1.Entendendo a organização e seu contexto

A organização precisa definir as questões externas e internas que são relevantes para o seu propósito e que afetam sua habilidade de alcançar o(s) resultados(s) pretendido(s) do seu sistema de gerência de segurança da informação.

2.Compreendendo as necessidades e expectativas das partes interessadas

Enquanto a ISO 27001:2005 focava internamente, as organizações colaboradoras da ISO percebem que no período entre 2005 e 2013 o mundo havia mudado. Organizações estão mais e mais conectadas. Muitas vezes os sistemas de informação são terceirizados, a informação é compartilhada com outras empresas com quem têm relação ou organismos governamentais. Os requisitos das partes interessadas podem incluir requisitos legais e regulatórios e obrigações contratuais. A organização deve, portanto, definir: as partes interessadas que são relevantes para o sistema de gerenciamento de segurança da informação; os requisitos relevantes dessas partes interessadas para a segurança da informação.

3.Definindo o escopo do Sistema de Gerenciamento de Segurança da Informação (SGSI)

A organização deve definir os limites e a aplicabilidade do sistema de gerenciamento de segurança da informação, a fim de estabelecer seu escopo. Ao definir o seu escopo, a organização deve considerar as questões internas e externas, conforme previamente descrito, as interfaces e dependências entre as atividades desempenhadas pela organização, bem como aquelas desempenhadas por outras organizações e que são aplicáveis ao escopo da organização. O escopo deve estar disponível como informação documentada.