UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA POSIN/STI Nº 08, DE 24 DE NOVEMBRO DE 2025

Estabelece diretrizes e procedimentos para a gestão de continuidade 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 as diretrizes e procedimentos para a gestão de continuidade das operações no âmbito da Universidade Federal do Espírito Santo (Ufes).

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

I. Gestão de Continuidade: Processo abrangente de gestão que identifica ameaças potenciais e os impactos que estas possam causar nas operações do negócio, fornecendo uma estrutura para aumentar a resiliência organizacional;
II. Incidente de Segurança da Informação: Evento que compromete a confidencialidade, integridade ou disponibilidade dos ativos de informação;
III. Plano de Continuidade de Negócios (PCN): Documento formal que define as estratégias e procedimentos para assegurar a continuidade das operações críticas;
IV. Plano de Gestão de Riscos (PGR): Documento formal que identifica, avalia e prioriza os riscos associados às operações organizacionais, estabelecendo estratégias e ações para mitigar impactos e assegurar a continuidade das atividades críticas.

CAPÍTULO II

DOS OBJETIVOS E PRINCÍPIOS

Art. 3º A gestão de continuidade visa:

I. Assegurar que as atividades essenciais da Ufes não sejam interrompidas ou, na impossibilidade, sejam retomadas no menor intervalo de tempo possível;
II. Minimizar os impactos de incidentes de segurança, falhas ou desastres sobre as atividades da Universidade;

III. Recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação;
IV. Proteger a reputação e a imagem institucional da Ufes.

Art. 4º São princípios que regem a gestão de continuidade:

I. Proatividade: Antecipar-se a potenciais interrupções e preparar respostas eficazes;
II. Resiliência: Desenvolver a capacidade de recuperação rápida e eficiente após incidentes;
III. Melhoria Contínua: Revisar e aprimorar constantemente os planos e procedimentos de continuidade.

CAPÍTULO III
DO PROCESSO DE GESTÃO DE CONTINUIDADE

Art. 5º O processo de gestão de continuidade deve incluir:

I. Identificação de Ativos Críticos: Mapeamento dos ativos de informação e processos críticos para a operação da Ufes;
II. Análise de Impacto nos Negócios: Avaliação dos efeitos potenciais de interrupções nas operações;
III. Desenvolvimento de Estratégias de Continuidade: Definição de abordagens para mitigar impactos e assegurar a continuidade das operações;
IV. Implementação e Testes: Estabelecimento de procedimentos e realização de testes regulares dos planos de continuidade;
V. Revisão e Atualização: Atualização periódica dos planos de continuidade com base em mudanças organizacionais e lições aprendidas.

Art. 6º Os setores da Ufes deverão manter um processo formal de gestão de continuidade de negócios, visando:

I. Evitar que as atividades sejam interrompidas;
II. Assegurar a retomada das atividades no menor intervalo de tempo possível, quando necessário.

Art. 7º Todos os titulares das unidades administrativas da Ufes deverão:

I. Atuar proativamente para aumentar a resiliência contra interrupções dos serviços;
II. Proteger a reputação e a imagem institucional da Ufes.

Art. 8º Todos os setores da Ufes deverão formalizar, no Plano de Gestão de Riscos:

I. Estratégias e procedimentos que serão adotados em situações que comprometam o andamento normal dos processos e a prestação dos serviços;
II. Medidas para assegurar:
    a) A disponibilidade dos ativos de informação;
    b) A recuperação de atividades críticas;
    c) A minimização dos impactos sofridos diante de situações inesperadas, como desastres, falhas de segurança e outras interrupções.

Parágrafo único. Deve-se evitar que pessoas externas à Ufes respondam por ativos de informação importantes, uma vez que a suspensão de atividades e a falta de documentação colocam em risco a gestão de continuidade.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 9º Compete à Superintendência de Tecnologia da Informação (STI) fornecer suporte técnico em situações de interrupção ou falha nos serviços de TIC.

Art. 10. Compete aos gestores das unidades:

I. Identificar e priorizar os processos críticos de suas áreas;
II. Desenvolver e manter atualizado o PGR específico de sua unidade;
III. Desenvolver e manter atualizado o PCN específico de sua unidade;
IV. Garantir que as equipes estejam treinadas e preparadas para atuar em situações de interrupção na continuidade dos serviços.
V. Garantir que as estratégias de gestão de continuidade sejam devidamente documentadas e comunicadas a todas as partes envolvidas;
VI. Implementar controles e verificações regulares para evitar interrupções críticas.

CAPÍTULO V

DA RESPOSTA A INCIDENTES

Art. 11. Em caso de incidente, devem ser adotadas medidas que assegurem a continuidade das operações e a integridade dos serviços críticos de TIC, conforme os seguintes princípios:

I. Detecção e Avaliação: Identificação rápida do incidente e análise de seu impacto sobre as atividades da Ufes e os ativos de informação;
II. Resposta e Contenção: Adoção de ações imediatas para controlar e minimizar os efeitos do incidente, garantindo que os processos críticos não sejam comprometidos;
III. Recuperação: Implementação de ações para restaurar a normalidade das operações, assegurando a confiabilidade e a disponibilidade de serviços e informações;
IV. Comunicação: Notificação adequada às partes interessadas e registro detalhado das ações tomadas, incluindo a documentação de alterações realizadas em equipamentos, sistemas e recursos de processamento da informação.

Art. 12. Para prevenir falhas e garantir a confiabilidade dos serviços, especialmente em situações críticas, devem ser observados os seguintes requisitos no gerenciamento de modificações nos recursos de processamento da informação:

I. As mudanças em sistemas operacionais e aplicativos devem ser realizadas somente quando houver justificativa válida para o negócio, como aumento no risco ou necessidade de melhorias essenciais;

II. As alterações devem estar sujeitas a um rígido controle de gestão de mudanças, com manutenção de registros de auditoria contendo informações relevantes sobre as modificações realizadas;

III. Mudanças em ambientes operacionais, especialmente durante a transição de serviços para a produção, devem ser planejadas e testadas para evitar impactos na confiabilidade das aplicações;

IV. A atualização de serviços para versões mais recentes deve ser precedida de análise detalhada, considerando:

a) Potencial introdução de vulnerabilidades e instabilidades;
b) Necessidade de treinamento adicional, custos de licenciamento, suporte e manutenção;
c) Sobrecarga administrativa e necessidade de novos equipamentos durante a migração.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 13. Compete à Superintendência de Tecnologia da Informação (STI) orientar e fiscalizar o cumprimento desta Instrução Normativa.

Art. 14. Os casos omissos serão resolvidos pelo Comitê de Governança Digital da Ufes.

Art. 15. Esta Instrução Normativa entra em vigor na data de sua publicação.

gov.br
Documento assinado digitalmente
PAULO ALEXANDRE LOBATO
Data: 08/12/2025 16:49:57-0300
Verifique em https://validar.iti.gov.br

PAULO ALEXANDRE LOBATO

Superintendente de Tecnologia da Informação