

# Segurança e Auditoria de Sistemas

## INTRODUÇÃO À AUDITORIA E AUDITORIA DE SISTEMAS

Profª. Ms. Adriane Ap. Loper

1

- Unidade de Ensino: 4
- Competência da Unidade: Fundamentos de Auditoria de Sistemas, Controles gerais de auditoria de sistemas, Técnicas e Ferramentas para auditoria de sistemas
- Resumo: Principais definições auditoria de sistemas, controles e técnicas
- Palavras-chave: auditoria, técnicas, ferramentas
- Título da Teleaula: INTRODUÇÃO À AUDITORIA E AUDITORIA DE SISTEMAS:
- Teleaula nº: 4

2

## Contextualização

- Você trabalha para um provedor de nuvem que está crescendo de uma forma muito rápida e tem recebido como clientes muitas empresas tradicionais, principalmente pelo processo de transformação digital.
- Como sua empresa tem clientes de diferentes setores, como financeiro, saúde e governo, há uma exigência para que os serviços sejam seguros e que estejam em conformidade com regulamentos e leis específicas.
- Monte um planejamento visando melhorar a segurança da empresa e para fortalecer a imagem do provedor de nuvem diante do mercado quanto ao tratamento das necessidades de segurança e conformidade.



Fonte: Shutterstock

3

## Conceitos e Princípios

4

## Contextualização

- Justifique cada ponto do seu planejamento, já que ele será distribuído para a diretoria executiva para que haja a aprovação de seu planejamento.
- Uma sugestão de itens do planejamento que não podem faltar são:
  - Como é a segurança do provedor de nuvem, em linhas gerais.
  - Por que a segurança é importante, focando nos clientes.
  - Demanda dos clientes para a conformidade.
  - Auditoria de segurança, por que fazer.
  - Principais fases da auditoria.
  - Conclusão.



Fonte: Shutterstock

5

## Auditoria



<https://vidadesuporte.com.br/suporte-a-serie/auditoria/>

6

## Auditoria

- A **auditoria de sistemas** é cada vez mais importante para as empresas e tem como papel assegurar que os controles internos sejam eficientes e efetivos.
- A **segurança da informação e privacidade**, que é feita a partir de uma visão de **riscos** que direciona a definição e implantação de **controles de segurança**, é uma das áreas em que a auditoria é parte essencial para garantir que a empresa esteja de fato protegida contra as **ameaças**.



Fonte: shutterstock

7

## Auditoria - Objetivos

- A auditoria tem como **objetivo** verificar e validar atividades, processos e sistemas das empresas de acordo com o que está estabelecido, incluindo aspectos legais e regulatórios, visando também a eficiência e eficácia.
- Ela é feita em diferentes contextos, como o ambiental, contábil, financeiro, fiscal, riscos, segurança, sistemas, social, tributário ou trabalhista.
- Outro **objetivo** da auditoria é atestar a conformidade com regulações administrativas, regulatórias e legais.



Fonte: adaptada de ISACA (2016, 2017, 2020).

8

## Auditoria - Objetivos

- A auditoria visa ainda **confirmar para a alta gestão** da empresa que o negócio está funcionando bem e está preparado para enfrentar os potenciais desafios.
- E, principalmente, ela visa **assegurar aos diferentes atores** envolvidos no negócio sobre a estabilidade financeira, operacional e ética da organização (ISACA, 2016).



Fonte: adaptada de ISACA (2016, 2017, 2020).

9

## Auditoria de sistemas

- Segundo a *Information Systems Audit and Control Association (ISACA)*, que foca em **sistemas de informação**, a **auditoria** é uma inspeção e verificação formal para checar se um padrão ou conjunto de guias está sendo seguido, se os registros estão corretos e se os objetivos de eficiência e eficácia estão sendo alcançados (ISACA, 2016).



Fonte: adaptada de ISACA (2016).

10

## Auditoria de sistemas

- **Pode detectar problemas em:**
  - ✓ Fraudes em e-mail;
  - ✓ Uso inadequado de hardwares;
  - ✓ Fraudes, erros e acidentes;
  - ✓ Vazamento de informações;
  - ✓ Falta de segurança física (acessos indevidos).



Fonte: shutterstock

11

## Benefícios da Auditoria de Sistemas

- ✓ Superação de **resistências** a tecnologia;
- ✓ Avaliação, escolha e implantação de **softwares e hardwares**;
- ✓ Gerenciamento dos **arquivos** eletrônicos;
- ✓ Maior transferência de **conhecimento**;
- ✓ Independência das limitações impostas pelos **arquivos de auditoria em papel**;
- ✓ Maior **produtividade**.



Fonte: shutterstock

12

### Auditoria de Segurança e Controles de Segurança

- Para a segurança e privacidade das empresas, é importante que os processos estejam bem definidos e a equipe responsável tenha as competências para as ações necessárias.
- A governança garante que as ações do cotidiano sejam tratadas de modo que as ameaças correntes e as emergentes sejam sempre tratadas e alinhadas com a alta gestão (ISACA, 2017).



Fonte: Shutterstock

13

### Auditoria de Segurança e Controles de Segurança

- Os investimentos em **controles de segurança** são necessários para proteger as empresas contra os ataques cibernéticos, que estão crescendo em sofisticação e abrangência. Somada à necessidade regulatória, a segurança da informação e privacidade faz parte da estratégia e framework das empresas, o que leva à necessidade de revisão gerencial, avaliação de riscos e auditoria dos controles de segurança (ISACA, 2017).
- Os investimentos para melhorar a **proteção e as respostas aos incidentes** são definidos nos programas de segurança e privacidade das empresas.

14

### Auditoria de Segurança e Controles de Segurança

- Do ponto de vista da alta gestão, as questões envolvem os **valores investidos**, se eles estão adequados e se foram direcionados e implementados corretamente, também em comparação com os concorrentes.
- Com isso, há dois elementos importantes para as empresas: a **avaliação dos riscos atuais e emergentes** para a empresa e a **auditoria dos controles de segurança** atuais e que estão planejados para protegerem os ativos da empresa.
- Assim, a **gestão de riscos** é importante para identificar, analisar e avaliar os riscos, que direcionarão a definição dos controles para o tratamento dos riscos.
- Com a auditoria, a empresa assegura que os controles protegem a empresa de uma forma adequada.

15

## Auditoria

16

A auditoria de sistemas e de segurança é um processo importante para as empresas. Considere as seguintes afirmativas.

- I. Valida atividades, processos e sistemas.
- II. Avalia a eficiência e eficácia dos controles.
- III. Atesta a conformidade administrativa, regulatória e legal.
- IV. Assegura a estabilidade organizacional para a alta gestão e os diferentes atores.

17

Sobre os objetivos da auditoria, é correto o que se afirma em:

- a) II, apenas.
- b) II e III, apenas.
- c) II, III e IV, apenas.
- d) I, II e III, apenas.
- e) I, II, III e IV.

18

Sobre os objetivos da auditoria, é correto o que se afirma em:

- a) II, apenas.
- b) II e III, apenas.
- c) II, III e IV, apenas.
- d) I, II e III, apenas.
- e) I, II, III e IV.

19

## Auditor

20

### Auditor

- Uma das principais características da auditoria é que ela só pode ser feita por **auditores**, os quais são profissionais que normalmente têm certificação para exercer esta função.
- Outra característica é que a **auditoria** é independente das funções operacionais, o que permite que sejam providas opiniões objetivas e sem viés sobre a efetividade do ambiente de controle interno (ISACA, 2016).

21

### Auditor

- *Information Technology Audit Framework* (ITAF) da ISACA é um **framework de auditoria de TI** que define padrões para as auditorias de TI relacionadas aos papéis e responsabilidades, ética, comportamento esperado e conhecimento e qualificação requeridas, além de termos e conceitos específicos ao assunto.
- Além disso, o ITAF provê guias e técnicas para planejar, executar e reportar auditoria de TI (ISACA, 2020).

22

### Auditor

- *Information Technology Audit Framework* (ITAF) da ISACA é um **framework de auditoria de TI** que define padrões para as auditorias de TI relacionadas aos papéis e responsabilidades, ética, comportamento esperado e conhecimento e qualificação requeridas, além de termos e conceitos específicos ao assunto.
- Além disso, o ITAF provê **guias e técnicas** para planejar, executar e reportar auditoria de TI (ISACA, 2020).
- A auditoria requer que o **auditor** busque evidências, avalie as forças e fraquezas de controles internos com base nas evidências coletadas e prepare um relatório de auditoria que apresenta as fraquezas e recomendações para a remediação de uma forma objetiva para apresentar aos atores envolvidos.

23

### Auditor

- As fases do processo de auditoria são importantes, com o planejamento, trabalho em campo e relatórios.
- O mais importante é, porém, o **conhecimento do auditor**, que precisa definir as **técnicas e as ferramentas para a auditoria**, a qual exige conhecimentos amplos e profundos para que seja possível fazer uma análise da eficiência e eficácia dos controles da empresa.
- A **efetividade da auditoria** depende, em grande parte, da qualidade do **programa de auditoria**.
- No caso da **auditoria de controles de segurança**, há a exigência de um conjunto de habilidades que envolvem aspectos especializados, tais como para os **pentests**, as análises de configurações de servidores ou **firewalls**, a revisão de regras de ferramentas de segurança (ISACA, 2017).

24

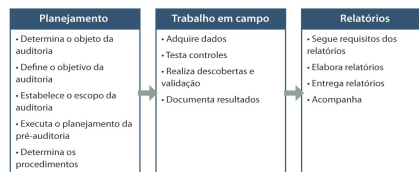
## Plano de auditoria e programa de auditoria



Fonte: adaptada de ISACA (2016).

25

## Principais fases de um processo de auditoria e os passos



Fonte: adaptada de ISACA (2016).

26

## Técnicas de Auditoria de TI

Alguns **métodos para avaliar controles** são (ISACA, 2016):

- ✓ Software de auditoria para analisar o conteúdo de arquivos de dados, como os logs de sistemas e a lista de acesso de usuários.
- ✓ Software especializado para avaliar conteúdo de sistemas operacionais, banco de dados e arquivos de parâmetros de aplicações.
- ✓ Técnicas de desenho de fluxos para documentar processos de negócios e controles automatizados.
- ✓ Logs de auditorias e relatórios para avaliar parâmetros.
- ✓ Revisão de documentação.
- ✓ Perguntas e observação.
- ✓ Simulações passo a passo.
- ✓ Execução de controles.

27

## Relatório planejamento para melhorar a segurança

28

Você trabalha para **um provedor de nuvem em franca expansão**, que tem demandas diretas de seus clientes.

Eles exigem cada vez mais segurança e precisam estar em conformidade legal e regulatória, o que significa que só se tornarão clientes caso o próprio provedor esteja em conformidade com as melhores práticas de segurança e tecnologia da informação.

O **planejamento**, assim, precisa incluir um elemento que aumente a confiança dos potenciais clientes, os quais precisam de um provedor seguro para operar seus sistemas e dados.

O planejamento segue os itens gerais:

- **Como é a segurança do provedor de nuvem, em linhas gerais:** a segurança segue os processos essenciais de **identificação, proteção, detecção, resposta e recuperação**.
- São processos importantes para que a **confidencialidade, integridade e disponibilidade** dos dados e informações dos clientes sejam maximizados.
- A segurança é feita com base nos **riscos**, que é a probabilidade de um agente de ameaça explorar vulnerabilidades de um ativo, fazendo com que uma ameaça se torne um incidente de segurança, o que resulta em impactos para a empresa.

29

30

- Os controles de segurança são identificados e implantados com base nos riscos avaliados, com este tratamento dos riscos envolvendo ainda os riscos aceitos.
- **Por que a segurança é importante, focando nos clientes:** os clientes demandam a segurança porque precisam proteger seus negócios, e o provedor de nuvem operará seus sistemas e dados. Além disso, há a necessidade de conformidade legal e regulatória, exigida para todo o setor.
- **Demanda dos clientes para a conformidade:** a conformidade é baseada em regulamentos e leis, como a do setor financeiro, que exige proteção dos ativos tecnológicos, e a do setor de saúde, que exige a segurança e privacidade dos dados dos pacientes, por exemplo.

31

- O conjunto de controles deve ser verificado sob a óptica destas necessidades legais e regulatórias e atestado pelo auditor.
- **Auditoria de segurança, por que fazer:** os controles de segurança implantados podem não ser eficientes e eficazes, o que compromete a segurança do provedor de nuvem e de todos os seus clientes. Além disso, riscos não identificados podem não estar sendo tratados. A auditoria é necessária para validar atividades, processos e sistemas; avaliar a eficiência e eficácia dos controles; atestar a conformidade administrativa, regulatória e legal; e assegurar para a alta gestão e diferentes atores a estabilidade organizacional.

32

- **Principais fases da auditoria:** (1) planejamento, que envolve principalmente a definição do escopo e das técnicas e ferramentas a serem utilizadas na auditoria; (2) trabalho em campo, em que dados são adquiridos e controles são testados e verificados; (3) relatórios, em que os resultados da auditoria são organizados e apresentados.
- **Conclusão:** o provedor de nuvem **é seguro** com a gestão de riscos e a gestão de segurança da informação, com um processo de melhoria contínua que culmina com a assertividade cada vez maior da visão de riscos e dos controles implantados.

33

- As validações dos controles, tanto do ponto de vista da existência de acordo com as necessidades e do ponto de vista da eficiência e eficácia, precisam ser feitas por uma auditoria.
- Os resultados da auditoria elevam a confiança dos potenciais clientes, já que são realizadas de uma forma independente e formal, com uso de técnicas e ferramentas específicas.
- Com a auditoria, assim, pode ser confirmada para a alta gestão da empresa que o negócio está funcionando bem e está preparado para enfrentar os potenciais desafios. E, principalmente, ela visa assegurar aos diferentes atores envolvidos, principalmente clientes, sobre a estabilidade financeira, operacional e ética da organização.

34

Iteração

35

- Entenderam a importância da auditoria e do auditor?



Fonte: <https://piller.com.br/2020/>

36

## Controles Gerais de Auditoria de Sistemas

37

### Contextualizando

Você deve partir para o detalhamento do planejamento, com foco nos controles. Justifique cada ponto de seu material sobre os controles, já ele será distribuído para a diretoria executiva para aprovação.

Uma sugestão de itens do material que você irá desenvolver sobre controles que não podem faltar são:

- Tipos de controles considerados e para que servem.
- Como os controles são definidos.
- Normas ou *frameworks* que podem ser a base para a definição dos controles.
- Controles para aquisição, desenvolvimento e manutenção de sistemas.
- Controle de acesso.
- Auditoria.

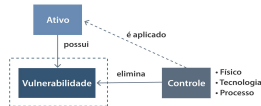


Fonte: Shutterstock

38

### Controles de Segurança e Privacidade

- Os controles podem ser *físicos* (como monitoramento de circuito fechado de TV, de acesso a data center), *tecnológicos* (como *firewall*, VPN) ou *processuais* (como atualização periódica de sistema operacional ou atualização das regras do firewall ) e são aplicados nos ativos para que as vulnerabilidades sejam tratadas.



39

### Controles de Segurança e Privacidade

- Os controles de segurança são *salvaguardas* ou *contramedidas* aplicadas em sistemas ou organizações para proteger a confidencialidade, integridade e disponibilidade dos sistemas e suas informações e para gerenciar os riscos de segurança.
- Os *controles de privacidade* são salvaguardas administrativas, técnicas e físicas aplicadas em sistemas e organizações para gerenciar riscos de privacidade e para assegurar conformidade com requisitos de privacidade aplicáveis.
- Os requisitos de *segurança e privacidade* direcionam a seleção e implementação de controles de segurança e privacidade e



Fonte: Shutterstock

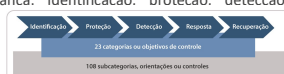
40

### Controles de Segurança e Privacidade

são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades de missão para assegurar a confidencialidade, integridade e disponibilidade das informações processadas, armazenadas e transmitidas, e também para gerenciar riscos (NIST, 2020).

- O *NIST Cybersecurity Framework* (NIST, 2018) define as cinco funções da segurança: identificação, proteção, detecção, resposta e recuperação.

Fonte: adaptada de NIST (2018).



41

### Controles Organizacionais e relação com segurança e continuidade do Serviço

- A *segurança e privacidade* fazem parte do contexto das empresas e estão integradas com outros assuntos, como a governança de TI.
- A *governança de TI* visa a transformação digital e a relação com a entrega de valor, a mitigação dos riscos de negócios e a otimização de recursos.
- A governança tem como principais objetivos (COBIT, 2018):
- Avaliação de necessidades, condições e opções de todos os atores envolvidos, em busca de determinar objetivos corporativos balanceados.
- Direcionamento para a priorização e tomada de decisão.
- Monitoramento do desempenho e conformidade de acordo com os direcionamentos e objetivos definidos.



Fonte: Shutterstock

42

### COBIT (Control Objectives for Information and Related Technology)

- O **COBIT** é um framework de governança de TI que trata de uma **visão organizacional**, a qual tem relação com a segurança e privacidade.
- O **COBIT** define os componentes para construir e sustentar um sistema de governança, composto por processos, estrutura organizacional, políticas, procedimentos, fluxos de informação, cultura, comportamentos, qualificações e infraestrutura.
- Há **cinco domínios no COBIT**, um para a governança e quatro para o gerenciamento (COBIT, 2018), sendo composto por um total de **40 processos**, que podem ser entendidos como controles organizacionais.



Fonte: shutterstock

43

### COBIT (Control Objectives for Information and Related Technology)

- Os exemplos citados dos 40 processos organizacionais são referentes aos controles de segurança:
- **Avaliar, direcionar e monitorar;**
- **Alinhar, planejar e organizar;**
- **Construir, adquirir e implementar;**
- **Entregar serviço e suporte;**
- **Monitorar, verificar e avaliar.**
- Alguns processos ou objetivos de controle organizacionais definidos no COBIT, estão voltados diretamente para a segurança. Por exemplo, a **condução de auditorias do sistema de gestão da segurança da informação** em intervalos definidos é uma das atividades que devem ser feitas (COBIT, 2018).



Fonte: shutterstock

44

### ITIL (Information Technology Infrastructure Library)

- O ITIL é um framework de melhores práticas que visa auxiliar as empresas a **entregar e suportar serviços de TI**, provendo uma estrutura alinhada com a visão, missão, estratégia e objetivos da organização.
- Há um sistema de valor dos serviços, composto por :
  - Cadeia de valor de serviços.
  - Princípios.
  - Governança.
  - Melhoria contínua.
- 34 práticas de gerenciamento.



Fonte: shutterstock

45

### ITIL (Information Technology Infrastructure Library)

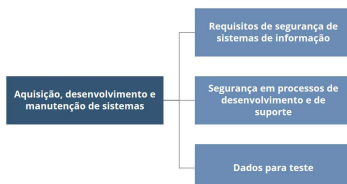
- Dentre os benefícios do ITIL para as empresas, estão :
- Padronização do modelo de operação de TI.
- Cumprimento dos requisitos de clientes e funcionários.
- Maior agilidade e capacidade para inovação.
- Entregas em ambientes em constante mudança.
- Maior controle e governança.
- Demonstração do valor de TI.
- Oportunidade para melhorias.
- As 34 práticas do ITIL envolvem guias que são agrupadas em três categorias :
  - Práticas de gerenciamento geral.
  - Práticas de gerenciamento de serviço.
  - Práticas de gerenciamento técnico.



Fonte: shutterstock

46

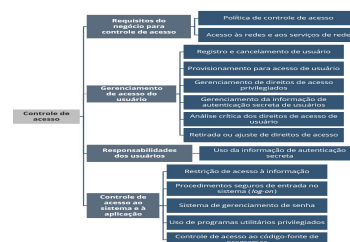
### Controles de Segurança(ISO 27002) para aquisição, desenvolvimento e manutenção de sistemas



Fonte: adaptada de ISO 27002 (2013).

47

### Controles de Acesso



Fonte: adaptada de ISO 27002 (2013).

48



## Controles Lógico, Físico e Processual

Os controles de segurança envolvem investimentos em pessoas, processos e tecnologias, principalmente para o desenvolvimento de uma cultura de segurança, e podem ser administrativos, técnicos ou operacionais.

Alguns exemplos são (ISACA, 2017):

- ✓ Conscientização.
- ✓ Políticas.
- ✓ Sistemas de detecção de intrusão.
- ✓ Registro de eventos (logging).
- ✓ Varredura de vulnerabilidades.
- ✓ Classificação da informação.
- ✓ Hardening de arquitetura e de tecnologia.
- ✓ Hardening de sistemas.



49

## Relatório do planejamento com foco nos controles

50

- **Tipos de controles considerados e para que servem:** controles são salvaguardas ou contramedidas aplicadas em sistemas ou organizações para proteger a confidencialidade, integridade e disponibilidade dos sistemas e suas informações e para gerenciar os riscos de segurança, e também para assegurar conformidade com requisitos aplicáveis.
- Os controles podem ser (i) técnicos, tecnológicos ou lógicos, como o antivírus ou o *backup*; (ii) processuais, administrativos ou operacionais, como a política de segurança ou o processo de revisão de contas de usuários; (iii) físicos, como o cadeado para que o *desktop* utilizado pelo presidente da empresa não seja roubado.

51

- **Como os controles são definidos:** os controles são definidos pelos riscos existentes na empresa, que direcionam as necessidades com base na probabilidade das ameaças se tornarem incidentes de segurança e os impactos envolvidos.
- Além dos riscos, a definição dos controles pode ser feita a partir de requisitos que direcionam a seleção e implementação de controles, e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades da empresa.
- **Normas ou frameworks que podem ser a base para a definição dos controles:** a ABNT NBR ISO/IEC 27002 define um conjunto de objetivos de controle de segurança da informação, e pode ser utilizada para a definição dos controles.

52

- **COBIT** é um *framework* para governança de TI e possui um conjunto de controles mais amplos que podem ser implantados, incluindo os de segurança e privacidade.
- **ITIL** é um conjunto de melhores práticas para o gerenciamento de serviços e estabelece também um conjunto de controles mais amplos que inclui aspectos de segurança.
- **Controles para aquisição, desenvolvimento e manutenção de sistemas:** os controles para este assunto devem incluir os requisitos de segurança de sistemas de informação, para garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação.

53

- É necessário ainda que controles de segurança sejam definidos em processos de desenvolvimento e de suporte, para garantir que a segurança da informação esteja projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação.
- Os controles de segurança devem ainda abordar os dados para teste, principalmente nos aspectos de privacidade, que devem ser reforçados devido à Lei Geral de Proteção de Dados Pessoais (LGPD).
- **Controle de acesso:** o controle de acesso deve ser tratado pelos requisitos do negócio para controle de acesso, com a política de controle de acesso e o acesso às redes e aos serviços

54

- de rede.
- O **gerenciamento de acesso do usuário** deve incluir aspectos como o registro e cancelamento de usuário, provisionamento para acesso de usuário, gerenciamento da informação de autenticação secreta de usuários e análise crítica dos direitos de acesso de usuário. O controle para as responsabilidades dos usuários deve envolver o uso da informação de autenticação secreta. O controle de acesso ao sistema e à aplicação deve envolver a restrição de acesso à informação, procedimentos seguros de entrada no sistema (*log-on*), uso de programas utilitários privilegiados e controle de acesso ao código-fonte de programas.

55

- **Auditoria:** a auditoria visa garantir que os controles sejam adequados, tanto na definição quanto na implantação, de modo que os objetivos da empresa estejam sendo alcançados de uma forma eficiente e eficaz. Assim, a auditoria de sistemas é essencial para a efetiva proteção da empresa, ao analisar a eficiência e eficácia dos controles definidos e implementados.

56

## Técnicas e Ferramentas para Auditoria de Sistemas

57

### Contextualizando

- Você deve agora fazer uma **auditoria para validar a eficiência e eficácia dos controles**. Além disso, a auditoria deve também validar se os **controles** necessários foram realmente definidos.
- Apresente as **técnicas e ferramentas que você utilizará** no trabalho em campo para validar se todos os controles necessários foram definidos, e se os que foram implantados são eficientes e eficazes.
- O material que você irá produzir será distribuído para a diretoria executiva para aprovação.
- Uma sugestão de objetivo e escopo da auditoria que você irá fazer na empresa para a definição das técnicas e ferramentas que serão utilizadas é o data center do provedor de nuvem, que possui:



Fonte: shutterstock

58

### Contextualizando

- A área segura.
- Os **racks** com os servidores e os equipamentos de comunicação.
- Os administradores de sistemas.
- As máquinas virtuais.
- Sistemas operacionais disponibilizados para os clientes.
- Sistema de provisionamento de acesso aos clientes.
- Você verá que a **auditoria** requer um profissional com várias habilidades e competências, com uma visão abrangente, para definir as técnicas e ferramentas necessárias para a auditoria e para utilizá-las no trabalho em campo. Uma empresa segura de fato precisa da auditoria, então a aplicação de todo o conhecimento é importante.



Fonte: shutterstock

59

### Técnicas e Tipos de Ferramentas para Auditoria de Sistemas

- O **objetivo e o escopo da auditoria** podem estar relacionados com a conformidade com normas, padrões, frameworks, leis e requisitos de negócios.
- A auditoria avalia e verifica a eficácia e eficiência dos controles implantados, que são necessários de acordo com a avaliação de riscos e das normas, padrões, frameworks, leis e requisitos de negócios relacionados.
- Alguns exemplos de abordagens para as auditorias :
  - **Governança**
  - **Riscos**
  - **Gestão**
  - **Processos de gestão de riscos.**



Fonte: shutterstock

60

## Objetivos de Auditoria de Sistemas

- Alguns exemplos de objetivos de auditoria para a segurança e privacidade das empresas, que exigem o planejamento de procedimentos, técnicas e ferramentas específicos, são (ISACA, 2017):
- Políticas, padrões e procedimentos de segurança adequados e efetivos.
- Riscos emergentes identificados, avaliados e tratados de uma forma confiável e adequada.
- Ataques e brechas são identificados e tratados no tempo e na forma apropriados.



Fonte: shutterstock

61

## Principais Técnicas e Ferramentas para Auditoria de Sistemas

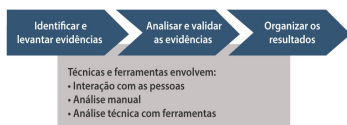
- Auditoria de controles de segurança e privacidade exige um conjunto de habilidades que envolvem aspectos especializados, tais como para os pentests, a análise de configurações de servidores ou firewalls, ou revisão de regras de ferramentas de segurança (ISACA, 2017).
- As auditorias são normalmente compostas por um conjunto de metodologias, técnicas e ferramentas.
- Elas devem ser utilizadas para identificar, levantar evidências e para analisar e validar as evidências. Além disso, as metodologias, técnicas e ferramentas devem auxiliar o auditor a organizar e documentar os resultados. Há técnicas para interagir com as pessoas em busca das informações, que se complementam às análises manuais e às análises técnicas.



Fonte: shutterstock

62

## Objetivos das técnicas e ferramentas



- Dentre as técnicas e ferramentas que envolvem interação com pessoas, estão (BENETON, 2017) (ISACA, 2016) (ISACA, 2017) (KAMAL, 2020) (LIMA, 2020):
- Entrevistas
- Questionários
- Pesquisas



Fonte: shutterstock

63

## Objetivos das técnicas e ferramentas

- Perguntas e observação
- Dinâmicas em grupo.
- Já a análise manual pode ser feita com (BENETON, 2017) (ISACA, 2016) (ISACA, 2017) (KAMAL, 2020) (LIMA, 2020):
- Análise e revisão de documentação.
- Análise de políticas, procedimentos e processos.
- Análise de configurações.
- Desenho de fluxos para documentar processos de negócios e controles automatizados.
- Simulação de mesa.
- Revisões gerenciais.
- Autoavaliação.
- Análise de código.



Fonte: shutterstock

64

## Objetivos das técnicas e ferramentas

- A análise técnica com uso de ferramentas é um dos principais métodos que exige um conhecimento técnico amplo dos auditores e inclui:
- Planilhas eletrônicas
- Scripts
- Software de auditoria Ferramentas de auditoria específicas
- Software especializado - S.O, B.D, arquivos.
- Logs de auditorias e relatórios
- Simulações passo a passo
- Execução de controles:
- Metodologias para coleta de transações.
- Pentests ou testes de penetração.



Fonte: shutterstock

65

## Aplicabilidade das técnicas e ferramentas para auditorias

- O universo a ser avaliado em uma auditoria de segurança e privacidade pode ser baseado em três linhas de defesa, que direcionam como as técnicas e ferramentas podem ser aplicadas (ISACA, 2017):
- Gestão interna
- Gestão de riscos
- Auditoria interna



Fonte: shutterstock

66

## Auditoria Interna

▪ A auditoria interna é essencial para a avaliação de desempenho do SGSI e é bastante similar com a auditoria de certificação (MCCREANOR, 2020):

- Definição de escopo e levantamento de pré-auditoria;
- Planejamento e preparação
- Trabalho em campo
- Análise
- Reporte.



Fonte: Shutterstock

67



68

## Relatório das técnicas e ferramentas que serão utilizadas na auditoria

69

Os controles implantados no data center foram resultados da **avaliação de riscos**, que direcionaram as necessidades com base na probabilidade das ameaças se tornarem incidentes de segurança e os impactos envolvidos.

Além dos **riscos**, a **definição dos controles** foi feita a partir de requisitos que direcionam a seleção e implementação de controles e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades da empresa, como a norma de certificação de data centers TIA-942, o padrão de segurança PCI DSS da indústria de cartões de pagamento e as melhores práticas de gerenciamento de serviços ITIL.

70

O primeiro ponto da auditoria é a realização de uma **avaliação de riscos**, para que todos os riscos do escopo referente ao datacenter tenham sido mapeados.

Na **avaliação de riscos**, devem ser identificados e mapeados ameaças, agentes de ameaças, ativos, suas vulnerabilidades, e calculados a probabilidade e os impactos.

Os **ativos** são:

- ✓ A área segura.
- ✓ Os racks com os servidores e os equipamentos de comunicação.
- ✓ Os administradores de sistemas.
- ✓ As máquinas virtuais.

71

✓ Sistemas operacionais disponibilizados para os clientes.

✓ Sistema de provisionamento de acesso aos clientes.

Após a **avaliação dos riscos**, o **tratamento dos riscos** pode se basear nos controles do TIA-942, PCI DSS, ABNT NBR ISO/IEC 27002, NIST Cybersecurity Framework, ITIL e COBIT, entre outros, focando nestes ativos. Os controles das diferentes normas, padrões e frameworks são equivalentes e complementares.

A verificação dos controles pode ser feita pensando nos controles técnicos, físicos e processuais, que são utilizados pela empresa.

Os **principais controles** existentes na empresa devem estar cumprindo os objetivos de, pelo menos:

- ✓ Políticas de segurança da informação.

72

- ✓ Organização da segurança da informação.
- ✓ Segurança em recursos humanos.
- ✓ Gestão de ativos.
- ✓ Controle de acesso.
- ✓ Criptografia.
- ✓ Segurança física e do ambiente.
- ✓ Segurança nas operações.
- ✓ Segurança nas comunicações.
- ✓ Aquisição, desenvolvimento e manutenção de sistemas.
- ✓ Relacionamento na cadeia de suprimento.

73

- As técnicas e ferramentas para a auditoria no provedor de nuvem podem incluir, pelo menos:
- ✓ Análise das políticas, processos e procedimentos de segurança e privacidade.
  - ✓ Entrevistas com todas as áreas da empresa para percepção sobre se a política de segurança é de conhecimento organizacional e se está sendo seguida.
  - ✓ Visita ao data center para analisar a segurança física.
  - ✓ Análise de configuração do firewall.
  - ✓ Análise do fluxo para gestão de identidades.
  - ✓ Pentest para identificar vulnerabilidades do ambiente.
  - ✓ Análise de logs do banco de dados.

74

- ✓ Análise dos relatórios do IDS/IPS.
- ✓ Análise dos antivírus.
- ✓ Análise de código do sistema corporativo.
- ✓ Teste de phishing.

75

## Auditoria

76

Entenderam os pontos principais de auditoria?



Fonte: <https://gfxer.com/en/00019>

77

## Recapitulando

78

- ✓ Fundamentos de Auditoria de Sistemas
- ✓ Controles gerais de auditoria de sistemas
- ✓ Técnicas e Ferramentas para auditoria de sistemas

79



80