UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA STI/POSIN 09 – AUDITORIA E CONFORMIDADE

Para que uma política seja eficaz, deve haver mecanismos que permitam a verificação do seu cumprimento. Para isso, a norma ISO 27001 estabelece um modelo de processo baseado num ciclo PDCA (*Plan-Do-Check-Act*) de quatro fases:

- **Planejamento (*Plan*):** nesta fase, de forma geral, são planejadas as atividades referentes a gestão de segurança da informação, estabelecendo-se, por exemplo, políticas e procedimentos de segurança;
- **Execução (*Do*):** nesta fase, são implantadas e devidamente operacionalizadas as políticas, controles, processos e procedimentos da gestão de segurança da informação;
- **Verificação (*Check*):** nesta fase é feita uma auditoria da gestão de segurança da informação, analisando-se e avaliando a eficiência de suas políticas, controle, processos e procedimentos;
- **Ações corretivas (*Act*):** utilizando o resultado da auditoria da fase anterior, devem ser tomadas ações para prevenir ou corrigir as deficiências da gestão de segurança da informação, conforme especificadas na fase de planejamento e/ou implantadas na fase de execução.

Conforme a NBR ISO 19011, auditoria é definida como um processo sistemático, documentado e independente para obter evidências de auditoria e avaliá-las objetivamente de modo a determinar a extensão na qual os critérios de auditoria são atendidos. Essa definição (quase circular) usa o conceito de evidências de auditoria, que são registros, apresentação de fatos ou outras informações, pertinentes aos critérios de auditoria, e o de critérios de auditoria, que são um conjunto de políticas, procedimentos ou requisitos. Os critérios de auditoria são usados como uma referência contra a qual as evidências da auditoria são comparadas.

Uma auditoria deve ser caracterizada pela confiança e por princípios, para que sejam possíveis conclusões de auditoria relevantes e suficientes. Uma condição é que auditores trabalhem de forma independente e sejam consistentes, ou seja, cheguem a conclusões semelhantes em situações semelhantes. A NBR ISO 19011 apresenta alguns desses princípios:

- Integridade;
- Apresentação justa;
- Devido cuidado profissional;
- Confidencialidade;
- Independência; e
- Abordagem baseada em evidência;

O cumprimento da POSIN deverá ser avaliado periodicamente por meio de auditorias, que inclusive poderão ser feitas com o apoio de entidades externas e independentes.

Deverão ser instituídos processos de auditoria e tratamento de não-conformidades, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades no âmbito da Universidade, bem como os da POSIN, de forma a obter o absoluto cumprimento dos instrumentos legais e normativos.

Devem ser implementados mecanismos que automatizem a criação e armazenamento de trilhas para auditoria, que são conjuntos de evidências de auditoria inter-relacionados. Essas trilhas de auditoria devem ter nível de detalhe suficiente para rastrear acessos e modificações nas informações identificando os responsáveis, além de possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, devem ser implantados controles de integridade, de modo a torná-las juridicamente válidas.