Segurança e Auditoria de Sistemas

AUDITORIA DE SISTEMAS E SEGURANÇA

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: Auditoria de Sistemas e Segurança
- 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

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

4

Contextualização

- A auditoria exige o entendimento de seus conceitos e princípios, que demonstram a importância das competências do auditor, as quais devem ser abrangentes e profundas para serem aplicadas nas fases do processo de auditoria.

Fonte: Shutterstock

5

Fundamentos de Auditoria de Sistemas

6

Contextualizando

- A gestão de riscos identifica, analisa, avalia, comunica e trata os riscos em um contexto determinado.
- Os controles de segurança são definidos e implementados a partir desta visão de riscos e de acordo com padrões e requisitos regulatórios e legais.
- A auditoria valida a eficiência e eficácia dos controles, com uma análise criteriosa que segue processos e aplica técnicas e ferramentas.
- O papel do auditor é, assim, fundamental, e o resultado é uma empresa mais segura e em conformidade com padrões, regulações e leis aplicáveis.

7

Contextualizando

- A auditoria exerce uma influência positiva para as empresas também no aspecto de comunicação e relações institucionais, melhorando o nível de confiança com todos os atores envolvidos.
- Do ponto de vista de padrão, um exemplo é o Payment Card Industry Data Security Standard (PCI DSS), aplicado para empresas que fazem parte do ecossistema de cartões, o qual tem como objetivo melhorar o tratamento de dados de portadores de cartão, o que é benéfico para todo o ecossistema.
- Um outro exemplo de auditoria é a ISO 27001, que certifica a segurança das empresas em um determinado escopo de auditoria.

8

Contextualizando

- A forma de executar a auditoria é importante, com o uso das técnicas e ferramentas mais adequadas para cada objetivo.
- Uma exigência é que, tendo aspectos abrangentes, o auditor precisa definir e utilizar seus conhecimentos e ferramentas para analisar detalhes do ambiente para validar a efetividade dos controles.
- As técnicas de auditoria podem ir de entrevistas a testes técnicos com o uso de ferramentas para análise de logs e até mesmo de código-fonte, por exemplo.
- Com a auditoria, o ciclo de segurança e privacidade fica completo, visando a efetiva segurança das empresas.

9

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.
- A auditoria de sistemas de informação provê uma série de benefícios para as empresas, tais como a garantia de eficácia, eficiência, segurança e confiabilidade das operações dos sistemas de informação, que são críticos para o sucesso organizacional.

Fonte: adaptada de ISACA (2016).

10

Auditoria - Objetivos

- 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.
- Outro objetivo da auditoria é atestar a conformidade com regulações administrativas, regulatórias e legais.
- 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).

11

O papel do auditor de sistemas

O 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).
Para o auditor, o ITAF estabelece algumas responsabilidades (ISACA, 2020):

12

O papel do auditor de sistemas

O 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).
Para o auditor, o ITAF estabelece algumas responsabilidades (ISACA, 2020):

13

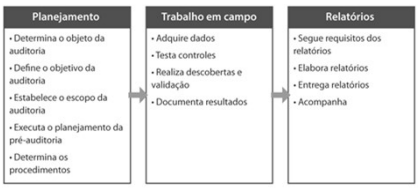
Auditor - responsabilidades

- Documentar a função em um estatuto, indicando propósito, responsabilidade, autoridade e a prestação de contas.
- Obter aprovação formal do estatuto pela diretoria executiva e/ou comitê de auditoria.
- Comunicar a alta gestão sobre o estatuto da auditoria.
- Atualizar o estatuto a fim de manter o alinhamento com a missão e estratégia da organização.
- Ser livre de conflitos de interesses e influências indevidas.
- Ser objetivo nos assuntos de auditoria.
- Definir um escopo claro e sem limitações, o escopo deve levar a conclusões.

Fonte: Shutterstock

14

Fases do processo de auditoria de sistema de informação



Fonte: adaptada de ISACA (2016).

15

Técnicas de Auditoria de T.I

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.
- Simulações passo a passo.
- Execução de controles.

Fonte: Shutterstock

16

17

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.
Os controles de segurança são identificados e implantados com base nos riscos avaliados, com este tratamento dos riscos envolvendo ainda os riscos aceitos.

18

O planejamento segue os itens gerais:

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.
O conjunto de controles deve ser verificado sob a óptica destas necessidades legais e regulatórias e atestado pelo auditor.

19

O planejamento segue os itens gerais:

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.

20

O planejamento segue os itens gerais:

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.
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.

21

O planejamento segue os itens gerais:

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.

22

Controles Gerais de Auditoria de Sistemas

23

Sua missão

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.
Agora, 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 :
•Tipos de controles considerados e para que servem.
•Como os controles são definidos.

Fonte: Shutterstock

24

Sua missão

•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.
O auditor precisa ter conhecimentos e competências para avaliar os controles quanto à eficiência e eficácia. Isto faz com que os controles discutidos nesta aula sejam importantes para a construção deste conhecimento e desta competência.
Além disso, normas e frameworks como a ISO 27001, de Sistema de Gestão de Segurança da Informação (SGSI), COBIT e ITIL são frequentemente utilizados nas auditorias.

Fonte: Shutterstock

25

Tipos de Controles de Segurança e Privacidade

Os controles podem ser físicos (como monitoramento de circuito fechado de TV), tecnológicos (como firewall, VPN) ou processuais (como atualização periódica de sistema operacional).
E os controles têm objetivos diversos, como para o processo de aquisição, desenvolvimento e manutenção de sistemas, ou para o controle de acesso lógico e físico.
Há controles voltados para a segurança e privacidade, como os definidos na norma ABNT NBR ISO/IEC 27002. E há controles voltados para outras finalidades, como para a governança de TI (COBIT) ou para o gerenciamento de serviços (ITIL).

Fonte: Shutterstock

26

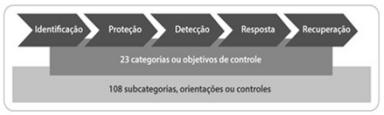
Tipos de Controles de Segurança e Privacidade

O importante é que eles têm relação com a segurança e privacidade, como a continuidade de serviços do ITIL, que é importante para a proteção da disponibilidade da informação.
O auditor precisa conhecer as normas, padrões, frameworks, regulações e leis que exigem a implantação de controles, assim como conhecer esses últimos.
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.

Fonte: Shutterstock

27

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



Fonte: adaptada de NIST (2018).

28

Frames de Segurança

29

Ano: 2019 Banca: COMPERVE Órgão: UFRN Prova: COMPERVE - 2019 - UFRN - Analista de Tecnologia da Informação
A organização tida como referência para o estabelecimento de boas práticas na área da segurança computacional, sendo inclusive mantenedora de um framework para cibersegurança que inclui padrões, diretrizes e melhores práticas para gerenciar o risco relacionado a esse tema é a
a) ITU-T (Telecommunication Standardization Sector)
b) ISO (International Organization for Standardization).
c) TCP/IP (Transmission Control Protocol/Internet Protocol).
d) NIST (National Institute of Standards and Technology).

30

Ano: 2019 Banca: COMPERVE Órgão: UFRN Prova: COMPERVE - 2019 - UFRN - Analista de Tecnologia da Informação
A organização tida como referência para o estabelecimento de boas práticas na área da segurança computacional, sendo inclusive mantenedora de um framework para cibersegurança que inclui padrões, diretrizes e melhores práticas para gerenciar o risco relacionado a esse tema é a
a) ITU-T (Telecommunication Standardization Sector)
b) ISO (International Organization for Standardization).
c) TCP/IP (Transmission Control Protocol/Internet Protocol).
d) NIST (National Institute of Standards and Technology).

31

32

Entendeu a importância da organização de uma auditoria?

Fonte: https://gifer.com/en/XIOL9

33

Controles Organizacionais e relação com segurança e continuidade do serviço

34

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.

35

Governança

Para que a segurança seja efetiva, é importante que os processos estejam bem definidos e a equipe tenha as competências para as ações necessárias.
A governança garante que as ações do cotidiano sejam tratadas para que as ameaças correntes e emergentes sejam sempre tratadas e alinhadas com a alta gestão (ISACA, 2017).
COBIT
O COBIT, de Control Objectives for Information and Related Technology, é um framework de governança de TI que trata de uma visão organizacional, a qual tem relação com a segurança e privacidade.

36

Governança

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.
ITIL
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.

37

Governança

O COBIT também trata da continuidade, como o gerenciar continuidade (DSS04) no domínio de entregar serviço e suporte. Além do ITIL e do COBIT, o assunto é tratado também na norma ABNT NBR ISO/IEC 27001:2013 e 27002:2013, em um objetivo de controle específico para aspectos da segurança da informação na gestão da continuidade do negócio.
O sistema de gestão de continuidade de negócios é tratado na norma ABNT NBR ISO 22301:2020, que considera a segurança e resiliência. E a norma ABNT NBR ISO/IEC 27031:2015 trata de diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação.

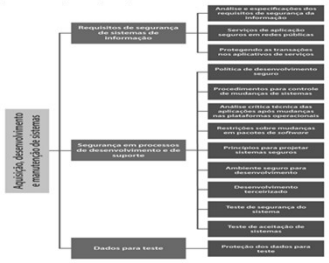
38

Controles para aquisição, desenvolvimento e manutenção de sistemas

a) ISO 27002

39

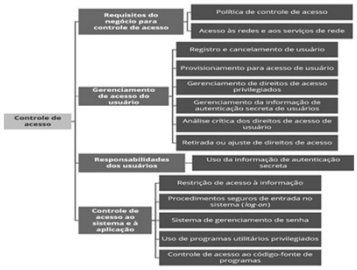
Controles para aquisição, desenvolvimento e manutenção de sistemas



Fonte: adaptada de ISO 27002 (2013).

40

Controles da ISO 27002 para controle de acesso



41

Controles Lógicos, Físicos e Processuais

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.

42

43

Você já montou um planejamento para melhorar a segurança do provedor de nuvem e agora irá detalhar o planejamento, com foco nos controles. Os principais tópicos que você pode considerar na elaboração do material são:
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

44

de revisão de contas de usuários; (iii) físicos, como o cadeado para que o desktop utilizado pelo presidente da empresa não seja roubado.
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

45

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. 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. Já o 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.

46

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 de rede. O gerenciamento de acesso do usuário deve incluir aspectos como o registro e cancelamento de usuário,

47

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.
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.

48

Os principais controles existentes na empresa devem estar cumprindo os objetivos de, pelo menos:
Políticas de segurança da informação.
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.

49

OBJETIVOS DAS TÉCNICAS E FERRAMENTAS EM AUDITORIA DE SISTEMAS

50

Sua Missão

Você já montou um planejamento para melhorar a segurança do provedor de nuvem, que está crescendo de uma forma muito rápida.

As ações de implantação dos controles foram adiante e agora você deve planejar as técnicas e ferramentas que serão utilizadas na auditoria.

Fonte: Shutterstock

51

Contextualizando

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.
Com o modelo operacional expandindo para a distribuição dos dados e uso mais abrangente dos provedores de nuvens, os dados vão para além das fronteiras da própria empresa.

52

Contextualizando

Do lado das empresas, há a necessidade de que o nível de segurança e privacidade dos provedores e fornecedores seja no mínimo equivalente ao que é requerido para os negócios da empresa.
Já do lado dos provedores e fornecedores, há a necessidade de demonstrar a conformidade com normas e legislações, para que as oportunidades de negócios possam ser aproveitadas.

53

Exemplos de abordagens para as auditorias (ISACA, 2017)

- Governança, com a política de segurança da informação e os procedimentos operacionais técnicos relacionados.
- Riscos, com as atualizações dos registros dos riscos, e o tratamento e reporte dos riscos, envolvendo a acurácia, completude e atualizações apropriadas dos registros.
- Gestão, com as revisões dos incidentes de segurança, com base nos ataques, brechas e incidentes atuais.
- Processos de gestão de riscos, para a eficiência e efetividade.
- Estas abordagens podem seguir *frameworks* de governança como o *Control Objectives for Information and Related Technologies* (COBIT), melhores práticas como o *Information Technology Infrastructure Library* (ITIL) ou o sistema de gestão de segurança da informação (ISO 27001).

54

Objetivos das técnicas e ferramentas

55

Técnicas e ferramentas que envolvem interação com pessoas

Dentre as técnicas e ferramentas que envolvem interação com pessoas, estão:
•Entrevistas: reuniões com profissionais de áreas-chave para a auditoria.
•Questionários: questionários a serem respondidos pelos profissionais de áreas-chave.
•Pesquisas: obtenção de dados via pesquisas individuais ou para grupos.
•Perguntas e observação: conversas e observações no contexto do cotidiano da empresa.
•Dinâmicas em grupo: exercícios ou atividades especializadas direcionadas a grupos.

56

Análise manual

Já a análise manual pode ser feita com :
•Planilhas eletrônicas: organização e análise obtida de diferentes fontes.
•Scripts: execução automatizada para obtenção ou filtragem de dados específicos.
•Software de auditoria para analisar o conteúdo de arquivos de dados, como os logs de sistemas, lista de acesso de usuários.
•Ferramentas de auditoria específicas (Computer-Assisted Audit Tools, CAATs): softwares especializados para gerar amostras, importar dados, sumarizar e testar os controles, condições e processos implantados nos sistemas a partir de amostras.

57

Análise manual

•Software especializado para avaliar conteúdo de sistemas operacionais, banco de dados e arquivos de parâmetros de aplicações.
•Logs de auditorias e relatórios para avaliar parâmetros.
•Simulações passo a passo: utiliza as informações do sistema para mapear e construir os passos a serem simulados em outra ferramenta a fim de chegar ao mesmo resultado do sistema.
•Execução de controles: submete parâmetros de teste com dados reais, sem impactar na rotina normal de processamento do sistema.
•Metodologias para coleta de transações.
•Pentests ou testes de penetração: identificação e análise de vulnerabilidades.

58

Linhas de Defesa

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: há o interesse em garantir que os controles de segurança e privacidade estejam presentes e operando efetivamente, com as devidas responsabilidades e cobranças. Algumas atividades são a autoavaliação de controles, testes de penetração, testes funcionais e técnicas, testes sociais e de comportamento, e revisões gerenciais.
•Gestão de riscos: as operações da empresa são sustentadas por controles necessários de acordo com uma visão de riscos,

59

Linhas de Defesa

envolvendo os cálculos da probabilidade e do impacto de um agente de ameaça explorar vulnerabilidades de ativos, fazendo com que uma ameaça se torne um incidente de segurança. Controles já implementados são considerados na gestão de riscos, já que diminuem os riscos existentes.
•Auditoria interna: para a segurança, é importante que os processos estejam bem definidos e a equipe tenha as competências para as ações necessárias. A governança garante que as ações do cotidiano sejam tratadas para que as ameaças correntes e emergentes sejam sempre tratadas e alinhadas com a alta gestão. A auditoria interna auxilia na comunicação das ações entre as diferentes áreas da empresa, e provê os testes dos controles, a conformidade, a aceitação formal dos riscos e o suporte para as investigações e análises forense.

60

PCI DSS

Construir e manter a segurança de rede e sistemas	**1. Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão.**
	2. Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança.
Proteger os dados do titular do cartão	3. Proteger os dados armazenados do titular do cartão.
	4. Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas.
Manter um programa de gerenciamento de vulnerabilidades	5. Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus.
	6. Desenvolver e manter sistemas e aplicativos seguros.
Implementar medidas rigorosas de controle de acesso	7. Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio.
	8. Identificar e autenticar o acesso aos componentes do sistema.
	9. Restringir o acesso físico aos dados do titular do cartão.
Monitorar e testar as redes regularmente	10. Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão.
	11. Testar regularmente os sistemas e processos de segurança.
Manter uma política de segurança de informações	12. Manter uma política que aborde a segurança da informação para todas as equipes.

61

62

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.

63

Análise dos relatórios do IDS/IPS.
Análise dos antivírus.
Análise de código do sistema corporativo.
Teste de phishing.
Sobre a segurança física, no exemplo do PCI DSS, um requisito é que "haja câmeras de vídeo ou outros mecanismos de controle de acesso (ou ambos) para monitorar o acesso físico individual a áreas sensíveis. Analise os dados coletados e relacione com outras entradas. Armazene, por pelo menos três meses, a menos que seja restringido de outra forma pela lei".

64

Auditoria

65

Entenderam a complexidade da auditoria?

Fonte: https://gifer.com/en/6IOL9

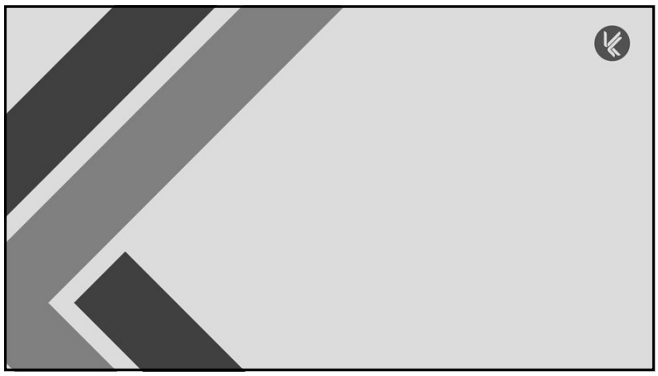
66

Recapitulando

67

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

68



69