**INTRODUÇÃO**

A difusão e o uso intensificado dos sistemas de informação em um mundo cada vez mais interconectado leva a uma crescente preocupação com relação ao aparecimento de ameaças e sobretudo vulnerabilidades desses sistemas.  
A auditoria de sistemas de informação tem como objetivo assegurar a integridade e a segurança dos dados que trafegam pelas redes e pelos sistemas de informação.

A segurança dos sistemas de informação é bastante solicitada. Nesse campo, destaca-se o auditor de sistema

poderá contribuir para a construção de sistemas de informação cada vez mais seguros.

**PRINCIPAIS CONCEITOS**

**Conceitos e princípios da auditoria de sistemas**

Inicialmente torna-se necessário entender e definir o termo ‘auditoria’, que vem de cargo ou função de auditor, podendo ser definido como um processo de verificação e análise de atividades desenvolvidas por determinada empresa e cujo objetivo principal é examinar se estas atividades estão de acordo com o que foi planejado ou estabelecido anteriormente pela organização.  
Muitos autores definem auditoria como um exame sistemático de atividades desenvolvidas em determinada empresa ou setor, tendo como objetivo principal a sua averiguação para identificar se estão de acordo com o que foi planejado e estabelecido previamente.  
Para Lyra (2008), a auditoria de sistemas tem ligação com a adequação, revisão, avaliação e recomendações para o aprimoramento dos controles internos nos sistemas de informações de uma ou várias empresas.  
De acordo com Manotti (2010), a auditoria de sistemas tem vital importância para um bom desempenho dos sistemas de informação, pois possibilita a avaliação de controles necessários para que os sistemas sejam confiáveis e seu nível de segurança seja adequado.  
Importante aqui o entendimento de que a auditoria de sistemas de informação deve trabalhar na busca pela otimização de processos antes defasados e a inovação deve ser vista como um dos importantes fatores para a busca constante por eficácia e, sobretudo, segurança que devem ser vistos norteadores do processo de auditoria.  
Conforme Gil (1999), os resultados gerados para eficácia e eficiência das auditorias são fundamentais para a determinação de processos que permitam o alcance da qualidade da computação necessária.  
Aqui a TI (Tecnologia da Informação) pode ser vista como um mapa estratégico em que os processos desenhados nos sistemas empresariais estão alinhados com os principais processos da organização.  
Agora, para Imoniana (2005), um sistema de informação deve ser visto pela auditoria dividido em controles internos, que são planos da organização com objetivos a manter o ativo, verificando veracidade de registros, exatidão, promovendo a efetividade dos sistemas de informação para que as adesões às políticas organizacionais possam representar controles de segurança e privacidade de entrada, preparação, processamento e principalmente controles de recuperação, armazenamento de dados e saída.  
A equipe de gestão da TI deve ser composta por profissionais capacitados para a condução do programa e serão parte da equipe de auditoria da organização, tendo sido feita pelos auditores selecionados e recrutados conforme conhecimentos e habilidades das áreas de sistemas e negócios.  
Os objetivos gerais da auditoria de sistemas para Lyra (2008) são a integridade, confidencialidade, privacidade, acuidade, disponibilidade, auditabilidade, versatilidade e manutenabilidade.  
Importante destacar a LGPD ou Lei Geral de Proteção de Dados como fator talvez determinante e sobretudo oportunista no quesito oportunidades para que as organizações possam reavaliar os seus processos para o tratamento de dados e sobretudo sua segurança. Nesse ponto, a adoção da ‘auditoria de sistemas’ deve ser vista como uma contribuição não apenas para que a organização esteja em conformidade com a lei, mas também pensando-se em boas práticas relacionadas à governança de dados, visto que a auditoria tem por objetivo validar se os processos de uma organização estão em conformidade com diretrizes pré-determinadas pela organização.  
Portanto, a auditoria deve ser vista como um processo que visa verificar a estrutura de uma organização/corporação. Sua importância está principalmente na diminuição de falhas e fraudes que podem estar presentes nestes sistemas.

**VIDEOAULA: PRINCIPAIS CONCEITOS**

A auditoria de sistemas de informação tem em seus principais mecanismos de controle a adequação dos objetivos estratégicos da organização com os processos desenhados para os sistemas de informação. Para Manotti (2010), a auditoria de sistemas tem contribuído para a melhoria constante do negócio com suporte da tecnologia, em aspectos relacionados a desempenho, confiabilidade, integridade, disponibilidade, segurança, confidencialidade e privacidade.

Videoaula: Principais conceitos

**O PAPEL DO AUDITOR DE SISTEMAS**

O auditor de sistemas (TI) é o responsável por analisar e avaliar a infraestrutura tecnológica de uma empresa com objetivo de encontrar problemas relacionados a riscos e conformidade.   
Para White (2019), o papel do auditor de TI envolve desenvolvimento, implementação, teste e até mesmo a avaliação de procedimentos de revisão de auditoria, sendo papel de essencial importância nas organizações que têm determinada dependência tecnológica, visto que um pequeno erro técnico ou mesmo um passo em falso pode causar um impacto negativo em toda a empresa.  
Ainda segundo White (2019), o auditor de TI tem por responsabilidade avaliar e analisar a infraestrutura de uma empresa com objetivo de garantir que os processos e sistemas sejam executados com eficiência e precisão de forma a manter segurança e também atender às regulamentações de conformidade.  
White (2019) complementa que o auditor deve ser quem tem por finalidade identificar qualquer problema de TI que esteja relacionado à segurança e sobretudo ao gerenciamento de riscos, principalmente porque este profissional é o responsável hoje pela comunicação de suas descobertas a outras pessoas da organização e é também quem vai oferecer soluções para melhorar ou alterar processos e sistemas visando garantir a sua segurança e conformidade.  
A auditoria de TI tem sua extensão a redes, softwares, programas, sistemas de comunicação, sistemas de segurança e quaisquer outros serviços que sejam dependentes da infraestrutura tecnológica da empresa. Sua importância vai desde a avaliação dos processos e controles internos nas organizações, com esforços direcionados a manter a organização e seus dados protegidos contra ameaças externas e internas.  
White (2019) destaca que as auditorias podem ser auditorias automatizadas de processamento de dados, as quais são conhecidas como auditorias de computador. O autor complementa que as empresas podem executar uma ‘auditoria de segurança da informação’ para avaliação dos processos de segurança e gerenciamento de riscos da organização.  
Moscove, Simkin e Bagranoff (2002) destacam que o processo de Auditoria de Sistemas de informação vai englobar pessoas, procedimentos, equipamentos, aplicativos, comunicação de informações e banco de dados, ou seja, componentes que são parte da lista de elementos que o auditor examina.  
White (2019) vai tratar ainda dos requisitos do trabalho do auditor de TI com foco no descritivo da formação deste profissional, bem como das certificações que ele deve ter, sendo inicialmente exigido pelo menos um diploma básico em bacharelado em Ciência da Computação, Gerenciamento de Sistemas de Informação, Contabilidade ou Finanças.   
Este profissional também deverá ter grande experiência em TI ou SI (Sistemas de Informação), além de experiência em contabilidade pública ou mesmo auditoria interna.   
O trabalho do auditor vai exigir também um forte conjunto de habilidades técnicas, com ênfase em habilidades de segurança e, claro, comunicação, já que o papel do auditor é também explicar aos líderes o que está errado e o que precisa mudar. Aqui, as habilidades analíticas e de pensamento são cruciais já que estes profissionais precisarão encontrar as tendências e os padrões para identificar os problemas de segurança e infraestrutura de TI.

**VIDEOAULA: O PAPEL DO AUDITOR DE SISTEMAS**

A certificação CISA – *Certified Information Systems Auditor*, que atualmente é oferecida pela ISACA – *Information Systems and Control Association* é considerada uma das mais reconhecidas e avaliadas por organismos internacionais. O seu processo de seleção é composto de uma extensa prova que requer conhecimentos avançados além de experiência profissional comprovada.

Videoaula: O papel do auditor de sistemas

**INTRODUÇÃO AOS TIPOS DE AUDITORIA**

A classificação e os tipos de auditoria de sistemas de gestão vão ser importantes para empresas que já certificadas buscam ainda uma certificação nas normas ISO, pois somente por meio deste tipo de auditoria é que as empresas obterão o selo de certificação ou mesmo conseguirão manter o que já fora conquistado.  
Uma empresa pode, caso necessite, fazer diferentes tipos de auditoria, dependendo dos setores e das atividades que necessitem de abordagens específicas, visando certificar-se que estão em conformidade com os valores planejados ou estabelecidos previamente.  
A auditoria é, assim, uma ferramenta essencial para a boa gestão de qualquer negócio, permitindo avaliar se os processos estão sendo realizados adequadamente e propondo que a levem ao grau de qualidade desejado.  
As tipologias relacionadas à auditoria podem ser classificadas de várias formas. A auditoria de sistemas como um todo é o processo de verificação de todas as operações e transações de uma empresa. Ela deve ser feita de forma cuidadosa, sistemática, analítica, pericial e a avaliação periódica de como as tarefas planejadas estão sendo desempenhadas e sua eficácia também devem ser consideradas.  
Importante destacar aqui a existência dos diversos tipos de auditoria que variam conforme o setor que está em análise ou mesmo que realiza tal processo.  
Estes tipos de auditorias de sistema de gestão são importantes para empresas já certificadas ou mesmo que ainda buscam a certificação a partir das normas ISO, pois é a partir da auditoria que as empresas obterão ou manterão o selo de certificação.  
A Consultoriaiso (2018) destaca que as auditorias podem ser divididas em três tipos principais, a saber: auditoria interna, conhecida também como auditoria de primeira parte; a auditoria no fornecedor, ou chamada de auditoria de segunda parte e, por último, a auditoria externa, ou mesmo auditoria de terceira parte, podendo ser estabelecida para fins de certificação para propósitos legais, regulamentares e similares.  
Ainda segundo Consultoriaiso (2018), a auditoria interna é realizada pela própria empresa com o objetivo de auditar seus próprios sistemas, processos e procedimentos, visando validar se os próprios parâmetros dos sistemas de gestão estão sendo seguidos e os resultados esperados estão sendo alcançados com este processo. É a partir dessa auditoria que a informação para a melhoria contínua do sistema de gestão pode ser alcançado, na validação das não conformidades, observações levantadas e mesmo a partir da identificação das principais oportunidades de melhoria.  
Lembra Consultoriaiso (2018) que para a realização da auditoria se faz necessário a existência de colaboradores que sejam treinados na ISO 19011 e no sistema de gestão que será auditado, mas também é possível contratar uma outra empresa para a realização da auditoria interna.  
Já o auditor interno, segundo a Consultoriaiso (2018), deve ter competência para a execução das auditorias, ou seja, deve ter escolaridade, experiência, habilidades e conhecimentos necessários para atender ao que se espera desse processo.  
Normalmente, as auditorias internas funcionam como uma preparação para a auditoria de certificação, ou mesmo a recertificação, mas devem ser vistas como uma oportunidade de a empresa melhorar os seus processos, aumentando assim a satisfação de seus clientes.  
Cabe às empresas a definição da periodicidade destas auditorias internas, considerando assim o tipo de processo, ramo de atuação, a cultura organizacional, a política e principalmente o contexto organizacional.  
Consultoriaiso (2018) destaca que para a realização de uma auditoria interna existem etapas que devem existir, como a preparação (1), em que é analisada toda a documentação do sistema de gestão e desenvolvido o programa de avaliação e o planejamento detalhado. Trata-se da etapa em que todos os participantes ou partes interessadas vão ser comunicados sobre a realização do processo, sua data e escopo.  
Na parte 2 acontece a reunião de abertura, em que serão expostos os objetos a serem alcançados pela auditoria. Na parte 3 a auditoria de fato acontece, com avaliação no local, entrevistas com colaboradores e coleta de evidências.  
Em quarto (4) acontece a reunião de encerramento e aqui os resultados serão expostos e apresentados à empresa. Finalmente (5) será elaborado o relatório de auditoria interna, em que serão abordadas as ações corretivas com o acompanhamento e a manutenção das avaliações.  
Na auditoria no fornecedor, a característica principal, segundo Consultoriaiso (2018), seria a realização pela empresa ou mesmo por outras pessoas em nome da empresa, tendo por objetivo avaliar a conformidade do sistema, dos requisitos legais e ou mesmo contratuais.  
Esta auditoria, continua Consultoriaiso (2018), desenvolve uma relação de confiança com os fornecedores, potencializando produtos com maior qualidade, minimizando riscos e diminuindo as não conformidades.  
Neste tipo de auditoria, a avaliação é relacionada à organização e qualificação dos recursos humanos; cumprimento da legislação; gestão e controle da qualidade; política ambiental; localização e acessos às instalações; concepção e desenvolvimento do produto; compras; recebimento de matérias-primas; produção e acondicionamento do produto final; condições do trabalho (segurança, higiene e limpeza) e, por último e não menos importante, a expedição e o tratamento de reclamações.  
Complementa Consultoriaiso (2018) que a negligência com os fornecedores pode gerar muitos prejuízos, como negligenciar fornecedores uma vez que a responsabilidade por resíduos é compartilhada.  
O último dos tipos de auditoria, a auditoria externa (3), é segundo Consultoriaiso (2018) realizada por um auditor independente, designado por um órgão certificador credenciado pelo INMETRO, com objetivos de certificar o sistema de gestão da empresa.  
Esta fase da auditoria é vista como a última fase do processo de certificação, tendo por objetivo documentar, implementar e manter uma norma específica de um sistema de gestão da organização.  
Se tratarmos exclusivamente da auditoria de sistemas, podemos considerar diversos tipos que têm relação com esta auditoria, especificamente a ‘auditoria de planejamento e gestão’ que tem relação com a contratação de bens e serviços de TI, documentações, orçamentos, projetos e outros.  
A auditoria legal ou regulatória atende regulamentações locais e internacionais que como exemplo possui a Lei *Sarbanes-Oxley*, Basileia II, Comissão de Valores Mobiliários e outros. Já a auditoria de integridade de dados trata da classificação dos dados, atualização, banco de dados, aplicativos, acessos, estudo dos fluxos (entradas e saídas) de transmissão, controles de verificação de qualidade e confiabilidade das informações.  
A auditoria de segurança da informação trata de métodos de autenticação, autorização, criptografia, gestão de certificados digitais, segurança de redes, gestão dos usuários, configuração de antivírus, atualizações, políticas, normas e manuais operacionais.  
A auditoria de segurança física que trata da avaliação de localidades e riscos ambientais, que vai tratar da proteção de vidas (capital intelectual), furto/roubo, acesso, umidade, temperatura, acidentes, desastres e as proteções como perímetros de segurança, câmeras, sensores, guardas, dispositivos e proteções do ambiente.  
A auditoria de desenvolvimento de sistemas valida os processos de gestão de projetos, cumprimento de metodologia de qualidade, orçamentos previstos e realizados e também a avaliação de desvios.  
A auditoria da infraestrutura e operações de TI trata de processos que buscam averiguar a disponibilidade e robustez do ambiente a erros, acidentes e sobretudo fraudes das operações em servidores, estações, *software*, *hardware* e também canais de comunicação.

**VIDEOAULA: INTRODUÇÃO AOS TIPOS DE AUDITORIA**

A técnica de simulação de dados é considerada uma das técnicas utilizadas na auditoria de integridade de dados que é um dos tipos de auditoria de sistemas aplicáveis em uma auditoria. Segundo Manotti (2010), esta técnica corresponde à elaboração de um conjunto de dados de teste que são submetidos ao programa de computador ou mesmo a uma determinada rotina que compõe e que necessita ser verificada em sua lógica de processamento.   
Esta técnica aplicável ao processo auditado leva em consideração a correção de todos os resultados que forem gerados a partir daquela rotina irregular. O processo leva em consideração que o conjunto de dados precisa prever situações corretas e situações incorretas, como transações com campos inválidos, com valores ou quantidades nos limites de tabelas de cálculos, transações incompletas, incompatíveis ou mesmo em duplicidade.

Videoaula: Introdução aos tipos de auditoria

**ESTUDO DE CASO**

Uma *software house*(empresa que constrói software) tem um sistema de gestão, ou seja, um sistema ERP (*Enterprise Resource Planning*) ou Sistema de Planejamento Empresarial que funciona atualmente em vários clientes e necessita de um consultor para planejar uma auditoria. Inicialmente, esta empresa precisa que este consultor possa explicar os principais conceitos relacionados à auditoria, o papel do auditor de sistemas e quais seriam os principais tópicos e ou tipos auditáveis neste sistema.  
Considere que você trabalha em uma empresa de consultoria, como analista de suporte e foi escolhido para dar suporte a esta *software house* de forma a auxiliá-la inicialmente neste processo de auditoria.  
O seu papel será criar um vídeo e ou mesmo uma apresentação para os gestores da empresa que possa detalhar os conceitos iniciais e relacionados à auditoria, o papel do auditor de sistemas e quais seriam os tópicos e ou tipos de auditoria e ou mesmo as partes dos sistemas de informação e gestão que seriam auditáveis.

**RESOLUÇÃO DO ESTUDO DE CASO**

Para que uma *software house* consiga lucros relacionados à  venda de suas soluções deve fornecer um produto que seja livre de problemas relacionados à auditoria. Nesse contexto e conforme a necessidade apresentada, você deve criar uma apresentação que possa mostrar os conceitos iniciais estabelecidos na aula 1, constando os principais benefícios ligados à auditoria de sistemas, principalmente no quesito “entendimento da solução” e mesmo das possíveis soluções alcançáveis com uma auditoria de sistemas.  
Nesta apresentação não deve faltar a importância do auditor de sistemas que é a figura central em um processo de auditoria e que precisa de conhecimentos e certificações específicos – no exemplo, ele deve ter conhecimentos em gestão, pois é esse o sistema a ser autitado.  
Outro dos itens que deve fazer parte da apresentação é a lista dos principais tópicos que deverão ser tratados durante a auditoria: Auditoria de Planejamento e Gestão para validar documentação, orçamentos, projetos e outros; auditoria legal e regulatória, para atender leis e regulamentações; auditoria de integridade de dados, para classificação dos dados, bancos de dados e outros; auditoria de segurança da informação, para tratar métodos de autenticação, autorização e criptografia; auditoria de segurança física, para avaliação de localidades e riscos ambientais; auditoria de desenvolvimento de sistemas, para validação dos processos de gestão de projetos e a auditoria de infra estrutura e operações de TI que funciona na averiguação de processos que trabalhem com a disponibilidade e robustez do ambiente a erros.

**Saiba mais**

Levando-se em conta os recentes avanços tecnológicos, sobretudo a globalização e as exigências de mercado que levam as empresas a buscar cada vez mais o lucro, a consequente diminuição dos custos e o aperfeiçoamento dos seus processos.  
As instituições financeiras por sua vez são empresas que cada vez mais necessitam de informatização principalmente pelo ativo com que trabalham diariamente.  
A dissertação indicada no link a seguir apresenta *frameworks* que podem ser utilizados para auxiliar e avaliar os softwares utilizados pela auditoria na organização: <https://repositorio.ipl.pt/bitstream/10400.21/3487/1/Disserta%C3%A7%C3%A3oFinal.pdf>. Acesso em: 2 ago. 2021.

A evolução tecnológica da computação e sobretudo os últimos avanços tornaram necessária a adoção de processos de auditoria sobretudo no quesito segurança. A seguir, apresenta-se um mapa mental para reflexão sobre os tópicos abordados até o momento e que envolvem os tipos de auditoria e seus principais objetivos.

Figura | Tipos e objetivos de auditorias

Fonte: elaborada pelo autor.

Resolução do Estudo de Caso

**Aula 2**

**OBJETIVOS DA AUDITORIA DE SISTEMAS**

*A auditoria de sistemas de informação conforme Soares (2010) pode ser definida como a atividade que visa recolher e avaliar evidências com vista a determinar: se um sistema de informação tem integridade; se contribui de forma plena para o alcance eficaz dos objetos da organização; se utiliza de forma eficaz os recursos que lhe estão afetos de forma eficiente e se a função organizacional que o dirige tem competências, processos e recursos necessários e mesmo suficientes para o cumprimento da sua missão.*

*21 minutos*