UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA POSIN/STI Nº 09, DE 24 DE NOVEMBRO DE 2025

Estabelece diretrizes de auditoria e conformidade de Tecnologia da Informação e Comunicação (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 GERAIS

Art. 1º Esta Instrução Normativa estabelece diretrizes e procedimentos para a realização de auditorias e o cumprimento de normas de conformidade de Tecnologia da Informação e Comunicação (TIC) no âmbito da Universidade Federal do Espírito Santo (Ufes), visando garantir a segurança e integridade das informações institucionais.

Art. 2º Esta IN aplica-se a todas as unidades e setores da Ufes, bem como a colaboradores e prestadores de serviços que utilizem informações e recursos institucionais.

CAPÍTULO II

DAS DIRETRIZES PARA AUDITORIA E CONFORMIDADE

Art. 3º As atividades de auditoria e conformidade devem seguir os seguintes princípios:

I. Transparência: Garantir que os processos de auditoria sejam conduzidos de forma clara e objetiva;
II. Independência: Realizar auditorias com imparcialidade, assegurando que os auditores não tenham conflitos de interesse;
III. Regularidade: Realizar auditorias periódicas para monitorar a conformidade e identificar possíveis melhorias nos processos.

Art. 4º A Ufes adotará, por meio de sua Auditoria Interna, um cronograma de auditorias para assegurar o cumprimento das políticas e normativas de segurança da informação.

§ 1º. As auditorias previstas no *caput* deste artigo não serão prejudicadas pela existência de ações semelhantes realizadas por órgãos de controle externos.

§ 2º. O Comitê de Segurança da Informação (CSI) deverá propor à Reitoria a inclusão de temas prioritários, no âmbito da segurança da informação, a serem contemplados no Plano Anual de Atividades de Auditoria Interna (PAINT) até o dia 30/09 de cada ano.

Art. 5º As auditorias deverão avaliar:

I. A eficácia dos controles de segurança da informação;
II. O cumprimento das políticas e normas internas de segurança da informação;
III. A conformidade com legislações aplicáveis.

CAPÍTULO III

DO PROCESSO DE AUDITORIA

Art. 6º O processo de auditoria no âmbito da Posin deve adotar diretrizes complementares para assegurar sua eficácia e alinhamento às melhores práticas, conforme descrito abaixo:

I. Ciclo PDCA (Plan-Do-Check-Act):
   a) Planejamento (Plan): Definição das atividades de gestão de segurança da informação, estabelecendo políticas, controles e procedimentos;
   b) Execução (Do): Implantação e operacionalização das políticas, controles, processos e procedimentos definidos;
   c) Verificação (Check): Realização de auditorias sistemáticas para avaliar a eficiência das políticas e controles implementados;
   d) Ações corretivas (Act): Correção e prevenção de deficiências identificadas, alinhando-se ao planejamento inicial e às boas práticas.
II. Critérios de auditoria e evidências:
   a) As auditorias deverão ser conduzidas de forma sistemática, documentada e independente;
   b) Evidências de auditoria incluem registros ou informações pertinentes, avaliadas objetivamente em relação aos critérios estabelecidos.
III. Princípios de auditoria: Para garantir relevância e suficiência das conclusões, os processos de auditoria devem observar os seguintes princípios:
   a) Integridade;
   b) Apresentação justa;
   c) Devido cuidado profissional;
   d) Confidencialidade;
   e) Independência;
   f) Abordagem baseada em evidência.
IV. Trilhas de auditoria:
   a) Devem ser implementados mecanismos que automatizem a criação e o armazenamento de trilhas de auditoria, contendo registros detalhados sobre acessos e alterações em informações, identificando responsáveis e eventuais falhas ou fraudes;
   b) Trilhas geradas eletronicamente devem ser protegidas por controles de integridade para assegurar validade jurídica.

V. Tratamento de não-conformidades: Processos de auditoria devem incluir mecanismos para identificar e tratar não-conformidades, assegurando o cumprimento das leis, regulamentos e normas institucionais.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 7º Compete ao Comitê de Segurança da Informação (CSI):

I. Verificar os relatórios de auditoria e acompanhar a implementação das recomendações;
II. Propor ajustes nas políticas e procedimentos de segurança com base nos resultados das auditorias.

Art. 8º Compete ao Gestor de Segurança da Informação:

I. Coordenar a implementação das ações corretivas e preventivas recomendadas no relatório de auditoria no âmbito da segurança da informação; e
II. Reportar ao CSI o progresso e a situação das ações adotadas em resposta às recomendações.

CAPÍTULO V

DAS PENALIDADES

Art. 9º. O descumprimento das disposições desta IN, bem como a recusa de participação no processo de auditoria ou a obstrução de suas atividades, sujeitará os infratores às penalidades previstas na legislação vigente, no Código de Ética da Ufes e nas normas da Posin 2025-2028.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 10. Compete à Superintendência de Tecnologia da Informação (STI) orientar e fiscalizar o cumprimento desta Instrução Normativa.

Art. 11. Os casos omissos serão resolvidos pelo Comitê de Governança Digital da Ufes.

Art. 12. 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