Auditoria de Sistemas

Prof. Dr. Joseffe Barroso de Oliveira

AULA 08

Etapas de uma Auditoria de Sistemas

Introdução

Uma auditoria de sistemas segue um conjunto estruturado de etapas, desde o planejamento até a conclusão e o acompanhamento das ações corretivas. Cada etapa do processo de auditoria de sistemas é essencial para garantir que os sistemas da organização estejam protegidos, em conformidade e operando de maneira eficiente. Neste capítulo, iremos entender todas as etapas e suas atividades. Em resumo, são elas:

- **Planejamento:** Definição de escopo, objetivos, cronograma e equipe.
- **Execução:** Coleta de dados, testes de controles e análise.
- **Avaliação:** Revisão de achados e documentação de riscos.
- **Relatório:** Elaboração de relatórios e apresentação à administração.
- **Acompanhamento:** Implementação de ações corretivas e monitoramento.
- **Conclusão:** Encerramento formal da auditoria.

Planejamento da Auditoria

1

Definir os objetivos da auditoria: estabelecer o propósito da auditoria, como verificar conformidade, avaliar controles de segurança, identificar fraudes ou otimizar processos.

2

Determinar o escopo: identificar os sistemas, aplicações, redes e processos que serão auditados, podendo ser um departamento, função de TI ou toda a infraestrutura.

3

Avaliação de riscos: realizar uma análise preliminar dos riscos para identificar áreas críticas que exigem mais atenção, incluindo riscos de segurança, conformidade e operacionais.

4

Recursos e equipe: definir a equipe de auditoria, incluindo auditores internos e consultores externos, e determinar as ferramentas e tecnologias a serem usadas.

5

Cronograma: estabelecer um calendário com prazos para cada fase da auditoria, incluindo datas para entrega de relatórios e revisões.

6

Exemplo prático: em uma auditoria de conformidade com a LGPD, o objetivo é garantir que os sistemas de TI estejam protegendo adequadamente os dados pessoais dos clientes.

Execução da Auditoria

Coleta de Dados	Coletar evidências relevantes, como logs de sistemas, registros de acesso, configurações de segurança e documentos de políticas de TI. Isso pode ser feito por meio de entrevistas, revisões de documentos e análise de sistemas.
Testes de Controles	Realizar testes de auditoria para verificar se os controles internos estão funcionando corretamente. Isso pode incluir testes de vulnerabilidade, análise de logs, testes de integridade de dados e revisões de código.
Análise de Dados	Usar ferramentas de análise de dados, como ACL ou IDEA, para revisar grandes volumes de dados, identificar anomalias e avaliar o desempenho dos controles de segurança.
Amostragem	Em muitos casos, a auditoria se concentra em uma amostra de dados ou transações, especialmente quando os volumes são muito grandes. Técnicas de amostragem são usadas para garantir que as conclusões sejam representativas.

Avaliação e Documentação

Os auditores comparam as evidências coletadas com os padrões de controle definidos no planejamento, identificando irregularidades e vulnerabilidades.

Criar relatórios detalhados sobre os resultados da auditoria, incluindo evidências de falhas de conformidade e deficiências em controles.

Cada achado é classificado com base em sua severidade (crítico, alto, médio ou baixo) e impacto no negócio, facilitando a priorização de ações corretivas.

Exemplo prático: Em uma auditoria de segurança, os auditores documentam falhas como contas de usuário sem políticas de senha robustas.

Relatório de Auditoria

Criação do Relatório Final	O relatório é elaborado com uma visão geral do escopo da auditoria, achados principais, áreas de risco e recomendações de melhorias. Ele deve ser claro, objetivo e baseado em evidências.
Recomendações de Ações Corretivas	O relatório inclui sugestões detalhadas de como mitigar riscos identificados, como fortalecer controles de segurança, implementar novas políticas de governança ou realizar atualizações em sistemas.
Discussão com a Administração	O relatório é apresentado à alta administração, que deve discutir os achados e decidir sobre as ações a serem tomadas. Feedbacks podem ser coletados para ajustes nas recomendações.

Acompanhamento das Ações Corretivas

Implementação

A organização deve corrigir as deficiências identificadas na auditoria, incluindo mudanças em políticas de segurança e ajustes técnicos nos sistemas.

Planos de ação
Documentação das mudanças
Atualização de políticas

Monitoramento

Auditores realizam acompanhamento para garantir que as ações corretivas foram implementadas e estão funcionando como esperado.

Relatórios de acompanhamento
Métricas de performance
Avaliações de eficácia

Relatórios

Relatórios periódicos são gerados para avaliar o progresso das ações corretivas e se estão mitigando os riscos identificados.

Relatórios de progresso
Análise de riscos atualizada
Feedback das partes interessadas

Exemplo Prático

Se uma auditoria detectou falhas na proteção de dados, como a falta de criptografia, a equipe de TI implementa a criptografia e realiza auditoria de acompanhamento.

Relatório da auditoria de acompanhamento
Comprovante de implementação
Documentação de procedimentos

Conclusão da Auditoria

Encerramento formal é realizado quando todas as ações corretivas foram implementadas ou os riscos foram aceitos pela administração.

Um relatório final de auditoria é emitido, documentando todas as etapas, achados, ações corretivas e o encerramento do processo.

A auditoria de segurança é oficialmente concluída após verificar que todas as recomendações de segurança foram implementadas e que os sistemas críticos estão protegidos.

A documentação final serve como um registro das atividades e decisões tomadas ao longo do processo de auditoria.