Gestão da Tecnologia da Informação

Auditoria e Segurança da Informação

Francisco José Tosi

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Semana 09

Aula 15/16

Auditoria da Tecnologia da Informação

04/10

Francisco José Tosi

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Conceitos Básicos de Auditoria:

Auditoria é uma atividade que engloba o exame das operações, processos, sistemas e responsabilidades

Tem o intuito de verificar sua conformidade com certos objetivos políticas, orçamentos, regras, normas ou padrões.

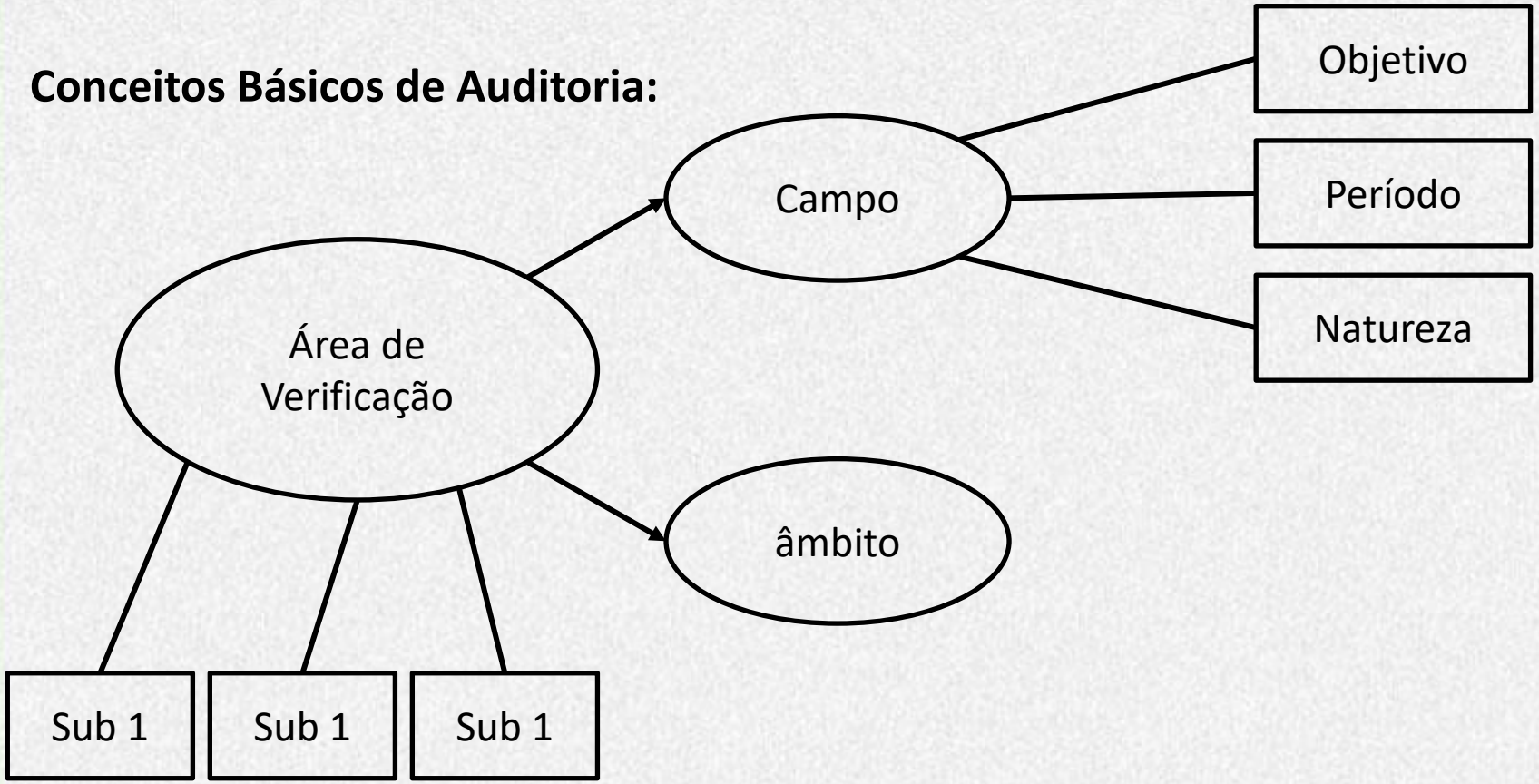
- ✓ Planejamento
- ✓ Execução
- ✓ Relatório

Dias, 2000, p. 8

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Conceitos Básicos de Auditoria:



Âmbito – Natureza da Auditoria – Área de Atuação

Dias, 2000, p. 9

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Conceitos Básicos de Auditoria:

Campo da Auditoria: aspectos como objetivo a ser fiscalizado, período, natureza (operacional, financeira, legalidade)

Objetivo: a entidade (pública ou privada), ou uma parte, uma função da instituição

Período: que será fiscalizado (mês, ano, ou um período completo de gestão)

Natureza: ou tipo de auditoria

Âmbito: Amplitude e execução dos processos de auditoria

Área de Verificação: conjunto formado por campo e âmbito

Dias, 2000, p. 9

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Conceitos Básicos de Auditoria:

Controle da auditoria:

Fiscalização exercida sobre as atividades de pessoas, órgãos, departamentos, produtos.

Controle preventivo: usados para prevenir erros, omissões ou atos fraudulentos (senhas de acesso a um sistema)

Controles detectivos: usados para detectar erros, omissões ou atos fraudulentos e ainda relatar sua ocorrências
(Software de controle de acesso e relatórios de tentativas de acesso não autorizado a um determinado sistema)

Controle corretivos: usados para reduzir impactos ou corrigir erros uma vez detectados
(planos de contingencias)

Dias, 2000, p. 9

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Conceitos Básicos de Auditoria:

Controle da auditoria:

Objetivos de controle: Metas a serem alcançadas, ou efeitos negativos a serem evitados, para cada tipo de transação, atividade ou função fiscalizada.

Procedimentos da auditoria: Conjunto de verificações e averiguações que permite obter e analisar informações necessárias à formulação do auditor

Achados de auditoria: Fatos significativos observados pelo auditor durante a execução da auditoria. Geralmente associados a falhas e irregularidades.

Dias, 2000, p. 10

Auditoria e Segurança da Informação

Conceitos Básicos de Auditoria:

Controle da auditoria:

Papeis da auditoria: registros que evidenciam atos e fatos pelo auditor. Podem ser documentos, tabelas planilhas, lista de verificação, arquivos informatizados, etc.

Relatórios de auditoria: recomendações de auditoria, medidas corretivas possíveis, sugeridas pela instituição fiscalizadora ou pelo auditor em seu relatório, para corrigir as deficiências detectadas.

Dias, 2000, p. 10

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Na auditoria da Tecnologia da Informação é analisado um conjunto de controles gerenciais e controles que afetam todo o ambiente de informática, os sistemas aplicativos.

políticas adotados pela organização;

operação sobre o sistemas de dados;

disponibilidade e manutenção do ambiente computacional;

utilização de recursos computacionais;

gerencia de baco de dados;

Rede;

aspectos ligados a segurança da informação;

Segurança física, lógica e ambiental; e

Continuidade de serviços de informática.

Dias, 2000, p. 137

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles organizacionais:

São políticas, procedimentos e estrutura organizacional estabelecidos para definir as responsabilidades de todos os envolvidos.

Abrangem todos os controles adotados pela gerencia em termos administrativos e institucionais.

Normalmente são o ponto de partida da maioria das auditorias de sistemas.

De acordo com a estrutura, o auditor deve adaptar os objetivos de controle e procedimentos a serem adotado.

EDUCAÇÃO METODISTA

Dias, 2000, p. 137

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles organizacionais:

Responsabilidade Organizacional: TI deve ter uma estrutura organizacional bem definida, com responsabilidades de suas unidades estabelecidas, documentadas e divulgadas.

Políticas, Padrões e Procedimentos: são base para o planejamento gerencial, o controle e avaliação das atividades do departamento de TI.

Estratégia: criação e divulgação do Plano Diretor de Informática pelo comitê de informática ou alta gerencia. Deve ser vir como base para qualquer investimento na área

Política sobre Documentação: deve ser criado políticas sobre documentação, estabelecendo padrões de qualidade e confiabilidade

Dias, 2000, p. 137

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles organizacionais:

Recursos Humanos: deve ser estabelecido políticas, controles e procedimentos de segurança focados no controle de atividades na área pessoal.

Recursos Computacionais: devem ser gerenciados para atender a necessidades e objetivos da organização levando em consideração economia, eficiência e eficácia.

Terceirização: focar nas cláusulas contratuais, atendendo as políticas e procedimentos estabelecidos para a segurança da informação. Processos de auditoria no parceiro também é opção.

Dias, 2000, p. 137

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Riscos Internos ao Controles organizacionais:

- Violação da segurança de acesso a recursos computacionais e de dados.
- Planejamento inadequado do crescimento computacional.
- Equipe insatisfeita ou ressentida.
- Equipe ineficiente que não cumpre com suas obrigações.
- Políticas inadequadas.

Dias, 2000, p. 149

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles sobre Organizacionais:

- ✓ Estabelecer e divulgar um plano estratégico de TI compatível com o da organização;
- ✓ Estabelecer, documentar e divulgar a todos os funcionários as políticas, padrões a serem adotados;
- ✓ Atender obrigações legais e contratuais, em relação a aspectos administrativos de segurança;
- ✓ Definir responsabilidade de cada unidade organizacional e seus cargos e hierarquia;
- ✓ Instituir políticas de contratação e treinamento de pessoal;
- ✓ Evitar a centralização excessiva de poderes e atividades;
- ✓ Estabelecer e manter atualizada documentação dos sistemas, aplicativos e equipamentos; etc.

Dias, 2000, p. 150

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles de mudanças:

O ambiente computacional passa por mudanças constantes para atualizar a plataforma de hardware, versão do sistema operacional, aplicações.

É importantes controlar as mudanças para minimizar riscos e erros ou detectar fraudes.

Todas as alterações devem ser devidamente testadas e autorizadas.

Deve ser definido um processo padrão para mudanças.

Dias, 2000, p. 151

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles de mudanças:

Mudanças emergenciais: não podem aguardar o procedimento normal, deve ser planejada a fim de ter controle e quando a situação for controlada deve ser registrado.

Controle de versão: garantia que todos os usuários utilizam a versão correta do software ou aplicativo.

Dias, 2000, p. 153

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Riscos associados ao Controles de mudanças:

- Uso de software ou hardware não autorizado.
- Processamento de relatórios incorretos.
- Dificuldades na manutenção.
- Mudanças emergenciais não controladas.

Dias, 2000, p. 154

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles de mudanças:

- ✓ Documentar todas as modificações e implementa-las apenas se aprovadas pela gerência;
- ✓ Avaliar o impacto da mudança antes de implementa-la e o efeito de sua não implementação;
- ✓ Definir os recursos necessários para implementar a alteração;
- ✓ Testar exaustivamente os programas antes de implantar em produção;
- ✓ Impedir alterações após os teses e aprovação da implantação;
- ✓ Comunicar com antecedência as mudanças;
- ✓ Preparar um plano de restauração da situação anterior;
- ✓ Preparara um plano de contingência;
- ✓ Manter controle de versões dos softwares;
- ✓ Manter e analisar log das atividades das mudança; etc.

Dias, 2000, p. 154

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles de operação de sistemas:

Está relacionada a infraestrutura de hardware e software.

Certos procedimentos dever existir para a equipe de operação processar cada aplicativo.

O auditor deve rever os procedimento gerais e os específicos de cada aplicação.

Dias, 2000, p. 151

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Riscos Inerentes a Controles de Operação de Sistemas:

- Perda ou corrupção de aplicativos e dados.
- Funcionamento incorreto dos aplicativos.
- Sobrecarga no sistema ou falta de espaço para armazenamento.
- Impossibilidade de execução de novas transações ou serviços.
- Falta de *backup* e planejamento de incontingência.

Dias, 2000, p. 162

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles de Operação de Sistemas:

- ✓ Distribuir a carga de trabalho entre os operadores, levando em conta horários de pico;
- ✓ Supervisionar as atividades de operação de sistemas;
- ✓ Analisar o desempenho dos sistemas, visando o planejamento de capacidade mais adequado às necessidades dos usuários;
- ✓ Implementar processos de controle de problemas de modo que os problemas possam ser identificados, analisados e corrigidos;
- ✓ Manter histórico dos problemas ocorridos;
- ✓ Estabelecer procedimentos de controle de acesso a arquivos e programas em dispositivos de armazenamento de dados;
- ✓ Estabelecer rotinas de backup e recuperação dos sistemas, aplicativos e dados;

Dias, 2000, p. 154

EDUCAÇÃO METODISTA

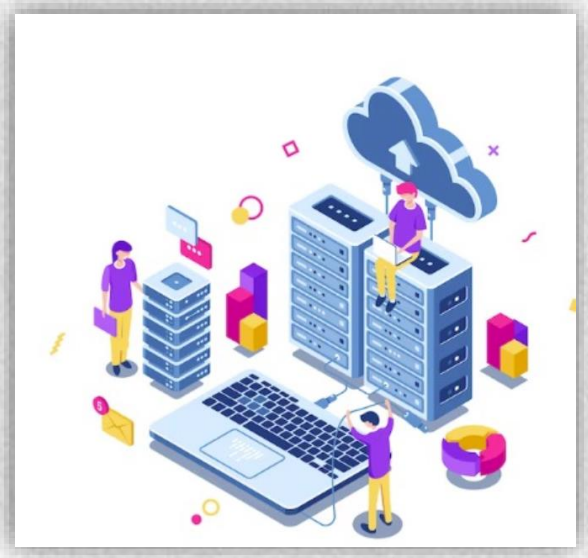
Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles sobre banco de dados:

Dados corporativos são os maiores patrimônio da empresa.

O controle sobre os dados e as estruturas de banco de dados são de suma importância .



Banco de dados devem ser monitorados e auditados constantemente.

Para auditar o banco de dados é necessário conhecimento profundo do SGBD.

Dias, 2000, p. 164

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles Sobre Banco de Dados:

- ✓ Definir e documentar as responsabilidades relacionadas à administração de base de dados;
- ✓ Utilizar dispositivos de segurança e procedimentos de autorização de acesso aos dados;
- ✓ Manter controle sobre as mudanças nas bases de dados;
- ✓ Registrar logs de todas as atividades de administração de dados;
- ✓ Manter atualizado o SGBD;
- ✓ Criar procedimentos de backup e restauração do banco de dados;
- ✓ Implementar mecanismo que limitem o acesso à configuração do SGBD; etc.

Dias, 2000, p. 168

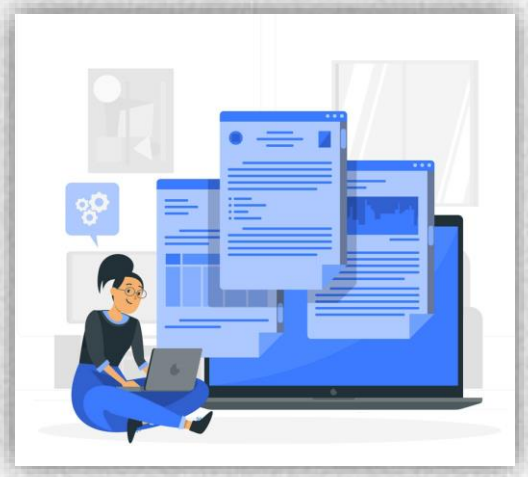
Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles sobre microcomputador:

Avaliar controles sobre ambiente de microcomputadores é mais difícil para os auditores.

O auditor é convocado para avaliar os controles específicos dos microcomputadores.



O auditor deve estabelecer objetivos de controles e procedimentos de auditoria compatíveis com os riscos envolvidos.

Dias, 2000, p. 169

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles Sobre Microcomputadores:

- ✓ Manter inventário dos equipamentos;
- ✓ Instituir controle de entrada e saída de peças e equipamentos, objetivando minimizar perda ou roubo de equipamentos e informações;
- ✓ Para notebooks instituir procedimentos com senhas que impossibilitem acesso a sistemas internos ou informações confidenciais não criptografadas;
- ✓ Utilizar proteção automática de tela com senha;
- ✓ Utilizar criptografia;
- ✓ Realizar backup regularmente;
- ✓ Carregar no computador software ;
- ✓ Manter atualizado o antivírus; etc

Dias, 2000, p. 178

EDUCAÇÃO METODISTA

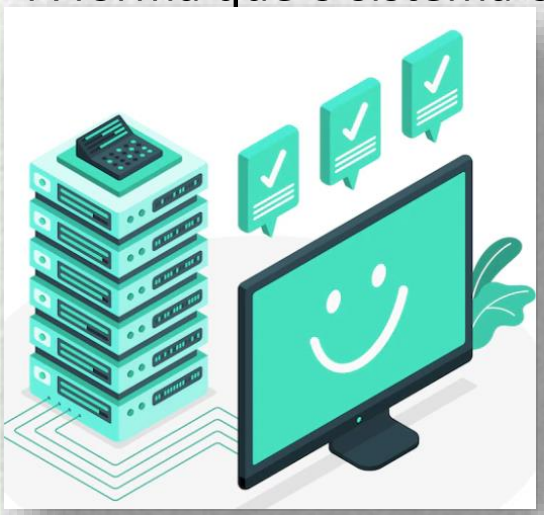
Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles sobre Ambiente Cliente-Servidor:

Desafio para equipe de auditoria de segurança, pois a arquitetura baseia-se em tecnologia de microinformática.

A forma que o sistema operacional e os aplicativos são distribuídos logicamente constitui um desafio.



Dependendo da auditoria e da forma como os componentes foram distribuídos a auditoria pode se concentrar no *Host* ou em múltiplos servidores, clientes e rede de comunicação.

Dias, 2000, p. 180

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Riscos Associados ao Ambiente Cliente-Servidor:

- Acesso não autorizado.
- Erro de configuração.
- Má definição de domínios.
- Falta de arquivo de logs.
- Acesso não autorizado arquivos de senhas.

Dias, 2000, p. 180

Auditoria e Segurança da Informação

Auditoria da Tecnologia da Informação:

Controles sobre Ambiente Cliente-Servidor:

- ✓ Utilizar versões mais atualizadas dos patches (correção).
- ✓ Utilizar criptografia.
- ✓ Não habilitar *features* desnecessárias.
- ✓ Utilizar o menor número possível de contas de usuários.
- ✓ Verificar definições de domínios e relacionamentos de confiança.
- ✓ Verificar definições de grupos de usuários e seus direitos de acesso.
- ✓ Utilizar mecanismo de acesso e utilização de senhas.
- ✓ Eliminar contas inativas.
- ✓ A senha do administrador ou root deve ser altamente restrito.
- ✓ Privilégios das contas deve ser o estritamente necessários.
- ✓ Monitorar o sistema e analisar logs regularmente, etc.

Dias, 2000, p. 180

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Atividade 5

Realizar a **leitura individual** do artigo:

Noções básicas de auditoria de SI: inovação no processo de auditoria de TI Disponível em: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/is-audit-basics-innovation-in-the-it-audit-process

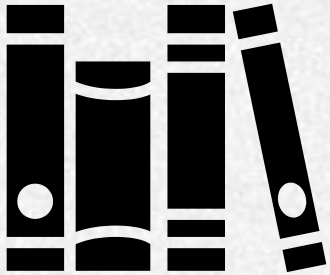
Em grupo debater sobre as questões, criar um documento com as conclusões do debate e disponibilizar no Moodle:

1. O Autor comenta sobre a utilização de software de gerenciamento de auditoria, faça uma pesquisa com o grupo e comente, qual a posição do grupo sobre o assunto.
2. O autor afirma que, tradicionalmente, o uso de análise de dados é considerado apenas no estágio de trabalho de campo da auditoria. Baseado no que está no parágrafo **Planejamento — Utilize a análise de dados com antecedência,** O que grupo conclui sobre isso?
3. O que o grupo entendeu sobre auditoria horizontal, e o quais benefícios teriam?
4. O que o grupo entendeu sobre **Trabalho de campo/Documentação — Obtenha acesso primário às evidências?**
5. O que o grupo entende sobre os benefícios e problemas na utilização de vídeos na auditoria?

O Assunto abordado neste artigo será pedido em prova

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação



Dias Claudia; Segurança e Auditoria da tecnologia da informação Claudia Dias Indaial : Editora Axcel Books, 2000

Gross, Christian Meinecke; Segurança em tecnologia da informação / Christian Meinecke Gross; Jan Charles Gross. Indaial : Uniasselvi, 2013.

Hintzbergen, Julie; Fundamentos de Segurança da Informação: Com base nas normas ISO 27001 e na ISO 27002 / Julie Hintzbergen, Kees Hintzbergen, André Smulders, Hans Baars; Tradução Alan Sá – Rio de Janeiro : Brasport, 2015

Imoniana, Joshua Onome; Auditoria de Sistemas de Informação / Joshua Onome Imoniana; 2. ed. – 2. reimpr; S;ao Paulo : Atlas, 2010

Lyra, Maurício Rocha; Governança da Segurança da Informação / Edição do Autor, 2015

Sêmola, Marcos; Gestão da Tecnologia da Informação: visão executiva da segurança da informação : aplicada a Security Officer / Marcos Sêmola e Módulo Security Solutions S.A. Rio de Janeiro : Elsevier, 2003 – 10ª reimpressão

Silva, Michel Bernardo Fernandes da, Cibersegurança uma visão panorâmica sobre segurança da informação na internet / Michel Bernardo Fernandes da silva. – Rio de Janeiro : Freitas Bastos, 2023.

EDUCAÇÃO METODISTA