# Prova de Segurança e Auditoria de Sistemas

## 1. Qual é a função e o objetivo do processo de auditoria?

A função de um processo de auditoria é promover **adequação**, **revisão**, **avaliação** e **recomendações** (**ARAR**) para aprimorar controles internos e avaliar a utilização de ativos no processamento dos sistemas. A auditoria atua em **níveis**, que são: **operacional**, **tático**, **estratégico (OTE)**, e os objetivos são pautados em **efetividade**, **eficiência**, **confidencialidade**, **integridade**, **disponibilidade**, **compliance** (cumprir leis e regulamentos) e **confiança** (**EECIDCC**).

Com relação aos objetivos globais, a **integridade** está relacionada a consistência das transações, a **confidencialidade** às informações estarem direcionadas a quem deve ser, a **privacidade** a autorização de tarefas essenciais por tipos de usuários, a **acuidade** a validação das transações e verificando da veracidade, a **disponibilidade** a continuidade do negócio, a **auditabilidade** aos logs operacionais serem necessários para gerar trilhas de auditoria, a **versatilidade** aos sistemas serem amigáveis e de fácil uso, e a **manutenibilidade** a possibilidade de controle de teste, conversão, implantação e documentação. (**ICPADAVM**)

## 2. Quais são os quatro tipos de auditoria em sistemas de informação?

Os quatro tipos de auditoria são: no **desenvolvimento de sistemas**, **sistema de produção**, **ambiente tecnológico** e em **eventos específicos**. Na auditoria no **desenvolvimento de sistemas**, o processo de construção do sistema de informação é auditado, da fase de requisitos até a sua implementação, e o ciclo de vida de desenvolvimento. Na auditoria de **sistemas de produção**, o sistema já implantado é auditado, juntamente com seus procedimentos, resultados, segurança, corretude e tolerância a falhas. Na auditoria no **ambiente tecnológico**, a análise é feita na estrutura organizacional, contratos, normas, técnicas, custos, planos de segurança e contingência. Já na auditoria de **eventos específicos**, é realizada a análise de causas, consequências e ações corretivas a eventos não cobertos por outras auditorias.

## 3. Como pode ser especificado o controle interno contábil para auditoria?

O controle interno contábil pode ser especificado através da **fidelidade das informações em relação aos dados**, **segurança física e lógica**, **confidencialidade**, **obediência à legislação**.

## 4. Como pode ser especificado o controle interno administrativo para auditoria?

O controle interno administrativo pode ser especificado através da **eficácia**, **eficiência** e **obediência a diretrizes corporativas**.

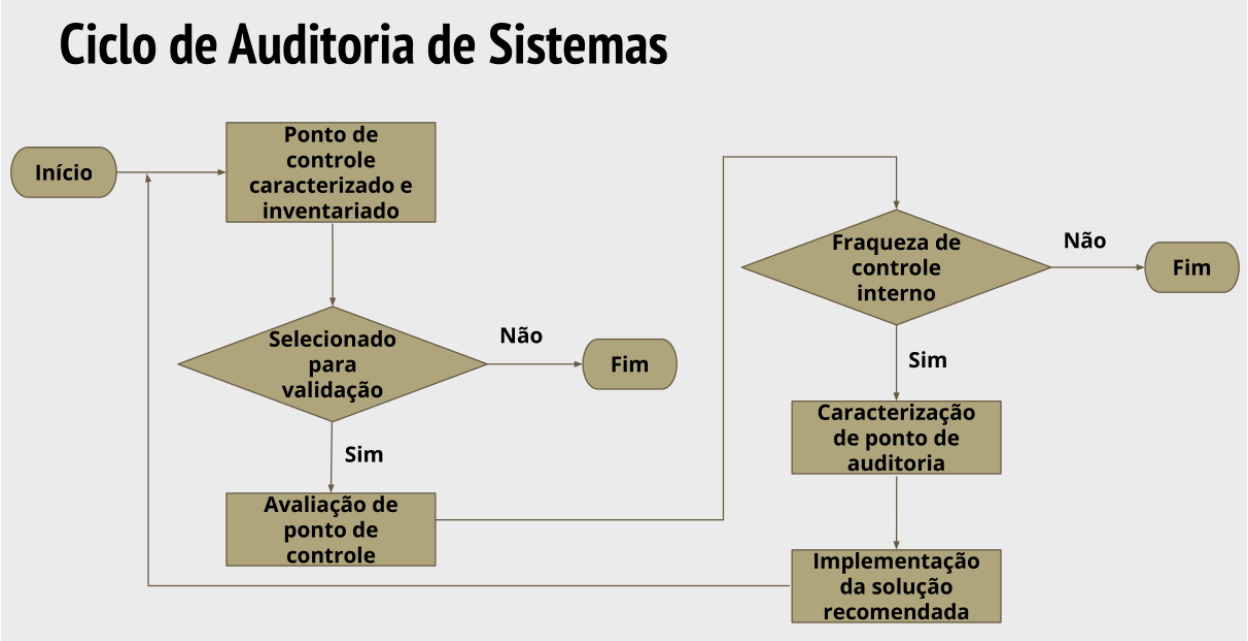
## 5. Como podem ser caracterizados os pontos de controle? Qual a relação com pontos de auditoria?

**Pontos de controle** é uma situação levantada que merece ser validada pela auditoria, podendo ser caracterizada quanto a **processo** e **resultado**. Quanto a **processo**, está relacionado a rotinas operacionais ou de controle, etapas do ciclo de desenvolvimento de software ou de manutenção de sistemas, e procedimentos administrativos. Já com relação a **resultados**, está relacionado a documentos, relatórios, arquivos, pontos de integração, estrutura lógica e física de sistemas, e modelo conceitual de base de dados. Os **pontos de controle** são validados devido a disponibilidade de recursos humanos, materiais, tecnológicos e financeiros, e prioridades determinadas pela administração. Nem todo ponto de controle é submetido à validação. A validação consiste em auditar segundo as especificações do controle interno. Os **pontos de controle** podem estar em duas situações, **não apresentando fraquezas nos controles internos**, estando dentro das especificações de controle interno, e **apresentando fraqueza nos controles internos**, sendo denominado ponto de auditoria.

## 6. Como se dá o processo de conversão de um ponto de controle para um ponto de auditoria?

Para converter um ponto de controle em um de auditoria, é necessário haver uma fraqueza nos controles internos, com isso, deve haver documentação comprobatória, descrição do tipo de fraqueza e recomendação de solução.

## Ciclo de Auditoria de Sistemas




## 7 - Quais são os tipos de abordagem de auditoria de sistemas e qual a diferença entre

**elas?**

As abordagens são : **ao redor do computador**, **através do computador** e **com o computador**. As vantagens da abordagem **ao redor do computador** são que não se exige muito conhecimento de tecnologia para executar o método e a sua aplicação envolve custos baixos e diretos. As desvantagens da abordagem abordagem **ao redor do computador** são que há uma restrição do conhecimento de como os dados são utilizados, tornando a auditoria incompleta e inconsistente, pois o processo operacional é dinâmico, atendendo às necessidades sociais, além disso, a eficiência dessa auditoria é mais difícil de ser avaliada, pois não há parâmetros claros e padronizados. Caso a auditoria exclua as CPU e as funções aritméticas e lógicas, não é possível afirmar que essa auditoria foi representativa e global, portanto as decisões podem ser distorcidas.

Na abordagem **através do computador**, há mais do que a confrontação com os documentos fontes, é necessário um alerta quanto ao manuseio de dados, aprovação e registro de transações econômicas, financeira e contábil sem deixar evidências. Com esse método é possível requisitar a verificação dos código fonte com dados intermediários, porém, cobra do auditor uma maior ênfase em técnicas do computador para testar a si mesmo e entradas de dados. As vantagens da abordagem **através do computador** são que capacita o auditor quanto aos conhecimentos de processamento eletrônico de dados e a verificação com maior frequência das áreas que necessitam de revisão constante. As desvantagens da abordagem **através do computador** são que se a operação for feita incorretamente, gera perdas incalculáveis, não recomendado executar no ambiente em produção, e pode ser caro, pois necessita de treinamento de auditores, aquisição e manutenção dos pacotes de software. Os pacotes podem estar completos e incorretos, podendo ser necessários técnicas manuais e risco de que os pacotes possam estar contaminados pelo uso frequente na auditoria organizacional.

Na abordagem **com o computador** há uma metodologia **assistida**, realizando uma compilação dos processos para atingir alguns objetivos. Nela, são verificadas as **capacidades lógicas e aritméticas do computador**, para ver se o que é feito por ele (cálculos das transações econômicas, financeiras e contábeis ou aqueles que dizem respeito às responsabilidades, como, por exemplo, o cálculo das depreciações, impostos e taxas, multiplicações e contabilizações) é correto, utilização das **capacidades de cálculos estatísticos e de geração de amostras** que facilitem confirmações da integridade dos dados de contas a receber, estoques, imobilizados, advogados e circulação, a utilização de **capacidades de edição e classificação do sistema** computadorizado para ordenar e selecionar os registros contábeis (dados eletrônicos ou físicos que documentam as transações financeiras de uma organização) e analisar as listas de amostras de auditoria e confirmação dos resultados de auditoria executada manualmente. As vantagens da abordagem **com o computador** são que é possível aplicar Técnicas de Auditoria Assistida por Computador (**TAAC**), possibilidade de desenvolver programas específicos para serem usados pelo auditor para dar uma opinião sobre o processo contábil, ganho de tempo com os passos aplicados no pacote generalizado de auditoria de tecnologia da informação, possibilidade de integrar processos de auditoria com os papéis de trabalho de auditoria e postar os documentos em uma rede de auditoria da firma, permitindo que as pessoas acessem os papéis.

A abordagem **ao redor do computador** é ineficiente, pois negligencia algumas qualidades dos controles internos dos sistemas e leva a falta de testes convincentes para ajudar na conclusão sobre os sistemas. Já a abordagem **através do computador,** é melhor, porém, pode produzir registros incompletos, e ao invés de fazer uma verificação de equilíbrio com as ferramentas, ela negligencia processos manuais, deixando incompleta a maioria das tarefas normalmente feitas manualmente.

### 8. Quais são as etapas da metodologia de auditoria de sistemas? (**PLIPCA**)

As etapas da metodologia de auditoria de sistemas são: **planejamento e controle**, **levantamento**, **identificação e inventário**, **priorização e seleção**, **avaliação**, **conclusão e acompanhamento**. Na etapa de **planejamento e controle**, são planejadas ações e recursos para a auditoria, formação da equipe de coordenação e execução. Métodos como **PMBok**, são usados para fazer o planejamento. Na etapa de **levantamento**, é identificado o escopo da auditoria e estudos sobre o sistema. Nessa etapa pode ser usado ferramentas como **MER**, diagramas de classes e etc, para estudar os comportamentos e relações no sistema. Na etapa de **identificação e inventário**, são identificados e descritos os pontos de controle. Com isso, é enviado um relatório para a coordenação de auditoria. Na etapa de **priorização e seleção**, é criada uma priorização dos pontos de controle com base no grau de risco, existência de ameaças, e disponibilidade de recursos. Na etapa de **avaliação,** são realizados testes de validação dos pontos de controle, técnicas que evidenciam falhas ou fraquezas, são aplicadas. Para cada ponto de controle existe uma técnica mais aplicável. Na etapa de **conclusão,** é elaborado um relatório da auditoria, tendo diagnóstico dos pontos de controle e as fraquezas dos controles internos, e suas soluções. A etapa de **acompanhamento** é feita até que todas as recomendações tenham sido feitas ou tenha sido atingido um nível tolerável pela organização.

### 9. Em que consiste a auditoria no processo de desenvolvimento de sistemas de informação?

A **auditoria no processo de desenvolvimento de sistemas** consiste em revisar e avaliar o processo de construção de sistemas, o método e metodologia utilizados no ciclo de vida de desenvolvimento. Segurança física, confidencialidade, legislação, eficiências das técnicas e ferramentas utilizadas devem ser observadas.

### 10. Quais são os objetivos de auditoria de controles de acessos?

Os objetivos de auditoria de controle de acessos, no quesito **físico**, são controle sobre o acesso físico ao hardware, CPUs, unidades de fita e disco, terminais, arquivos de dados como discos e fitas, já no **lógico**, diz respeito ao controle sobre o acesso de recursos do sistema, incluindo acesso a dados e processamentos de programas e transações.

# Questões Organizadas

## 1. Qual é a função da auditoria? (**ARAR)**

A função da auditoria é promover: **a**dequação, **r**evisão, **a**valiação e **r**ecomendações (**ARAR**) para aprimorar os controles internos e avaliar a utilização de ativos no processamento de informações.

## 2 - Quais os objetivos da auditoria? **(ICPADAVM)**

Os objetivos são: integridade, confidencialidade, privacidade, acuidade, disponibilidade, auditabilidade, versatilidade e manutenibilidade **(ICPADAVM)**.

- **I**ntegridade: consistências das transações.
- **C**onfidencialidade: informações são direcionadas a quem deve ser.
- **P**rivacidade: autorização de tarefas mediante a tipos de usuários.
- **A**cuidade: avaliação das transações e verificação da veracidade.
- **D**isponibilidade: continuidade do negócio.
- **A**uditabilidade: logs são necessários para gerar trilhas de auditoria.
- **V**ersatilidade: ser amigável e de fácil uso.
- **M**anutenibilidade : possibilidade de controle de testes, conversão, implementação e documentação.

Os objetivos são pautados em efetividade, eficiência, confidencialidade, integridade, disponibilidade, compliance e confiança (**EECIDCC**).

## 3. Quais são os quatro tipos de auditoria em sistemas de informação?

Os quatro tipos de auditoria são:

- **Sistemas em desenvolvimento**: a construção do sistema é auditada, da fase inicial até a implementação, juntamente com o ciclo de desenvolvimento.
- **Sistemas em produção**: o sistema implantado é auditado, junto com seus procedimentos, resultados, segurança, corretude e tolerância a falhas.
- **Ambiente tecnológico**: é feita uma análise organizacional, contratos, normas, técnicas, planos de segurança e contingência, e custos.
- **Eventos específicos**: é feita uma análise das causas, consequências e ações corretivas, para o que não é coberto pelas outras auditorias.

## 4. Como pode ser especificado o controle interno contábil para auditoria?

**Contábil — FSCO**
**Administrativo — EEO**

O controle interno **contábil** pode ser especificado pela: **(FSCO)**

- **F**idelidade das informações em relação aos dados.
- **S**egurança física e lógica.
- **C**onfidencialidade.
- **O**bediência a legislação.

## 5. Como pode ser especificado o controle interno administrativo para auditoria?

O controle interno **administrativo** pode ser especificados pela: **(EEO)**

- **E**ficiencia.
- **E**ficácia.
- **O**bediência às diretrizes corporativas.

## 6. Como podem ser caracterizados os pontos de controle?

Pontos de controle são situações levantadas que merecem ser validadas pela auditoria, podendo ser caracterizada quanto ao **processo** e **resultado**. Os pontos de controle podem estar em duas situações, **sem fraquezas nos controles internos e com fraqueza nos controles internos**. Quando há fraqueza nos controles internos são denominados **pontos de auditoria**.

Quanto ao **processos (REMP)**:

- Rotinas operacionais ou de controle.
- Etapas do ciclo de desenvolvimento.
- Manutenção de sistemas.
- Procedimentos administrativos.

Quanto ao **resultados (DRAPEM)**:

- Documentos.
- Relatórios.
- Arquivos.
- Pontos de integração.
- Estrutura lógica e física de sistemas.
- Modelo conceitual de bases de dados.

## 7. Como se dá o processo de conversão de um ponto de controle para um ponto de auditoria?

Para haver a conversão entre ponto de controle para ponto de auditoria, é necessário:

- Existência de fraqueza nos controles internos.
- Documentação comprobatória.
- Descrição do tipo de fraqueza.
- Recomendação de solução.

## 8. Quais são as etapas da metodologia de auditoria de sistemas? **(PLIPACA)**

As etapas da metodologia de auditoria de sistemas são:

- **P**lanejamento e controle: são planejadas ações e recursos para auditoria, e a formação da equipe de coordenação e execução.
- **L**evantamento: escopo da auditoria e estudos sobre os sistemas.
- **I**dentificação e inventário: identificação e descrição dos pontos de controle.
- **P**riorização e seleção: é criada a priorização dos pontos de controle quanto a existência de grau de risco, existência de ameaças e disponibilidade de recursos.
- **A**valiação: realização de testes de validação dos pontos de controle e aplicação de técnicas que evidenciam falhas e fraquezas.
- **C**onclusão: é construído um relatório da auditoria, que contém o diagnóstico dos pontos de controle e fraquezas, e suas soluções.
- **A**companhamento: essa etapa é realizada até que as recomendações da auditoria tenham sido feitas ou tenha sido atingido um nível tolerável pela organização.

## 9. Em que consiste a auditoria no processo de desenvolvimento de sistemas de informação?

A auditoria no processo de desenvolvimento de sistemas de informações consiste em revisar e avaliar a construção dos sistemas de informação, e o método e metodologia aplicado no ciclo de vida de desenvolvimento.

## 10. Quais são os objetivos de auditoria de controles de acessos?

Os objetivos de auditoria de controles de acesso são, no quesito físico, controle de acesso físico ao hardware, CPUs, unidades de fita e disco, terminais, na no quesito lógico, diz respeito ao controle de acesso a recursos do sistemas, incluindo o acesso a dados e processamento de programas  e transações.