Auditoria de Tecnologia da Informação e Comunicação (TIC) (Incluindo Tecnologias Emergentes e [IA])

I. APRESENTAÇÃO:

O treinamento **"Auditoria de Tecnologia da Informação e Comunicação (TIC)"** tem por objetivo orientar e capacitar profissionais de TIC, controladores e auditores de controle interno/externo, gestores e demais profissionais envolvidos na avaliação de controles de Tecnologia da Informação e Comunicação (TIC) na preparação e condução do planejamento, execução e elaboração de relatórios de auditoria no contexto TIC, bem como permitir a avaliação do uso e da gestão dos recursos de TIC em cenários distintos e permitir a seleção de controles adequados, de forma a mitigar riscos e garantir um melhor desempenho da organização com a consecução de seus objetivos estratégicos e resultados almejados.

A Estratégia Treinamentos adota metodologia direcionada para a prática, com aplicação de estudos de caso e realização de trabalhos práticos em equipe. Ao final do treinamento o aluno estará apto a participar do processo de planejamento e execução de auditorias de TIC nos cenários mais comuns da organização auditada, bem como ser capaz de avaliar os resultados e propor melhorias nos processos internos da organização.

II. PÚBLICO ALVO:

Profissionais de TIC, Controladores e Auditores de controle interno/externo, gestores de riscos corporativos e de TIC, gestores e fiscais de contrato, assessores jurídicos, equipes de apoio administrativo, membros do Comitê Gestor de TIC, membros do Comitê Gestor de Segurança da Informação, Auditores de controle externo de Tribunais de Contas, estudantes e profissionais independentes interessados na temática.

III. CARGA HORÁRIA: 32 horas.

IV. BENEFÍCIOS DO TREINAMENTO:

Melhoria dos processos internos da organização em contextos relacionados à TIC; melhoria na Governança, na gestão e no uso eficiente dos recursos disponíveis de TIC; maior eficiência e mitigação de riscos em contratações de TIC; maior segurança e confiabilidade das informações processadas, melhor alinhamento entre a TIC e o negócio, conformidade legal e técnica nos processos de TIC, melhoria no desempenho organizacional com o alcance dos objetivos estratégicos e resultados almejados.

Aperfeiçoamento profissional e capacitação de equipes de auditoria de Controle Interno/Externo de Tribunais de Contas e equipes de Auditoria de Sistemas de Controle interno na área de TIC.

V. CONTEÚDO PROGRAMÁTICO:

- **MÓDULO 1: INTRODUÇÃO À AUDITORIA (4h)**
- **MÓDULO 2: AUDITORIA DE TIC (12h)**
- **MÓDULO 3: ETAPAS DO PROCESSO DE AUDITORIA DE TIC (8h)**
- **MÓDULO 4: AUDITORIA DE TIC NA PRÁTICA: CASE: AUDITORIA DE GOVERNANÇA E GESTÃO DE TIC (8h)**

VI. CONTEÚDO DETALHADO DO CURSO

MÓDULO 1: INTRODUÇÃO À AUDITORIA (4h)

1.1 OBJETIVOS ESPECÍFICOS:

Compreender os conceitos fundamentais de auditoria e controles internos, identificando seus objetivos, tipos, etapas e a estrutura organizacional responsável por sua execução e avaliação.

1.2 TÓPICOS:

- **Estrutura dos Controles Internos: O Modelo das Três Linhas:**
  - Conceito de controle interno e sua importância;
- **Estrutura tradicional segundo o Modelo das Três Linhas:**
  - **Primeira Linha:** equipes operacionais/responsáveis pela execução dos controles;
  - **Segunda Linha:** áreas de controles internos, gestão de riscos e conformidade (incluindo elaboração de normas e procedimentos);
  - **Terceira Linha:** auditoria interna, com atuação independente e de avaliação;
- **Conceitos Fundamentais de Auditoria**
  - Definição e relevância da auditoria no contexto organizacional;
  - Diferença entre auditoria interna e auditoria externa;
- **Objetivos, Escopo e Tipos de Auditoria**
  - Objetivos da auditoria;
  - Principais tipos: auditoria de conformidade, auditoria financeira, auditoria contábil, auditoria operacional. Esses tipos podem ser focados em temáticas especializadas, também chamadas de auditorias especializadas (**Tecnologia da Informação e Comunicação**, Concessões Públicas, Saúde, Educação, etc.).
- **Papéis e Responsabilidades do Auditor**
  - Perfil do auditor e competências exigidas;
  - Princípios éticos, independência e responsabilidade profissional;
- **Etapas do Processo de Auditoria**
  - **Principais fases**: planejamento, execução, comunicação dos resultados e acompanhamento;
  - Visão geral dos métodos e ferramentas utilizados.

MÓDULO 2: AUDITORIA DE TIC (12h)

2.1. OBJETIVOS ESPECÍFICOS:

Analisar as práticas, os desafios e as tendências em auditoria de TIC, com ênfase nos impactos das tecnologias emergentes, sobretudo Inteligência Artificial, na governança, segurança, conformidade e avaliação de riscos em ambientes digitais complexos.

2.2. TÓPICOS:

- **Panorama Atual de Tecnologia da Informação e Comunicação:**

- **Conceitos e componentes essenciais:** hardware, software, redes, telecomunicações, serviços digitais, cloud, gestão e governança de dados;

- **Tendências tecnológicas atuais:** Inteligência Artificial, Big Data, Analytics, Edge Computing, Blockchain, e computação quântica;

- **Segurança da Informação:** desafios recentes, aumento das ameaças cibernéticas, LGPD e outras regulamentações relevantes;

- **Introdução e Evolução da Auditoria de TIC:**

- **Conceitos atualizados de auditoria de TIC**;

- **Papel do auditor de TIC na era digital e de IA:** novas competências, ética e responsabilidade;

- **Principais normativos, legislações e jurisprudências atuais relacionadas à TIC e à proteção de dados** (LGPD, GDPR, Marco Civil, etc.).

- **Abordagens e Tipos de Auditoria de TIC:**

- **Auditoria de contratações e terceirizações em TIC:** Planejamento e justificativa da contratação (estudos técnicos preliminares, termo de referência), Processo seletivo e critérios de avaliação de fornecedores, Análise do contrato: escopo, prazos, níveis de serviço (SLA), garantias e penalidades, Cláusulas de segurança da informação e privacidade (LGPD, confidencialidade), Gestão de riscos terceirizados (supply chain, continuidade de serviço), Monitoramento e fiscalização da execução contratual, Gestão de mudança de escopo e aditivos contratuais, Gestão de conflitos de interesse, Avaliação de desempenho do fornecedor, Conformidade do serviço prestado com as normas e os padrões da organização, Adequação técnica e compliance dos sistemas e serviços contratados, Desmobilização e transferência de conhecimento ao fim do contrato, Gestão documental (provas, autorizações, aprovações e relatórios de acompanhamento);

- **Auditoria de governança e gestão de TIC:** Aderência a frameworks de governança (COBIT, ISO/IEC 38500, ITIL, NIST, etc.), Estruturas de tomada de decisão e responsabilidades, Gestão estratégica de TIC (planejamento, alinhamento com os objetivos organizacionais), Gestão de portfólio de projetos e priorização, Gestão de riscos de TIC e planos de continuidade de negócio, Conformidade com políticas internas e externas, Gestão e proteção de ativos de informação, Monitoramento de desempenho dos serviços de TIC (SLA, KPIs, OLAs), Gestão de mudanças e controles de alterações, Capacidade e maturidade da equipe de TIC, Gestão de incidentes e resposta a crises, Gestão de custos e orçamento de TIC, Atendimento a requisitos de auditoria, ética e transparência, Cultura de inovação e adoção de novas tecnologias;

- **Auditoria de segurança da informação e cibersegurança**: Governança e política de segurança da informação, Gestão de riscos de segurança, Gestão de acessos e identidades, Proteção física e lógica dos ativos, Segurança em redes e comunicações, Proteção de dados pessoais e sensíveis, Gestão de vulnerabilidades e correção, Monitoramento, detecção e resposta a incidentes, Treinamento, conscientização e cultura de segurança, Gestão de continuidade de negócios e backup, Auditoria de logs e trilhas de auditoria, Conformidade legal e regulatória, Testes de segurança e avaliações técnicas, Avaliação da segurança em ambientes de nuvem, IoT e dispositivos móveis, Gestão de fraudes digitais e proteção contra ameaças avançadas;

- **Auditoria de processos negócio de TI x Auditoria de sistemas de informação**: Processo de Negócio informatizado, alinhamento do sistema ao processo de negócio, segregação de funções, levantamento de requisitos do sistema, projeto e desenvolvimento de Sistema de Informação, usabilidade e Funcionalidades do Sistema de Informação, conformidade legal do Sistema de Informação, desempenho do Sistema de Informação, autenticação e integridade das Transações, validação de dados de entrada, validação de dados de saída (processamento), trilhas de auditoria e Logs de Sistema, fraudes em Sistema de Informação;

- **Auditoria em bancos de dados e gerenciamento de dados automatizados**: Modelo de governança de dados (políticas, papéis e responsabilidades), Segurança lógica e física dos bancos de dados, Controles de acesso e segregação de funções, Políticas de backup, recovery e continuidade, Integridade e qualidade dos dados, Conformidade com normas e regulamentações (LGPD, GDPR, etc.), Auditoria de logs de acesso e de manipulação de dados, Gerenciamento de bases de teste, dados mascarados e anonimização, Desempenho e disponibilidade dos bancos de dados, Gestão de vulnerabilidades e atualizações, Automação de processos (robôs, scripts, IA para gestão de dados), Monitoramento de operações automatizadas (batch, ETL, replicações), Gerenciamento do ciclo de vida dos dados (retenção, exclusão segura), Auditoria de mudanças em estruturas e objetos dos bancos de dados;

- **Auditoria de Dados**: Completude e Integridade de dados, Cruzamento de bases de dados, Testes e avaliação de controles, Ferramentas de CAAT (*Computer Assisted Audit Techniques*), Fraudes em base de dados.

- **Auditoria de algoritmos e sistemas baseados em IA**: Transparência e explicabilidade dos algoritmos (explainable AI), Aderência a princípios éticos (equidade, não discriminação, responsabilidade), Documentação e governança do ciclo de vida dos modelos de IA, Validação de dados de treinamento e de produção (qualidade, integridade, vieses), Gestão e mitigação de riscos de vieses e discriminação algorítmica, Rastreabilidade das decisões automatizadas, Conformidade legal e regulatória (LGPD, AI Act, etc.), Controles de segurança e privacidade dos dados utilizados pelos algoritmos, Monitoramento de performance e "drift" dos modelos (robustez em operação), Gestão de logs e trilhas de auditoria específicas de IA, Controle de acesso a modelos/algoritmos e segregação de funções, Gestão de atualizações e versões dos modelos, Procedimentos para resposta a incidentes ou falhas em IA, Validação dos resultados (outputs) gerados por IA em cenários críticos ou regulados

- **Indicadores de Avaliação de Boas Práticas em TIC:**
  - Avaliação de impactos e medidas para mitigar riscos não previstos
  - Indicadores e Dados Atuais sobre Boas Práticas em TIC:
  - Estatísticas atuais sobre conformidade, maturidade e práticas em TIC no setor público: **IGovTI**;
  - Principais relatórios e benchmarks internacionais (ex: IBM Cost of a Data Breach

Report, Relatórios do Gartner);

- Adoção de IA e automação em processos de auditoria: casos práticos e impactos mensuráveis.

MÓDULO 3: ETAPAS DO PROCESSO DE AUDITORIA DE TIC (8h)

3.1. OBJETIVOS ESPECÍFICOS:

Prover os conhecimentos necessários para a realização do planejamento e elaboração de papéis de trabalho em auditorias de TIC.

3.2. TÓPICOS:

- **Planejamento da Auditoria de TIC**
  - **Levantamentos preliminares e compreensão do ambiente tecnológico:**
    - Levantamento de dados;
    - Mapeamento de processos digitais;
    - Identificação de ativos críticos (incluindo uso de ferramentas tecnológicas e automação);
    - Adoção de papéis de trabalho;
  - **Análise de riscos e definição do escopo:**
    - Avaliação de riscos tecnológicos, priorização de áreas ou processos sensíveis (IA, cloud, dados pessoais);
    - Definição de escopo, objeto, objetivos gerais e específicos;
    - Elaboração da Matriz de Riscos;
  - **Critérios de seleção, questões de auditoria e benefícios esperados:**
    - Formulação de perguntas-chave de auditoria, critérios baseados em normas/falhas anteriores e objetivos de valor agregado, benefícios almejados, possíveis achados,
  - **Metodologia, técnicas, recursos, benefícios e limitações:**
    - Metodologia empregada, Recursos disponíveis, limitações da auditoria, possíveis achados, papéis de trabalho, seleção de técnicas e/ou ferramentas de auditoria (incluindo softwares de análise, data analytics e IA), limitações e restrições técnicas, regulatórias ou operacionais;
  - **Identificação preliminar de possíveis achados e desenvolvimento dos papéis de trabalho:**
    - Planejamento inicial dos documentos de apoio e papéis de trabalho que guiarão a auditoria;
    - Elaboração de Check List;
    - Elaboração da Matriz de Planejamento;
  - **Execução da Auditoria de TIC:**
    - **Aplicação de técnicas e ferramentas modernas de auditoria:**

- Uso de listas de verificação atualizadas conforme os riscos e ambiente digital.
- Aplicação prática de técnicas de auditoria, testes automatizados, análise de logs, Data Analytics e IA.

- **Coleta e validação de evidências:**
  - Critérios de auditoria: normativos, legais, melhores práticas e diretrizes;
  - Obtenção de evidências, análise de achados, identificação de causas e efeitos (utilização de automação na coleta quando possível);
- **Documentação e controle de qualidade durante a execução:**
  - Registro sistemático das etapas, conformidade com normas, limitações e salvaguardas;
  - Atualização dos papéis de trabalho;

- **Elaboração e Comunicação do Relatório de Auditoria de TIC:**
  - **Estruturação do relatório:**
    - Padrão e formato ideal para relatórios de auditoria de TIC (objetividade, clareza, transparência e recomendações práticas);
    - Papéis de Trabalho (relatório padrão);
  - **Comunicação dos resultados:**
    - Técnicas para relatar achados complexos, riscos emergentes (como riscos de IA e dados), recomendações e plano de ação;
    - Inclusão de gráficos, dashboards e sumários executivos para públicos diversos;
    - Tratamento de informações sensíveis, LGPD e comunicação responsável dos resultados;

- **Papéis de Trabalho e Documentação da Auditoria de TIC:**
  - **Principais instrumentos de suporte à auditoria:**
    - **Matriz de Planejamento:** definição de riscos, objetivos, critérios e fontes de informação.
    - **Matriz de Achados:** registro sistemático de não conformidades, evidências, causas, efeitos e recomendações.
    - **Matriz de Responsabilização:** identificação de responsáveis e ações corretivas.

MÓDULO 4: AUDITORIA DE TIC NA PRÁTICA: CASE: AUDITORIA DE GOVERNANÇA E GESTÃO DE TIC (8h)

4.1. OBJETIVOS ESPECÍFICOS:

Prover os conhecimentos necessários para a compreensão, planejamento e execução de auditorias de TIC. CASE: Governança e Gestão de TIC.

4.2. TÓPICOS:

- **Governança Pública**: princípios básicos de governança para o setor público, diretrizes para a boa governança;
- **Instrumentos de Planejamento e Orçamento:** Introdução aos principais instrumentos de planejamento e orçamento: Planejamento Estratégico Organizacional, Planejamento Estratégico de TIC, Plano Diretor de TIC, Orçamento de TIC;
- **Análise de Cenários e Diagnóstico Organizacional de Governança e Gestão de TIC**
  - Estudo de caso sobre governança e gestão de TIC (simulado ou real);
  - Mapeamento de processos, estruturas e principais ativos de TIC;
- **Planejamento da Auditoria Prática:**
  - Elaboração do planejamento da auditoria com base em riscos e indicadores do cenário apresentado;
  - Definição do escopo, critérios, objetivos e questões de auditoria aplicadas à governança e gestão de TIC;
  - Seleção das normas e frameworks de referência (COBIT, ITIL, ISO/IEC 38500, ISO/IEC 27001, entre outros);
- **Execução da Auditoria em Ambiente Controlado:**
  - Aplicação de listas de verificação, coleta e análise de evidências em cenário prático;
  - Utilização de ferramentas de auditoria de TIC: checklists, de coleta e análise de dados, etc.
  - Identificação e registro de não conformidades, riscos e oportunidades de melhoria;
- **Elaboração e Apresentação do Relatório Prático:**
  - Estruturação de relatório de auditoria de governança e gestão de TIC a partir dos achados simulados;
  - Análise crítica dos resultados: recomendações, plano de ação e comunicação dos achados para diferentes públicos;
  - Discussão sobre desafios na elaboração e entrega do relatório;
- **Debriefing, Feedback e Melhoria de Processos:**
  - Discussão coletiva sobre dificuldades encontradas, acertos e aprendizados durante a atividade prática;
  - Avaliação de diferentes abordagens na auditoria e sugestões para aprimorar o

processo de governança e gestão de TIC;

- Reflexão sobre a integração de novas tecnologias (IA, automação, análise de dados) no processo de auditoria.

VII. RECURSOS DIDÁTICOS

Apresentação de slides e vídeos e uso de material de apoio (legislação aplicável, papéis de trabalho, textos técnicos, estudo de casos, exercícios).

VIII. METODOLOGIA

- Aulas expositivas, com a participação dos alunos;
- Apresentação de Estudos de caso ou Exercício Prático para fixação do conhecimento acerca procedimentos de planejamento e execução de auditoria de tecnologia da informação e Comunicação.
- Resolução de problemas e exercícios práticos.

IX. INSTRUTOR: A nossa equipe de professores associados é formada por Doutores, Mestres e especialistas com notórios conhecimentos em sua área de atuação e experiência de mercado ou na área pública.

X. TREINAMENTOS IN COMPANY

Solicite a sua proposta em nosso website.