O procedimento de backup não deve ser confundido ou utilizado como uma estratégia de temporalidade, guarda ou preservação de longo prazo, mas para a recuperação de desastres, perda de dados originados por apagamentos acidentais ou corrupção de dados.

Seção II - Do Escopo

Art. 2° Essa política está limitada nas informações ou dados armazenados nos servidores institucionais sob a tutela e guarda da Pró-reitora de Tecnologia da Informação e Comunicação (PROTIC) da Universidade Federal do Delta do Parnaíba.

Art. 3° Os dados e máquinas locais e individuais não têm cobertura por essa política, sendo que a proteção e cópia de segurança (backup) dos dados são de responsabilidade do usuário.

CAPÍTULO II

DOS PRINCÍPIOS GERAIS

Art. 4° Essa política é norteada pela Política de Segurança da Informação e Comunicação da UFDPar (PoSIC), que considera os preceitos básicos da segurança da informação, a confidencialidade, a legalidade, a autenticidade, o não-repúdio, a conformidade, o controle de acesso, a auditabilidade, a integridade e a disponibilidade.

Art. 5º Para proteção de informação e, em atendimento aos padrões de segurança e regulamentações governamentais, estabelecer políticas de segurança não deixam a universidade livre de erros humanos, ataques de vírus, catástrofe natural, e outras ameaças.

Art. 6º 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. 7º As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 8º 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. 9º O armazenamento de backup, se possível, será realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.

Art. 10 A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

Art. 11 As rotinas de backup devem manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.

Art. 12 Em situações em que a confidencialidade é importante, as cópias de segurança devem ser protegidas por encriptação.

CAPÍTULO III

CONCEITOS E DEFINIÇÕES

Art. 13 Para efeitos desta política considera-se:

I- Cópia de Segurança (backup): 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;

II- Data Center: Ambiente destinado aos equipamentos de hardwares, softwares e núcleo da rede da UFDPar, que dão suporte às atividades de ensino, pesquisa, extensão e gestão administrativa;

III- TIC: Tecnologia da Informação e Comunicação;

IV- SIG - UFDPar: Sistema Integrado de Gestão da UFDPar;

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 por meio da rede da UFDPar;

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

VIII- Restore: recuperação dos arquivos existentes em um backup;

IX- 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;

X- 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;

XI- 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;

XII- Sistema de Informação: software computacional que manipula dados e gera informações;

XIII- Rede Institucional: Infraestrutura de comunicação de dados e voz da UFDPar;

XIV- 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.;

XV- 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.;

XVI- 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.

XVII- 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 UFDPar.

XVIII- Logs: Dados pessoais: nome, endereço, matrícula, cargo e quaisquer atributos de informação relevantes a respeito dos usuários que compõem o Sistema Integrado de Gestão da UFDPar.

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 dado;

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.

XIX- 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.

XX- 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.

XXI- 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.

b) custodiante da informação: pessoa ou unidade com 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.

c) administrador de Backup: servidor responsável pelos procedimentos de configuração criação e/ou implantação do plano de backup, execução, monitoramento, testes dos procedimentos de backup e restore;

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.

XXII- Janela de Backup: é o período definido para realização do backup. Deve- se escolher, preferencialmente, realizar em horário não comercial;

XXIII- Tipos de backup:

a) completo ou full: 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.

XXIV- Modos de Backup:

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

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

XXV- Locais para o armazenamento do backup:

a) data center da UFDPar: Localizado nas dependências do STI, 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 UFDPar;

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

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

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

Seção II - Das Instâncias Administrativas

Art. 14 Para os efeitos desta Política e das normas dela originadas, entende-se por:

I- Reitoria: é o órgão executivo superior, ao qual compete dirigir, administrar, planejar, coordenar, estabelecer parcerias e fiscalizar as atividades da universidade;

II- Comitê de Governança Digital (CGD): Portaria nº 449, de 20 de julho de 2023. Comitê responsável por elaborar e revisar periodicamente a PoSIC e normas relacionadas, submetendo à aprovação da Reitoria, entre outras competências; participa e orienta o planejamento dos investimentos e Tecnologia da Informação e Comunicações de acordo com as diretrizes do Plano de Desenvolvimento Institucional (PDI) em execução; estabelece as políticas, diretrizes e prioridades na área de Tecnologia da Informação e Comunicações (TIC); promove e estimula o desenvolvimento da Tecnologia da Informação e Comunicações no âmbito da UFDPar; elabora, acompanha e avalia o Plano Diretor de Tecnologia da Informação

e Comunicação (PDTIC) para a UFDPar; elabora, acompanha e avalia as Políticas de Segurança da Informação e Comunicações da UFDPar.

III- Diretoria de Sistemas e Infraestrutura de TIC (DSITIC): instância administrativa/executiva responsável pelo desenvolvimento, implantação e manutenção dos ativos de sistema de informação;

IV- Coordenadoria de Infraestrutura e Segurança da Informação: responsável por monitorar e analisar o cumprimento das políticas, normas e procedimentos de segurança dos sistemas de informação e comunicações, além de elaborar estratégias para comunicação, publicação e divulgação das políticas, normas e procedimentos de segurança dos sistemas de informação e comunicações;

V- Coordenadoria de Sistemas: Coordena a execução das atividades inerentes à Sistemas para a implementação das políticas de segurança da informação (e demais políticas que envolvam o uso de sistemas) seguindo as normas vigentes;

VI- Divisão de Datacenter e Segurança da informação: Gerencia e executa as Políticas de Backup nas bases de dados da instituição, em especial, as gerenciadas pela PROTIC;

VII- Divisão de Bancos de Dados: Implementa a estratégia de Backup e Recovery dos bancos de dados da instituição.

CAPÍTULO III

DO PLANO DE BACKUP

Art. 15 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 offline) 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. 16 As diretrizes desta política devem considerar, prioritariamente, os requisitos legais, os objetivos estratégicos, a estrutura e a finalidade da instituição.

Art. 17 É necessário disponibilizar o nível apropriado de proteção física e ambiental às informações de backup contidas nas mídias de armazenamento.

Art. 18 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. 19 As mídias de backup devem ser testadas regulamente para garantir que elas sejam confiáveis.

Art. 20 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. 21 A realização do backup ocorrerá diariamente ou agendada, preferencialmente, fora do horário comercial, para não ocasionar problemas de acesso e atualização dos dados.

Art. 22 A solicitação de restauração de dados está sujeita à verificação das permissões de proprietário e de solicitante do backup.

Art. 23 A restauração do backup está sujeita à disponibilidade do dado dentro do período de retenção determinado no plano de backup.

Art. 24 O backup de dados confidenciais e sensíveis será criptografado.

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 25 À DSITIC compete a salvaguarda dos dados de serviços de TIC desenvolvidos, mantidos ou gerenciados, por suas subunidades tais como:

I- SIG-UFDPar (todos os módulos);

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 STI / UFDPar: Portal da UFDPar, Pró-Reitorias, Procuradoria, Prefeitura e unidades vinculadas externas e internas;

IV- regras e configuração dos firewalls de borda e perímetro da UFDPar;

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;

VIII- configurações da rede de telefonia da UFDPar;

IX- Logs:

a) de sistemas de informação;

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

c) de acesso aos sistemas de internet;

d) de ativos de rede.

Art. 26 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- a classificação das informações de acordo com esta política ou orientação da DSITIC;

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. 27 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 UFDPar, 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 UFDPar não é responsável pela salvaguarda dos arquivos, dados sigilosos e pessoais dos usuários, armazenados em seus terminais.

Art. 28 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 da DSITIC / UFDPar, serão processados e armazenados seguindo procedimentos de controle de acesso e segurança da informação para garantir ao máximo o não vazamento das informações.

Art. 29 Os dados pessoais e dados sensíveis dos usuários coletados pelo Sistema Integrado de Gestão da UFDPar (SIG-UFDPar) são tratados, armazenados e salvaguardados conforme plano de backup, seguindo a natureza e classificação da informação definidas nesta política.

Art. 30 É de responsabilidade do usuário que necessitar recuperar arquivos, entrar em contato com o setor de suporte ao usuário, registrar a solicitação por meio do sistema de chamados à PROTIC no endereço eletrônico "cs.ufdpar.edu.br" informando, obrigatoriamente, o usuário, o setor, e-mail, título do chamado, a descrição e anexos de arquivos (quando houver). A solicitação será atendida conforme a classificação da informação, infraestrutura de recursos de TIC e corpo técnico disponível.

Art. 31 A retenção dos backups de TI críticos da UFDPar deverá observar os seguintes prazos:

I- periodicidade diária: 7 dias;

II- periodicidade semanal: 4 semanas;

III- periodicidade mensal: 12 meses; e

IV- periodicidade anual: 5 anos.

§ 1º Em casos especiais, o gestor do ativo de informação poderá definir, em conjunto com os administradores de backup, prazos diferenciados para retenção dos backups.

§ 2º Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada.

Art. 32 Os serviços de TI não críticos da UFDPar devem ser resguardados sob padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I- Diária: 1 mês;

II- Semanal: 2 meses;

III- Mensal: 6 meses;

IV-Anual: 2 anos

§ 1º Em casos especiais, o gestor do ativo de informação poderá definir, em conjunto com os administradores de backup, prazos diferenciados para retenção dos backups.

§ 2º Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada.

Art. 33 Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

Art. 34 A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelo responsável, com a anuência prévia e formal da DSITIC, 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 do backup (diária, semanal, mensal, anual);

IV- Retenção;

V- RPO;

VI- RTO.

Art. 35 A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao administrador de backup. A aprovação para execução da alteração depende da anuência da DSITIC.

Art. 36 Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

Art. 37 A solicitação de backup e recuperação de objetos deverá obedecer aos artigos 34º, 35º e 36º desta resolução e deverá ser realizado por meio de chamado pela ferramenta de controle de atendimentos disponibilizado pela PROTIC pelo link (cs.ufdpar.edu.br).

Art. 38 O administrador de backup da DSITIC deverá ser capacitado para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

Parágrafo único. O administrador de backup será designado dentre os servidores da DSITIC.

Art. 39 São atribuições dos administradores de backup:

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

II- criar e manter os backups;

III- configurar a ferramenta de backup, com periodicidade, conteúdo e relatórios;

IV- preservar as mídias de backup;

V- testar os procedimentos de backup e restore;

VI- executar procedimentos de restore;

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

VIII- realizar manutenções periódicas dos dispositivos de backup;

IX- comunicar o gestor sobre os erros e ocorrências nos backups dos ativos de informação e de software sob sua responsabilidade;

X- documentar os procedimentos dos incisos II a IX deste artigo; e

XI- registrar a execução dos procedimentos elencados neste artigo, visando a manutenção de histórico de ocorrências;

XII- realizar testes periódicos de restauração, no intuito de averiguar os processos de backup e estabelecer melhorias;

XIII- avaliar a viabilidade técnico-econômica de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso;

XIV- Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;

XV- Definir os procedimentos de restauração e neles auxiliar;

XVI- Tomar medidas preventivas para evitar falhas;

XVII- Reportar imediatamente à DSITIC os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de backups;

Art. 40 São atribuições do responsável técnico pelo serviço de TICs da UFDPar:

I- Solicitar, ao administrador de backup, a salvaguarda dos dados referentes aos serviços de TIC, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

a) escopo (dados digitais a serem salvaguardados);

b) frequência temporal de realização do backup (diária, semanal, mensal, anual);

c) retenção;

d) pontos de restauração.

II- Validar o resultado das restaurações eventualmente solicitadas; e

III- Validar o resultado dos testes de restauração dos backups.

Art. 41 A criação e operação de backups deverão obedecer às seguintes diretrizes:

I- o backup deverá ser programado para execução automática em horários de menor ou nenhuma utilização dos sistemas e da rede;

II- os administradores de backups deverão certificar-se da conclusão bem-sucedida dos backups, analisando, se for o caso, os arquivos de log, para garantir o resultado da operação;

III- em caso de problemas na operação de backups, as causas deverão ser analisadas, reparadas e, quando necessário, um novo backup deverá ser imediatamente realizado;

IV- as mídias utilizadas no processo de realização do backup deverão possuir identificação suficiente para permitir, direta ou indiretamente, a localização e extração das informações nelas armazenadas;

V- os backups deverão ser armazenados em ao menos duas cópias, em mídias diferentes;

VI- os backups dos sistemas críticos, deverão ter cópias mantidas em locais fisicamente distintos, bem como deverá ser mantida uma cópia offline, em dispositivo de proteção de mídia;

VII- quando as cópias de segurança forem armazenadas em mais de um local físico, a distância entre os dois locais deve ser suficiente para escapar dos danos decorrentes de desastre ocorrido em um deles, e;

VIII- as cópias de segurança deverão ser armazenadas em um local diferente do servidor físico onde são utilizadas em produção.

Art. 42 O backup deverá ser realizado com base nas seguintes disposições:

I- os backups quinzenais, mensais e anuais deverão ser realizados, preferencialmente, na modalidade completo, de forma a poderem recuperar integralmente todas as informações sem a necessidade de outros backups;

II- o backup semanal ocorrerá, preferencialmente, aos sábados, referindo-se à semana que se encerra;

III- o backup mensal ocorrerá, preferencialmente, no primeiro dia de cada mês, referindo-se ao mês anterior;

IV- o backup diário ocorrerá, preferencialmente, fora do horário de expediente, na modalidade completo e incremental de forma a poder reverter os dados recentes de forma mais rápida;

V- em caso de falha em algum procedimento de backup ou impossibilidade da sua execução, os administradores de backup deverão adotar as providências no sentido de salvaguardar as informações através de outro mecanismo, como por

exemplo, cópia dos dados para outro servidor ou execução do backup em horário de produção; e

VI- as bases de dados dos sistemas críticos deverão ser realizadas pelo menos uma vez ao dia, na modalidade incremental, para reduzir a perda de transações.

CAPÍTULO VI

DOS PROCEDIMENTOS DE RESTORE

Art. 43 O procedimento de restore deverá obedecer ao seguinte processo:

I- o gestor do ativo de informação que precise recuperar informações deverá solicitar formalmente, por meio definido pela unidade responsável pelo Data Center onde o ativo se encontra, justificando o motivo da solicitação; e

II- a solicitação prevista no inciso anterior será encaminhada aos administradores de backup para que realizem a recuperação e comuniquem o resultado do procedimento.

Parágrafo único. É vedado o restore diretamente nos ambientes de produção, exceto em situações de recuperação de desastre ou plano de contingência.

CAPÍTULO VII

DO DESCARTE E SUBSTITUIÇÃO DAS MÍDIAS DE BACKUP

Art. 44 Os administradores de backup deverão respeitar os critérios definidos pelos fabricantes para assegurar a validade e a qualidade das mídias utilizadas na realização de backups.

Art. 45 No caso de substituição da solução utilizada nos backups, as informações contidas nas mídias da antiga solução deverão ser transferidas em sua totalidade para as mídias da nova solução.

Parágrafo Único. A solução antiga somente poderá ser completamente desativada após a confirmação, por intermédio do teste de restore, de que todas as informações foram transferidas para a nova solução implementada.

Art. 46 O descarte das mídias utilizadas para backup deve ser realizado de forma a impossibilitar a recuperação total ou parcial das informações.

Art. 47 A DSITIC é responsável, antes do descarte, inutilizar mídias defeituosas, ou aquelas que não serão mais utilizadas, a fim de impossibilitar a recuperação dos dados por terceiros.

CAPÍTULO VIII

DOS PADRÕES OPERACIONAIS

Seção I - Princípios Gerais

Art. 48 A administração dos backups deverá ser orientada para que os trabalhos respeitem as janelas para execução, inclusive com previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art. 49 O serviço de backup deverá ser orientado para a restauração das informações no menor tempo possível, principalmente quando houver indisponibilidade de serviços que dependam da operação de recuperação de dados digitais e sejam considerados críticos para a UFDPar.

Seção II - Das Frequências e Retenção dos Dados

Art. 50 Os serviços de TIC deverão ser resguardados sob um padrão mínimo, estabelecido no Plano de backup da UFDPar, considerando o tipo de dado armazenado.

Art. 51 A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança.

Parágrafo único - Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de backup.

Art. 52 Os procedimentos de backup deverão ser atualizados quando houver:

I- Novas aplicações desenvolvidas;

II- Novos locais de armazenamento de dados ou arquivos;

III- Novas instalações de bancos de dados;

IV- Novos aplicativos instalados.

Seção III - Das Unidades de Armazenamento

Art. 53 As unidades de armazenamento utilizadas na salvaguarda dos dados digitais deverão 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, e;

VI- A vida útil da unidade de armazenamento de backup.

Art. 54 Poderão ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável pelos responsáveis pelos serviços de TIC.

Art. 55 As unidades de armazenamento dos backups deverão ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo administrador de backup.

Art. 56 Além das validações automatizadas, os pontos de restauração dos sistemas institucionais utilizados no território da UFDPar, deverão passar por inspeção e validação manual.

CAPÍTULO IX

DOS TESTES DE BACKUP

Art. 57 Os backups serão verificados periodicamente:

I- Diariamente, os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup;

II- Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha;

III- A DSITIC manterá registros de backups e testes de restauração para demonstrar conformidade com esta política;

IV- Os testes devem ser realizados em todos os backups produzidos independente do ambiente.

Art. 58 Os testes de restauração dos backups devem ser realizados, por amostragem uma vez por semana, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos.

Art.59 Deverá ser verificado se foi atendido os níveis de serviço pactuados, tais como os *Recovery Time Objective* – RTOs.

Art.60 Os registros deverão conter, no mínimo, 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.

Art. 61 Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo Comitê de Governança Digital da UFDPar.

Art. 62 Os casos omissos serão resolvidos pelo Comitê de Governança Digital da UFDPar, no âmbito das suas competências.

Art. 63 Esta política será reavaliada a cada 2 (dois) anos ou sempre que surgirem novos requisitos tecnológicos, corporativos e/ou legais.

Art. 64 A implementação dessa política está sujeita a disponibilidade de recursos financeiros e humanos.

Art. 65 Casos excepcionais ou não previstos serão tratados pela Direção do Centro de Processamento de Dados.

Art. 66 Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

Art.67 A DSITIC deve fornecer termo de concordância que inclua uma seção de confirmação do entendimento e acordo para cumprir a política, assinada e datada, conforme segue: "Eu li e entendi a Política de backup e Restauração de Dados Digitais da UFDPar. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais e/ou disciplinares de acordo com as leis aplicáveis e as normas internas da UFDPar".

Art. 68 Compete ao Comitê de Segurança da Informação (CSI) a elaboração de normas técnicas que visem a atender a esta política.

Art. 69 Os casos omissos ou não previstos nesta Resolução serão tratados pelo Comitê de Segurança Digital (CSD) e, se necessário, pelo Conselho Universitário da UFDPar.

Art. 70 Esta Resolução se aplica a todos os usuários, às unidades e às subunidades da UFDPar