1.Diretivas gerenciais para a segurança da informação

1.1 Políticas para a segurança da informação

Ao estabelecer uma política para a segurança da informação, a administração provê as diretivas e o apoio para a organização. Essa política deve ser escrita em conformidade com os requisitos do negócio, bem como com as leis e os regulamentos relevantes. A política de segurança da informação deve ser aprovada pelo conselho de administração e publicada para todo o seu pessoal e todos os parceiros externos relevantes, tais como clientes e fornecedores. Na prática, ela é distribuída normalmente como uma versão resumida, delineando os principais pontos. Deve haver algum programa de conscientização bem balanceado para alcançar todos os funcionários. É comum um documento de políticas ter uma estrutura hierárquica. Vários documentos de políticas são desenvolvidos, tendo como base uma política de segurança corporativa de alto nível. Eles devem estar sempre em conformidade com a política corporativa e prover diretrizes mais detalhadas para uma área específica.

Os seguintes itens podem então ser escritos, com base em documentos de política:

- **Regulamentos:** Um regulamento é mais detalhado que um documento de política. Regulamentos são normalmente considerados obrigatórios e a sua não observância pode levar a procedimentos disciplinares.
- **Procedimentos:** Eles descrevem em detalhes como medidas particulares devem ser conduzidas e podem, por vezes, incluir instruções de trabalho, como uma política de mesa limpa. Visando assegurar que materiais sensíveis não sejam facilmente removidos, é necessário a política de mesas limpas.
- **Diretrizes:** Como o próprio termo sugere, fornecer orientações. Elas descrevem quais aspectos têm de ser examinados em função de determinados pontos de vista de segurança. As Diretrizes não são obrigatórias, mas são de caráter consultivo.
- **Normas:** As normas podem compreender a configuração padrão de certas plataformas. Um exemplo importante é a norma ISO/IEC 27001:2013. Trata-se de uma norma para estabelecer a segurança da informação na organização. A parte 1 descreve sistemas de gestão (ISMS); a parte 2, a qual também é chamada de Código de prática para controles de segurança da informação, desenvolve esse sistema de gestão por meio de diretivas práticas. Uma organização pode ser certificada com a ISO/IEC 27001:2013 e, consequentemente, mostrar aos seus fornecedores e clientes que atende aos requisitos de qualidade de segurança da informação. O código de prática para controles de segurança da informação é aplicável a todas as organizações, pequenas ou grandes, governo ou empresas.

1.2 Revisão das políticas de segurança da informação

A ISO/IEC 27002:2013 estabelece que as políticas de segurança da informação devem ser revisadas em intervalos planejados ou se ocorrerem mudanças significativas, a fim de assegurar sua contínua conformidade, adequação e eficácia. Cada política deve ter um encarregado, que tenha responsabilidade gerencial aprovada para o desenvolvimento, a revisão e a avaliação de políticas. A revisão deve incluir a avaliação de oportunidades de

melhoria de políticas da organização e a abordagem da gestão da segurança da informação em resposta a mudanças no ambiente organizacional, nas circunstâncias de negócio, nas condições legais ou no ambiente técnico. A revisão de políticas para a segurança da informação deve levar em conta os resultados das revisões gerenciais. Deve ser obtida aprovação da gerência para a política revisada.