Unidade 1- ISO/IEC-27001

Segurança da Informação

ABNT NBR ISO/IEC 27001:2013

Tecnologia da informação

Técnicas de segurança – Sistemas de Gestão da Segurança da Informação Requisitos

Segurança da Informação

Escopo

Esta norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação (SGSI) dentro do contexto da organização.

Segurança da Informação

Sistemas de Gestão de Segurança da Informação – (SGSI)

A organização deve estabelecer, implementar, manter e continuamente melhorar um sistema de gestão da segurança da informação (SGSI).

Determinando o escopo do SGSI (1/2)

Deve-se considerar:

- as questões internas e externas que são relevantes para o seu propósito;

Segurança da Informação

- os requisitos das partes interessadas, incluindo os legais e regulamentares, bem como as obrigações contratuais;

- as interfaces e dependências entre as atividades desempenhadas pela organização e aquelas desempenhadas por outras organizações; (2/2)

Liderança (1/5)

Liderança e Comprometimento

A alta direção deve demonstrar sua liderança e comprometimento em relação ao SGSI pelos seguintes meios:

Segurança da Informação

Liderança (2/5)

- assegurando que a política de segurança e os objetivos de segurança da informação estejam estabelecidos e que são compatíveis com a direção estratégica da organização;

Segurança da Informação

Liderança (3/5)

- garantindo a integração dos requisitos do SGSI dentro dos processos da organização;

- assegurando que os recursos necessários para o SGSI estejam disponíveis;

Segurança da Informação

Liderança (4/5)

- comunicando a importância de uma gestão eficaz de segurança da informação e da conformidade com os requisitos do SGSI;

- assegurando que o SGSI alcance os seus resultados pretendidos;

Segurança da Informação

- orientando e apoiando pessoas que contribuam para a eficácia do SGSI;

- promovendo a melhoria continua;

- apoiando outros papéis relevantes da gestão para demonstrar como sua liderança aplica às áreas sob sua coordenação; (5/5)

Política (1/3)

A alta direção deve estabelecer uma política da informação que:

- seja apropriada ao propósito da organização;

- inclua os objetivos de segurança da info;

Política (2/3)

- inclua o comprometimento em satisfazer os requisitos aplicáveis, relacionados com a segurança da informação;

- inclua o comprometimento com a melhoria contínua do SGSI;

Segurança da Informação

A política da informação deve: (3/3)

- estar disponível como informação documentada;

- ser comunicada dentro da organização;

- estar disponível para as partes interessadas, conforme apropriado;

Segurança da Informação

Autoridades, responsabilidades e papeis organizacionais

A alta direção deve atribuir responsabilidade e autoridade aos papeis relevantes para:

Segurança da Informação

- assegurar que o SGSI está em conformidade com as normas e regras;

- relatar sobre o desempenho do SGSI para a mesma;

Segurança da Informação

Planejamento

Quando do planejamento do SGSI, a organização deve considerar as questões internas e externas que são relevantes, os requisitos das partes interessadas e determinar os riscos e oportunidades que precisam ser consideradas.

Segurança da Informação

Objetivos da Segurança da Informação e planejamento para alcança-los (1/2)

Os objetivos devem:

- ser consistentes com a política de segurança da informação;

- ser mensuráveis (quando aplicável);

Segurança da Informação

(2/2)

- levar em conta os requisitos aplicáveis e os resultados da avaliação e tratamento dos riscos;

- ser comunicados;

- ser atualizados;

Segurança da Informação

Para o planejamento, a organização deve determinar:

- o que será feito; - quem será responsável;

- quais recursos serão necessários;

- quando estará concluído;

- como os resultados serão avaliados;

Apoio ao SGSI (1/4) - Recursos

- a organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão da segurança da informação;

Apoio ao SGSI (2/4) - Competência

- a organização deve determinar a competência necessária das pessoas envolvidas com a segurança da informação;

- assegurar que essas pessoas são competentes, com base na educação, treinamento ou experiência adquirida;

Apoio ao SGSI (3/4) - Conscientização

As pessoas que realizam trabalhos na organização devem estar cientes da:

- política de segurança;

- suas contribuições para a eficácia do SGSI;

- implicações com as não conformidades com os requisitos do SGSI;

Apoio ao SGSI (4/4) - Comunicação

A organização deve determinar as comunicações internas e externas relevantes para o SGSI incluindo:

Segurança da Informação

- o que comunicar;

- quando comunicar;

- quem comunicar;

- quem será comunicado; e

- o processo pelo qual a comunicação será realizada;

Operação (1/3)

Planejamento operacional e controle (1/2)

- a organização deve planejar, implementar e controlar os processos necessários para atender aos requisitos de segurança da informação e implementar as ações previstas;

Planejamento operacional e controle (2/2)

- deve assegurar também, que os processos terceirizados estão determinados e são controlados;

Operação (2/3)

Avaliação de riscos de segurança da infor.

- a organização deve realizar avaliações de riscos de segurança da informação em intervalos planejados, ou quando mudanças significativas forem propostas ou ocorrerem;

Operação (3/3)

Tratamento de riscos de segurança da informação

- a organização deve implementar o plano de tratamento de riscos de segurança da informação;

Avaliação de Desempenho (1/3)

Monitoramento, medição, análise e avaliação (1/2)

- a organização deve avaliar o desempenho da segurança da informação e a eficácia do sistema de gestão de segurança da informação;

Segurança da Informação

(2/2)

Para tal deve determinar:

- o que precisa ser monitorado e medido;

- os métodos para monitoramento, medição, análise e avaliação;

Avaliação de Desempenho (2/3)

Auditoria Interna

- a organização deve conduzir auditorias internas em intervalos planejados para prover informações sobre o quanto o SGSI está em conformidade e o quanto está efetivamente implementado e mantido;

Avaliação de Desempenho (3/3)

Análise crítica pela Direção

- A alta direção deve analisar criticamente o SGSI em intervalos planejados, para assegurar a contínua adequação, pertinência e eficácia.

Melhoria (1/2)

Não conformidade e ação corretiva

Quando uma não conformidade ocorre, a organização deve:

Segurança da Informação

- reagir a não conformidade;

- avaliar a necessidade de ações para eliminar as causas de não conformidade para evitar a repetição da mesma;

- implementar quaisquer ações necessárias, analisar criticamente as mesmas e realizar as mudanças quando necessário;

Melhoria (2/2)

Melhoria Contínua

A organização deve continuamente melhorar a pertinência, adequação e eficácia do sistema de gestão da segurança da informação – SGSI.