UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA STI/POSIN 07 – GESTÃO DE RISCOS

A Ufes deverá adotar a abordagem sistemática do processo de Gestão de Riscos em Segurança da Informação (GRSI), conforme preconizado na Norma ABNT NBR ISO/IEC 27005:2019, com o objetivo de manter os riscos em níveis aceitáveis.

O processo de GRSI da Ufes deverá ser definido pelas atividades de:

- Análise de contexto e identificação de riscos de Segurança da Informação (SI);
- Identificação da possibilidade de ocorrência de tais eventos e dos impactos associados;
- Levantamento dos ativos pertencentes aos grupos de risco;
- Classificação dos riscos segundo o grau de probabilidade, o impacto e as consequências para a segurança da informação;
- Definição da estratégia de aceitação dos riscos;
- Definição do plano de tratamento de riscos, que podem incluir, mas não estão restritos, a aquisição de hardware, aquisição de software, definição de processos, alocação de pessoal, estratégia de comunicação, sistema de documentação, contratação de serviços, entre outros;
- Implementação do plano de tratamento dos riscos;
- Monitoramento e análise crítica;
- Melhoria do processo de GRSI; e
- Comunicação do risco.

O processo de GRSI deve ser contínuo, utilizar indicadores que permitam a avaliação, auditoria e acompanhamento e estar alinhado ao modelo denominado PDCA (*Plan-Do-Check-Act*) visando fomentar a sua melhoria contínua.

A sua implementação e operação deverá produzir subsídios para suportar a Segurança da Informação (SI) e a Gestão de Continuidade de Negócios em Segurança da Informação.

A Universidade deve difundir a cultura de gestão de risco, no qual procedimentos e sistemas de controle sejam disseminados em todas as áreas administrativas e operacionais, com total comprometimento da Alta Administração.

Todas os setores da Universidade deverão manter um processo permanente de divulgação de suas normas e procedimentos para capacitar, conscientizar e sensibilizar seus usuários

à correta conduta na utilização dos ativos.

A adoção de uma linguagem padrão de GRSI é essencial ao processo, possibilitando melhor entendimento entre as partes e um processo livre de interferências.