

AUDITORIA EM TECNOLOGIA E SISTEMAS DE INFORMAÇÃO

A decorative graphic element consisting of several horizontal lines of varying lengths and colors (teal, light blue, and white) extending from the left side of the slide towards the right, positioned below the main title.


Introdução

O aumento da utilização de sistemas informatizados nas empresas e sua importância estratégica levaram as organizações a reforçar o controle sobre o processamento de dados.


Isso é feito por meio de auditorias, cujo objetivo é identificar irregularidades e áreas de preocupação nos setores de processamento de dados e nos centros de processamento da empresa.

A auditoria também ajuda a identificar áreas que podem requerer correções e desagradar a alta administração.

No passado, a investigação estava principalmente concentrada nas finanças, levando as empresas a não manterem departamentos internos de auditores, preferindo contratar empresas especializadas.



Atualmente, devido à crescente dependência da tecnologia, a manutenção de um departamento de auditoria interna tornou-se essencial.



Essa prática começou nos Estados Unidos e na Europa nos anos 1980 devido ao rápido avanço das técnicas de processamento e estratégias para contornar os controles, exigindo que os auditores estejam constantemente vigilantes às mudanças no campo.

A auditoria sistemas de informação deve abranger todas as suas áreas, como:

- Coordenação de problemas.
- Coordenação de mudanças.
- Sistemas em processamento "batch".
- Recuperação de desastre.
- Capacidade dos sistemas.
- Desempenho dos sistemas.
- Desenvolvimento de sistemas.
- Sistemas em processamento online.
- Sistemas financeiros.
- Rede de telecomunicações.
- Segurança de informação.
- Centro de computação.
- Equipamentos.
- Distribuição dos custos.

Perfil do profissional auditor em informática

- O auditor, designado pela alta administração, avalia e examina os setores auditados em busca de falhas.
- O auditado é o departamento ou pessoa sujeita à auditoria.
- O auditor deve ser altamente especializado em tecnologia e demonstrar objetividade, discrição, raciocínio lógico e independência.
 - Seus relatórios devem manter integridade e apontar problemas na administração do auditado.

Posicionamento da auditoria dentro da organização

O departamento de auditoria deve ser independente e manter uma ligação direta com a alta administração.

O planejamento antecipado, com datas e procedimentos definidos para as auditorias, é crucial.

A confidencialidade do planejamento é essencial para evitar ajustes de última hora que possam distorcer os relatórios e prejudicar a organização.

Importância da auditoria e suas fases

- Conforme mencionado anteriormente, a auditoria dentro de um departamento, especialmente na área de tecnologia da informação, desempenha um papel crucial para a empresa. Através dela, a alta administração define a direção da organização, previne fraudes e assegura o adequado desempenho dos setores sujeitos à auditoria.
- Esse processo envolve etapas de pré-auditoria, auditoria e pós-auditoria.

Pré-auditoria

Nesta etapa, o departamento sujeito à auditoria recebe uma notificação formal com até duas semanas de antecedência, detalhando as áreas e planos de trabalho a serem auditados.

A alta administração e os auditores realizam reuniões iniciais para esclarecer pontos e planos de trabalho.

Os auditores cuidam das atividades administrativas necessárias, como a definição das áreas a serem auditadas, orientação da equipe, preparação da notificação e comunicação com o setor de auditoria.

O departamento auditado se prepara administrativamente, educando sua equipe sobre o processo, determinando informações necessárias e conduzindo uma revisão final.

Auditoria

Após as reuniões iniciais e definição das ações, a auditoria começa com solicitações formais por escrito do auditor chefe ao departamento auditado.

As descobertas são apresentadas e registradas em reuniões de acordo com as datas estabelecidas na fase de pré-auditoria.

O departamento auditado emite um relatório com justificativas para qualquer discordância, que é incluída no resumo executivo se não for aceita pelos auditores.

Auditoria

O relatório final, que também inclui uma avaliação da área auditada, é apresentado à alta administração após cerca de seis semanas de auditoria.

O grupo de auditores avalia os controles, documenta discrepâncias, valida soluções e prepara o relatório final.

O departamento auditado fornece informações, analisa as discrepâncias, desenvolve planos de ação, faz correções e revisa o resumo executivo.

Pós-auditoria



Após a auditoria, é elaborado um relatório final que descreve o objetivo da auditoria, áreas avaliadas, descobertas, recomendações corretivas e uma avaliação geral.



O relatório é distribuído a todas as instâncias administrativas, começando pela presidência e chegando ao departamento auditado.

Pós-auditoria



O departamento auditado deve abordar as discrepâncias, preparar uma resposta ao relatório final e gerenciar as correções para garantir eficácia e prevenir recorrências.



O grupo de auditores distribui o relatório, revisa respostas, assegura a implementação das ações acordadas e monitora tendências de correção ao longo do tempo.

A auditoria em segurança da informação

A segurança e a auditoria estão interligadas, com a segurança garantindo a integridade dos dados e a auditoria confirmando essa integridade para um processamento adequado. Isso é essencial para a competitividade das empresas.

A auditoria verifica se os requisitos de segurança da informação estão sendo implementados de maneira satisfatória, protegendo os dados e ativos da empresa. O auditor avalia o plano de segurança, atualiza-o conforme necessário e verifica sua aplicação no departamento auditado.

- O auditor deverá examinar os seguintes aspectos, verificando se:
 - O proprietário (aquele que tem permissão para acessar um conjunto de informações), periodicamente faz uma revisão em todos os dados que ele possui acesso para averiguar se houver perdas, alterações, ou outros problemas de qualquer natureza.
 - O centro de computação deve ser avisado sobre os resultados obtidos pela revisão, tanto quando eles forem favoráveis (os dados estão corretos) quanto quando for encontrada alguma irregularidade.
 - Todos os proprietários estão identificados, ou seja, os que possuem acesso a um conjunto de informações específicas.

- Os inventários são realizados conforme requerido e padronizados periodicamente.
- Os dados possuem a proteção necessária para garantir sua integridade, protegendo-os contra acessos e alterações indevidas.
- As documentações necessárias devem ser avaliadas pelas áreas competentes, garantindo que demonstrem o que realmente ocorre dentro do setor a que se referem.
- Os programas críticos, ou seja, os programas de sobrevivência da empresa mais importantes são seguros o suficiente para que qualquer tentativa de fraude não consiga alterar o sistema.
- Um terminal tem acesso somente às informações inerentes àqueles que irão manipulá-lo
- As senhas devem possuir trocas automáticas garantidas.

Fundamentos de auditoria em segurança da informação

- A **ISO 27001** estabelece os requisitos para a implementação de um **Sistema de Gerenciamento de Segurança da Informação (SGSI)** em uma organização. A auditoria é uma parte importante do processo de manutenção e avaliação contínua do SGSI.
- A ISO 27001 possui uma estrutura que inclui várias seções e categorias relacionadas à auditoria. A estrutura geral da norma é a seguinte:

- Introdução e contexto da organização
- Escopo
- Referências normativas
- Termos e definições
- Contexto da organização
- Liderança
- Planejamento
- Apoio
- Operação
- Avaliação de desempenho
- Melhoria

- A auditoria é principalmente abordada nas seções 9 (Operação) e 10 (Avaliação de desempenho). As seções específicas relacionadas à auditoria na ISO 27001 incluem:
 - **Seção 9.2: Avaliação de riscos e tratamento.**
 - **Seção 9.3: Controles e operações.**
 - **Seção 10.1: Monitoramento, medição, análise e avaliação.**
 - **Seção 10.2: Auditoria interna.**
 - **Seção 10.3: Análise crítica da alta administração.**
- **A Seção 10.2 é particularmente relevante para as atividades de auditoria, uma vez que estabelece os requisitos para a realização de auditorias internas, que são essenciais para a manutenção e avaliação do SGSI de acordo com a ISO 27001.** Essas auditorias internas visam assegurar que os controles de segurança da informação estejam funcionando conforme planejado e que o SGSI esteja atendendo aos requisitos da norma.

Como estabelecer requisitos de segurança da informação?

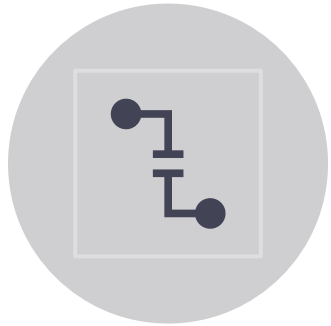
- É fundamental que uma organização identifique seus requisitos de segurança da informação, que podem ser originados a partir de três principais fontes:
 - **A primeira fonte é derivada da análise e avaliação de riscos da organização**, levando em consideração seus objetivos e estratégias globais de negócio. Através desse processo, são identificadas ameaças aos ativos e suas vulnerabilidades, com uma estimativa da probabilidade de ocorrência dessas ameaças e do potencial impacto nos negócios.
 - **Outra fonte relevante são as regulamentações legais em vigor**, estatutos, regulamentos e cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviços devem cumprir. Esses requisitos também são influenciados pelo contexto sociocultural em que a organização opera.

- **A terceira fonte de requisitos de segurança da informação consiste em um conjunto específico de princípios, objetivos e necessidades de negócio relacionados ao processamento de informações que uma organização deve desenvolver para sustentar suas operações.**

Analizando/avaliando os riscos de segurança da informação

- Os requisitos de segurança da informação são identificados por meio de uma análise sistemática e avaliação dos riscos em potencial. É crucial encontrar um equilíbrio entre os investimentos em controles de segurança e os possíveis danos aos negócios resultantes de falhas na segurança da informação.
- Os resultados dessa análise e avaliação desempenham um papel fundamental na orientação e definição de ações de gestão apropriadas, bem como na priorização do gerenciamento dos riscos de segurança da informação e na implementação dos controles selecionados para proteção.
- É recomendável que a análise e avaliação de riscos sejam realizadas periodicamente para abranger quaisquer mudanças que possam impactar os resultados.

Controles



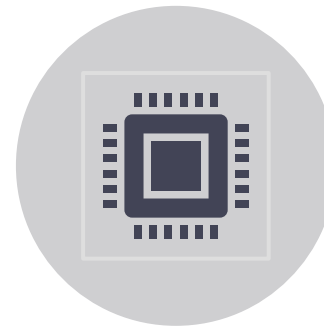
Os controles podem ser selecionados a partir da norma ISO/IEC 27001:2013 ou de um conjunto de controles ou novos controles podem ser desenvolvidos para atender as necessidades específicas, conforme apropriado.



A seleção de controles de segurança da informação depende das decisões da organização, com base nos critérios para aceitação de risco, nas opções para tratamento e no enfoque geral da gestão de risco aplicado à organização.



Convém que também seja sujeito a todas as legislações e regulamentações nacionais e internacionais relevantes.



Alguns dos controles da norma ISO/IEC 27001:2013 podem ser considerados como princípios básicos para a gestão da segurança da informação e podem ser aplicados na maioria das organizações.

- Aqui estão algumas das principais seções e categorias de controles da norma ISO/IEC 27001:2013:
 - **Política de Segurança da Informação:** Esta seção trata da definição das diretrizes e princípios gerais da segurança da informação na organização.
 - **Organização da Segurança da Informação:** Aborda a estrutura organizacional, funções e responsabilidades relacionadas à segurança da informação.
 - **Gestão de Ativos:** Envolve a identificação e classificação de ativos de informação, bem como a definição de medidas de proteção adequadas.
 - **Controle de Acesso:** Estabelece requisitos para garantir que o acesso às informações seja controlado e restrito de acordo com as necessidades.

- **Criptografia:** Aborda o uso de técnicas de criptografia para proteger as informações confidenciais.
- **Segurança Física e do Ambiente:** Lida com medidas de segurança física para proteger instalações, equipamentos e informações.
- **Segurança nas Operações:** Inclui requisitos para a operação segura de sistemas e redes, gerenciamento de incidentes de segurança e backups.
- **Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação:** Estabelece requisitos para garantir a segurança durante o ciclo de vida de desenvolvimento de sistemas.

- **Relacionamento com Fornecedores:** Aborda a segurança da informação em contratos com fornecedores e terceiros.
- **Monitoramento e Avaliação:** Envolve a monitorização contínua do SGSI, revisões de desempenho e auditorias internas.
- **Melhoria:** Aborda o processo de melhoria contínua do SGSI com base em resultados de auditorias, revisões de desempenho e incidentes de segurança.
- A norma ISO/IEC 27001:2013 requer a implementação de todos os controles, manutenção de registros para documentar a conformidade e a melhoria contínua do Sistema de Gerenciamento de Segurança da Informação (SGSI). Auditorias internas e revisões regulares são fundamentais para garantir a conformidade contínua.

Técnicas de auditoria em TI e SI

- Principais técnicas de auditoria:
 - **Exames físicos:** consistem na verificação in loco, permitindo ao auditor formar opinião quanto à existência física do objeto ou item a ser examinado. Este exame deve possuir as seguintes características:
 - **Existência física:** comprovação visual da existência do item.
 - **Autenticidade:** discernimento da fidedignidade do item.
 - **Quantidade:** apuração adequada da quantidade real física.
 - **Qualidade:** comprovação visual ou laboratorial de que o objeto examinado permanece em perfeitas condições de uso.

- **Circularizações/confirmações formais:** é a técnica utilizada na obtenção de declaração formal e independente de pessoas não ligadas ao órgão/entidade, seja por interesses comerciais, afetivos, etc., de fatos ligados às operações de tal entidade.
- **Entrevistas:** consiste na formulação de perguntas e obtenção de respostas adequadas e satisfatórias.
- As técnicas descritas são algumas dentre várias existentes para os diversos tipos de auditoria.
- A seguir, são listadas as técnicas específicas para auditoria de tecnologia da informação e sistemas de informação.
- **A primeira ação é perguntar qual técnica será utilizada?**

Programas de computador

- Relaciona-se com arquivos, analisando seu conteúdo.
 - **Passos:**
 - Análise do fluxo do sistema.
 - Identificação do arquivo a ser auditado.
 - Entrevista com o analista/usuário.
 - Identificação do código/layout do arquivo.
 - Elaboração do programa para auditoria.
 - Cópia do arquivo a ser auditado.
 - Aplicação do programa de auditoria.
 - Análise dos resultados.
 - Emissão de relatórios.
 - Documentação.

Questionários a distância

- Verifica a adequação do ponto de controle aos parâmetros de controle interno (segurança física, lógica, eficácia, eficiência, etc.). Analisa:
 - Segurança em redes de computadores.
 - Segurança do centro de computação.
 - Eficiência no uso de recursos computacionais.
 - Eficácia de sistemas aplicativos.

• **Passos:**

- Análise do ponto de controle.
- Elaboração do questionário.
- Seleção dos profissionais que irão responder o questionário.
- Elaboração de instruções.
- Distribuição/remessa dos formulários.
- Controle do recebimento pelo usuário.
- Análise das respostas.
- Formação de opinião quanto às respostas.
- Elaboração do relatório de auditoria.

Simulação de dados (test deck)

- Elaboração de massa de teste a ser submetida ao programa ou rotina. Deve prever as seguintes situações:
 - Transações com campos inválidos.
 - Transações com valores nos limites.
 - Transações incompletas.
 - Transações incompatíveis.
 - Transações em duplicidade.

• **Passos:**

- Compreensão da lógica do programa.
- Simulação dos dados (pertinentes ao teste a ser realizado).
- Elaboração dos formulários de controle.
- Transcrição dos dados para o computador.
- Preparação do ambiente de teste.
- Processamento do teste.
- Avaliação dos resultados.
- Emissão de opinião sobre o teste.

Mapeamento estatístico (mapping)

- Permite verificar situações como:
 - Rotinas não utilizadas.
 - Quantidade de vezes que cada rotina foi utilizada.
 - Rotinas existentes em programas, mas já desativadas.
 - Rotinas mais utilizadas.
 - Rotinas fraudulentas ou irregulares.
 - Rotinas de controle.

Rastreamento de programas

- Possibilita seguir o caminho de uma transação durante o processamento do programa.
- Tem como objetivo identificar as inadequações e ineficiência na lógica de um programa.

Entrevistas no ambiente computacional

- Realização de reuniões entre o auditor e o auditado.
- **Passos:**
 - Analisar o ponto de controle.
 - Planejar a reunião.
 - Elaborar o questionário da entrevista.
 - Realizar a reunião.
 - Elaborar ata da reunião.
 - Analisar a entrevista.
 - Emitir relatório da auditoria.

Análise de relatórios/telas

- Analisar relatórios e tela referentes a:
 - Nível de utilização pelo usuário.
 - Esquema de distribuição e número de vias.
 - Grau de confidencialidade.
 - Forma de utilização de integração com outras telas/relatórios.
 - Padronização dos layouts.
 - Distribuição das informações conforme layout.

- **Passos:**

- Relacionar telas e relatórios por usuário.
- Obter modelo ou cópia de todas as telas/relatórios.
- Elaborar um checklist para levantamento.
- Marcar data e hora para obter opiniões dos usuários.
- Realizar entrevistas e anotar opiniões.
- Analisar as respostas.
- Emitir opinião

- **Permite detectar:**

- Relatórios e telas não mais utilizados.
- Layout inadequado.
- Distribuição indevida de vias.
- Confidencialidade não respeitada.

Simulação Paralela

- Elaboração de um programa de computador para simular as funções da rotina sob auditoria enquanto o test deck simula a lógica do programa.
- **Passos:**
 - Identificação da rotina a ser auditada.
 - Elaboração de programa com a mesma lógica.
 - Preparação do ambiente.
 - Aplicação da rotina.
 - Elaboração de relatório.

Análise do programa fonte

- Consiste na análise visual do programa e na comparação da versão do objeto que está sendo executado com o objeto resultante da última versão do programa fonte compilado.
- **Permite verificar:**
 - Se o programador cumpriu as normas de padronização do código (tabelas de rotinas, arquivos, programas).
 - Qualidade de estruturação do programa fonte.

Função e responsabilidades do auditor

- Os auditores são muitas vezes percebidos negativamente pelos funcionários das organizações, o que pode dificultar seu trabalho.
- No entanto, é importante notar que a responsabilidade legal dos auditores é baixa em comparação com o número de auditorias realizadas.

Função e responsabilidades do auditor

- Falhas de auditoria não são raras e têm implicações legais significativas quando ocorrem. Antes de firmar um contrato com um auditor, a empresa contratante deve revisar a proposta comercial para definir claramente o escopo de trabalho e responsabilidades de ambas as partes.
- Além disso, é essencial verificar se as normas adotadas pela empresa contratada são amplamente aceitas e atualizadas de acordo com as mudanças no mercado contábil, financeiro e tecnológico.

Incidente

- Vulnerabilidades referem-se a fragilidades em ativos que lidam com informações e que podem ser exploradas por ameaças, resultando em incidentes de segurança que prejudicam **os princípios da confidencialidade, integridade e disponibilidade da informação**.
- É essencial que o auditor compreenda os objetivos de negócios da organização para desenvolver políticas, conformidades e planos de resposta a incidentes, considerando fatores específicos.
- Embora as vulnerabilidades por si só não causem incidentes de segurança, quando combinadas com agentes causadores, como ameaças, podem resultar em danos ao ambiente.

Vulnerabilidades

- As vulnerabilidades podem ser:
 - **Físicas:** ambiente não adequado as regras de segurança física.
 - **Naturais:** desastres naturais, falta de energia, poeira etc.
 - **Hardware:** falha e/ou desgastes de recursos tecnológicos.
 - **Software:** software sem proteção, mal escrito, mal dimensionado etc.
 - **Comunicação:** perda de comunicação ou violação.
 - **Humanas:** falta de treinamento, erros, omissões etc.
 - **Mídia:** mídia utilizada para backup de informações.

- O auditor deve realizar uma análise de riscos, levando em consideração o ciclo de vida da informação, que como sabemos pode ser dividido nas seguintes etapas:
 - **Manuseio.**
 - **Armazenamento.**
 - **Transporte.**
 - **Descarte.**
- É crucial abranger todas essas etapas no ciclo de vida da informação para garantir um nível adequado de segurança, já que proteger apenas um ou outro momento não seria suficiente. Portanto, a avaliação de todo o processo é de grande importância.

- Incidentes de segurança podem assumir várias formas e ocorrer a qualquer momento, afetando a **confidencialidade, integridade e disponibilidade da informação**. Tais incidentes podem causar prejuízos significativos.
- Um auditor deve implementar procedimentos de auditoria para avaliar a segurança da informação, identificar vulnerabilidades e auxiliar na criação de políticas, conformidades e planos de resposta a incidentes.
- Portanto, é essencial que as organizações adotem medidas para proteger suas informações e estejam preparadas para uma resposta rápida e eficaz em caso de incidentes.