MINISTÉRIO PÚBLICO DA UNIÃO
ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DA UNIÃO
DIRETORIA GERAL

PORTARIA Nº 052, DE 30 DE MARÇO DE 2023.

Regulamenta a Política de Backup e Retenção de Dados na Escola Superior do Ministério Público da União.

O **DIRETOR-GERAL DA ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DA UNIÃO**, no uso das atribuições que lhe foram conferidas pelos incisos I, II e XIV do art. 7º do Estatuto da ESMPU, aprovado pela Portaria PGR/MPU nº 95, de 20 de maio de 2020,

CONSIDERANDO as diretrizes estratégicas da Política de Segurança Institucional, Portaria ESMPU n. 92/2021;

CONSIDERANDO a Política de Segurança da Informação nos Meios de Tecnologia da Informação (PSIMTI), Portaria ESMPU n. 161/2021;

CONSIDERANDO a Política de Gestão Documental e Memória, Portaria n. 130/2022;

CONSIDERANDO obrigatoriamente o Catálogo de Sistemas/Serviços administrativos e acadêmicos da ESMPU, disponível na intranet, como fonte para definição das diretrizes das rotinas de backup e restauração;

CONSIDERANDO que a perda dos ativos de dados da Escola pode significar graves dificuldades administrativas e acadêmicas, é necessário assegurar a continuidade de negócio através de uma política de cópia de segurança que observe criteriosamente o modo e a periodicidade de cópia dos dados pertencentes aos seus serviços computacionais, bem como definir procedimentos para solicitação de serviço de recuperação dos ativos de dados eventualmente indisponíveis;

CONSIDERANDO também que deve ser definida a periodicidade que as mídias de cópia de segurança permanecerão guardadas até serem reutilizadas ou destruídas; resolve

Art. 1° Instituir a Política de Backup e Retenção de Dados no âmbito da ESMPU.

Art. 2° Esta política tem como objetivo estabelecer as diretrizes dos processos de cópias de segurança e retenção de dados, em lista não exaustiva, visando a garantir a segurança, integridade e recuperação das informações.

CAPÍTULO I

DEFINIÇÕES E FUNÇÕES

Art. 3° Para o disposto neste ato considera-se:

I - administrador de Banco de Dados: responsável técnico pelo serviço de instalação, configuração e gerenciamento do ambiente de banco de dados;

II - administrador da Virtualização: responsável técnico pelo serviço de instalação, configuração e gerenciamento dos ambientes virtuais;

III - backup: atividade que consiste em realizar cópias de segurança de dados digitais de um ambiente físico ou virtual, documentos, softwares ou qualquer arquivo digital, com o intuito de recuperá-los em caso de perdas acidentais ou falhas no sistema em que os arquivos estão armazenados, tendo as seguintes tipificações:

a) backup Completo (Full): modalidade de backup na qual todos os dados são copiados integralmente;

b) backup Diferencial: modalidade de backup na qual somente os arquivos novos e modificados desde o último backup completo são copiados;

c) backup Incremental: modalidade de backup na qual somente os arquivos novos e modificados desde o último backup realizado;

d) backup de primeiro nível: armazenamento do backup em disco local;

e) backup de segundo nível: armazenamento do backup em mídia externa, exemplo: fita magnética;

f) backup off-site: estratégia de backup que abrange a replicação de dados do backup em um local geograficamente separado do ambiente de produção interno;

IV - catálogo de Serviços: Listagem com todos os serviços ativos oferecidos pela STI que necessitam ou não de backup;

V - colaborador: integrante do quadro de funcionários da ESMPU;

VI - equipe de Backup e Restauração de Dados: equipe técnica responsável pelos procedimentos de configuração, execução, monitoramento e testes de backup e restauração de dados;

VII - mídia: meio físico no qual efetivamente armazenam-se os dados de um backup (fita magnética, disco rígido etc.);

VIII - retenção: período em que o conteúdo da mídia de backup deve ser preservado;

IX - recuperação de desastre: estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;

X - responsável pelo Serviço: colaborador responsável pela operação de determinados serviços ou recursos computacionais da ESMPU;

XI - RPO (Recovery Point Objective): diz respeito à quantidade de informação que é tolerável perder, no caso de indisponibilidade nos serviços.

XII - RTO (Recovery Time Objective): diz respeito à quantidade de tempo que as operações levam para estarem acessíveis, após uma indisponibilidade; e

XIII - serviço de backup: todo ativo que possui informações ou dados que foram incluídos na rotina de backup em conformidade com as regras definidas.

CAPÍTULO II

DOMÍNIO DE DADOS

Art. 4° Os serviços que serão contemplados nesta política de backup e retenção estarão divididos em seis categorias, para que cada tipo de dado possa ser tratado com maior especificidade, sendo eles de:

I - infraestrutura de Rede;

II - virtualização;

III - banco de Dados;

IV - compartilhamento de Arquivos;

V - sistemas Administrativos; e

VI - sistemas Acadêmicos.

CAPÍTULO III

ATRIBUIÇÕES E RESPONSABILIDADES

Art. 5° O responsável pelo Núcleo de Segurança de Tecnologia da Informação será o líder da Equipe de Backup e Restauração de Dados, delegando assim as atribuições de manter a política e procedimentos relativos aos serviços de backup e restauração, bem como de guardar as mídias e assegurar o cumprimento das normas aplicáveis.

§1º Será indicado um colaborador do Núcleo de Operações e Produção de Serviços - NOPS, um colaborador do Núcleo de Banco de Dados - NUBAN e um colaborador do Núcleo de Políticas de Gestão Documental - NUGED para compor a Equipe de Backup e Restauração de Dados com objetivo de auxiliarem no processo de operacionalização de cópia e restauração.

§2º O líder da Equipe de Backup e Restauração de Dados poderá solicitar auxílio a outras áreas pertinentes para melhor configuração dos procedimentos de cópia e restauração.

Art. 6° São atribuições da Equipe de Backup e Restauração de Dados:

I - propor o aperfeiçoamento da Política de Backup e Retenção de Dados;

II - configurar e operar os serviços e os ambientes de cópia e restauração;

III - criar e manter os backups conforme a classificação da criticidade dos serviços;

IV - executar os procedimentos de restauração conforme a necessidade;

V - criar e testar cenários de restauração de acordo com a classificação de criticidade dos backups, no intuito de otimizar as atividades envolvidas e reduzir o tempo de indisponibilidade;

VI - gerenciar as mídias necessárias;

VII - criar notificações e relatórios de backup;

VIII - criar relatórios de execução de restauração;

IX - gerenciar mensagens, logs ou relatórios diários de 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;

XI - fazer o carregamento dos backups programados para as mídias necessárias;

XII - fazer o armazenamento das mídias de backup no lugar adequado e determinado;

XIII - realizar o correto descarte de mídias, quando necessário; e

XIV - definir quais diretórios e arquivos não serão inclusos no backup, ponderando custos ou possíveis prejuízos e tendo como referência:

a) arquivos do sistema operacional ou de aplicações que possam ser obtidos através de uma nova instalação;

b) arquivos temporários;

c) arquivos salvos nas unidades locais das estações de trabalho;

d) arquivos particulares dos usuários; e

e) arquivos ou diretórios que sejam objetos de discussão técnica da Equipe de Backup e Restauração de Dados, com a devida justificada de suas exclusões.

Art. 7° Todo e qualquer serviço a ser anexado em backup deverá ser ponderado e estudado antes de sua inclusão. Após incluído, obrigatoriamente deverá seguir os procedimentos de cópia e restauração estabelecidos no Capítulo IV desta política.

Parágrafo único. Para os aplicativos e bancos de dados de terceiros devem ser seguidas as recomendações sugeridas pelo desenvolvedor ou fabricante, observado o cumprimento do disposto nesta Política.

Art. 8° Os procedimentos de backup deverão ser atualizados mediante solicitação feita pelo Responsável do Serviço e enviada à Equipe de Backup e Restauração de Dados quando houver:

I - novas aplicações desenvolvidas;

II - novos locais de armazenamento de dados;

III - novos arquivos com relevância para funcionamento de um serviço;

IV - novas instalações de bancos de dados; e

V - novos aplicativos instalados.

Art. 9° Para cada aplicação/serviço com a classificação de criticidade definida no catálogo de serviços:

§1º O backup deverá ser programado prioritariamente na ferramenta de backup ou em dispositivos definidos pela Equipe de Backup e Restauração de Dados com este objetivo;

§2º Todos os backups criados deverão ser posteriormente testados conforme o nível de criticidade adotado.

Art. 10. A ESMPU deverá disponibilizar uma infraestrutura capaz de atender ao modelo de continuidade da instituição em nível de recuperação de desastres, a fim de que se torne viável à STI a implementação de uma estratégia de backup off-site.

CAPÍTULO IV

DA RETENÇÃO DE DADOS E PROCEDIMENTOS DE BACKUP E RECUPERAÇÃO

Art. 11. A retenção de dados, procedimentos de backups e suas restaurações serão regulamentadas tecnicamente por Procedimento Operacional Padrão a ser definido pela Equipe de Backup e Restauração de Dados observando a classificação feita no catálogo de serviços. Nele estarão os critérios como: a periodicidade do backup, tempo de recuperação, tempo de retenção,

reuso de mídias e descarte (conforme Tabela de Temporalidade e Destinação da ESMPU), determinações legais aplicáveis, observando a capacidade operacional e financeira da instituição.

CAPÍTULO V

DOS AMBIENTES ANÁLOGOS AOS PRODUTIVOS

Art. 12. Os backups dos ambientes de produção (aplicações, arquivos, dados e configurações), virtualizados ou não, com a finalidade de criação de ambientes de testes, desenvolvimento, controle de qualidade ou homologação não seguirão os parâmetros de periodicidade e retenção previstos no Capítulo IV;

Art. 13. Para cópias de aplicações ou dados de produção serão considerados os seguintes aspectos:

I - para cópia de ambiente de produção, o utilizador ou solicitante do ambiente será responsável por manter a Equipe de Backup e Restauração de Dados informada sobre a necessidade do backup e frequência da cópia;

II - os backups e cópias dos ambientes de produção não devem ocasionar perdas ou concorrência aos backups já existentes;

III - a frequência e demais parâmetros dos backups destes ambientes copiados deverão consumir menos recursos computacionais do que seus equivalentes em produção; e

IV - os backups e cópias dos dados de ambientes análogos aos de produção deverão seguir práticas e procedimentos adequados à legislação de Proteção de Dados quanto a anonimização de dados pessoais ou identificáveis.

CAPÍTULO VI

DA TRANSCRIÇÃO DE DADOS E DO DESCARTE DE MÍDIAS

Art. 14. A fita magnética só será considerada confiável durante os dois terços da vida útil estabelecida pelo fabricante. Após a expiração deste prazo, as informações nela contidas deverão ser transcritas para uma nova mídia, a fim de zelar pela integridade dos dados.

Art. 15. O descarte das mídias de backup não confiáveis deverá ser feito mediante proposta apresentada pela Equipe de Backup e Restauração de Dados à STI.

Parágrafo único. As fitas a serem descartadas deverão ser destruídas fisicamente, seguindo orientações do fabricante quanto a vida útil, de forma a impedir a sua reutilização ou acesso indevido às informações por pessoas não autorizadas.

CAPÍTULO VII

DA SOLICITAÇÃO DE RESTAURAÇÃO

Art. 16. A recuperação dos backups por solicitação deverá obedecer às seguintes orientações:

I - deverá ser solicitada a STI através da ferramenta de chamados técnicos;

II - para os domínios de dados V e VI do Capítulo II, a solicitação deverá ser feita pelo gestor do sistema constante no catálogo de sistemas;

III - o chamado técnico deverá conter o nome e setor do usuário, o(s) arquivo(s), dado(s) e a data de versão que deseja recuperar, sendo essas informações obrigatórias para viabilizar a recuperação dos dados;

IV - o chamado técnico será encaminhado à Equipe de Backup e Restauração de Dados, que após a conclusão da tarefa, realizará o fechamento do chamado indicando a restauração do(s) dado(s);

V - o gestor do sistema será responsável pela validação de todos os dados restaurados pela Equipe de Backup e Restauração de Dados;

VI - deverá ser mantido registro de todos os arquivos/dados cuja restauração foi solicitada, juntamente com as informações relativas ao solicitante, nome do arquivo/dado, data da versão restaurada e data e hora da solicitação; e

VII - a restauração dos arquivos/dados somente será possível nos casos em que o arquivo/dado tenha sido coberto pela estratégia de backup.

CAPÍTULO VIII

DOS TESTES DE RESTAURAÇÃO

Art. 17. As cópias de segurança armazenadas deverão ser testadas periodicamente, a fim de percorrer anualmente todos os domínios dispostos no Capítulo II e seguirá de acordo com a capacidade operacional disponível na instituição.

§1º A Equipe de Backup e Restauração de Dados deverá definir quando os domínios de dados serão testados.

§2º O teste será realizado com o intuito de validar a suficiência dos dados armazenados e a integridade das mídias de backup.

CAPÍTULO IX

DIRETRIZES DE OPERAÇÃO

Art. 18. A criação e operação dos backups deverá obedecer às seguintes orientações:

I - o backup deverá ser programado, de preferência, para execução automática em horário de menor impacto na utilização dos sistemas e da rede;

II - o backup deverá ser monitorado pela Equipe de Backup e Restauração de Dados;

III - para todos os backups realizados com sucesso deve ser gerado um extrato automatizado pela própria ferramenta de backup, confirmando a execução dele; e

IV - para todos os backups que apresentarem falhas deverá ser gerado extrato automatizado pela própria ferramenta de backup, no qual deverá constar a data, os horários de início e término, os objetos, a causa da falha, a ação corretiva adotada e qual parte do backup ficou comprometida.

Art. 19. Os backups deverão ser realizados de acordo com as regras de cada nível de criticidade observado na classificação feita no catálogo de serviços.

Parágrafo único. Em caso de falha em algum procedimento de backup ou impossibilidade da sua execução, a Equipe de Backup e Restauração de Dados deverá adotar as

providências no sentido de guarda das informações através de outro mecanismo, como por exemplo: cópia dos dados para outro servidor, execução do backup em outro horário de agendamento etc.

Art. 20. Quaisquer procedimentos programados nos servidores e que impliquem riscos de mal funcionamento em quaisquer serviços ou equipamentos da instituição, somente deverão ser executados após a realização de backup dos seus dados.

Art. 21. O backup off-site deverá armazenar os dados atendendo no mínimo os requisitos elencados nesta Política, observando a capacidade financeira e técnica da instituição.

§1º A armazenagem do backup off-site deve estar obrigatoriamente fora das instalações da ESMPU, onde encontra-se o data center de produção.

§2º Os dados que serão transportados ao backup off-site deverão estar criptografados.

§3º O armazenamento off-site deve estar em conformidade com padrões acordados entre a STI e o CSGI, e aprovado pelo CTI.

Art. 22. As ferramentas que realizam as cópias de segurança deverão ter suporte a criptografia segura.

CAPÍTULO X

DAS CONSIDERAÇÕES FINAIS

Art. 23. Esta política entra em vigor na data de sua publicação.

ALCIDES MARTINS
Diretor-Geral da ESMPU

Documento assinado eletronicamente por **Alcides Martins**, **Diretor-Geral**, em 31/03/2023, às 15:21 (horário de Brasília), conforme a Portaria ESMPU nº 21, de 3 de março de 2017.

A autenticidade do documento pode ser conferida no site https://sei.escola.mpu.mp.br/sei/autenticidade informando o código verificador **0402168** e o código CRC **AE0CFBC5**.