Auditoria de Sistemas

Prof. Dr. Joseffe Barroso de Oliveira

AULA 09

Habilidades do Auditor de Sistemas

Introdução

Responsabilidades do Auditor de Sistemas	Os auditores de sistemas são responsáveis por garantir que os sistemas de TI de uma organização estejam seguros, eficientes e em conformidade com regulamentos.
Conjunto Diversificado de Habilidades	Um auditor de sistemas precisa de um conjunto diversificado de habilidades, que vão desde conhecimentos técnicos avançados até competências comportamentais e de gestão.
Importância da Função	Assegurar que os sistemas de TI estejam em conformidade é crucial para a proteção de dados e a integridade das operações empresariais.

Habilidades Técnicas Essenciais

Conhecimento em Arquitetura de TI

Entender a arquitetura de sistemas de TI, incluindo servidores, redes, banco de dados, e infraestrutura de hardware e software. Auditores de sistemas precisam compreender como os componentes de TI se interconectam e como fluxos de dados são gerenciados.

Segurança da Informação

Conhecimento sobre princípios de segurança da informação, como confidencialidade, integridade, disponibilidade, autenticação, criptografia e proteção contra ataques cibernéticos.

Ferramentas de Auditoria e Análise

Experiência no uso de ferramentas como Audit Command Language (ACL), IDEA, Wireshark, Splunk, e ferramentas de testes de penetração como Nmap, Nessus, e Metasploit.

Conhecimento em Normas e Padrões de TI

Compreensão das principais normas e frameworks de TI e segurança, como ISO 27001, COBIT, ITIL, PCI-DSS, GDPR e SOX.

Conhecimentos em Bancos de Dados e Linguagens de Consulta

Entendimento dos principais bancos de dados (SQL, Oracle, NoSQL) e a capacidade de usar linguagens de consulta, como SQL, para extrair dados necessários para a auditoria.

Conhecimentos em Desenvolvimento de Software

Familiaridade com o ciclo de vida do desenvolvimento de software (SDLC), práticas de desenvolvimento seguro e auditoria de código-fonte.

Habilidades Comportamentais Necessárias

Pensamento Crítico e Analítico

Habilidade de avaliar sistemas e dados com precisão, identificar anomalias e correlacionar informações para chegar a conclusões lógicas. Exemplo prático: Detectar uma inconsistência em um conjunto de dados que, à primeira vista, parece normal, mas que pode indicar uma fraude ou falha de sistema.

Capacidade de Solução de Problemas

Capacidade de identificar problemas de TI e propor soluções viáveis e práticas. Exemplo prático: Em uma auditoria de rede, identificar a causa raiz de vulnerabilidades abertas em uma infraestrutura crítica e recomendar ações corretivas específicas.

Comunicação Eficaz

Habilidade de explicar achados técnicos complexos de forma clara e acessível a stakeholders não técnicos. Exemplo prático: Apresentar um relatório de auditoria a executivos de uma empresa, traduzindo questões técnicas em termos de risco e impacto nos negócios.

Ética e Integridade

Auditores de sistemas precisam ter um forte senso de ética, pois lidam com informações confidenciais. Exemplo prático: Durante uma auditoria, um auditor encontra evidências de fraude interna e deve manter sigilo e seguir os protocolos apropriados.

Gestão de Tempo e Organização

Auditores frequentemente gerenciam várias auditorias simultaneamente, cada uma com prazos apertados. Exemplo prático: Durante uma auditoria de conformidade, o auditor precisa gerenciar o progresso de diferentes equipes e garantir a entrega dos relatórios finais.

Elaboração de Relatórios

Preparação de relatórios detalhados que descrevem os achados da auditoria, explicam os riscos e oferecem recomendações de melhorias. Exemplo prático: Criar um relatório detalhado para a alta administração, destacando as áreas de risco de conformidade.

Rotina do Auditor de Sistemas

01

Revisão de Documentação: Os auditores revisam políticas de TI, manuais operacionais e regulamentos internos para garantir conformidade com as melhores práticas.

02

Coleta de Evidências: Coletam dados de logs, acessos a sistemas e relatórios de uso para validar a conformidade e identificar problemas.

03

Testes e Verificações: Realizam testes de vulnerabilidade e auditoria de configuração de rede para identificar falhas de segurança.

04

Análise de Dados: Analisam grandes volumes de dados para detectar inconsistências ou padrões incomuns que possam indicar fraudes.

05

Reuniões e Colaboração: Participam de reuniões com equipes de TI para discutir achados da auditoria e colaborar na resolução de problemas.

06

Elaboração de Relatórios: Preparação de relatórios detalhados que descrevem os achados da auditoria, explicando os riscos e oferecendo recomendações.

Ferramentas e Técnicas de Auditoria

Audit Command Language (ACL)

O ACL é uma ferramenta poderosa para análise de dados que permite aos auditores realizar auditorias detalhadas em grandes volumes de transações financeiras em busca de anomalias.

IDEA

IDEA é uma ferramenta de auditoria de dados que ajuda na análise e visualização de grandes conjuntos de dados, facilitando a identificação de fraudes e erros.

Wireshark

Wireshark é uma ferramenta de análise de tráfego de rede que permite capturar pacotes de dados e identificar tráfego suspeito em tempo real.

Testes de Penetração

Métodos de testes de penetração, como Nmap, Nessus e Metasploit, são utilizados para identificar vulnerabilidades em sistemas e redes, simulando ataques cibernéticos.

Certificações Relevantes para Auditores

CISA (Certified Information Systems Auditor): Focada em auditoria de sistemas e controle de TI.

CISM (Certified Information Security Manager): Focada em gestão de segurança da informação.

CISSP (Certified Information Systems Security Professional): Focada em segurança da informação.

ISO 27001 Lead Auditor: Focada em auditorias de sistemas de gestão de segurança da informação.

As habilidades do auditor de sistemas são fundamentais para a segurança e eficiência dos sistemas de TI.

Auditores de sistemas desempenham um papel crítico na proteção das informações e na manutenção da integridade dos sistemas de tecnologia da informação. A combinação de habilidades técnicas e comportamentais permite que esses profissionais identifiquem vulnerabilidades e garantam a conformidade com regulamentos. "Um auditor de sistemas precisa de um conjunto diversificado de habilidades" para assegurar que os sistemas de TI estejam seguros.