**ISO 27000 – séries**

Para que o controle seja eficaz é necessário que os usuários declarem formalmente que conhecem seus direitos e obrigações em relação aos acessos. Se não for assim, um usuário pode agir de má fé e dizer apenas que não sabia.

Na fase de planejamento, os objetivos de segurança devem ser: elaborados considerando os tratamentos de riscos. **Planejamento da Segurança**  
  
***Durante a fase do planejamento de segurança, o gestor de segurança deve estudar e entender os requisitos da ISO 27001***. Nessa fase, também é definido o SGSI que deve ser apresentado à direção e a todos os envolvidos com os negócios da empresa (incluindo clientes, fornecedores e colaboradores).  
  
Também é feito o desenvolvimento do SGSI, que define os participantes do comitê do SGSI. Também é desenvolvido quais serão os objetivos, responsabilidades e limites de atuação do SGSI.  
  
**Essa fase é importante, pois busca manter o projeto em conformidade com os fatores legais e contratuais envolvidos nos negócios da empresa, além de estabelecer critérios para avaliação de riscos nos negócios.**

**Incidente de segurança da informação**: Um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

**Evento de segurança da informação**: Uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

A gestão de ativos visa alcançar e manter a proteção adequada dos ativos da organização, sendo que:

o proprietário do ativo deve ser responsável por definir e, periodicamente, analisar criticamente as classificações e restrições ao acesso aos ativos importantes, levando em conta as políticas de controle de acesso aplicáveis.

Segundo o Glossário da NBR ISO 27002:

* **Ativo**: qualquer coisa que tenha valor para a organização.
* **Evento**: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.
* **Controle**: ***forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais***, que podem ser de natureza administrativa, técnica, de gestão ou legal. É também usado como sinônimo para ***proteção ou contramedida***.
* **Recurso de processamento de informação**: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem.
* **Política**: intenções e diretrizes globais formalmente expressas pela direção.

***Segundo a ISO 27002:***

7.2.1 Recomendações para classificação  
  
Controle  
  
Convém que a informação seja classificada em termos do seu **valor, requisitos legais, sensibilidade e criticidade** para a organização.   
  
**\*\*Portanto**, conforme o controle da norma, a informação não é classificada pelo seu tamanho.

Opções de Tratamento do Risco:

* **Transferir o Risco:** transferir o risco para outra entidade
* **Evitar o Risco:** que a atividade ou condição que dá origem ao risco seja evitada.
* **Reduzir o Risco:** reduzir o nível de risco através da seleção de controles.
* **Reter o Risco:**a retenção do risco é realizada com base na avaliação dos riscos.

**Políticas para segurança da informação**  
  
Controle: Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e **comunicado para todos os funcionários e partes externas relevantes.**

O risco de auditoria é uma função dos riscos de distorção relevante e do risco de detecção, a seguir discriminados:

* **Risco de detecção:** é o risco de que os procedimentos executados pelo auditor não detectem uma distorção potencialmente relevante, individualmente ou em conjunto com outras distorções.
* **Risco de distorção relevante:**é o risco de que as demonstrações contábeis contenham distorção relevante antes da auditoria. Consistem em dois componentes, o risco inerente e o risco de controle:
* **Risco inerente:** é a suscetibilidade de uma afirmação a respeito de uma transação, saldo contábil ou divulgação, a uma distorção que possa ser relevante, individualmente ou em conjunto com outras distorções, antes de se considerar qualquer controle preexistente;
* **Risco de controle:** é o risco de que uma distorção não seja prevenida, detectada e corrigida tempestivamente pelo controle interno da entidade.

Na NBR ISO/IEC 27002:2013, que os 3 objetivos de controle da seção **7 Segurança em Recursos Humanos** são justamente:

**7.1 Antes da contratação**

Objetivo: Assegurar que funcionários e partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais eles foram selecionados.

**7.2 Durante a contratação**

Objetivo: Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.

**7.3 Encerramento e mudança da contratação**

Objetivo: Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

Vale observar que esses objetivos de controles (assim como seus controles) estão presentes tanto na NBR ISO/IEC 27002:2007 como NBR ISO/IEC 27002:2013.

O padrão AES utiliza apenas**blocos de 128 bits** e **chaves de 128, 192 e 256 bits**.

**ISO 27002 Seção 8 – Segurança em recursos humanos**

Antes de realizar a contratação de um funcionário – ou mesmo de fornecedores – é importante que ele seja devidamente analisado, principalmente se for lidar com informações de caráter sigiloso. A intenção desta seção é mitigar o risco de roubo, fraude ou mau uso dos recursos. E quando o funcionário estiver trabalhando na empresa, ele deverá estar ciente das ameaças relativas à segurança da informação, bem como de suas responsabilidades e obrigações.

Segundo a ISO 27001,"4.3.1 Geral

**A documentação do SGSI deve incluir:**

* declarações documentadas da política (ver 4.2.1b)) e objetivos do SGSI;
* **o escopo do SGSI** (ver 4.2.1a));
* **procedimentos e controles que apoiam o SGSI;    ( LETRA A )**
* uma descrição da metodologia de análise/avaliação de riscos (ver 4.2.1c));
* **o relatório de análise/avaliação de riscos**(ver 4.2.1c) a 4.2.1g));
* **o plano de tratamento de riscos** (ver 4.2.2b));
* procedimentos documentados requeridos pela organização para assegurar o planejamento efetivo, a operação e o controle de seus processos de segurança de informação e para descrever como medir a eficácia dos controles (ver 4.2.3c));
* registros requeridos por esta Norma (ver 4.3.3); e
* a Declaração de Aplicabilidade.

Segundo a ISO 27002,

**15 Conformidade**

15.1 Conformidade com requisitos legais

**Objetivo: Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.**

15.1.1 Identificação da legislação vigente

Controle

**Convém que todos os requisitos estatutários, regulamentares e contratuais relevantes**, e o enfoque da organização para atender a esses requisitos, sejam explicitamente definidos, documentados e mantidos atualizados para cada sistema de informação da organização.