Auditoria de Sistemas

Prof. Dr. Joseffe Barroso de Oliveira

AULA 02

Conceitos e Objetivos da Auditoria de Sistemas

Introdução

A Auditoria de Sistemas é um processo sistemático e independente que tem como objetivo avaliar a eficácia, segurança e conformidade dos sistemas de tecnologia da informação (TI) de uma organização. Seus conceitos envolvem a análise de controles internos, a detecção de vulnerabilidades e a verificação do cumprimento de normas e regulamentos. O principal objetivo é garantir que os sistemas operem de forma eficiente, protegendo dados sensíveis e suportando os objetivos estratégicos da empresa, além de mitigar riscos de segurança e fraudes.

Organização Nacional de Padronização

A ISO (Organização Internacional de Padronização) é um órgão de reconhecimento mundial que já publicou mais de 22 mil padrões internacionais, promovendo a normatização de produtos e serviços.

A ABNT (Associação Brasileira de Normas Técnicas) representa a ISO no Brasil e é responsável por implementar normas que conferem qualidade aos produtos e serviços.

A norma ISO 19001:2018 é referência para auditorias de gestão, enquanto a norma ISO 27000:2018 aborda especificamente auditoria de sistemas de informação e segurança da informação.

Tipos de Auditoria de Sistemas

Auditoria Interna

- A auditoria interna é um processo realizado pela própria organização para auditar seus sistemas e procedimentos.
- O objetivo é garantir que os parâmetros estejam sendo seguidos e que os resultados esperados sejam atingidos.
- Identifica processos que não estão em conformidade e oportunidades de melhorias.

Auditoria Externa

- A auditoria externa é realizada por um auditor independente.
- É fundamental para averiguar se os processos estão adequados às normas e diretrizes.
- Pode ser contratada pela empresa ou ser obrigatória por leis do setor.

Auditoria Interna

A auditoria interna é um processo realizado pela própria organização para auditar seus sistemas e procedimentos, garantindo que seus parâmetros estejam sendo seguidos devidamente.

Os auditores internos devem ter as competências necessárias, habilidades e experiências para executar sua função com êxito, incluindo treinamento na norma ISO 19011.

Esse tipo de auditoria permite que a organização identifique processos que não estão em conformidade e descubra oportunidades de melhorias.

É fundamental para medir, de forma eficaz, o desempenho da organização em relação às normas e diretrizes a serem seguidas.

Auditoria Externa

Independência do Auditor Externo

A auditoria externa é realizada por um auditor independente, cuja opinião não pode sofrer nenhum tipo de influência da organização auditada.

Avaliação de Conformidade

Esse tipo de auditoria é fundamental para averiguar se os processos estão, de fato, adequados às normas e diretrizes pré-determinadas.

Mandato Legal

A auditoria externa pode ser obrigatória por leis relacionadas ao setor de atuação da empresa, sendo realizada por órgãos reguladores.

Aplicação da Auditoria nas Empresas

Planejamento

Definição de objetivos, escopo, recursos e cronograma da auditoria. Um plano detalhado assegura que todos os aspectos sejam abordados e que os auditores estejam prontos.

Plano de auditoria
Cronograma de atividades
Recursos necessários

Execução

Coleta de dados através de entrevistas, revisão de documentos e observações. Essa fase é essencial para identificar conformidades e não conformidades.

Relatório de coleta de dados
Análise de conformidade
Identificação de não conformidades

Relatório de Resultados

Análise das informações coletadas e elaboração de um relatório com os resultados. O relatório deve apresentar descobertas, evidências e avaliação do sistema auditado.

Relatório de auditoria
Resumo das descobertas
Recomendações

Plano de Ação

Desenvolvimento de um plano de ação com base nas conclusões da auditoria. O plano deve abordar não conformidades e propor medidas corretivas.

Plano de ação
Medidas corretivas propostas
Cronograma para implementação

LGPD e Auditoria de Sistemas

Objetivos da LGPD

A LGPD foi criada para estabelecer regras para a regulamentação das práticas do uso de dados no ambiente digital, visando proteger o direito à liberdade e privacidade dos usuários.

Requisitos Legais

A LGPD impõe que as empresas devem oferecer mais controle ao cidadão digital sobre o tratamento de suas informações pessoais, incluindo o consentimento explícito para coleta e uso de dados.

Sanções para Inadimplemento

As empresas que não cumprirem a LGPD estão sujeitas a sanções, o que torna a adaptação à nova legislação uma prioridade para garantir a conformidade.

Auditorias Externas pela ANPD

Conforme o art. 20 da LGPD, a Autoridade Nacional de Proteção de Dados pode realizar auditorias para verificar aspectos discriminatórios em tratamento automatizado de dados pessoais.

Auditoria de Sistemas como Proteção Legal

+ Vantagens da Auditoria de Sistemas

- A auditoria de sistemas permite que as empresas se resguardem de possíveis sanções legais, garantindo que estejam em conformidade com a LGPD.
- Com uma auditoria interna eficaz, as organizações podem identificar e corrigir falhas em seus processos de tratamento de dados antes que se tornem um problema legal.
- A realização de auditorias externas pela Autoridade Nacional de Proteção de Dados (ANPD) pode ser uma exigência, e estar preparado para isso é fundamental para evitar penalidades.

× Desafios e Considerações

- Implementar auditorias de sistemas pode demandar tempo e recursos significativos, o que pode ser um desafio para empresas com orçamento limitado.
- Nem todas as organizações possuem o conhecimento técnico necessário para conduzir auditorias de forma eficaz, o que pode limitar sua eficácia.
- A dependência de auditorias externas pode gerar preocupações sobre a imparcialidade e a confidencialidade dos dados auditados.