NÃO PODE FALTAR

TÉCNICAS E FERRAMENTAS PARA AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

QUAIS SÃO OS OBJETIVOS DAS TÉCNICAS E FERRAMENTAS EM AUDITORIA DE SISTEMAS?

Elas devem ser utilizadas para identificar, levantar evidências e para analisar e validar as evidências, além disso, elas devem auxiliar o auditor a organizar e documentar os resultados.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

PRATICAR PARA APRENDER

Olá, aluno! Nesta seção focaremos na fase de trabalho em campo, onde serão aplicadas as ferramentas para auditoria de sistemas, com base nos objetivos e escopos de auditoria.

O trabalho em campo é feito a partir do que foi planejado, com a aplicação das técnicas e ferramentas que foram definidas de acordo com os objetivos e o escopo da auditoria, além da pré-auditoria.

Utilizando as técnicas e ferramentas, o auditor poderá fazer a auditoria para verificar se o controle implantado está cumprindo o seu papel e se os controles necessários foram de fato definidos e implantados.

As técnicas e ferramentas podem ser utilizadas para a interação com as pessoas, para análises manuais ou para análises técnicas. Os principais exemplos são as entrevistas, que possibilitam obter informações com a interação com as pessoas, e as análises e revisões de documentação, políticas, procedimentos, processos e configurações, que são técnicas manuais. Outro exemplo é o uso de *softwares* especializados para gerar amostras, importar dados, sumarizar e testar os controles, condições e processos implantados nos sistemas a partir de amostras, que correspondem a ferramentas para análises técnicas.

A aplicabilidade da auditoria direciona a escolha das melhores técnicas e ferramentas a serem utilizadas no trabalho em campo, e podem ser baseadas em normas, padrões e *frameworks* como COBIT, ITIL, NIST *Cybersecurity Framework*, CIS *Controls*, PCI DSS e ISO 27001. As auditorias visam a conformidade, o que resulta na segurança e na maior confiança de todos os envolvidos, de clientes a investidores, passando por parceiros, funcionários e fornecedores.

A ISO 27001 possibilita a certificação da empresa do Sistema de Gestão de Informação (SGSI), em um escopo definido de auditoria.

Para finalizarmos a seção, discutiremos alguns cases de auditoria, que reforçam a busca da conformidade e apresentam escopos que variam de acordo com os objetivos da auditoria.

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.

Você já montou um planejamento para melhorar a segurança da empresa e para fortalecer a imagem do provedor de nuvem perante o mercado quanto ao tratamento das necessidades de segurança e conformidade. Você também já tem um planejamento detalhado dos controles.

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:

- 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.

Boa aula!

Ver anotações

CONCEITO-CHAVE

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).

Uma auditoria é normalmente feita em três etapas, de planejamento, de trabalho em campo e de relatórios. Na fase de planejamento, de acordo com o objeto, os objetivos, o escopo e a pré-auditoria, os procedimentos, técnicas e ferramentas para a realização dos testes e verificações das evidências são definidos para serem aplicados na fase de trabalho em campo.

Nesta seção discutiremos os principais procedimentos, técnicas e ferramentas que podem ser utilizados em auditorias.

INTRODUÇÃO ÀS 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.

EXEMPLIFICANDO

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. 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.

Alguns exemplos de abordagens para as auditorias (ISACA, 2017) são:

- **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).

REFLITA

Com o ambiente tecnológico das empresas sempre evoluindo, como o uso de provedores de nuvem ou a expansão da internet das coisas, o desafio das empresas em manter a segurança e privacidade aumenta, assim como as

> auditorias. Somado a essa mudança constante do ambiente tecnológico há o ambiente regulatório e legal que também evolui e eleva as necessidades de segurança e privacidade.

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):

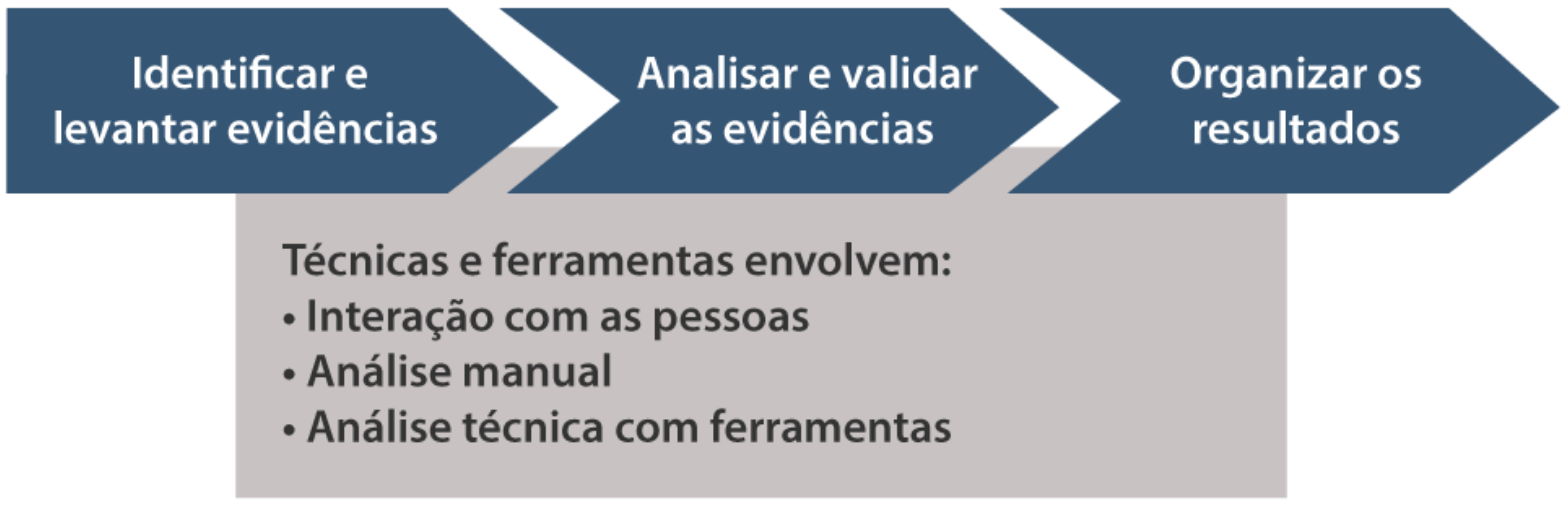
- **Políticas, padrões e procedimentos de segurança adequados e efetivos:** verificar se a documentação está completa e atualizada, confirmar que há aprovação formal e divulgação, verificar se a documentação está cobrindo todos os requisitos de segurança e privacidade e verificar se os controles estão cobrindo tudo o que foi citado em políticas, padrões e procedimentos.
- **Riscos emergentes identificados, avaliados e tratados de uma forma confiável e adequada:** confirmar a confiabilidade do processo de identificação de riscos, avaliar processo, ferramentas, métodos e técnicas de avaliação de riscos utilizados, confirmar que todos os riscos foram tratados de acordo com os resultados, verificar que o tratamento dos riscos está adequado ou se há uma aceitação formal do risco.
- **Ataques e brechas são identificados e tratados no tempo e na forma apropriados:** confirmar soluções de monitoramento e reconhecimento de ataques, avaliar as interfaces para os processos e planos da gestão de incidentes de segurança e de gestão de crises, avaliar o tempo de resposta aos ataques passados.

Assim, a 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).

PRINCIPAIS TÉCNICAS E FERRAMENTAS PARA AUDITORIA DE SISTEMAS

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 (Figura 4.12). 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.

Figura 4.12 | Objetivos das técnicas e ferramentas



Fonte: elaborada pelo autor.

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

- **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.

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.

A **análise técnica com uso de ferramentas** é um dos principais métodos que exige um conhecimento técnico amplo dos auditores e inclui (BENETON, 2017) (ISACA, 2016) (ISACA, 2017) (KAMAL, 2020) (LIMA, 2020):

- **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.

- ***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.

> **ASSIMILE**
>
> Os procedimentos, técnicas e ferramentas para auditoria são utilizados para obter dados e informações e para analisar e validar as evidências e os controles existentes. Além disso, são utilizados para organizar os resultados. O conhecimento e a competência técnica do auditor são essenciais para definir procedimentos, técnicas e ferramentas na fase de planejamento da auditoria, e para utilizá-los no trabalho em campo.

APLICABILIDADE DAS TÉCNICAS E FERRAMENTAS PARA AUDITORIA DE SISTEMAS

Os procedimentos, técnicas e ferramentas para auditoria de sistemas são utilizadas de acordo com o objetivo e escopo da auditoria, e são definidos no momento de planejamento.

A aplicação das técnicas e ferramentas é feita no trabalho em campo e depende da abordagem da auditoria, que pode ser baseadas em *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).

No caso da segurança da informação, a auditoria visa assegurar que os controles protegem a empresa de uma forma adequada, com base na gestão de riscos.

Ver anotações

> **EXEMPLIFICANDO**
>
> Controles de segurança são implementados para tratar vulnerabilidades. Quando as vulnerabilidades são tratadas, o risco diminui, já que a probabilidade de um agente de ameaça explorá-la diminui ou deixa de existir. Há, porém, o risco residual, que sempre deve ser considerado após a implementação dos controles de segurança. Um exemplo é o controle de segurança que atualiza o sistema com versões de *software* sem vulnerabilidades conhecidas. Porém, novas vulnerabilidades são descobertas o tempo todo e o processo de atualização pode ser definido ou executado de forma incompleta. A auditoria é importante para que a efetividade dos controles seja alcançada.

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,

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.

> **EXEMPLIFICANDO**
>
> O padrão ANSI/TIA-942 trata de infraestrutura de telecomunicações e outros aspectos de datacenters, como a localização, estrutura física e de arquitetura, infraestrutura elétrica e mecânica, além de segurança física e contra incêndios. Os data centers podem ser certificar, de acordo com os requisitos do padrão (TIA, 2020).

CASES DE AUDITORIA EM SISTEMAS DE INFORMAÇÃO

O *Payment Card Industry Data Security Standard* (PCI DSS) é um padrão de segurança de dados da indústria de cartões de pagamento, que estabelece requisitos de segurança que devem ser cumpridos por todos os estabelecimentos e empresas que processam, transmitem ou armazenam dados de cartões de pagamento. As empresas devem cumprir os 12 requisitos de segurança definidos (Quadro 4.3), que são analisados em um processo de avaliação feito por profissionais como assessores e empresas qualificadas.

Quadro 4.3 | Os 12 requisitos de segurança do 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.

Fonte: adaptado de PCI (2018).

Ver anotações 0

ASSIMILE

As empresas que processam, transmitem e armazenam dados de cartões de pagamento devem estar em conformidade com a PCI DSS, cumprindo os requisitos de segurança definidos que são avaliados pelos assessores qualificados. O objetivo do PCI é proteger a indústria de cartões, uma vez que a confiança no uso dos cartões pode ser comprometida por incidentes de segurança em qualquer ponto da cadeia (comerciantes, processadores, adquirentes, emissores e prestadores de serviço). Assim, quem não está em conformidade com o padrão de segurança pode perder a permissão de utilizar os cartões de pagamento.

Sem a conformidade com a PCI DSS, as empresas ficam sujeitas a não poderem mais participar do ecossistema de cartões de pagamento, por colocar em risco os demais atores da cadeia e prejudicar a confiança no sistema.

REFLITA

O PCI DSS trata o trabalho de avaliação de conformidade como uma avaliação e não uma auditoria. Isso faz com que exista uma característica fundamental no PCI DSS que o

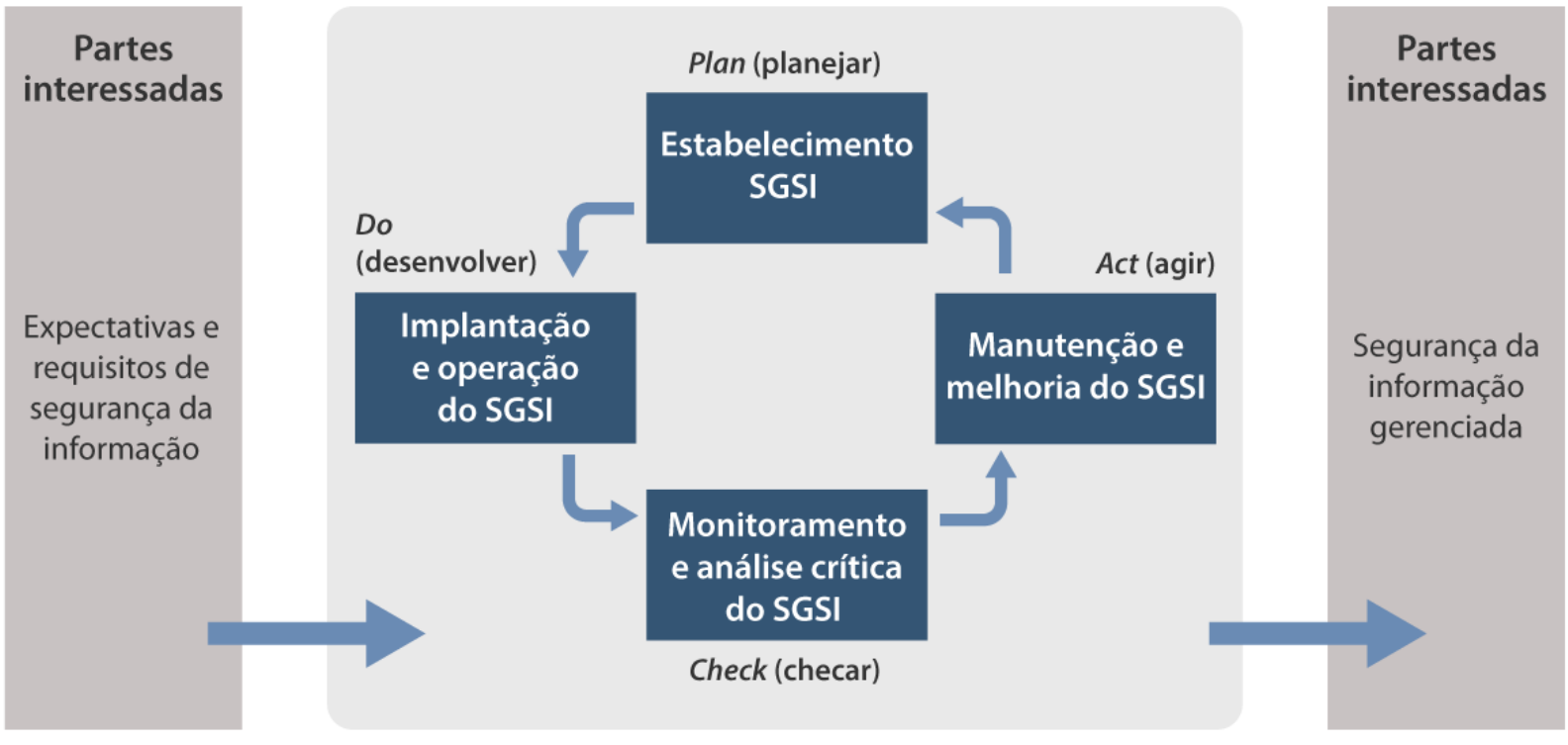
diferencia de um potencial conflito de interesses que pode existir nas auditorias: os assessores qualificados podem participar do processo de adequação das empresas ao PCI DSS, não sendo limitados a apenas auditá-los. O resultado, assim, é o relatório de conformidade ou *Report on Compliance* (RoC), que apresenta os resultados dos testes feitos nos controles definidos no padrão.

Ver anotações 0

As empresas podem se certificar em segurança da informação com a ISO 27001, que estabelece um sistema de gestão de segurança da informação, após uma auditoria de certificação.

A ABNT NBR ISO/IEC 27001 especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação dentro do contexto da organização (Figura 4.13). A norma inclui também requisitos para a avaliação e o tratamento de riscos de segurança da informação voltados para as necessidades da organização. E os requisitos (Figura 4.14) da norma (contexto da organização, liderança, planejamento, apoio, operação, avaliação de desempenho e melhoria) são genéricos e são aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza, e todos devem fazer parte do SGSI (ISO 27001, 2013).

Figura 4.13 | Ciclo PDCA do SGSI



Fonte: adaptada de ISO 27001 (2013).

Figura 4.14 | Requisitos da ABNT NBR ISO/IEC 27001

Fonte: elaborada pelo autor.

Em uma auditoria de certificação ISO 27001, que pode ser aplicável para as empresas de diferentes tamanhos e naturezas, a auditoria deve levar em consideração o escopo e os requisitos do SGSI.

ASSIMILE

A certificação ISO 27001 avalia o sistema de gestão de segurança da informação (SGSI), de acordo com um escopo definido. A aplicação dos controles muda de empresa para empresa, dependendo do apetite ao risco, e do escopo envolvido. E ambas as empresas podem obter a certificação ISO 27001, mesmo com controles diferentes implantados.

Para a certificação, a empresa não precisa implantar todos os controles de segurança indicados na norma e detalhados na ABNT NBR ISO/IEC 27002 (ISO 27002, 2013). Os requisitos regulatórios e legais, além dos objetivos de negócios e os resultados da avaliação indicam os controles de segurança necessários. E, para a auditoria, é preciso organizar estas informações.

A declaração de aplicabilidade é um dos principais elementos de uma auditoria da ISO 27001. Ela declara quais controles de segurança são aplicáveis para a empresa, com base nos riscos específicos do ambiente e do escopo que está sendo auditado (HERON, 2019).

Para a criação da declaração de aplicabilidade, os passos são (HERON, 2019):

- Considerar os assuntos, partes interessadas e o escopo do SGSI.
- Identificar os ativos de informação, centros de processamento e dispositivos.
- Analisar os riscos de segurança da informação, considerando a confidencialidade, integridade e disponibilidade.
- Avaliar os riscos e decidir quais dos 114 controles da norma são necessários.
- Entender e avaliar as legislações e contratos aplicáveis.
- Definir a implementação dos controles, incluindo políticas, procedimentos, pessoas, tecnologias etc.
- Criar a declaração de aplicabilidade com as justificativas.
- Relacionar detalhes dos controles, os riscos e os ativos, com o SGSI funcionando.
- Gerenciar.

A auditoria interna é uma parte importante para as empresas e faz parte do processo de avaliação de desempenho do SGSI, o qual indica que elas devem conduzi-las a intervalos planejados para prover

informações sobre o quanto o sistema de gestão da segurança da informação está em conformidade com os próprios requisitos da organização para o seu sistema de gestão da segurança da informação e os requisitos da ABNT NBR ISO/IEC 27001 e que o SGSI está efetivamente implementado e mantido (ISO 27001, 2013).

A ABNT NBR ISO/IEC 27001 define o que a organização deve fazer quanto à auditoria interna (ISO 27001, 2013):

- Planejar, estabelecer, implementar e manter um programa de auditoria, incluindo frequência, métodos, responsabilidades, requisitos de planejamento e relatórios. Os programas de auditoria devem levar em conta a importância dos processos pertinentes e os resultados de auditorias anteriores.
- Definir os critérios e o escopo da auditoria, para cada auditoria.
- Selecionar auditores e conduzir auditorias que assegurem objetividade e imparcialidade do processo de auditoria.
- Assegurar que os resultados das auditorias são relatados para a direção pertinente.
- Reter a informação documentada como evidência dos programas da auditoria e dos seus resultados.

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:** condução de uma avaliação de riscos para determinar o foco da auditoria e identificar as áreas que estão fora de escopo. Fontes de informação incluem pesquisas de indústria, políticas e o SGSI. O escopo deve ser relevante para a empresa, incluindo diferentes localidades de unidades de negócios. Durante o levantamento pré-auditoria, a documentação que será revisada durante a auditoria deve ser juntada.

- **Planejamento e preparação:** com o escopo da auditoria de SGSI, o detalhamento envolve o planejamento da auditoria, com a definição do tempo e recursos. Pontos de checagem com a gestão da empresa possibilitam ajustes para agilizar o acesso às informações e pessoas, bem como para a gestão acompanhar o andamento da auditoria e reforçar as preocupações.

- **Trabalho em campo:** o planejamento da auditoria é aplicado, com os auditores coletando evidências com as técnicas definidas, como as entrevistas com equipes, áreas e demais atores envolvidos com o SGSI. Há ainda a revisão de documentação e de dados, com a observância dos processos do SGSI em funcionamento. Os testes das evidências devem ser feitos para validar as evidências coletadas, junto das documentações destes testes.

- **Análise:** as evidências da auditoria devem ser organizadas e revisadas com relação aos riscos e objetivos de controles. A análise pode identificar necessidades de novas evidências ou de novos testes, que devem ser realizados.

- **Reporte:** Os componentes essenciais do relatório consistem em: introdução que justifica escopo, objetivos, tempo e extensão dos trabalhos; sumário executivo indicando os principais resultados, uma análise resumida e uma conclusão; lista de pessoas ou áreas que terão acesso ao relatório, incluindo a classificação da informação e as regras de circulação; resultados e análises detalhadas; conclusão e recomendações; declaração do auditor detalhando as recomendações ou limitações do escopo. O relatório de auditoria deve ser apresentado e discutido previamente com a gestão de projetos, devido a eventuais necessidades de revisões e análises adicionais. A gestão deve se comprometer com o plano de ação.

SAIBA MAIS

Uma auditoria de segurança engloba um conjunto de elementos, como as configurações dos sistemas operacionais, compartilhamentos de redes, aplicações e acessos, a validação de processos e do nível de maturidade em segurança dos usuários. Alguns assuntos que são normalmente alvos de auditoria são:

- Proteção de *e-mail*, principalmente contra *phishing* e filtros de *spam*.
- Senhas de usuários, para verificar se estão de acordo com a política de senha da empresa.
- Gerenciamento de usuários, para verificar se há contas ativas que não deveriam, como de ex-funcionários.
- *Backups*, para verificar se é feito e se está íntegro.
- Acesso físico, para evitar acessos indevidos de pessoas não autorizadas.
- Atualização de *software*, para verificar se os sistemas estão em versões livres de vulnerabilidades.
- Vulnerabilidades, para identificar pontos fracos que podem ser explorados em ataques.

PESQUISE MAIS

O livro *Auditoria e controle de acesso*, de Beneton (2017) apresenta no capítulo 5 uma discussão sobre a auditoria de sistema operacional e aplicativos, abordando questões de logs, monitoração de violações, gestão de mudanças e gestão de liberações.

BENETON, E. **Auditoria e controle de acesso**. São Paulo: Editora Senac, 2017.

Ver anotações 0

Chegamos ao fim desta aula, em que a auditoria deve ser planejada com a definição das técnicas e ferramentas a serem aplicadas no trabalho em campo na auditoria. Esta definição depende do objetivo e escopo da auditoria, que pode ser para a conformidade com padrões, normas, leis ou regulações. Em segurança da informação, a auditoria deve validar a eficácia e eficiência dos controles, que são definidos de acordo com a avaliação dos riscos, fechando, assim, o objetivo de tornar a empresa mais segura, de fato. O conhecimento e a competência para definir e utilizar as técnicas e ferramentas é essencial para uma auditoria de sucesso.

FAÇA VALER A PENA

Questão 1

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. Ela é realizada em três grandes fases, que são o planejamento, o trabalho em campo e os relatórios.

As técnicas e ferramentas de auditoria são definidas na fase de:

a. Planejamento.

b. Trabalho em campo.

c. Relatórios.

d. Entre o planejamento e o trabalho em campo.

e. Entre o trabalho em campo e os relatórios.

Questão 2

Uma auditoria verifica e inspeciona formalmente a eficiência e eficácia de controles e valida a conformidade de acordo com normas, padrões, *frameworks*, leis ou regulações. Há, assim, auditorias com objetivo de conformidade e outras com objetivo de certificação.

Assinale a alternativa que possibilita uma certificação da empresa.

a. COBIT.

b. ITIL.

c. NIST *Cybersecurity Framework.*

d. ISO 27001.

e. COSO.

Questão 3

As técnicas e ferramentas para auditoria envolvem interação com pessoas, análise manual e análise técnica. Com base nas técnicas e ferramentas, associe a coluna A com a coluna B.

A	**B**
I. Perguntas e observação	1. Interação com pessoas
II. Análise de configurações	2. Análise manual
III. *Pentest*	3. Análise técnica
IV. *Scripts*	

A seguir, assinale a alternativa que apresenta a associação correta.

a. I-1; II-1; III-3, IV-3.

b. I-1; II-1; III-2; IV-3.

c. I-1; II-2; III-2; IV-3.

d. I-1; II-2; III-3; IV-3.

e. I-1; II-3; III-3; IV-3.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27002:2013** Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2013.

ABNT. **NBR ISO/IEC 27002:2013 Tecnologia da informação** — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2013.

AXELOS. **Building IT and Digital Excellence with ITIL 4, 2018**. Disponível em: https://bit.ly/3dlnlI8. Acesso em: 10 jan. 2021.

BENETON, E. **Auditoria e controle de acesso**. São Paulo: Editora Senac, 2017. Disponível em: https://bit.ly/39uB3rd. Acesso em: 13 jan. 2021.

HERON, J. The ISO 27001:2013 Statement of Applicability (SoA): The Complete Guide. **ISMS online**, 3 dez. 2019. Disponível em: https://bit.ly/3sF6VAF. Acesso em: 14 jan. 2021.

ISACA, Information Systems Audit and Control Association. **COBIT 2019 *Framework***. Introduction and Methodology, 2018. Disponível em: https://bit.ly/3uc08PC. Acesso em: 4 jan. 2021.

ISACA, Information Systems Audit and Control Association. **COBIT 2019 *Framework***. Governance and Management Objectives, 2018. Disponível em: https://bit.ly/3m9CjFc. Acesso em: 7 jan. 2021.

ISACA, Information Systems Audit and Control Association. **Information Systems Auditing: Tools and Techniques Creating Audit Programs**, 2016. Disponível em: https://bit.ly/39sed3i. Acesso em: 7 jan. 2021.

ISACA, Information Systems Audit and Control Association. **Auditing Cyber Security:** Evaluating Risk and Auditing Controls, 2017. Disponível em: https://bit.ly/3mdxIC3. Acesso em: 9 jan. 2021.

ISACA, Information Systems Audit and Control Association. IT Audit Framework (ITAFTM). **A Professional Practices *Framework* IT Audit**, 4 ed., 2020. Disponível em: https://bit.ly/3rIJRjk. Acesso em: 4 jan. 2021.

ISACA, Information Systems Audit and Control Association. **IT Audit's Perspectives on the Top Technology Risks for 2021**, Protiviti, 2020. Disponível em: https://bit.ly/3sGMYK3. Acesso em: 4 jan. 2021.

ITIL Process Map & ITIL Wiki. **ITIL 4**, 3 dez. 2019. Disponível em: https://bit.ly/3sRRwNu. Acesso em: 10 jan. 2021.

ITIL Process Map & ITIL Wiki. **IT Service Continuity Management**, 24 jul. 2020. Disponível em: https://bit.ly/3wezfw4. Acesso em: 10 jan. 2021.

KAMAL, S.; HELAL, I. M. A.; MAZEN, S. A. Computer-Assisted Audit Tools for IS Auditing – A comparative study. Faculty of Computers and Artificial Intelligence, Cairo University, Giza, Egypt. Disponível em: https://bit.ly/3fyWg70. Acesso em 16 jan. 2021.

MCCREANOR, N. The five stages of a successful ISO 27001 audit. **It governance**, 19 maio 2020. Disponível em: Link. Acesso em: 14 jan. 2021.

NAKAMURA, E. T. **Segurança da informação e de redes**. Londrina: Editora e Distribuidora Educacional S.A., 2016.

NATIONAL Institute of Standards and Technology, NIST. ***Framework* for Improving Critical Infrastructure *Cybersecurity***. Version 1.1, 16 abr. 2018. Disponível em: https://bit.ly/31CTPIl. Acesso em: 24 out. 2020.

NATIONAL Institute of Standards and Technology, NIST. Security and Privacy *Controls* for Information Systems and Organizations. **NIST Special Publication 800-53 Revision 5**, set. 2020. Disponível em: https://bit.ly/3mbzH9P. Acesso em: 9 jan. 2021.

PCI Security Standards Council, LLC. **Indústria de cartões de pagamento (PCI) Padrão de Segurança de Dados** – Requisitos e procedimentos da avaliação de segurança – Versão 3.2.1, maio de 2018. Disponível em: https://bit.ly/2QXgtcv. Acesso em: 16 jan. 2021.

TELECOMMUNICATIONS Industry Association, **TIA. TIA-942 Certification**. Disponível em: https://bit.ly/31xLN3y. Acesso em: 12 fev. 2021.