UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA POSIN/STI Nº 07, DE 24 DE NOVEMBRO DE 2025

Estabelece diretrizes e procedimentos para a gestão de riscos de TIC 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 riscos de segurança da informação no âmbito da Universidade Federal do Espírito Santo (Ufes).

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

I. Risco: Possibilidade de ocorrência de um evento que impacte os objetivos organizacionais;

II. Gestão de Riscos: Processo contínuo e sistemático de identificação, análise, tratamento, monitoramento e comunicação de riscos;

III. Incidente: Materialização de um risco que afeta a confidencialidade, integridade ou disponibilidade das informações;

IV. Probabilidade: Chance de um evento indesejado ocorrer;

V. Impacto: Magnitude das consequências caso o risco se concretize;

VI. Controles: Medidas implementadas para reduzir, transferir, aceitar ou evitar os riscos.

CAPÍTULO II

DOS OBJETIVOS E PRINCÍPIOS

Art. 3º A gestão de riscos visa:

I. Identificar, analisar e tratar os riscos que possam comprometer a continuidade as operações;

II. Garantir a continuidade das operações institucionais em cenários adversos;

III. Promover uma cultura organizacional orientada à prevenção de riscos;

IV. Assegurar o alinhamento com os requisitos legais e normativos aplicáveis.

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

I. Prevenção: Antecipar potenciais problemas e reduzi-los proativamente;

II. Melhoria Contínua: Aprimorar os processos de gestão de riscos com base em lições aprendidas;

III. Transparência: Garantir a comunicação clara e eficiente dos riscos aos envolvidos.

CAPÍTULO III

DO PROCESSO DE GESTÃO DE RISCOS

Art. 5º O processo de gestão de riscos deve abranger:

I. Identificação: Levantamento de ameaças, vulnerabilidades e ativos associados;

II. Análise e Avaliação: Avaliação do impacto e probabilidade, com classificação de criticidade;

III. Tratamento: Implementação de medidas para reduzir, transferir, aceitar ou evitar os riscos identificados;

IV. Monitoramento e Revisão: Acompanhamento contínuo dos riscos e eficácia dos controles aplicados.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 6º Compete à Superintendência de Tecnologia da Informação (STI):

I. Realizar acompanhamentos e capacitações periódicas sobre gestão de riscos;

II. Realizar revisões periódicas do processo de gestão de riscos;

III. Coordenar ações de resposta a incidentes de segurança.

Art. 7º Compete aos gestores das unidades:

I. Identificar e comunicar riscos específicos ao Comitê de Governança Digital;

II. Implementar controles aprovados e revisar periodicamente o cenário de riscos do seu setor.

CAPÍTULO V

DO TRATAMENTO DE INCIDENTES

Art. 8º Em caso de incidente, devem ser seguidas as seguintes etapas:

I. Identificação e Contenção: Isolamento do incidente para minimizar o impacto;

II. Análise e Mitigação: Investigação das causas e aplicação de medidas corretivas;

III. Registro e Comunicação: Documentação do incidente e comunicação às partes interessadas.

CAPÍTULO VI

DA GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO (GRSI)

Art. 9º. A Ufes deverá adotar uma abordagem sistemática no processo de Gestão de Riscos em Segurança da Informação (GRSI) visando manter os riscos em níveis aceitáveis. Este processo deve ser contínuo, aplicando as boas práticas de gestão de riscos com foco na segurança da informação.

Art. 10. O processo de GRSI da Ufes será definido pelas seguintes atividades:

I. Análise de contexto e identificação de riscos de segurança da informação;

II. Identificação da possibilidade de ocorrência e impactos associados;

III. Levantamento dos ativos pertencentes aos grupos de risco;

IV. Classificação dos riscos segundo o grau de probabilidade, o impacto e as consequências para a segurança da informação;

V. Definição da estratégia de aceitação dos riscos;

VI. Definição de medidas de controle para resposta a riscos, o qual pode incluir, mas não se limita a, ações como:

a) Aquisição de hardware e software;

b) Definição e atualização de processos e procedimentos;

c) Alocação de pessoal especializado;

d) Implementação de estratégias de comunicação e treinamento;

e) Desenvolvimento de sistemas de documentação;

f) Contratação de serviços especializados, entre outras ações.

VII. Implementação das medidas de controle para resposta a riscos;

VIII. Monitoramento e análise crítica;

IX. Melhoria contínua do processo de GRSI;

X. Comunicação do risco.

Art. 11. O processo de GRSI deve estar alinhado ao modelo PDCA (Plan-Do-Check-Act), visando garantir a melhoria contínua e a adaptação constante às mudanças do ambiente de risco.

Parágrafo único. A implementação e operação do processo de GRSI deverá produzir subsídios para suportar a Segurança da Informação e a Gestão de Continuidade de Negócios em Segurança da Informação.

Art. 12. A Ufes deverá disseminar a cultura de gestão de riscos em todas as suas áreas operacionais e administrativas, com o total comprometimento da Reitoria.

Art. 13. Todos os setores da Universidade deverão manter um processo contínuo de divulgação e treinamento de suas normas e procedimentos de segurança da informação, capacitando seus usuários a adotarem as melhores práticas no uso e proteção dos ativos de informação.

Art. 14. A adoção de uma linguagem padrão e comum de GRSI é essencial para assegurar a compreensão e a eficácia do processo, evitando falhas na comunicação entre as partes envolvidas.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 15. Compete à Superintendência de Tecnologia da Informação (STI) orientar e fiscalizar o cumprimento desta Instrução Normativa.

Art. 16. Os casos omissos serão resolvidos pelo Comitê de Governança Digital da Ufes.

Art. 17. 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