FOCO NO MERCADO DE TRABALHO

CONTROLES GERAIS DE AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

O QUE O AUDITOR PRECISA SABER PARA IMPLANTAÇÃO DE CONTROLES?

O auditor precisa ter conhecimentos e competência técnica para verificar os controles. É preciso conhecer as principais normas e *frameworks* utilizados para a definição de controles.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

Você já montou um planejamento para melhorar a segurança do provedor de nuvem e agora irá detalhar o planejamento, com foco nos controles. Os principais tópicos que você pode considerar na elaboração do material são:

- **Tipos de controles considerados e para que servem:** controles são salvaguardas ou contramedidas aplicadas em sistemas ou organizações para proteger a confidencialidade, integridade e disponibilidade dos sistemas e suas informações e para gerenciar os riscos de segurança, e também para assegurar conformidade com requisitos aplicáveis. Os controles podem ser (i) técnicos, tecnológicos ou lógicos, como o antivírus ou o *backup*; (ii) processuais, administrativos ou operacionais, como a política de segurança ou o processo de revisão de contas de usuários; (iii) físicos, como o cadeado para que o *desktop* utilizado pelo presidente da empresa não seja roubado.
- **Como os controles são definidos:** os controles são definidos pelos riscos existentes na empresa, que direcionam as necessidades com base na probabilidade das ameaças se tornarem incidentes de segurança e os impactos envolvidos. Além dos riscos, a definição dos controles pode ser feita a partir de requisitos que direcionam a seleção e implementação de controles, e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades da empresa.
- **Normas ou *frameworks* que podem ser a base para a definição dos controles:** a ABNT NBR ISO/IEC 27002 define um conjunto de objetivos de controle de segurança da informação, e pode ser utilizada para a definição dos controles. COBIT é um *framework* para governança de TI e possui um conjunto de controles mais amplos que podem ser implantados, incluindo os de segurança e privacidade. Já o ITIL é um conjunto de melhores práticas para o

gerenciamento de serviços e estabelece também um conjunto de controles mais amplos que inclui aspectos de segurança.

- **Controles para aquisição, desenvolvimento e manutenção de sistemas:** os controles para este assunto devem incluir os requisitos de segurança de sistemas de informação, para garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. É necessário ainda que controles de segurança sejam definidos em processos de desenvolvimento e de suporte, para garantir que a segurança da informação esteja projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação. Os controles de segurança devem ainda abordar os dados para teste, principalmente nos aspectos de privacidade, que devem ser reforçados devido à Lei Geral de Proteção de Dados Pessoais (LGPD).

- **Controle de acesso:** o controle de acesso deve ser tratado pelos requisitos do negócio para controle de acesso, com a política de controle de acesso e o acesso às redes e aos serviços de rede. O gerenciamento de acesso do usuário deve incluir aspectos como o registro e cancelamento de usuário, provisionamento para acesso de usuário, gerenciamento da informação de autenticação secreta de usuários e análise crítica dos direitos de acesso de usuário. O controle para as responsabilidades dos usuários deve envolver o uso da informação de autenticação secreta. O controle de acesso ao sistema e à aplicação deve envolver a restrição de acesso à informação, procedimentos seguros de entrada no sistema (*log-on*), uso de programas utilitários privilegiados e controle de acesso ao código-fonte de programas.

- **Auditoria:** a auditoria visa garantir que os controles sejam adequados, tanto na definição quanto na implantação, de modo que os objetivos da empresa estejam sendo alcançados de uma forma eficiente e eficaz. Assim, a auditoria de sistemas é essencial para a

efetiva proteção da empresa, ao analisar a eficiência e eficácia dos controles definidos e implementados.

AVANÇANDO NA PRÁTICA

SEGURANÇA É MAIS DO QUE PROTEÇÃO

Você deve definir os controles a serem implantados em sua empresa, mas não deve se restringir à proteção. Considere os processos de segurança: identificação, proteção, detecção, resposta e recuperação. Cite alguns exemplos de controles que podem ser utilizados para cada um destes processos de segurança, que serão depois auditados.

RESOLUÇÃO

Os controles para cada um dos processos de segurança que podem ser implantados na empresa são:

- **Identificação:** gestão de ativos, análise do ambiente de negócio, governança, avaliação de riscos, estratégia de gestão de riscos, gestão de riscos de cadeia de fornecedor.
- **Proteção:** gestão de identidades e controle de acesso, conscientização e treinamento, segurança de dados, processos e procedimentos de proteção de informação, manutenção, tecnologia de proteção.
- **Detecção:** anomalias e eventos, monitoramento contínuo de segurança, processos de detecção.
- **Resposta:** planejamento de resposta, comunicação, análise, mitigação, melhorias.
- **Recuperação:** planejamento de recuperação, melhorias, comunicação.