GESTÃO DE SEGURANÇA DA INFORMAÇÃO

GESTÃO DE SEGURANÇA DA INFORMAÇÃO SEGUNDO A NBR ISO/IEC 27001

Olá!

Nesta aula, você irá:

Conhecer a norma que trata da implementação da Gestão de Segurança da Informação - NBR ISO/IEC 27001

1. Objetivo.

2. Abordagem de processo de gestão do SGSI.

3. Aplicação da norma.

4. Sistema de gestão de segurança da informação (SGSI).

5. Responsabilidades da direção.

6. Auditorias internas do SGSI.

7. Análise crítica do SGSI pela direção.

8. Melhoria do SGSI

Objetivo

Diferentemente da norma NBR ISO/IEC 27002 que estabelece as melhores práticas em segurança da informação, a norma NBR ISO/IEC 27001 tem como objetivo especificar os requisitos necessários para o estabelecimento, implementação, operação, monitoração, análise critica, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação (SGSI) dentro do contexto dos riscos de negócio da organização.

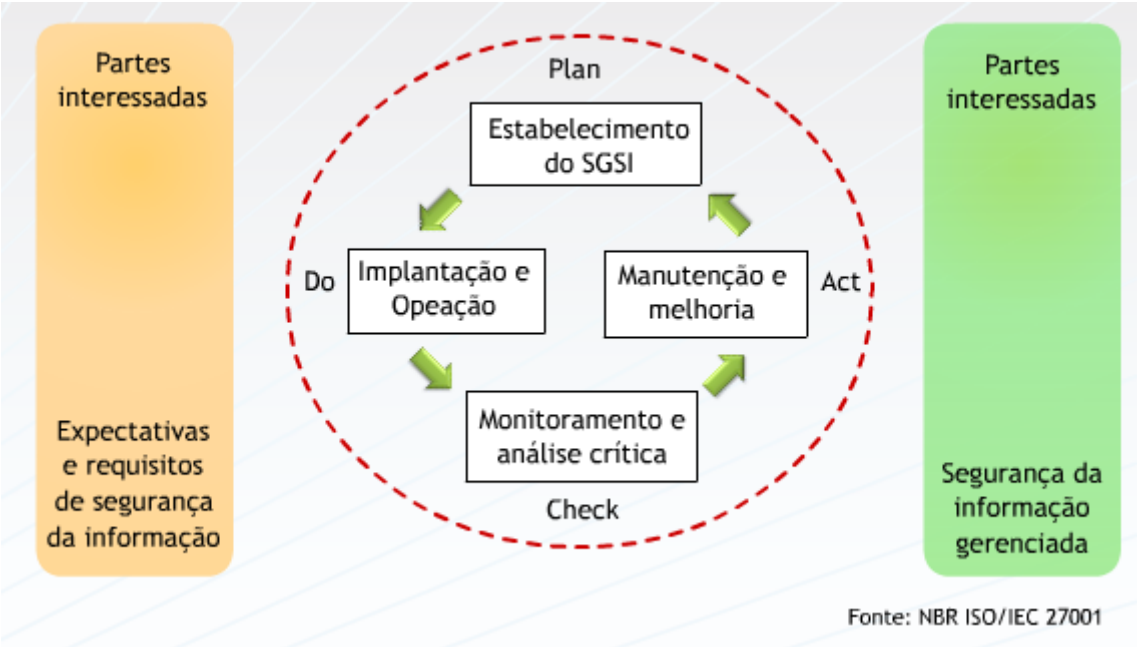
Fique ligado

A adoção de um Sistema de Gestão de Segurança de Informação (SGSI) deve ser uma decisão estratégica para as organizações.

Abordagem de processo de gestão do SGSI

A proposta de integração dos dispositivos de proteção de maneira organizada, contemplando um ciclo de revisões periódicas e melhoria contínua, dimensionadas de acordo com as necessidades de segurança da informação estabelecidas para o negócio da organização, está prevista na norma ISO/IEC 27001:2005, a primeira a abordar segurança da informação com uma visão sistémica de gestão e não somente como

recomendações de instalação de controles de segurança isolados. A norma adota uma abordagem de processo para o estabelecimento e relacionamento com o SGSI, ou seja, a aplicação de um sistema de processos, a identificação e iterações destes processos, e a sua gestão e utiliza como modelo o Plan-Do-Check-Act (PDCA), aplicado para estruturar todos os processos do SGSI.



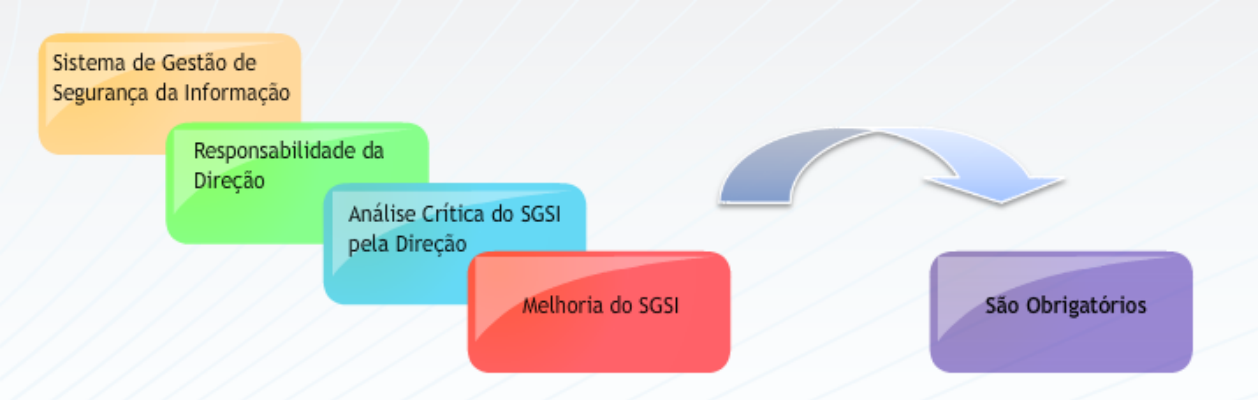
Fonte: NBR ISO/IEC 27001

A abordagem de processo utilizada nesta norma fará com que a organização enfatize a importância de:

- Entendimento dos requisitos de segurança da informação e a necessidade de estabelecer uma política e objetivos para a segurança da informação.
- Implementação e operação de controles para gerenciar os riscos de segurança da informação no contexto dos risco globais da organização.
- Monitoração e análise critica do desempenho da eficácia do SGSI.
- Melhoria continua baseada em medições objetivas.

Aplicação da norma

Independente do tamanho, da natureza e do tipo da organização, os requisitos definidos pela norma são genéricos e podem ser aplicados a todas as organizações. Caso a organização queira estar em conformidade com a norma os itens, deverá implementar os seguintes itens obrigatórios:



Fique ligado

A norma NBR ISSO/IEC 27001 orienta que caso a organização já possua um sistema de gestão de processo de negócio em operação baseado na NBR ISSO/IEC 9001 ou NBR ISSO/IEC 14001, é preferível satisfazer os requisitos da norma 27001 dentro dos sistemas já existentes.

Sistema de gestão de segurança da informação (SGSI)

Para estabelecer um Sistema de gestão de segurança da informação documentado, baseado no modelo PDCA, e dentro do contexto das atividades de negócio da organização e dos riscos que ela enfrenta, a organização deve:

- **Plan (estabelecer o SGSI)**

  Para estabelecer o SGSI a organização deve definir:

  - O escopo do SGSI alinhado com as características de negócio, da organização, sua localização, ativos e tecnologia;
  - A política do SGSI;
  - A abordagem de análise/avaliação de risco da organização;
  - Identificar os riscos;
  - Analisar e avaliar os riscos;
  - Identificar e avaliar as opções para o tratamento de riscos;
  - Selecionar objetivos de controle e controles para o tratamento de riscos;
  - Obter aprovação da direção dos riscos residuais propostos;
  - Obter autorização da direção para implementar e operar o SGSI;
  - Preparar uma declaração de Aplicabilidade;

Declaração de Aplicabilidade: Documento exigido pela NBR ISO/IEC 27001 no qual a empresa tem que relacionar quais controles são aplicáveis e justificar os que não são aplicáveis ao seu SGSI.

Controles: São pontos específicos que definem o que deve ser feito para assegurar aquele item;

- **Do (implementar e operar o SGSI)**

  Nesta fase a organização deve implementar e operar a política, controles, processos e procedimentos do SGSI, buscando não burocratizar o funcionamento das áreas . Deve formular e implementar um plano de tratamento de riscos para identificar a ação de gestão apropriada, implementar um plano de conscientização e treinamento e gerenciar as ações e os recursos do SGSI.

- **Check (monitorar e analisar criticamente o SGSI)**

  A organização deve implementar procedimentos de monitoração e análise critica para detectar erros nos resultados de processamento, identificar as tentativas e violações de segurança bem-sucedida, e os incidente de segurança da informação. Os procedimentos de análise críticas da eficácia do SGSI, devem levar em consideração os resultados das auditorias de segurança, dos incidentes de segurança, dos resultados das medições e sugestões. Deve ser realizado também a análise crítica das análises/avaliações de risco a intervalos regulares e ainda realizadas auditorias regularmente. Em função dos resultados das atividades de monitoramento e análise crítica os planos de segurança devem ser atualizados.

- **Act (manter e melhorar o SGSI)**

  A organização deve implementar as melhorias identificadas no SGSI. Deve ainda executar as ações preventivas e corretivas necessárias para o bom funcionamento do SGSI.

Responsabilidades da Direção

A organização deve demonstrar o comprometimento da Direção em todos processos envolvidos para o estabelecimento, manutenção, avaliação e melhorias do SGSI. O comprometimento da Direção é evidenciado através:

- Da implementação da politica do SGSI;
- Da garantia que são estabelecidos os planos e objetivos do SGS1;
- Do estabelecimento de papéis e responsabilidades pela segurança da informação;
- Na garantia de todo o pessoal que tem responsabilidades atribuidas no SGSI, receba o treinamento adequado e seja competente para desempenhar as tarefas requeridas;
- Da comunicação à organização da importância da Implementação da segurança da informação na organização;
- Na garantia de recursos para a implementação e manutenção do SGSI;
- No estabelecimento de critérios para a aceitação de riscos; Na garantia de que as auditorias serão realizadas;
- Na condução das análise criticas do SGSI;

Auditorias internas do SCSI

A organização deve realizar auditorias internas do SGSI em intervalos regulares para determinar se os objetivos de controle, controles, processos e procedimentos atendem aos requisitos da norma NBR ISO/IEC 27001 e à legislação ou regulamentações pertinentes;

A organização deve implementar um programa de auditoria levando em consideração a importância dos processos e áreas as serem auditadas, bem como as auditorias anteriores. Devem ser implementados os critérios da auditoria, tais como: escopo, frequência e métodos de auditoria.

Você sabe o que é uma auditoria?

" Um exame sistemático e independente para determinar se as atividades e seus resultados estão de acordo com as disposições planejadas, se estas foram implementadas com a eficácia e se são adequadas à consecução dos objetivos."

Fique ligado

Uma boa fonte de consulta para a compreensão do processo de auditoria é a norma NBR 150 19011 - Diretrizes para auditoria de sistema de gestão da qualidade e/ou ambiental.

Análise critica do SCSI pela direção

A organização deve analisar criticamente seu SGSI em intervalos planejados para assegurar a sua continua pertinência, adequação, eficácia, oportunidade de melhoria ou necessidade de mudanças. Para a realização desta análise critica a organização deve ser considerar:

Entrada/insumo

- os resultados das auditoria anteriores e análises criticas;
- vulnerabilidades ou ameaças não contempladas adequadamente nas análise/avaliações de risco anteriores;

- as situações das ações preventivas ou corretivas;
- realimentação das partes interessadas;
- a avaliação das ações preventivas e corretivas;
- A realimentação por parte dos envolvidos no SGSI.
- As recomendações para a melhoria

Saída

- Melhoria da eficácia do SGSI;
- Atualização da análise/avaliação de riscos e do plano de tratamento de risco;
- Modificação de procedimentos e controles que afetem a segurança da informação.
- Necessidade de recursos;
- Melhoria no processo de medição da eficácia dos controles;

Melhoria do SGSI

A organização deve executar ações para melhorar continuamente a eficácia do SGSI. Estas ações ocorrem através: do uso da política de segurança, dos objetivos de segurança, resultados de auditorias, da análise dos eventos monitorados e através de ações corretivas ou preventivas.

Ações corretivas	Devem ser executadas ações para eliminar as causas da não-conformidade com os requisitos do SGSI de forma a evitar a sua repetição, neste sentido é necessário identificar as não conformidades e determinar suas causas. Avaliar a necessidade de implementar ações para assegurar que não se repitam, ou seja, implementar e analisar criticamente as ações corretivas documentando os resultados.
Ações preventivas	Neste caso devem ser estabelecidas ações para eliminar as causas de não-conformidades potenciais com os requisitos do SGSI, de forma a evitar a sua ocorrência. Desta forma é necessário a identificação das não-conformidades potenciais e suas causas. Avaliar a necessidade de implementar ações preventivas para assegurar que não ocorram, ou seja, implementar e analisar criticamente as ações preventivas documentado os resultados.

Certificação

A série ISO 27000 está de acordo com outros padrões de sistemas de gerência ISO, como ISO 9001 (sistemas de gerência da qualidade) e ISO 14001 (sistemas de gerência ambiental), ambos em acordo com suas estruturas gerais e de natureza a combinar as melhores práticas com padrões de certificação. Certificações de organizações que implementaram a NBR ISO/IEC 27001 é um meio de garantir que a organização certificada implementou um sistema para gerência da segurança da informação de acordo com os padrões.

Como ocorre o processo de certificação? A certificação ISO/IEC 27001 envolve um processo de auditoria em dois etapas:

1) Auditoria da Documentação: Revisão da existência e completude de documentações e informações do SGSI.

2) Auditoria de certificação: auditoria envolvendo a existência e efetividade do controle de segurança do SGSI, bem como a documentação de suporte.

Muitas vezes pode ocorrer também uma fase de pré-auditoria. A renovação do certificado envolve auditoria periódicas confirmando que o SGSI continua operando como desejado.

Saiba mais

Para visualizar a lista com todas os países e o número de certificações, acesse a página, e dique na oção "Certicate Register": www.iso27001certificates.com

O que vem na próxima aula

Tema: Gestão da Conformidade do Negócio Segundo a NBR ISO/IEC 15999

•Objetivo e escopo

•Termos e definições

•Visão geral da gestão da continuidade de negócios (GCN)

•Elementos do ciclo de vida da gestão da continuidade de negócios

CONCLUSÃO

Nesta aula, você:

- Conheceu o objetivo e a aplicação da norma NBR ISO/IEC 27001 e a sua abordagem do processo de gestão do SGSI.
- Estudou as recomendações para a implementação de um Sistema de gestão de segurança da informação (SGSI).
- Compreendeu o conceito da Responsabilidades da direção dentro do contexto de um SGSI; a importância das Auditorias internas, da análise crítica e melhoria do SGSI.