Capítulo 4

Diretrizes para auditoria de sistemas

Neste capítulo apresentaremos as regras fundamentais das diretrizes para auditoria de sistemas, conforme estabelece a norma ISO/IEC 27007. Ao longo deste capítulo, enfatizamos a importância da auditoria de sistemas de informação e como ela pode garantir que todas as rotinas e processamentos da área de TI estejam em conformidade com o compliance da organização.

Outro detalhe importante é sobre a visão macro de como esta auditoria deve ser realizada e quais os responsáveis pelo seu desenvolvimento.

1 ISO/IEC 27007 – Diretrizes para auditoria de sistemas de gestão da segurança da informação

A última edição da publicação da norma ISO/IEC 27007 pela ABNT é datada de 11 de maio de 2021. Trata-se de um documento que orienta os responsáveis a como gerenciar um programa de auditoria de sistemas de gestão da informação (SGSI), além de auxiliar na execução e habilidade dos auditores em realizar o trabalho.

O conjunto de normas conhecido como ISO 27000, apresentado na figura 1, foi criado para dar suporte às empresas de diferentes tamanhos e áreas de atuação a fim de definir e implementar uma abordagem consistente e sistemática de proteção das informações.

Figura 1 – Normas ISO 27000 e as respectivas áreas de atuação

Fonte: adaptado de Aguilera-Fernandes (2017).

2 Escopo da norma

Segundo a ABNT (2021), a norma ISO/IEC 27007 tem como objetivo fornecer orientações sobre a segurança cibernética e proteção da privacidade de informações, criar diretrizes para auditoria de sistemas de gestão, orientar sobre o gerenciamento de um programa de auditoria de sistemas de gestão da informação (SGSI), como executar essas auditorias e quais as competências que devem possuir os auditores de SGSI, em complemento às orientações descritas na NBR ISO 19011.

3 Termos e definições da norma 27007

A norma ABNT NBR ISO/IEC 19011:2018 fornece orientação sobre a auditoria de sistemas de gestão, incluindo os princípios de auditoria, a gestão de um programa de auditoria e a condução de auditoria de sistemas de gestão, como também orientação sobre a avaliação de competência de pessoas envolvidas no processo de auditoria. Essas atividades incluem as pessoas que gerenciam o programa de auditoria, os auditores e a equipe de auditoria (BRASIL, 2021).

A norma aponta os riscos que podem acometer os negócios, formas de operar, monitorar, revisar e manter a segurança de toda a informação existente na empresa.

O planejamento de um processo de auditoria, conforme explicitado pela ISO 27007, evidencia fatores importantes que as empresas devem seguir para obterem melhores resultados e realizarem um processo de auditoria justo.

Sabe-se que é necessário considerar a realização de auditorias recorrentes para prevenção, análise da complexidade dos sistemas, da confidencialidade, integridade, disponibilidade das informações, além do risco do negócio. É importante verificar os requisitos legais, contratuais

e de confiabilidade. Este último é fundamental para evitar problemas graves com os envolvidos com a auditoria.

Para tanto, deve-se estabelecer um cronograma de auditoria que possibilite aos auditores uma análise crítica e eficaz, avaliar processos e determinar a abrangência da conformidade dos controles de segurança da informação, além de ponderar os riscos no sistema.

O responsável pela realização da auditoria deve prezar por questões como políticas de segurança, procedimentos adotados, definição de um controle frente aos riscos, utilizando métodos confiáveis e eficientes.

A norma recomenda que o processo de auditoria ocorra de forma legal e que, para ser bem-sucedida, seja capaz de entregar às partes envolvidas soluções que possam ajudar dentro do negócio.

PARA SABER MAIS

Para aprofundar os conhecimentos neste tema, confira o livro *Auditoria e controle de acessos*, de Emerson Beneton (2017).

4 Princípios de auditoria

Um processo de auditoria tem a função de atestar conformidades e não conformidades de processos de uma organização. Na gestão da informação, a auditoria atua com o objetivo de identificar o uso da informação, com análise de evidências e de documentos, atrelado aos objetivos empresariais.

Um processo de auditoria caracteriza-se por alguns princípios, como:

- É uma ferramenta confiável e eficaz para apoiar as políticas de gestão e controle da empresa.

- Tem alto caráter ético.
- Apresenta as informações encontradas de forma justa, reportando com veracidade e exatidão.
- Profissionalismo com toda a destreza necessária.
- Independência, para garantir a imparcialidade.
- Abordagem baseada em evidências, com amostragens de informações claras.

A figura 2 apresenta exemplos de composição de um sistema de gestão de segurança na informação, destacando as auditorias.

Figura 2 – Sistema de gestão de segurança da informação

Fonte: adaptado de Aguilera-Fernandes (2017).

5 Gerenciamento de auditoria

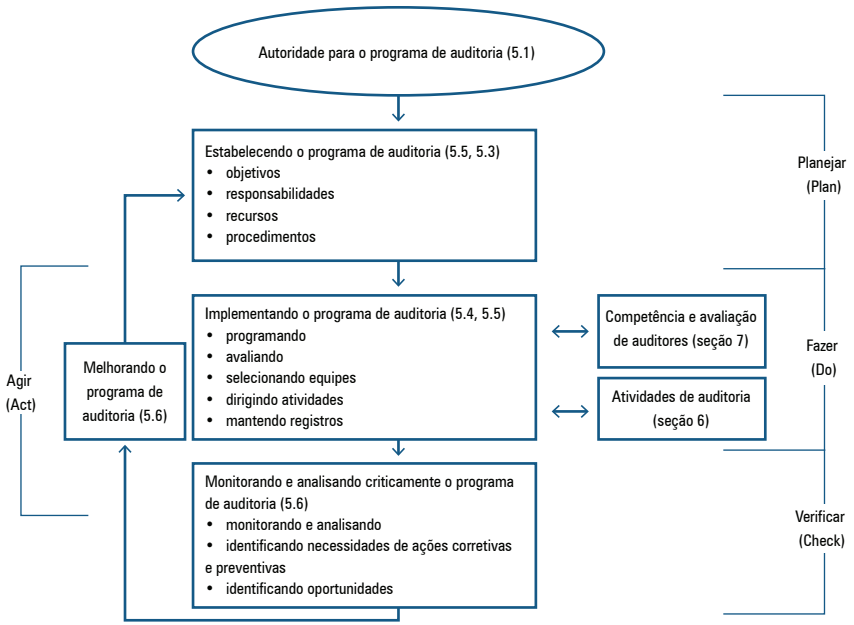
Para gerenciar a auditoria é necessária a execução de um plano de auditoria de sistemas da informação da empresa, prevendo um cronograma de atividades. Assim, as evidências obtidas são confrontadas com os resultados esperados.

De acordo com Teixeira (2013), o responsável pela auditoria gerencia a equipe e os processos envolvidos para a geração de resultados. Sendo assim, seu trabalho engloba: o planejamento, o qual estabelece planos para análise de riscos e informações coletadas; comunicação e aprovação, necessárias para que o projeto seja aceito e suas limitações evidenciadas; gerenciamento de recursos, mostrando que os recursos são adequados, suficientes e efetivos para o processo de auditoria; políticas e procedimentos estabelecidos com a finalidade de orientar todo o trabalho que será executado; coordenação, na qual o responsável compartilha informações e coordena atividades; natureza do trabalho, que mostra a importância da auditoria na melhoria de processos de gerenciamento de riscos e controle; e, por fim, o gerenciamento de riscos, no qual a auditoria auxilia a empresa por meio de identificação e avaliação de exposições a riscos de segurança.

É importante destacar que cada fase do processo de auditoria é fundamental, especialmente seu gerenciamento, para que tudo corra dentro do esperado e da lei. A falta de gerenciamento pode ocasionar problemas mais graves, como perda de informação ou acusações sem fundamento.

A figura 3 a seguir evidencia toda a metodologia envolvida e auxilia na visualização do papel do responsável e dos procedimentos que serão realizados durante o processo, conforme já foi descrito anteriormente.

Figura 3 – Fluxo de um programa de auditoria conforme NBR ISO 19001



Fonte: adaptado de ABNT (2002).

6 Conduzir uma auditoria

Segundo Aguilera-Fernandes (2017), no caso de serem identificadas algumas não conformidades em elementos do SGSI, serão realizadas as devidas correções, sempre em alinhamento com as políticas existentes e as normas e boas práticas adotadas. Também são implementadas alterações nos controles e procedimentos em caso de falha no atendimento dos requisitos de segurança dos ativos de informação da empresa.

Para a realização da auditoria, os responsáveis utilizam ferramentas para identificar e analisar requisitos importantes para segurança de dados. As ferramentas envolvem plano de documentação, análise de requisitos, conceito de rastreabilidade, auditorias manuais e automáticas, ferramentas, evidências, conclusões do auditor e realização do relatório.

O plano de documentação da auditoria envolve quesitos como planejamento, avaliação de riscos, supervisão e controle de qualidade, estudos de controles internos, aplicação de procedimentos e amostragens. Esses são alguns aspectos que fidedignam todo o processo. A fim de que não ocorram impactos e surpresas na instituição, a auditoria deve ser constante e os responsáveis precisam desenvolver uma matriz de risco, a qual identifica e prioriza ações e áreas mais importantes (IMONIANA, 2012).

A análise de requisitos objetiva a coleta de dados relevantes e necessários para que seja realizado o trabalho. Ela estabelece: identificação e avaliação do problema, modelagem, especificação do requisito e revisão entre o autor do projeto e o cliente.

Já a rastreabilidade, refere-se à possibilidade de reconhecer informações relevantes nas etapas do processo de auditoria. Um fato muito importante é a rastreabilidade dos sistemas internos da empresa e externos, pois mostra as necessidades e ajustes necessários. É importante destacar que o rastreamento deve responder às seguintes questões: o que, de onde veio e para onde foi (BENETON, 2017).

As auditorias manuais e automáticas definem a metodologia que será utilizada em determinado processo. As ferramentas que podem auxiliar nas auditorias são: CAATs (computer assisted audit techniques), que possibilitam coletar informações a partir de dados independentes; alguns softwares para extração e análise de dados, como o ACL (Audit Command Language) e IDEA (Interactive Data Extraction).

Após os passos executados, o auditor gera um relatório que é composto por três seções: Findings (descobertas) e Follow-Up (recomendações e acompanhamento) (BENETON, 2017).

Portanto, a auditoria passa por grandes passos como: Planejamento, Preparação, Execução, Encerramento e Follow-up.

7 Competência e avaliação dos auditores

A qualidade da auditoria está intimamente ligada às competências das pessoas que estão envolvidas nesse processo. Entre as características necessárias aos profissionais estão:

- Aspectos pessoais (competências comportamentais): ética, relacionamento interpessoal, capacidade de observação, persistência e autoconfiança. É importante que saiba conduzir a equipe de auditoria, prevenir e solucionar conflitos, liderando todas as situações. Sua boa conduta resulta em bons resultados para a auditoria realizada na empresa. Neutralidade no momento da auditoria faz com que haja uma apresentação justa daquilo que foi pesquisado e seja gerado um relatório condizente com a verdade.

- Confiabilidade: outra questão muito importante é a confiabilidade. O auditor deve ser discreto na realização de suas atividades e cuidar dos resultados encontrados para não gerar problemas jurídicos.

- Competências técnicas: conhecimento dos sistemas de informação, coleta de informações, planejamento sistemático, priorização de tarefas, elaboração de relatórios, entre outros. O auditor deve possuir uma abordagem com base em evidências.

- Nível de formação: o nível de educação profissional deve ser compatível com os exigidos da área de sistemas da informação. Além de habilidades na área de TI (formação em área da tecnologia), os auditores devem ter conhecimento específico da questão que irão auditar, conhecer os princípios de auditoria, procedimentos e métodos, sistema de gestão e documentos de referência, contexto organizacional e conhecimento de requisitos legais do auditado e entendimento da gestão de riscos. É importante também que saibam contabilidade e regras tributárias.

Sendo assim, o trabalho do auditor é muito importante e necessário para que os fatos sejam expostos de forma correta e os resultados sejam satisfatórios.

Considerações finais

Para poder realizar todos os quesitos necessários, a auditoria de sistemas de informação compreende todo o ambiente de uma área de TI, tais como: os equipamentos, o centro de processamento de dados, todos os softwares envolvidos nos processos de entrada e manipulação de informação, controles internos, cópias de segurança e, por fim, a conformidade com os requisitos técnicos e legais envolvidos. É através dessa atividade de controle e monitoramento que a organização caminhará sempre a favor da prevenção, detecção, correção ou recuperação de dados e informações.

As diretrizes para a auditoria de sistemas não é apenas para a segurança da área de TI como um todo: ela também permite que a organização esteja inteiramente em conformidade tanto na órbita técnica como na legal, além de oferecer credibilidade perante os stakeholders.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27007**: 2021. Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 19011**. Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental. Rio de Janeiro: ABNT, 2002.

AGUILERA-FERNANDES, Edson. **Padrões, normas e política de segurança da informação**. São Paulo: Editora Senac São Paulo, 2017. (Série Universitária)

BENETON, Emerson. **Auditoria e controle de acesso**. São Paulo: Editora Senac, 2017. (Série Universitária)

BRASIL. Conselho Nacional de Justiça (CNJ). **Manual de referência** – Prevenção e mitigação de ameaças cibernéticas e confiança digital. 2021. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2021/03/AnexoVManualReferenciaPrevencaoMitigacaoeAmeacasCiberneticasConfiancaigitalRevisadoREV.docx.pdf. Acesso em: 28 maio 2021.

IMONIANA, Joshua Onome. **Auditoria de Sistemas de Informação**. São Paulo: Atlas, 2012.

TEIXEIRA, Francisco. Gerenciamento da atividade de auditoria interna. **Grupo Portal de Auditoria**, [s.l.], 20 dez. 2013. Disponível em: https://auditoriaoperacional.com.br/gerenciamento-da-atividade-de-auditoria-interna/. Acesso em 21 ago. 2021.