NÃO PODE FALTAR

FUNDAMENTOS DE AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

O QUE É UMA AUDITORIA DE SISTEMAS?

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.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

CONVITE AO ESTUDO

Olá, aluno! Nesta unidade avançaremos pela auditoria de sistemas e de segurança da informação, que tem um papel importante para a efetiva proteção das informações da empresa.

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.

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, incluindo funcionários, clientes, fornecedores, parceiros de negócios e investidores. 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.

Já a análise dos controles das empresas pode ser feita com base em diferentes normas, padrões e frameworks, tais como o *Control Objectives for Information and related Technology* (COBIT) ou *Information Technology Infrastructure Library* (ITIL). Controles de segurança como os relacionados à aquisição, desenvolvimento e manutenção de software ou o controle de acesso podem ser baseados em normas e padrões como a NBR ISO/IEC 27002 ou o NIST 800-53, que definem controles de diferentes tipos, como os administrativos, técnicos e operacionais. Os controles também podem ser classificados como físico, técnico ou lógico e processual.

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.

Bons estudos!

PRATICAR PARA APRENDER

Olá, nesta seção, você conhecerá o papel do auditor de sistemas e de segurança, que é importante para que a empresa esteja de fato protegida contra os riscos existentes. Você já viu que é a partir dos riscos identificados, analisados e avaliados que os controles de segurança são identificados para serem implantados. Este tratamento dos riscos com os controles de segurança pode resultar em riscos residuais, além daqueles que foram aceitos ou que não foram identificados. Como é possível verificar que a empresa está segura? É preciso analisar se os controles são suficientes para o contexto da empresa, se eles foram implantados de uma forma correta e se estão funcionando de forma adequada.

Este é o papel da auditoria que será discutido nesta aula. 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.

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.

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. 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.

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.

Boa aula!

CONCEITO-CHAVE

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.

INTRODUÇÃO À AUDITORIA E AUDITORIA DE SISTEMAS: CONCEITOS E PRINCÍPIOS

Com a evolução constante do ambiente das empresas, junto do dinamismo dos objetivos de negócios, a auditoria é cada vez mais importante. De uma forma geral, 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. 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). Os objetivos da auditoria podem ser vistos na Figura 4.1.

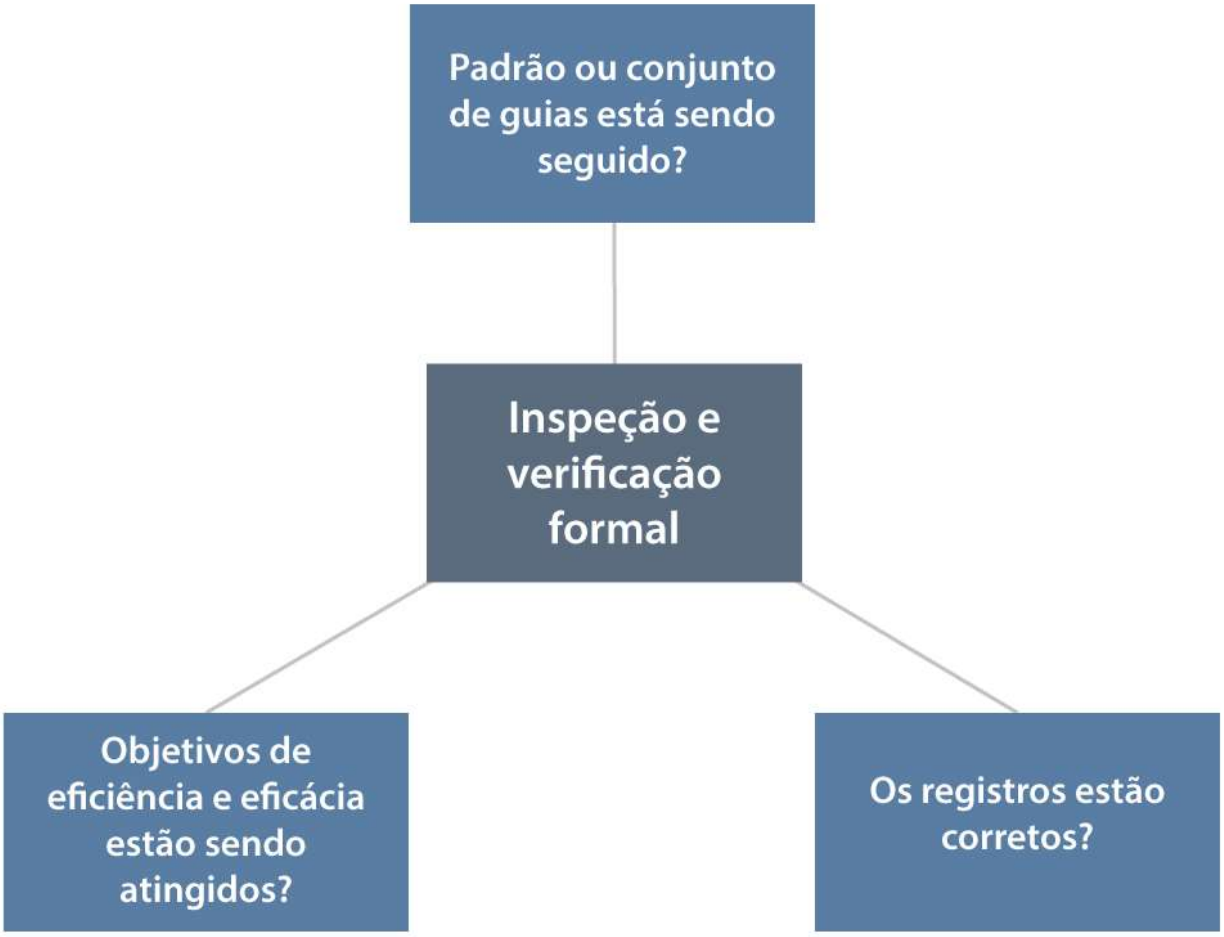
Figura 4.1 | Objetivos da auditoria

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

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).

Segundo a *Information Systems Audit and Control Association* (ISACA), que foca em sistemas de informação, a auditoria (Figura 4.2) 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).

Figura 4.2 | O que é uma auditoria de sistemas



Fonte: adaptada de ISACA (2016).

A auditoria de sistemas de informação tem foco na informação e nos sistemas relacionados, os quais têm importância cada vez maior, principalmente com a transformação digital. 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.

ASSIMILE

A auditoria de sistemas visa garantir que os controles de TI sejam adequados, tanto na definição quanto na implantação, de modo que os objetivos da empresa estejam sendo alcançados de uma forma eficiente e eficaz.

Algumas suposições críticas de auditoria de sistemas são (ISACA, 2020):

- O escopo da auditoria é identificável e sujeito à auditoria.
- Há grande probabilidade de sucesso da auditoria ser concluída.
- A abordagem e a metodologia não são enviesadas.
- O projeto de auditoria tem escopo suficiente para os objetivos da auditoria de sistemas.
- O projeto de auditoria irá gerar um relatório objetivo e que não levará a entendimentos dúbios do leitor.

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).

> **EXEMPLIFICANDO**
>
> Os principais desafios para as organizações, principalmente em um cenário como o de uma pandemia, são a segurança cibernética, privacidade, dados e resiliência, segundo uma pesquisa feita em 2020. Estes assuntos ganharam importância com a transformação digital e ainda mais com o trabalho remoto e os novos processos de negócios, os quais exigem avaliações de riscos mais estruturadas, com mais frequência, em resposta ao novo contexto. Soma-se a isso a maior conectividade e a Internet das Coisas (*Internet of Things*, IoT), que cresce ainda mais com o advento do 5G. A maturidade digital gera vantagens de negócios e tem acelerado a transformação digital, que exige mais segurança, privacidade e resiliência (ISACA, 2020).

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. 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.

> **REFLITA**
>
> Para as empresas, qual a melhor forma de priorizar investimentos? A gestão de riscos avalia as oportunidades e ameaças, e as ações podem assim ser definidas. No contexto da segurança da informação, os riscos com níveis mais altos, que são produto do cálculo da probabilidade e do impacto, levando em consideração os ativos, vulnerabilidades, agentes de ameaça, ameaças e controles existentes, são naturalmente priorizados. O tratamento dos riscos com a definição e implementação dos controles de segurança, além da proteção, elevam a confiança com os diferentes atores envolvidos, incluindo clientes, público, investidores e a própria gestão interna. A auditoria dá a força e visibilidade sobre a eficácia e efetividade da proteção.

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):

- 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.
- Responder para uma área organizacional que seja livre de influências indevidas.
- Ser objetivo nos assuntos de auditoria.
- Seguir padrões de auditoria e de indústria, além de leis e regulações aplicáveis que levarão a uma opinião ou conclusão profissional.
- Definir um escopo claro e sem limitações, o escopo deve levar a conclusões.
- Deixar clara as obrigações e responsabilidades para que sejam providas informações apropriadas, relevantes e no tempo correto.
- Ter diligência e cuidados profissionais de acordo com código de ética, incluindo a conduta e o caráter, a privacidade e a confidencialidade, e o uso das informações obtidas para fins particulares.
- Ter a competência profissional para executar as atividades requeridas.
- Ter conhecimento adequado sobre o assunto em auditoria.
- Manter a competência profissional com educação e treinamento contínuo.
- Revisar as informações obtidas de modo que elas sejam suficientes, válidas e relevantes.
- Selecionar critérios de auditoria objetivos, completos, relevantes, confiáveis, mensuráveis, entendíveis, reconhecidos amplamente, que tenham autoridade e sejam entendidos por todos os envolvidos.

- Considerar a aceitação de critérios reconhecidos, oficiais e disponíveis publicamente.

A efetividade da auditoria depende, em grande parte, da qualidade do programa de auditoria, que será visto a seguir. E as capacidades necessárias para o auditor desenvolver um bom programa de auditoria são (ISACA, 2016):

- Bom entendimento da natureza da empresa e de sua indústria, para identificar e categorizar os tipos de riscos e ameaças.
- Bom entendimento sobre TI e seus componentes, incluindo o conhecimento sobre as tecnologias que afetam o ambiente.
- Entendimento do relacionamento entre riscos de negócios e riscos de TI.
- Conhecimento básico das práticas de avaliação de riscos.
- Entendimento de diferentes procedimentos de testes para avaliar controles de sistemas de informação e identificar o melhor método para a avaliação.

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).

AS FASES DO PROCESSO DE AUDITORIA DE SISTEMA DE INFORMAÇÃO

O **planejamento** da auditoria é essencial para o sucesso, e o escopo e objetivo da auditoria devem estar claros, entendidos e aceitos pelo auditor e pelo auditado. Uma vez que o propósito da auditoria é definido, o plano de auditoria (Figura 4.3) pode ser criado, englobando o escopo acordado, os objetivos e os procedimentos necessários para a obtenção de evidências que sejam relevantes, confiáveis e suficientes para construir e suportar as conclusões e opiniões da auditoria (ISACA, 2016).

Um componente importante do plano de auditoria é o programa de auditoria, também conhecido como programa de trabalho. O programa de auditoria é composto por procedimentos e passos específicos que serão utilizados para testar e verificar a efetividade dos controles. A qualidade do programa de auditoria possui um impacto significativo na consistência e na qualidade dos resultados da auditoria, de modo que os auditores devem entender como desenvolver programas de auditoria completos e abrangentes (ISACA, 2016).

4

Ver anotações

Figura 4.3 | Plano de auditoria e programa de auditoria

Fonte: adaptada de ISACA (2016).

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 os atores envolvidos (ISACA, 2016). As principais fases da auditoria são o planejamento, trabalho em campo e relatórios (Figura 4.4). A fase de planejamento da auditoria tem como resultado o programa de auditoria.

Figura 4.4 | Principais fases de um processo de auditoria e os passos

Fonte: adaptada de ISACA (2016).

PLANEJAMENTO

O **objeto** da auditoria pode ser um sistema, uma localidade ou uma unidade de negócio. Um exemplo de **objetivo** da auditoria é determinar se as mudanças no código-fonte de um sistema crítico ocorrem em um ambiente bem definido e controlado. O **escopo** da auditoria, neste exemplo, é o sistema que é composto por diferentes componentes que precisam passar por uma avaliação completa. É o escopo que direciona o auditor a definir o conjunto de testes relevantes para a auditoria, junto de qualificações técnicas e recursos necessários para avaliar diferentes tecnologias e seus componentes.

Na execução do **planejamento de pré-auditoria**, a condução de uma avaliação de riscos ajuda na justificativa das atividades e no refinamento do escopo. Além disso, uma entrevista ajuda no entendimento das atividades e áreas que devem ser incluídas no escopo de trabalho, junto da identificação dos requisitos regulatórios de conformidade. Os recursos necessários podem assim ser definidos, incluindo o orçamento necessário para o trabalho, as localidades ou plantas a serem auditadas, as regras e responsabilidades da equipe de auditoria, o tempo determinado para cada estágio da auditoria, as fontes de informação para os testes ou revisões (fluxos, políticas, padrões, procedimentos, documentações), os pontos de contato para necessidades administrativas e logísticas e o plano de comunicação da auditoria.

O planejamento da auditoria é finalizado com a definição dos **procedimentos**, que envolvem a identificação da documentação (políticas, padrões e guias), dos requisitos de conformidade regulatória, da lista de indivíduos para as entrevistas e dos métodos e ferramentas para a avaliação. Além disso, há o desenvolvimento de ferramentas e metodologia para testar e verificar controles. As ferramentas da auditoria podem ser tão simples quanto questionários ou tão complexas quanto scripts que buscam informações em sistemas e devem incluir os critérios para as avaliações. O planejamento inclui também a metodologia para avaliar a acurácia dos testes e resultados.

TRABALHO EM CAMPO

Após o planejamento da auditoria, a execução dos passos definidos com o uso dos recursos é feita na fase de trabalho em campo. Esta fase inclui **obtenção dos dados**, **testes dos controles**, **realização das descobertas** e **validações** e a **documentação dos resultados**.

RELATÓRIOS

A fase de relatórios representa a entrega da auditoria, com a elaboração, revisão, entrega e acompanhamento dos resultados.

Um exemplo de auditoria tem os seguintes passos (ISACA, 2016):

- Revisão de documentação.
- Entrevista com indivíduos-chave.
- Estabelecimento de critérios de auditoria.
- Condução de visitas ao data center.
- Condução de revisão de áreas de alto risco.
- Documentação dos resultados.
- Preparação do relatório e revisão pelos atores.
- Entrega do relatório final.

ASSIMILE

É importante que informações técnicas e operacionais sejam identificadas, utilizadas e façam parte da auditoria. Por exemplo: se o escopo da auditoria inclui uma nova tecnologia de autenticação, o auditor deve entendê-la para identificar os riscos, os controles internos e os procedimentos de testes.

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.

EXEMPLIFICANDO

Exemplos de ferramentas de auditoria são: questionários, *scripts*, banco de dados relacionais, planilhas eletrônicas, ferramentas de auditoria específicas (*Computer-Assisted Audit Tools*, CAATs) e metodologias para coleta de transações (ISACA, 2016).

SAIBA MAIS

Os riscos e os controles devem ser identificados e documentados pelo auditor. A avaliação de riscos é necessária para a auditoria e determina prioridades para a alocação de recursos da auditoria. Algumas informações

a serem consideradas:

- Propósito de negócio da auditoria.
- Ambiente em que a empresa opera.
- Resultados de auditorias anteriores.
- Regulações e legislação para conformidade.
- Riscos tecnológicos específicos.

O escopo da auditoria e a estratégia de execução são resultado da avaliação dos objetivos da auditoria, dos riscos identificados e dos controles existentes.

PESQUISE MAIS

O livro de Beneton (2017) *Auditoria e controle de acesso* é uma importante referência sobre auditoria e o capítulo 1 traz conteúdo sobre a auditoria, certificações profissionais de auditores, requisitos e critérios de avaliação, além de *frameworks* e processos de auditoria NBR ISO 19001 e ABNT NBR ISO/IEC 27007.

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

Chegamos, assim, ao final do entendimento sobre os principais conceitos, necessidades e atividades envolvidos com o processo de auditoria de sistemas e de segurança. O conhecimento amplo e detalhado que o auditor tem sobre a segurança e privacidade é fator crítico para uma auditoria, que exige o uso de diferentes técnicas e ferramentas para a análise dos controles. Avançaremos sobre estes pontos nas próximas aulas. Até lá!

FAÇA VALER A PENA

Questão 1

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.

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.

Correto!

Todas as afirmativas são verdadeiras para os objetivos da auditoria: validar atividades, processos e sistemas; avaliar a eficiência e eficácia dos controles; atestar a conformidade administrativa, regulatória e legal; e assegurar a estabilidade organizacional para a alta gestão e os diferentes atores.

4

Ver anotações

Questão 2

Em segurança da informação, um risco é a probabilidade de um agente de ameaça explorar vulnerabilidade de um ativo, fazendo com que uma ameaça se torne um incidente de segurança, o que leva a impactos para a empresa. É entendendo o que é e quais são os riscos que existem na empresa que os controles podem ser definidos e implantados.

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.

Assinale a alternativa que apresenta qual é a relação entre os riscos de segurança da informação e a auditoria de sistemas e de segurança.

a. Auditoria é feita para validar somente os riscos.

b. Auditoria é feita para implantar os controles.

c. Auditoria é feita para validar os riscos e os controles.

Correto!

A auditoria de sistemas e de segurança avalia a eficiência e eficácia dos controles, que são definidos a partir de uma visão de riscos. Assim, a auditoria valida os riscos para que nenhum controle tenha deixado de ser implantado, e

os controles devem ter sido implantados de uma forma adequada.

d. Riscos indicam a necessidade de auditoria.

e. Se riscos são avaliados, auditoria não é necessária.

4

Ver anotações

Questão 3

As principais fases de uma auditoria são o planejamento, o trabalho em campo e os relatórios. Considere as atividades listadas a seguir:

I. Define o objetivo da auditoria.

II. Determina os procedimentos.

III. Testa controles.

IV. Realiza descoberta e validação.

V. Documenta resultados.

VI. Elabora relatórios.

Sobre as atividades que fazem parte da fase de trabalho em campo, é correto o que se afirma em:

a. I e II, apenas.

b. III, IV e V, apenas.

Correto!

Dentre as atividades citadas, fazem parte do planejamento: I. Define o objetivo da auditoria e II. Determina os procedimentos. Fazem parte do trabalho em campo: III. Testa controles, IV. Realiza descoberta e validação e V. Documenta resultados. Faz parte dos relatórios: VI. Elabora relatórios.

c. I, II e V, apenas.

d. I, II, V e VI, apenas.

e. I, II, III, IV, V e VI.

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.

AXELOS. **Building IT and Digital Excellence with ITIL 4**. Disponível em: https://bit.ly/31ub9PU. Acesso em: 10 jan. 2021.

BENETON, E. **Auditoria e controle de acesso**. São Paulo: Editora Senac, 2017. Disponível em: https://bit.ly/3rBgWxy. Acesso em: 13 jan. 2021.

ISACA, Information Systems Audit and Control Association. **COBIT 2019 Framework**. Introduction and Methodology. 2018. Disponível em: https://bit.ly/31uXeJr. 2018. 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/3dnOWbw. 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/3rx5Cm1. 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/3sVDgUl. Acesso em: 9 jan. 2021.

ISACA, Information Systems Audit and Control Association. **IT Audit Framework (ITAF™).** A Professional Practices Framework IT Audit. 4th Edition. Disponível em: https://bit.ly/2Poo17z. Acesso em: 4 jan. 2021.

ISACA, Information Systems Audit and Control Association. Protiviti. **IT Audit's Perspectives on the Top Technology Risks for 2021**. 2020. Disponível em: https://bit.ly/3u8Ag6Y. Acesso em: 4 jan. 2021.

ITIL Process Map & ITIL Wiki. **ITIL 4**. 3 dez. 2019 Disponível em: https://bit.ly/39pu3vt. Acesso em: 10 jan. 2021.

ITIL Process Map & ITIL Wiki. **IT Service Continuity Management**. 24 jul. 2020. Disponível em: https://bit.ly/3sBsSkp. Acesso em: 10 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/3wm4xBa. 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/39uqMLr. Acesso em: 9 jan. 2021.