Técnicas de Auditoria de Sistemas de Informação

Segurança e Auditoria de Sistemas

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Planejamento e Execução de uma Auditoria de Sistemas de Informação

As **auditorias de sistemas de informação (SI)**, por vezes também chamada de **auditoria de tecnologia da informação (TI)**, possui abordagens considerando a **avaliação dos riscos dos negócios** quanto a asseguração da **veracidade** das transações financeiras, econômicas e contábeis, devendo ser avaliadas sob a luz de **efetividade**. Nesse ínterim, cabe ao profissional, ao auditar as informações em um ambiente de tecnologia, desenhar as abordagens que julgar convenientes e aplicáveis ao contexto.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Planejamento e Execução de uma Auditoria de Sistemas de Informação

É importante enfatizar que a auditoria de SI (ou de TI) é apenas uma **parte** da função total de uma auditoria interna ou externa. A responsabilidade dos profissionais envolvidos com a auditoria de sistemas de informação é **dar suporte à auditoria geral** em aspectos relacionados às **tecnologias envolvidas** no trabalho, fornecendo cobertura de auditoria adequada dos sistemas de informações da empresa. Compete ao gestor do time de auditoria assegurar que o trabalho de auditoria geral e o da auditoria de tecnologia se complementem, articulando-se para fornecer uma cobertura de auditoria adequada para a empresa.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Planejamento e Execução de uma Auditoria de Sistemas de Informação

O **planejamento de uma auditoria de TI** envolve a definição das áreas de envolvimento da auditoria. Estes poderiam ser a revisão de sistemas comerciais da companhia, sistemas e aplicações em desenvolvimento, gerenciamento das instalações de TI, controles de segurança e recuperação, eficiência e eficácia da TI, etc.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Planejamento de uma Auditoria de Sistemas de Informação

O planejamento deve possuir metas de curto e longo prazo. O curto prazo deve levar em consideração questões que serão cobertas durante o ano. Já de longo prazo deve levar em consideração as questões relativas às mudanças na direção estratégica de TI da organização. Importante ressaltar que as questões de longo e curto prazo devem ser revisadas pelo menos anualmente.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Planejamento de uma Auditoria de Sistemas de Informação

Ainda sobre o planejamento, vale trazer algumas considerações:
As avaliações de risco devem ocorrer de forma periódica;

- Fique atento e considere eventuais mudanças na tecnologia;
- Alterar problemas de privacidade, conforme regulamentações aplicáveis;
- Considerar os requisitos regulamentares;
- Observar os prazos de implementação ou atualizações dos sistemas envolvidos;
- Enxergar as tecnologias futuras;
- Lembrar das limitações de recursos de SI.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Obtendo Informações para o Trabalho

O auditor precisa ter uma compreensão do ambiente geral, incluindo também as práticas de negócios e funções relacionadas à auditoria. Além disso, deve-se verificar quais são os tipos de sistemas de informação e tecnologias que suportam a operação do negócio e listar todos os requisitos regulamentares em que o negócio opera.

Os padrões de auditoria da ISACA requerem que o auditor trate dos objetivos da auditoria e cumpra os padrões profissionais de auditoria. O auditor de SI deve ter outro plano que considere os objetivos da organização que sejam relevantes para o que está sendo auditado na infraestrutura de tecnologia. Este plano deve incluir uma compreensão da arquitetura de TI da organização e a direção tecnológica.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Diretrizes Básicas para o Auditor de Sistemas

O auditor de sistemas de informação, no ato de seus trabalhos de campo, deve considerar algumas questões para nortear a condução de seu trabalho. A seguir, são apresentados alguns exemplos não exaustivos:

- Revisar publicações do setor e/ou relatórios anuais emitidos internamente e externamente;
- Revisar relatórios de auditorias anteriores;
- Entender os planos de negócios e de TI a longo prazo;
- Conversar com os gerentes e executores dos processos para visualizar sobre os problemas de negócios;
- Pesquisar as regulações específicas que se aplicam ao negócio;
- Alguma função de TI é terceirizada?
- Percorrer as instalações da organização.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Efeito das Leis e Regulamentos no Planejamento de Auditoria de SI

A maior parte das organizações precisam cumprir requisitos governamentais ou outros requisitos externos relacionados a práticas de sistemas de informação. Isso pode incluir como os dados são processados, transmitidos e armazenados.

Vale ressaltar que uma consideração especial deve ser dada a questões de setores altamente regulamentados. Essas considerações devem incluir todos os países nos quais a organização opera.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Problemas de Privacidade

Os auditores devem levar em conta todos os requisitos das leis e regulamentos de privacidade. Por exemplo: no Brasil, temos a Lei nº 13.709, que é a Lei Geral de Proteção de Dados (LGPD), além do Marco Civil da Internet (Lei n° 12.965). No Canadá, são 28 regulamentações entre leis provinciais e federais, e a legislação nacional referente ao tema é a *Personal Information Protection and Electronic Documents Act (PIPEDA).* Na União Europeia, temos a *General Data Protection Regulation (GDPR),* ou *Regulamento Geral de Proteção de Dados (RGPD).* Nos Estados Unidos não há uma única lei, mas sim, várias legislações específicas para diferentes setores ou vigentes em determinados estados. Entre muitos e muitos outros pelo mundo.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Problemas de Privacidade

Algumas das possíveis regulações a serem considerados podem ser as seguintes:

- Estabelecimento e organização dos requisitos regulamentares;
- Responsabilidades atribuídas à organização;
- Funções financeiras, operacionais e de auditoria de TI.

Podemos considerar duas áreas como principais de preocupação: requisitos legais para os auditores (as leis, regulamentos e acordos contratuais), e os requisitos legais para o auditado (os requisitos para sistemas, gerenciamento de dados, relatórios, etc. Essas duas áreas terão impacto no escopo e nos objetivos da auditoria. Alguns exemplos disso poder citados: SOX (Sarbanes-Oxley) e HIPAA.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Passos para Determinar o Nível de Conformidade da Organização

Os seguintes passos podem ser considerados pelo auditor de sistemas de informação para determinar o nível de conformidade da empresa. Obviamente, não se trata de um “manual” que deve ser seguido, e há muitas outras questões que podem ser consideradas, cabendo ao auditor a avaliação e aplicabilidade.

- Identificar os requisitos que tratam de:
  - Dados eletrônicos, como informações pessoais, direitos autorais etc;
  - Práticas e controles do sistema de informação;
  - Como as informações são armazenadas e como trafegam.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Passos para Determinar o Nível de Conformidade da Organização

- Verificar a existência de documentações das leis, dispositivos legais e regulamentos aplicáveis;
- Determinar se a empresa planejou atender aos requisitos regulatórios;
- Determinar se a empresa abordou a adesão às leis e regulações aplicáveis;
- Determinar se existem procedimentos estabelecidos e disseminados na empresa para seguir esses requisitos.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Exemplo de Escopo para uma Auditoria de Sistemas de Informação (SI)

Como forma de finalizar esse artigo, trago esse exemplo de escopo que, apesar de meramente ilustrativo, poderia muito bem ser enquadrado em uma situação real de inúmeras empresas:

Auditoria da arquitetura de segurança da informação e a implementação da política de segurança cibernética e da informação, com referência específica às seguintes áreas:

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Exemplo de Escopo para uma Auditoria de Sistemas de Informação (SI)

- Estrutura da organização da segurança cibernética e da informação;
- Papeis e responsabilidades;
- Política de classificação de dados;
- Política de segurança da aplicação e sistemas;
- Práticas adotadas no desenvolvimento seguro de software;
- Rotina de verificação periódica e correção de vulnerabilidades;
- Segurança da aplicação do caixa eletrônico (ATM);
- Política de senha;
- Política de controle de malwares;

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Exemplo de Escopo para uma Auditoria de Sistemas de Informação (SI)

- Política de backup;
- Política de rede;
- Política de segurança física
- Política de segurança ambiental;
- Política de gerenciamento de incidentes;
- Continuidade dos negócios e plano de recuperação de desastres;
- Política de uso da Internet;
- Política de uso de e-mail;
- Política de uso de redes sociais.

Segurança e Auditoria de Sistemas

Técnicas de Auditoria de Sistemas de Informação

Exemplo de Escopo para uma Auditoria de Sistemas de Informação (SI)

Auditoria dos sistemas de informação das principais aplicações de tecnologia da informação e recursos da companhia:

Referências

https://tiagosouza.com/planejamento-execucao-auditoria-sistemas-informacao/