UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA POSIN/STI Nº 13, DE 24 DE NOVEMBRO DE 2025

Estabelece diretrizes e procedimentos para a realização de cópias de segurança (backup) no âmbito da Universidade Federal do Espírito Santo.

O SUPERINTENDENTE DE TECNOLOGIA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO no uso das suas atribuições e considerando o disposto na Lei nº 13.709 (Lei Geral de Proteção de Dados Pessoais - LGPD), de 14 de agosto de 2018, no Programa de Privacidade e Segurança da Informação (PPSI) do Governo Federal e na Política de Segurança da Informação desta Universidade, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Instrução Normativa estabelece diretrizes e procedimentos para a realização de cópias de segurança (backup) dos dados e sistemas no âmbito da Universidade Federal do Espírito Santo (Ufes), visando garantir a integridade e a disponibilidade das informações.

Art. 2º Para os fins desta Instrução Normativa, considera-se:

I. Administrador de Backup: servidor público responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de *backup* e *restore*;
II. Ativos de Informação: base de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria, informações armazenadas e afins;
III. Ativos de Software: aplicativos, sistemas, ferramentas de desenvolvimento, utilitários e afins;
IV. Backup: Cópia de dados de um dispositivo de armazenamento a outro, para assegurar a recuperação em caso de perda dos dados originais;
V. Backup *full* ou completo: modalidade de backup na qual todos os dados são copiados;
VI. Backup incremental: modalidade de backup na qual somente os arquivos modificados desde o último backup são copiados;
VII. Gestor de Ativo de Informação: proprietário ou custodiante de ativo de informação;
VIII. Log: histórico de avisos, erros e mensagens de aplicativos, sistemas e serviços;
IX. Mídia de Armazenamento: Meio físico ou lógico onde as cópias de segurança são armazenadas;
X. *Restore*: Processo de recuperação dos dados a partir de uma cópia de segurança;
XI. Retenção: período em que o conteúdo da mídia de backup deve ser preservado; e
XII. Sistemas Críticos: sistemas, incluindo seus dados, cuja indisponibilidade afetem a execução das principais atividades acadêmicas e administrativas da Ufes.

CAPÍTULO II

DOS PRINCÍPIOS E DIRETRIZES

Art. 3º O processo de backup na Ufes visa:

I. Garantir a recuperação de informações em caso de perda, corrompimento ou indisponibilidade dos dados originais;
II. Assegurar a continuidade das operações de sistemas críticos da Universidade em situações de desastre;
III. Proteger a integridade e a confidencialidade das informações durante o processo de backup e armazenamento.

Parágrafo único. O mero procedimento de backup não pode 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.

Art. 4º São princípios que regem a realização de backups:

I. Regularidade: Realização de backups em intervalos de tempo definidos, conforme a criticidade dos dados;
II. Redundância: Armazenamento de cópias de segurança em múltiplas mídias ou locais para aumentar a resiliência;
III. Segurança: Proteção dos dados de backup contra acessos não autorizados e falhas físicas.

CAPÍTULO III

DAS RESPONSABILIDADES

Art. 5º As unidades responsáveis pelos sistemas devem indicar os administradores de backup, servidores públicos que administrarão os procedimentos relativos aos serviços de *backup* e *restore*.

Art. 6º Compete aos 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 no mínimo, periodicidade, conteúdo e relatórios;
IV. Preservar as mídias de backup;
V. Testar os procedimentos de *backup* e *restore*;
VI. Executar procedimentos de *restore* para garantir que os arquivos estejam íntegros e funcionais;
VII. Gerenciar mensagens e logs, de acordo com periodicidade, dos backups, por meio de relatórios, solucionando os erros para assegurar a continuidade do procedimento;
VIII. Realizar manutenções periódicas nos dispositivos de backup;

IX. Comunicar ao gestor qualquer erro ou ocorrência nos backups dos ativos de informação e software sob sua responsabilidade;
X. Documentar os procedimentos descritos nos itens anteriores; e
XI. Registrar a execução dos procedimentos, mantendo o histórico de ocorrências.

CAPÍTULO IV

DOS PROCEDIMENTOS DE BACKUP

Art. 7º Os procedimentos de backup devem incluir:

I. Backup Diário: Cópias diárias dos dados críticos, com retenção de sete dias, armazenadas em disco;
II. Backup Semanal: Cópias semanais dos dados, com retenção de quatro semanas, armazenadas em disco;
III. Backup Mensal: Cópias mensais dos dados, com retenção de três meses, armazenadas em disco;

Art. 8º O backup deverá ser realizado com base nas seguintes disposições:

I. Os backups mensais deverão ser realizados, preferencialmente, na modalidade *full*, de forma a permitir a recuperação integral das 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 *full*+incremental, para possibilitar a reversão de dados recentes de forma mais rápida;
V. Em caso de falha em algum procedimento de backup ou impossibilidade de execução, os administradores de backup deverão adotar providências para salvaguardar as informações por outro mecanismo, como cópia dos dados para outro servidor ou execução do backup em horário comercial;

Art. 9º Os backups devem ser testados regularmente para verificar a integridade e a capacidade de restauração dos dados.

Art. 10. Em casos especiais, o gestor do ativo de informação poderá definir prazos diferenciados para retenção dos backups, em conjunto com os administradores de backup.

Art. 11. Todo ativo de informação ou software deverá ter sua inclusão nos procedimentos de backup avaliada.

§1º. O gestor de cada ativo de informação, em conjunto com os administradores de backup, deverá definir e registrar formalmente o que será incluído no backup, bem como o tipo de backup estabelecido no Art. 7º desta Instrução Normativa.

§2º. A disponibilização do serviço de backup para um ativo será condicionada tanto à necessidade de preservação quanto à disponibilidade de recursos na infraestrutura para atender a demanda.

Art. 12. A criação e operação de backups deverão obedecer às seguintes diretrizes:

I. Backups devem ser programados para horários de menor utilização dos sistemas e da rede;
II. Administradores devem certificar-se da conclusão bem-sucedida dos backups analisando, se for o caso, os arquivos de log, para garantir o resultado da operação;
III. Problemas na operação de backups devem ser solucionados, e novos backups devem ser realizados imediatamente, se necessário;
IV. Backups devem ser armazenados em pelo menos duas cópias, preferencialmente em mídias ou locais distintos;
V. A confidencialidade dos backups deve ser assegurada com encriptação, se necessário.

Art. 13. Expirado o prazo de retenção, a mídia de backup ou espaço de armazenamento poderão ser reutilizados.

CAPÍTULO V

DA GESTÃO, ARMAZENAMENTO E RESTORE DE BACKUPS

Art. 14. Compete à Superintendência de Tecnologia da Informação (STI):

I. Configurar, monitorar e testar os procedimentos de *backup* e restore dos equipamentos hospedados na STI;
II. Preservar as mídias de backup em condições adequadas de segurança e integridade;
III. Garantir que os backups dos sistemas críticos sejam armazenados em locais fisicamente distintos e seguros.

Art. 15. As cópias de segurança devem ser armazenadas em local diferente do servidor de produção para garantir a proteção contra desastres locais.

Art. 16. Nas situações em que a confidencialidade é importante, as cópias de segurança devem ser protegidas por criptografia.

Art. 17. O procedimento de restore deverá seguir os seguintes procedimentos:

I. O gestor do ativo de informação deve solicitar formalmente a recuperação, justificando o motivo;
II. A solicitação será encaminhada aos administradores de backup, que realizarão o restore e comunicarão o resultado;

Art. 18. É vedado o restore diretamente nos ambientes de produção, exceto em casos de desastre ou plano de contingência.

CAPÍTULO VI

DOS TESTES, DESCARTE E SUBSTITUIÇÃO DE MÍDIAS

Art. 19. Os procedimentos de backup e restore deverão ser testados sempre que necessário.

Art. 20. Os backups mensais deverão ser testados no prazo máximo de uma semana após sua execução.

Parágrafo único. Caso detectada falha, um novo backup deverá ser realizado para assegurar o armazenamento correto.

Art. 21. O descarte de mídias de backup deve ser realizado de forma que impossibilite a recuperação total ou parcial das informações nelas contidas.

Art. 22. Em caso de substituição da solução de backup, as informações devem ser transferidas integralmente para a nova solução antes da desativação da antiga.

Art. 23. Os administradores de backup deverão respeitar os critérios definidos pelos fabricantes para assegurar a validade e a qualidade das mídias ou equipamentos utilizados na realização de backups.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 24. Compete à Superintendência de Tecnologia da Informação (STI) orientar e fiscalizar o cumprimento desta Instrução Normativa.

Art. 25. Os casos omissos serão resolvidos pelo Comitê de Governança Digital da Ufes.

Art. 26. Esta Instrução Normativa entra em vigor na data de sua publicação.

gov.br
Documento assinado digitalmente
PAULO ALEXANDRE LOBATO
Data: 08/12/2025 16:54:38-0300
Verifique em https://validar.iti.gov.br

PAULO ALEXANDRE LOBATO

Superintendente de Tecnologia da Informação