FOCO NO MERCADO DE TRABALHO

FUNDAMENTOS DE AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

FASES DO PROCESSO DE AUDITORIA

As principais fases do processo de auditoria são o planejamento, trabalho em campo e relatórios.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

Você trabalha para um provedor de nuvem em franca expansão, que tem demandas diretas de seus clientes. Eles exigem cada vez mais segurança e precisam estar em conformidade legal e regulatória, o que significa que só se tornarão clientes caso o próprio provedor esteja em conformidade com as melhores práticas de segurança e tecnologia da informação. O planejamento, assim, precisa incluir um elemento que aumente a confiança dos potenciais clientes, os quais precisam de um provedor seguro para operar seus sistemas e dados.

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.
- **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

- **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.

- **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. 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.

AVANÇANDO NA PRÁTICA

CONTRATANDO UM PROVEDOR DE NUVEM DEPOIS DE UMA AUDITORIA

Você é o dono de uma fábrica de peças que está sendo automatizada e que se conecta diretamente com sistemas de fornecedores e clientes. Você está procurando um provedor de nuvem e busca um alto nível de segurança. Para validar o provedor de nuvem, você irá conduzir uma auditoria em busca de 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.

Quais são as atividades que você pode seguir para fazer esta auditoria, com escopo nos controles físicos, relacionados à proteção do ambiente quanto a desastres naturais, controle de acesso e riscos de incêndio e enchentes?

RESOLUÇÃO

Uma auditoria tem como fases gerais o planejamento, o trabalho em campo e os relatórios. Para esta auditoria, serão feitas as seguintes atividades:

- 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.