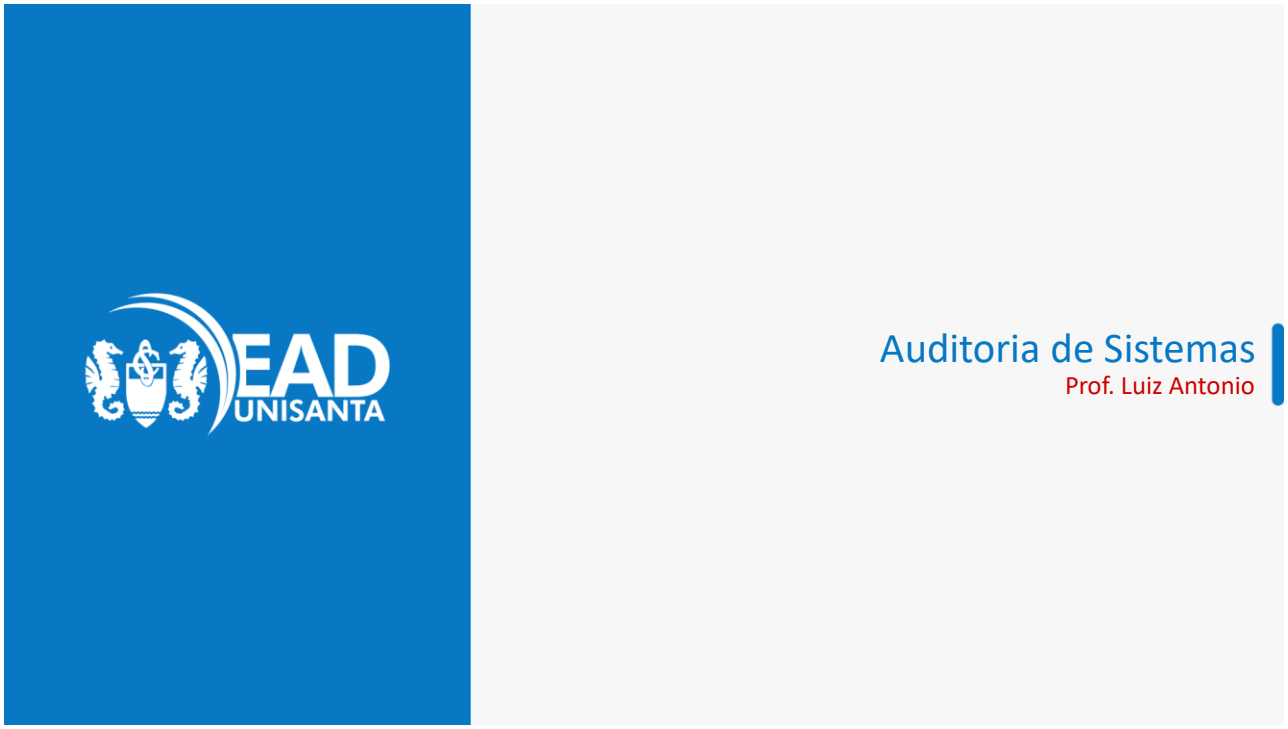


Auditoria de Sistemas

Prof. Luiz Antonio

AULA 01
Fundamentos da Auditoria de Sistemas

Conceito de auditoria

A auditoria é uma função independente que busca priorizar a qualidade dos processos e otimizar os resultados operacionais, envolvendo uma técnica, uma análise, um levantamento criterioso, um estudo e uma forma de avaliação sistemática dos procedimentos, práticas e rotinas internas de uma organização.

O objetivo da auditoria é em primeiro lugar compreender e reconhecer como o negócio da organização opera, quais são suas vantagens, dificuldades e seu processo de desenvolvimento, que são voltados os trabalhos para proporcionar informações sólidas e seguras que muito contribuirão com desenvolvimento organizacional. A responsabilidade de um processo de auditoria vai além de um simples parecer, uma vez que se propõem é manter uma preocupação contínua com os resultados da organização, envolvendo a postura dos dirigentes quanto a tomada de decisões, observando a confiabilidade das informações e sua transparência junto aos acionistas, sociedade e ao público em geral.

Tipos de auditoria

Auditoria Contábil

A auditoria contábil é um processo de análise da situação financeira da empresa que permite atestar a precisão dos registros contábeis, identificar falhas de controle ou mesmo fraudes e irregularidades na gestão.

Ela é realizada a partir do exame de documentos contábeis e de inspeções internas, contando ainda com a apuração de informações junto a fontes externas. Podem ser auditados o fluxo de caixa, o balanço patrimonial e a Demonstração de Resultado de Exercício (DRE).

Por suas características, a auditoria é capaz de apresentar ao empreendedor uma opinião embasada sobre a realidade financeira do negócio, com segurança e transparência, permitindo a ele conhecer os problemas, suas causas e consequências, além de receber orientações sobre possíveis correções a implantar.

Tipos de auditoria

Auditoria de controles internos

Toda empresa visa à continuidade, ou seja, a capacidade de produzir riqueza e gerar valor continuadamente sem interrupções. Porém, para que isto ocorra, é necessário a criação de mecanismos de controle interno. Dentre esses mecanismos, está a auditoria de controles internos. Pode-se definir como controle interno o conjunto de normas, políticas, procedimentos, instrumentos e ações estabelecidas pela empresa, com o objetivo de enfrentar riscos, visando:

a) Garantir a segurança e a integridade dos ativos e dos sistemas de informação;

b) Reduzir a possibilidade de perdas financeiras e do desgaste da imagem institucional;

c) Desenvolver o negócio, a fim de atingir o resultado das operações;

d) Prover eficiência e eficácia das operações;

e) Dar conformidade às leis, regulamentos, normas e dispositivos estatutários aplicáveis à organização;

f) Incrementar a qualidade das informações financeiras ou contábeis.

Tipos de auditoria

O controle interno, para ser prático, deve ser adequado ao tamanho e ao porte das operações da empresa. Além disso, precisa ser objetivo no que se pretende controlar e ser simples em sua aplicação. Precisa, principalmente, ser econômico, levando em consideração a relação custo-benefício.

Bons controles internos, acompanhados de uma auditoria independente, adicionam valor à sua empresa, e dão maior credibilidade aos clientes, fornecedores e investidores. Na ausência de controles internos, existe o risco de a administração tomar decisões (operacionais ou estratégicas) incorretas.

Tipos de auditoria

Auditoria ambientais

As Auditorias Ambientais são um processo sistemático no qual a empresa avalia a sua adequação aos critérios estabelecidos, que podem ser requisitos legais, normas ou exigências definidas pelos seus clientes ou pela própria empresa.

Pode-se dizer que a auditoria ambiental é uma ferramenta para levantamento, controle e monitoramento dos aspectos ambientais das empresas. Ela é realizada de forma clara e objetiva, sendo que os resultados do processo são comunicados para as partes interessadas.

Em relação aos objetivos, alguns exemplos de auditorias são descritos a seguir:

Tipos de auditoria

a) Auditoria de Conformidade Legal: a auditoria de conformidade legal tem o objetivo de avaliar a adequação da empresa às normas legais aplicáveis à sua atividade. Esse tipo de auditoria é empregado pelas empresas para prevenir eventuais penalidades pelo não atendimento à legislação ambiental. Pode ser utilizada também para verificação em auditorias de fornecedores, que tem como objetivo verificar o atendimento dos requisitos legais de seus fornecedores. De certa forma, toda a auditoria ambiental tem em sua base a avaliação da conformidade legal, uma vez que este é um requisito fundamental da organização;

b) Auditoria Ambiental de Acompanhamento: a auditoria ambiental de acompanhamento tem por objetivo verificar se as condições estabelecidas em uma auditoria estão sendo cumpridas. Por exemplo, uma empresa que deseja se certificar pode ter algumas não conformidades e/ou pontos de melhorias para serem tratados. Nesse caso, a auditoria de acompanhamento irá verificar se estes pontos levantados foram sanados para o processo de certificação;

c) Auditoria Ambiental de Responsabilidade ou *Due Diligence*: o principal objetivo desse tipo de auditoria é avaliar a existência de passivos ambientais da empresa que possam impactar o negócio em um processo de compra e venda. Estas auditorias também podem ser requeridas por investidores ou bancos em processos de garantias, que desejam verificar os riscos relacionados à determinada empresa.

Conceito de Sistemas

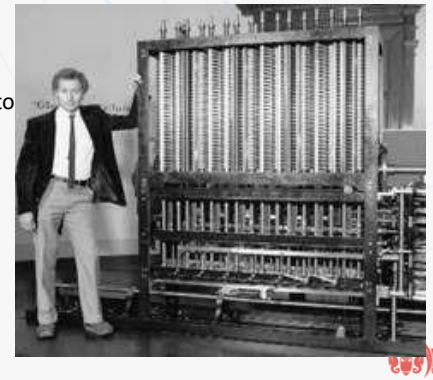
Um sistema é um conjunto de elementos inter-relacionados com um objetivo: produzir relatórios que nortearão a tomada de decisões gerenciais. Neste percurso, pode-se identificar o processo de transforma dados de entrada, agregados aos comandos gerenciais, em saídas. Assim, o feedback do sistema faz com que, no meio da manutenção do ciclo operacional, sejam ativadas novas estratégias empresariais visando à geração de informações qualitativas ou quantitativas para suportar o alcance do sucesso.

Os sistemas são abertos ou fechados. Os sistemas abertos podem receber dados controlados ou não controlados, uma vez que recebem influência do ambiente interno e externo onde operam, enquanto os sistemas fechados, devido à sua natureza, não têm interferência do ambiente e somente poderiam receber os dados controlados. As delimitações dos sistemas são feitas propositadamente durante seu desenho simplesmente para fomentara segregação das funções dos sistemas incompatíveis. Podem ser tanto adaptáveis, quando implantados para produzir um resultado desejado em um ambiente de grandes mudanças rotineiras, como também corretivos, implantados para produzir um resultado específico e não rotineiro.

Evolução dos sistemas computacionais

Um sistema computacional é um conjunto de dispositivos eletrônicos utilizados para todo um processamento de alguma informação, ou seja, união de hardware (parte física) e software (parte lógica). Cronologicamente falando, a evolução do sistema computacional se deu em 5 gerações, que foram elas: computadores a válvula, computadores a transistor, circuitos integrados, circuitos VLSI e a dos computadores invisíveis.

O primeiro computador digital foi projetado pelo matemático Charles Babbage (1792-1871). Embora Babbage tenha dispendido muito de sua vida e de sua fortuna tentando construir sua "máquina analítica", ele jamais conseguiu por o seu projeto em funcionamento porque era simplesmente um modelo matemático e a tecnologia da época não era capaz de produzir rodas, engrenagens, dentes e outras partes mecânicas para a alta precisão que necessitava.



A primeira geração (1945 -1955): Válvulas e painéis

Após os esforços de Babbage, quase não houve progresso nesta área até o início da Segunda Grande Guerra. Em torno de 1940, pesquisadores tiveram sucesso na construção de computadores baseados em válvulas. Tais máquinas eram enormes, ocupavam salas imensas e empregavam dezenas de milhares de válvulas em sua construção.

No ano de 1946, ocorreu uma revolução no mundo da computação com o lançamento do computador ENIAC (figura 2). A principal inovação nesta máquina é a computação digital, muito superior aos projetos mecânicos-analógicos desenvolvidos até então. Com o ENIAC, a maioria das operações era realizada sem a necessidade de movimentar peças de forma manual, mas sim pela entrada de dados no painel de controle. Cada operação podia ser acessada através de configurações-padrão de chaves e switches.

A primeira geração (1945 -1955): Válvulas e painéis

Toda a programação era feita em código absoluto, muitas vezes através da fiação de painéis para controlar as funções básicas da máquina. No início dos anos 50, houve uma sensível melhora no uso de tais máquinas como o advento do cartão perfurado que tornou possível a codificação de programas em cartões e leitura pela máquina, dispensando a programação através de painéis.

A segunda geração (1955 -1965): Transistores e Sistema Batch

O desenvolvimento do transistor em meados dos anos 50 veio a alterar substancialmente o quadro descrito na segunda geração. Com o emprego desta nova tecnologia, os computadores tornaram-se confiáveis a ponto de serem comercializados.

Os computadores da segunda geração eram usados maciçamente na realização de cálculos científicos e de engenharia, tal como a obtenção da solução de equações diferenciais parciais. Eles eram normalmente programados em linguagem FORTRAN ou em linguagem de montagem. Surgem os sistemas operacionais da época que eram o FMS e o IBSYS.

O IBM 7030 (figura 3), também conhecido por Strech, foi o primeiro supercomputador lançado na segunda geração, desenvolvido pela IBM. Seu tamanho era bem reduzido comparado com máquinas como o ENIAC, podendo ocupar somente uma sala comum. Ele era utilizado por grandes companhias, custando em torno de 13 milhões de dólares na época.

A terceira geração (1965 -1980): Cis e multiprogramação

Os sistemas de terceira geração vieram a popularizar várias técnicas que não estavam implementadas nos sistemas de segunda geração, a mais importante essas técnicas é a Multiprogramação.

Sistemas operacionais de terceira geração agora tinha a capacidade de ler Jobs (um programa ou um conjunto de programas) de cartão direto para disco. Desta forma, assim que um "job ativo" terminasse, o sistema operacional carregaria um novo "job" na partição livre da memória, proveniente do disco.

Um dos principais exemplos da terceira geração é o IBM 360/91, lançado em 1967, sendo um grande sucesso em vendas na época. Esta máquina já trabalhava com dispositivos de entrada e saída modernos, como discos e fitas de armazenamento, além da possibilidade de imprimir todos os resultados em papel. O IBM 360/91 foi um dos primeiros a permitir programação da CPU por microcódigo, ou seja, as operações usadas por um processador qualquer poderiam ser gravadas através de softwares, sem a necessidade do projetar todo o circuito de forma manual.

A quarta geração (1981-1990): Computadores pessoais

A grande disponibilidade de poder computacional, levou ao crescimento de uma indústria voltada para a produção de software s para os computadores pessoais. A maioria destes softwares é "amena ao usuário" (*user-friendly*), significando que eles são voltados para pessoas que não têm nenhum conhecimento de computadores, e mais que isto, não têm nenhuma vontade de aprender nada sobre esse assunto. Certamente esta foi uma mudança grande na filosofia de desenvolvimento dos sistemas operacionais.

E outro desenvolvimento importante que começou a tomar corpo em meados dos anos 80 foi o dos sistemas operacionais para redes e o dos sistemas operacionais distribuídos. Em uma rede de computadores, os usuários estão conscientes da existência de um conjunto de máquinas conectadas à rede, podendo, portanto, ligar-se a máquinas remotas e solicitar serviços destas. Cada uma destas máquinas roda seu próprio sistema operacional e tem seu próprio usuário ou usuários.

Em contraste, um sistema distribuído faz com que um conjunto de máquinas interligadas apareça para seus usuários como se fosse um única máquina com um só processador. Em tais sistemas, os usuários não tomam conhecimento de onde seus programas estão sendo processados ou mesmo onde seus arquivos estão sendo armazenados, pois tudo isso é manipulado automática e eficientemente pelo sistema operacional.

A quinta geração (1990 -hoje): Computação distribuída

Os computadores da quinta geração usam processadores com milhões de transistores. Nesta geração surgiram as arquiteturas de 64 bits, os processadores que utilizam tecnologias RISC (acrônimo de *Reduced Instruction Set Computer*; em português, "Computador com um conjunto reduzido de instruções") e CISC (sigla para *Complex Instruction Set Computer*, ou, em uma tradução literal, "Computador com um Conjunto Complexo de Instruções"), discos rígidos com capacidade superior a 600 Gb, pendrives com mais de 100GB de memória e utilização de disco ótico com mais de 1 Tb de armazenamento.

A quinta geração está sendo marcada pela inteligência artificial e por sua conectividade. A inteligência artificial pode ser verificada em jogos e robores ao conseguir desafiar a inteligência humana. A conectividade é cada vez mais um requisito das indústrias de computadores. Hoje em dia, queremos que nossos computadores se conectem ao celular, a televisão e a muitos outros dispositivos como geladeira e câmeras de segurança.

A importância da segurança da informação

A auditoria de segurança da informação só tem sentido por permitir melhoria do tratamento da informação na organização. Ela cumpre basicamente as mesmas funções de uma auditoria de sistemas de informação, tais como descritos por Imoniana (2004) e por Schmidt, dos Santos e Arima (2005). A informação é produzida, identificada, armazenada, distribuída, usada e processada em todos os níveis da organização, visando o alcance dos objetivos de negócio, sejam eles públicos ou privados. Essas atividades constituem a gestão da informação, que tem suas práticas definidas pelos sistemas de informação que apoiam os processos de trabalho na organização, sejam eles manuais ou automáticos.

A mensagem da necessidade de segurança da informação é usualmente estabelecida por uma política. A política de segurança da informação, tratada em detalhes no texto de Souza Neto (2010), deve tornar claro que cada participante ou colaborador na organização (agentes em geral) é um ator relevante quando se trata de proteger ativos de informação, principalmente aqueles considerados estratégicos ou críticos. Além disso, responsabilidades claras devem ser atribuídas aos agentes, de modo que se possam distribuir tarefas específicas ou gerais para que se esteja sempre aperfeiçoando os mecanismos de segurança da informação implantados. De forma mais prática, a política de segurança da informação é o principal controle de segurança numa organização, e a ele se articulam (e na maioria dos casos se subordinam) todos os demais controles.

A importância da auditoria da segurança da informação

O objetivo é, basicamente, atestar que os controles de segurança em prática são eficientes e eficazes. Tal evita exposições da organização a riscos que podem provocar danos, se concretizados. Mair (1998) indica que a introdução de controles evita:

I. Manter registros de informação que estão errados;

II. Contabilizar informações que não são aceitáveis;

III. Interromper o negócio;

IV. Decidir erroneamente sobre gerenciamento; e dentre outras razões;

V. Evitar fraudes.

A importância da auditoria da segurança da informação

No ambiente desregulado dos sistemas de informação expostos à Internet, é também importante destacar que os controles evitam que a organização esteja sujeita a ataques de hackers. O que se busca, efetivamente, é a preservação dos princípios que norteiam o universo da tecnologia da informação: a disponibilidade, a integridade e o caráter confidencial da informação. Uma auditoria busca identificar fragilidades que podem ser exploradas por ameaças internas e externas à uma organização, assim considerando:

i. O comprometimento do sistema de informações, por problemas de segurança, pode causar grandes prejuízos à organização. Diversos tipos de incidentes podem ocorrer a qualquer momento, podendo atingir a informação confidencial, a integridade e disponibilidade;

ii. Problemas de quebra de confidencialidade, por vazamento ou roubo de informações sigilosas, podem expor para o mercado ou concorrência as estratégias ou tecnologias da organização, eliminando um diferencial competitivo, comprometendo a sua eficácia, podendo perder mercado e até mesmo ir à falência;

A importância da auditoria da segurança da informação

iii. Problemas de disponibilidade podem ter um impacto direto sobre o faturamento, pois deixar uma organização sem matéria-prima ou sem suprimentos importantes ou mesmo, o impedimento de honrar compromissos com clientes, prejudicam sua imagem perante os clientes, gerando problemas com custos e levando a margem de lucro a ficar bem comprometida;

iv. Problemas de integridade, causados por invasão ou fatores técnicos em dados sensíveis, sem uma imediata percepção, irão impactar sobre as tomadas de decisões. Decisões erradas fatalmente reduzirão o faturamento ou aumentarão os custos, afetando novamente a margem de lucros;

v. A invasão da página de Internet de uma empresa, com modificação de conteúdo, ou até mesmo a indisponibilidade de serviços on-line, revela a negligência com a segurança da informação e causa perdas financeiras a quem sofreu algum tipo de ataque.