Gestão de Segurança da Informação

NORMAS NBR ISO/IEC 27001, 27002 e 27005

@thiagofagury
www.fagury.com.br
http://groups.yahoo.com/group/timasters

As Normas

- NBR ISO/IEC 27001 - Requisitos para implantar um SGSI
- NBR ISO/IEC 27002 - Práticas para a gestão de SI
- NBR ISO/IEC 27005 - Gestão de riscos de SI
- 27004 e 27003 - Gestão de SI (Medição) e Guia de Impl. SGSI
- 27006 e 27007 - Requisitos e Diretrizes para auditoria de um SGSI

NBR ISO/IEC 27001
Estrutura

0. Introdução

1. Objetivo

2. Referência normativa

3. Termos e definições

4. Sistema de gestão de segurança da informação

(Requisitos gerais / Estabelecendo e gerenciando o SGSI / Requisitos de documentação)

5. Responsabilidades da direção

(Comprometimento da direção / Gestão de recursos)

6. Auditorias internas do SGSI

7. Análise crítica do SGSI pela direção

(Geral / Entradas para a análise crítica / Saídas da Análise Crítica)

8. Melhoria do SGSI

(Melhoria contínua / Ação corretiva / Ação preventiva)

NBR ISO/IEC 27001
Estrutura

Anexos:

Anexo A - normativo:
Objetivos de Controles e Controles (27002 - 5 a 15)

Anexo B - informativo:
Princípios da OECD*

Anexo C - informativo:
Correspondência c/ ISO 9001 e ISO 14001

**Organização para cooperação e desenvolvimento econômico*

NBR ISO/IEC 27001

0. Introdução

Esta Norma foi preparada para prover um modelo para EIOMAMM um Sistema de Gestão de Segurança da Informação (SGSI).

EIOMAMM = estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar

NBR ISO/IEC 27001

0. Introdução

- A adoção de um SGSI é estratégica;

- Necessidades e objetivos, requisitos de segurança, processos empregados, tamanho e estrutura da organização direcionam a implementação;

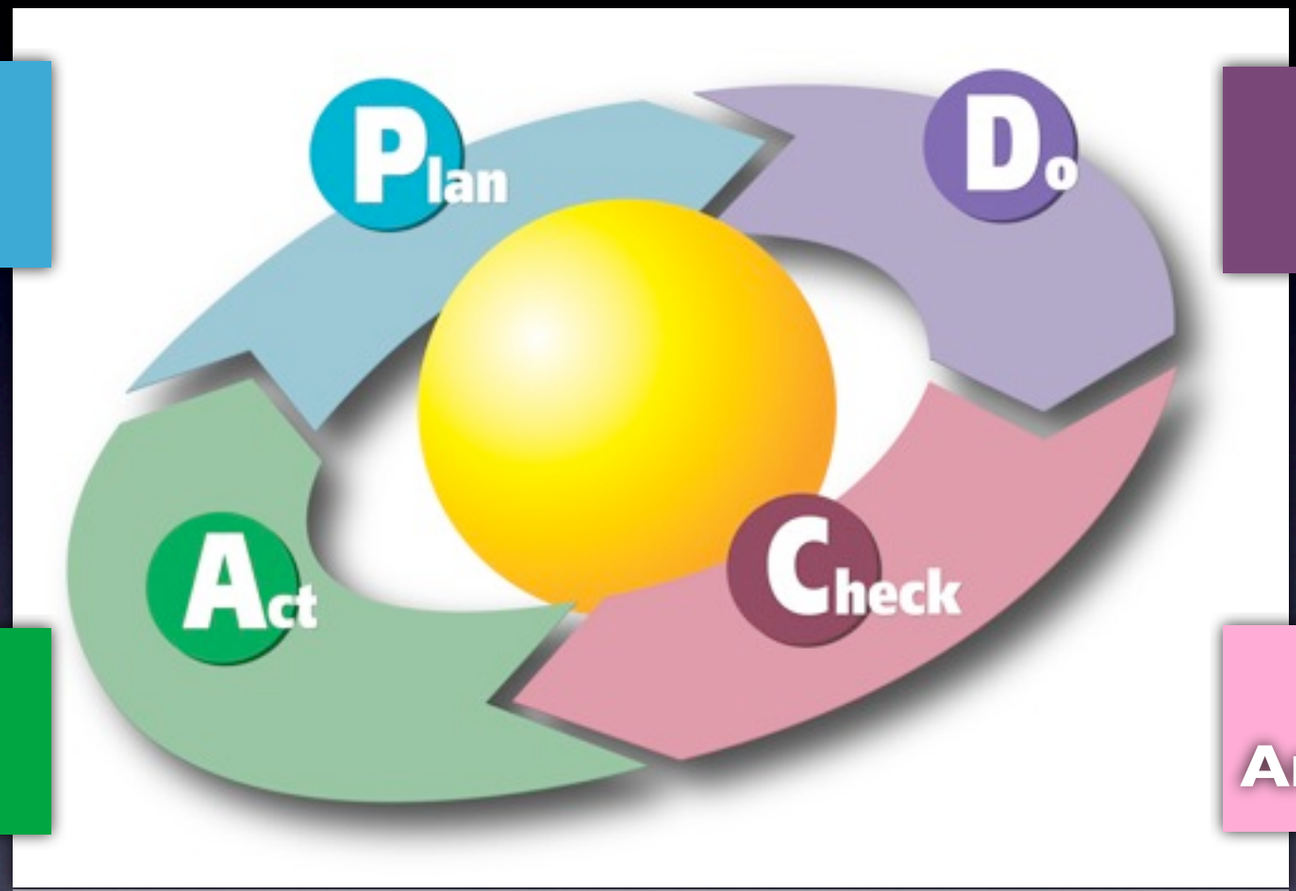
- SGSIs mudam ao longo do tempo;

- Norma pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas.

- Para fins de certificação a 27001 é a referência (antiga BS7799-2).

NBR ISO/IEC 27001
0. Introdução

Estabelecer



Implementar e Operar

Manter e Melhorar

Monitorar e Anal. Criticamente

- Abordagem de processo: indica processos definidos, geridos e interativos;

- Baseada no ciclo PDCA.

NBR ISO/IEC 27001
0. Introdução

Plan (planejar) - estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
Do (fazer) - implementar e operar a política, controles, processos e procedimentos do SGSI.
Check (checar) - avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresent. os resultados p/ a análise crítica pela direção.
Act (agir) - Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

NBR ISO/IEC 27001
0. Introdução

Conformidade:

- Esta Norma está alinhada às ABNT NBR ISO 9001:2000 e ABNT NBR ISO 14001:2004* para apoiar a implementação e a operação de forma consistente e integrada com normas de gestão relacionadas.

**Tratam do Sistema de Gestão da Qualidade e Sistema de Gestão Ambiental*

NBR ISO/IEC 27001

1. Objetivo

1.1 Geral:

- A norma cobre todos os tipos de organizações;
- Especifica os requisitos para EIOMAMM um SGSI documentado dentro do contexto dos riscos de negócio globais da organização;
- Projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas.

NBR ISO/IEC 27001
1. Objetivo

1.2 Aplicação:

- Os requisitos definidos são genéricos e aplicáveis a todas as organizações, independentemente de tipo, tamanho e natureza;

- A exclusão de quaisquer dos requisitos em 4, 5, 6, 7, e 8 não é aceitável quando uma organização reivindica conformidade com a norma;

- Exclusão de controle considerado necessário aos critérios de aceitação de riscos precisa ser justificada e evidências de que os riscos associados foram aceitos pelas pessoas responsáveis precisam ser fornecidas;

- A menos que tais exclusões não afetem a capacidade da organização, e/ou responsabilidade de prover segurança da informação que atenda os requisitos de segurança determinados pela análise/avaliação de riscos e por requisitos legais e regulamentares aplicáveis.

NBR ISO/IEC 27001

2. Ref. Normativa

O documento a seguir referenciado é indispensável para a aplicação desta Norma:

ABNT NBR ISO/IEC 17799:2005, Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.

**Ou seja, a 27002*

NBR ISO/IEC 27001

3. Termos e Definições

3.1 ativo

Qualquer coisa que tenha valor para a organização
[ISO/IEC 13335-1:2004]

3.2 disponibilidade

Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada
[ISO/IEC 13335-1:2004]

3.3 confidencialidade

Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados
[ISO/IEC 13335-1:2004]

NBR ISO/IEC 27001
3. Termos e Definições

3.4 segurança da informação

Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas

[ABNT NBR ISO/IEC 17799:2005]

3.5 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

[ISO/IEC TR 18044:2004]

NBR ISO/IEC 27001
3. Termos e Definições

3.6 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

[ISO/IEC TR 18044:2004]

3.7 sistema de gestão da segurança da informação SGSI

A parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação

NOTA O sistema de gestão inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.

NBR ISO/IEC 27001
3. Termos e Definições

3.8 integridade

Propriedade de salvaguarda da exatidão e completeza de ativos

[ISO/IEC 13335-1:2004]

3.9 risco residual

Risco remanescente após o tratamento de riscos

[ABNT ISO/IEC Guia 73:2005]

3.10 aceitação do risco

Decisão de aceitar um risco

[ABNT ISO/IEC Guia 73:2005]

NBR ISO/IEC 27001
3. Termos e Definições

3.11 análise de riscos

Uso sistemático de informações para identificar fontes e estimar o risco

[ABNT ISO/IEC Guia 73:2005]

3.12 análise/avaliação de riscos

Processo completo de análise e avaliação de riscos

[ABNT ISO/IEC Guia 73:2005]

3.13 avaliação de riscos

Processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco

[ABNT ISO/IEC Guia 73:2005]

NBR ISO/IEC 27001
3. Termos e Definições

3.14 gestão de riscos

Atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos

NOTA A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos.
[ABNT ISO/IEC Guia 73:2005]

3.15 tratamento do risco

Processo de seleção e implementação de medidas para modificar um risco

NOTA Nesta Norma o termo "controle" é usado como um sinônimo para "medida".
[ABNT ISO/IEC Guia 73:2005]

NBR ISO/IEC 27001
3. Termos e Definições

3.16 declaração de aplicabilidade

Declaração documentada que descreve os objetivos de controle e controles que são pertinentes e aplicáveis ao SGSI da organização

NOTA Os objetivos de controle e controles estão baseados nos resultados e conclusões dos processos de análise/avaliação de riscos e tratamento de risco, dos requisitos legais ou regulamentares, obrigações contratuais e os requisitos de negócio da organização para a segurança da informação.

NBR ISO/IEC 27001

4. SGSI

Requisitos gerais

A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta.

NBR ISO/IEC 27001
4. SGSI

Estabelecer o SGSI

A organização deve:

Definir o escopo e os limites do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo

NBR ISO/IEC 27001

4. SGSI

Estabelecer o SGSI

A organização deve:

- Definir a abordagem de análise/avaliação de riscos da organização (metodologia);
- Identificar os riscos (ativos/proprietários);
- Analisar/avaliar riscos (probabilidades e impacto);
- Identificar e avaliar as opções de tratamento;

NBR ISO/IEC 27001
4. SGSI

Estabelecer o SGSI

- Selecionar os objetivos de controle para tratamento de riscos (anexo A);

- Obter aprovação da direção dos riscos residuais propostos;

- Obter autorização da direção para implementar e operar o SGSI;

- Preparar uma Declaração de Aplicabilidade (controles aplicáveis e justificativas de exclusão).

NBR ISO/IEC 27001
4. SGSI

Implementar e Operar o SGSI

A organização deve:

- Formular um plano de tratamento de riscos que identifique a ação de gestão apropriada, recursos, responsabilidades e prioridades para a gestão dos riscos de segurança;
- Implementar o plano de tratamento de riscos para alcançar os objetivos de controle identificados, que inclua considerações de financiamentos e atribuição de papéis e responsabilidades.
- Implementar os controles selecionados para atender aos objetivos de controle.
- Definir como medir a eficácia dos controles selecionados;

NBR ISO/IEC 27001
4. SGSI

Implementar e Operar o SGSI

- Implementar programas de conscientização e treinamento;

- Gerenciar as operações do SGSI;

- Gerenciar os recursos para o SGSI;

- Implementar procedimentos e outros controles capazes de permitir a pronta detecção de eventos de SI e resposta a incidentes de segurança da informação

NBR ISO/IEC 27001
4. SGSI

Monitorar e Analisar Criticamente o SGSI

a) Executar procedimentos de monitoração e análise crítica e outros controles;

b) Realizar análises críticas regulares da eficácia do SGSI (incluindo o atendimento da política e dos objetivos do SGSI, e a análise crítica de controles de segurança), levando em consideração os resultados de auditorias de segurança da informação, incidentes de segurança da informação, resultados da eficácia das medições, sugestões e realimentação de todas as partes interessadas.

c) Medir a eficácia dos controles para verificar que os requisitos de segurança da informação foram atendidos.

NBR ISO/IEC 27001
4. SGSI

Monitorar e Analisar Criticamente o SGSI

d) Analisar criticamente as análises/avaliações de riscos a intervalos planejados e analisar criticamente os riscos residuais e os níveis de riscos aceitáveis identificados;

e) Conduzir auditorias internas do SGSI a intervalos planejados (Seção 6);

NOTA Auditorias internas, às vezes chamadas de auditorias de primeira parte, são conduzidas por ou em nome da própria organização para propósitos internos.

f) Realizar uma análise crítica do SGSI pela direção em bases regulares para assegurar que o escopo permanece adequado e que são identificadas melhorias nos processos do SGSI

NBR ISO/IEC 27001

4. SGSI

Manter e Melhorar o SGSI

a) Implementar as melhorias identificadas no SGSI.

b) Executar as ações preventivas e corretivas apropriadas. Aplicar as lições aprendidas de experiências de segurança da informação de outras organizações e aquelas da própria organização.

c) Comunicar as ações e melhorias a todas as partes interessadas com um nível de detalhe apropriado às circunstâncias e, se relevante, obter a concordância sobre como proceder.

d) Assegurar-se de que as melhorias atinjam os objetivos pretendidos.

NBR ISO/IEC 27001

4. SGSI

Requisitos de Documentação

- A documentação deve incluir registros de decisões da direção, assegurar que as ações sejam rastreáveis às políticas e decisões da direção, e assegurar que os resultados registrados sejam reproduzíveis;

- Deve incluir declarações documentadas da política, escopo, procedimentos e controles que apoiam o SGSI, metodologia e relatório da análise/aval. de riscos, procedimentos documentados para EIOMAMM o SGSI e declaração de aplicabilidade;

- Controle de documentos;

- Controle de registros.

NBR ISO/IEC 27001

5. Responsabilidade da Direção

5.1 Comprometimento da Direção:

A Direção deve fornecer evidência do seu comprometimento com o EIOMAMM do SGSI mediante:

a) o estabelecimento da política do SGSI;

b) a garantia de que são estabelecidos os planos e objetivos do SGSI;

c) o estabelecimento de papéis e responsabilidades pela segurança de informação;

d) a comunicação à organização da importância em atender aos objetivos de segurança da informação e conformidade;

NBR ISO/IEC 27001

5. Responsabilidade da Direção

5.1 Comprometimento da Direção:

e) a provisão de recursos suficientes para EIOMAMM o SGSI;

f) a definição de critérios para aceitação de riscos e dos níveis de riscos aceitáveis;

g) a garantia de que as auditorias internas do SGSI sejam realizadas;

h) a condução de análises críticas do SGSI pela direção.

NBR ISO/IEC 27001

5. Responsabilidade da Direção

5.2 Gestão dos Recursos:

5.2.1 - Provisão de recursos;

5.2.2 - Treinamento, conscientização e competência.

NBR ISO/IEC 27001

6. Auditorias Internas

A organização deve conduzir auditorias internas do SGSI a intervalos planejados para determinar se os objetivos de controle, controles, processos e procedimentos do seu SGSI são executados como esperado, se são eficazes e atendem aos requisitos de conformidade e de SI.

NBR ISO/IEC 27001

7. Análise Crítica pela Direção

A direção deve analisar criticamente o SGSI da organização a intervalos planejados (pelo menos uma vez por ano) para assegurar a sua contínua pertinência, adequação e eficácia.

Entradas:

- resultados de auditorias do SGSI e análises críticas;
- realimentação das partes interessadas;
- situação das ações preventivas e corretivas;
- vulnerabilidades ou ameaças não contempladas ant.;
- resultados da eficácia das medições;
- acompanhamento das ações oriundas de análises críticas anteriores;
- recomendações para melhoria.

NBR ISO/IEC 27001

7. Análise Crítica pela Direção

Saídas:

a) Melhoria da eficácia do SGSI.

b) Atualização da análise/avaliação de riscos e do plano de tratamento de riscos.

c) Modificação de procedimentos e controles que afetem a segurança da informação

d) Necessidade de recursos.

e) Melhoria de como a eficácia dos controles está sendo medida.

NBR ISO/IEC 27001

8. Melhoria do SGSI

Melhoria contínua

A organização deve continuamente melhorar a eficácia do SGSI por meio do uso da política de segurança da informação, objetivos de segurança da informação, resultados de auditorias, análises de eventos monitorados, ações corretivas e preventivas e análise crítica pela direção.

Ações corretivas e preventivas

Identificar não-conformidades; Determinar as causas de não-conformidades; Avaliar a necessidade de ações para assegurar que não haja recorrência; Determinar e implementar as ações necessárias; Registrar os resultados das ações executadas; Analisar Criticamente as Ações.

NBR ISO/IEC 27001
Exercícios e Observações

- Considerações sobre o Anexo A da norma;
- Dúvidas;
- Resolução de questões;
- O que vimos aqui?

NBR ISO/IEC 27002

"O único lugar onde o sucesso vem antes do trabalho é no dicionário" (Einstein)

NBR ISO/IEC 27002
Estrutura

0. INTRODUÇÃO
1. OBJETIVO
2. TERMOS E DEFINIÇÕES
3. ESTRUTURA DA NORMA
4. ANÁLISE/AVALIAÇÃO E TRATAMENTO DE RISCOS
5. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
6. ORGANIZANDO A SEGURANÇA DA INFORMAÇÃO
7. GESTÃO DE ATIVOS
8. SEGURANÇA EM RECURSOS HUMANOS
9. SEGURANÇA FÍSICA E DO AMBIENTE
10. GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES
11. CONTROLE DE ACESSOS
12. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS
13. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO
14. GESTÃO DA CONTINUIDADE DO NEGÓCIO
15. CONFORMIDADE

NBR ISO/IEC 27002
0. Introdução

- A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida.

- A informação pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas.

- Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

NBR ISO/IEC 27002
0. Introdução

- A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

- Estes controles precisam ser EIOMAMM.

- Fontes de requisitos de SI:
  * Análise/Avaliação de Riscos;
  * Legislação e normas vigentes;
  * Princípios e objetivos de negócio.

NBR ISO/IEC 27002
0. Introdução

- Os requisitos de segurança da informação são identificados por meio de uma análise/avaliação sistemática dos riscos de segurança da informação.

- Os gastos com os controles precisam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança da informação.

- Convém que a análise/avaliação de riscos seja repetida periodicamente para contemplar quaisquer mudanças que possam influenciar os resultados desta análise/avaliação.

NBR ISO/IEC 27002

0. Introdução

Seleção de controles:

- Os controles podem ser selecionados a partir desta Norma ou de um outro conjunto de controles ou novos controles podem ser desenvolvidos para atender às necessidades específicas, conforme apropriado;

- A seleção de controles de segurança da informação depende das decisões da organização, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à organização;

- Convém ser observados requisitos de conformidade.

NBR ISO/IEC 27002
0. Introdução

Ponto de partida para a SI:

Os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem, dependendo da legislação aplicável:

a) proteção de dados e privacidade de informações pessoais;
b) proteção de registros organizacionais;
c) direitos de propriedade intelectual.

Os controles considerados práticas para a SI incluem:

a) documento da política de segurança da informação;
b) atribuição de responsabilidades para a SI;
c) conscientização, educação e treinamento em SI;

NBR ISO/IEC 27002
0. Introdução

d) processamento correto nas aplicações;
e) gestão de vulnerabilidades técnicas;
f) gestão da continuidade do negócio;
g) gestão de incidentes de SI e melhorias.

- Esses controles se aplicam para a maioria das organizações e na maioria dos ambientes.

- Apesar deste ser um ponto de partida, é recomendável a seleção de controles com base na análise/avaliação de riscos.

NBR ISO/IEC 27002
0. Introdução

Fatores críticos de sucesso:

a) política de segurança da informação, objetivos e atividades, que reflitam os objetivos do negócio;

b) uma abordagem e uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional;

c) comprometimento e apoio visível dos níveis gerenciais;

d) um bom entendimento dos requisitos de segurança da informação, da análise/avaliação de riscos e da gestão de risco;

NBR ISO/IEC 27002
0. Introdução

e) divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcançar a conscientização;

f) distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas;

g) provisão de recursos financeiros para as atividades da gestão de segurança da informação;

NBR ISO/IEC 27002
0. Introdução

h) provisão de conscientização, treinamento e educação adequados;

i) estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;

j) implementação de um sistema de medição, que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria.

NBR ISO/IEC 27002

1. Objetivo

Esta Norma estabelece diretrizes e princípios gerais para IIManMe a gestão de segurança da informação em uma organização. Os objetivos definidos nesta Norma provêem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação.

IIManMe: iniciar, implementar, manter e melhorar

NBR ISO/IEC 27002

2. Termos e Definições

2.1 ativo

qualquer coisa que tenha valor para a organização
[ISO/IEC 13335-1:2004]

2.2 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
NOTA Controle é também usado como um sinômino para proteção ou contramedida.

2.3 diretriz

descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas
[ISO/IEC 13335-1:2004]

NBR ISO/IEC 27002

2. Termos e Definições

2.4 recursos de processamento da informação

qualquer sistema de processamento da informação, serviço ou infra-estrutura, ou as instalações físicas que os abriguem

2.5 segurança da informação

preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas

NBR ISO/IEC 27002
2. Termos e Definições

2.6 evento de segurança da informação
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
[ISO/IEC TR 18044:2004]

2.7 incidente de segurança da informação
um incidente de segurança da informação é indicado por um simples ou por 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
[ISO/IEC TR 18044:2004]

2.8 política
intenções e diretrizes globais formalmente expressas pela direção

NBR ISO/IEC 27002
2. Termos e Definições

2.9 risco
combinação da probabilidade de um evento e de suas conseqüências
[ABNT ISO/IEC Guia 73:2005]

2.10 análise de riscos
uso sistemático de informações para identificar fontes e estimar o risco
[ABNT ISO/IEC Guia 73:2005]

2.11 análise/avaliação de riscos
processo completo de análise e avaliação de riscos
[ABNT ISO/IEC Guia 73:2005]

2.12 avaliação de riscos
processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a importância do risco
[ABNT ISO/IEC Guia 73:2005]

NBR ISO/IEC 27002
2. Termos e Definições

2.13 gestão de riscos

atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos

NOTA A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos.

[ABNT ISO/IEC Guia 73:2005]

2.14 tratamento do risco

processo de seleção e implementação de medidas para modificar um risco

[ABNT ISO/IEC Guia 73:2005]

2.15 terceira parte

pessoa ou organismo reconhecido como independente das partes envolvidas, no que se refere a um dado assunto

[ABNT ISO/IEC Guia 2:1998]

NBR ISO/IEC 27002

2. Termos e Definições

2.16 ameaça

causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização

[ISO/IEC 13335-1:2004]

2.17 vulnerabildade

fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças

NBR ISO/IEC 27002

3. Estrutura da Norma

- 11 seções de controles de segurança , totalizando 39 categorias principais de segurança e seção preliminar que trata a análise/avaliação e o tratamento de riscos.

- A norma apresenta 39 objetivos de controle (categorias) e 133 controles de segurança.

- A ordem das seções não segue grau de importância , ficando a cargo de cada organização identificar as seções aplicáveis e a relevância de cada uma.

- Cada categoria principal de segurança da informação contém um objetivo de controle que define o que deve ser alcançado; e um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle.

NBR ISO/IEC 27002

3. Estrutura da Norma

Estrutura das Seções

- Objetivo do controle: o que deve ser alcançado;
- Controle: controle a ser implementado para atender o objetivo do controle;
- Diretrizes: informações mais detalhadas para apoiar a implementação do controle;
- Informações adicionais: informações que podem ser consideradas na implementação do controle, tais como aspectos legais e referências a outras normas.

NBR ISO/IEC 27002

4. Anál./Aval. e Tratamento de Riscos

- Convém que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para a organização.

- Convém que a análise/avaliação de riscos inclua um enfoque sistemático de estimar a magnitude do risco (análise de riscos) e o processo de comparar os riscos estimados contra os critérios de risco para determinar a significância do risco (avaliação do risco).

- Convém que as análises/avaliações de riscos também sejam realizadas periodicamente, para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco, ou seja, nos ativos, ameaças, vulnerabilidades, impactos, avaliação do risco e quando uma mudança significativa ocorrer.

NBR ISO/IEC 27002

4. Anál./Aval. e Tratamento de Riscos

- Antes de considerar o tratamento de um risco, a organização deve definir os critérios para avaliar se os riscos podem ser ou não aceitos;

- Para cada risco identificado, uma decisão de tratamento deve ser tomada;

- Opções de tratamento:
  *Aplicar controles para a redução do risco;
  *Conhecer objetivamente e aceitar o risco;
  *Evitar os riscos, proibindo ações que possam causar o risco;
  *Transferir para outras partes (Ex: Seguradoras).

NBR ISO/IEC 27002
5. Política de SI

- Convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

- Deve conter:
  * Uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação;
  * Uma declaração do comprometimento da direção;
  * Uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco;
  * Definição das responsabilidades gerais e específicas na GSI.

NBR ISO/IEC 27002
5. Política de SI

- Apenas uma categoria:

* Política de Segurança da Informação

- Controles:

* Documento da política de segurança da informação;
* Análise Crítica da política de segurança da informação.

NBR ISO/IEC 27002
6. Organizando a SI

Objetivo: Gerenciar a segurança da informação dentro da organização.

- Convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização.

- Convém que a direção aprove a política de segurança da informação, atribua as funções da segurança, coordene e analise criticamente a implementação da segurança da informação por toda a organização.

- Categorias:

* Infraestrutura da segurança da informação e Partes externas

NBR ISO/IEC 27002
6. Organizando a SI

- Controles:

* Comprometimento da direção com a SI;
* Coordenação da SI;
* Atribuição de responsabilidades para SI;
* Processo de autorização p/ os recursos de processamento da inf.;
* Acordos de confidencialidade;
* Contato com autoridades;
* Contato com grupos especiais;
* Análise Crítica Independente de SI;
* Identificação de riscos relacionados com partes externas;
* Identificação da SI ao tratar com clientes;
* Identificação da SI nos acordos com terceiros.

NBR ISO/IEC 27002

7. Gestão de Ativos

- Objetivo: Alcançar e manter a proteção adequada dos ativos da organização.

- Convém que todos os ativos sejam inventariados e tenham um proprietário responsável.

- Convém que os proprietários dos ativos sejam identificados e a eles seja atribuída a responsabilidade pela manutenção apropriada dos controles.

Categorias:

* Responsabilidade pelos ativos;
* Classificação da informação.

NBR ISO/IEC 27002
7. Gestão de Ativos

- Controles:

* Inventário dos ativos;
* Propriedade dos ativos;
* Uso aceitável dos ativos;
* Recomendações para classificação da informação;
* Rótulos e tratamento da informação.

NBR ISO/IEC 27002

8. Segurança em RH

- Objetivo: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos.

- Convém que as responsabilidades pela segurança da informação sejam atribuídas antes da contratação, de forma adequada, nas descrições de cargos e nos termos e condições de contratação.

- Convém que todos os candidatos ao emprego, fornecedores e terceiros sejam adequadamente analisados, especialmente em cargos com acesso a informações sensíveis.

- Convém que todos os funcionários, fornecedores e terceiros, usuários dos recursos de processamento da informação, assinem acordos sobre seus papéis e responsabilidades pela segurança da informação.

NBR ISO/IEC 27002

8. Segurança em RH

- Categorias:

* Antes da contratação;
* Durante a contratação;
* Encerramento ou mudança da contratação.

- Controles:

* Papéis e Responsabilidades
* Seleção;
* Termos e condições de contratação;
* Responsabilidades da direção;
* Conscientização, educação e treinamento em SI;
* Processo disciplinar;
* Encerramento de atividades;
* Devolução de ativos;
* Retirada de direitos de acesso.

NBR ISO/IEC 27002

9. Seg. Física e do Ambiente

- Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

- Convém que as instalações de processamento da informação críticas ou sensíveis sejam mantidas em áreas seguras, protegidas por perímetros de segurança definidos, com barreiras de segurança e controles de acesso apropriados. Convém que sejam fisicamente protegidas contra o acesso não autorizado, danos e interferências.

- Convém que a proteção oferecida seja compatível com os riscos identificados.

- 2 categorias:

* Áreas Seguras; e * Segurança de equipamentos.

NBR ISO/IEC 27002

9. Seg. Física e do Ambiente

- Controles:

* Perímetro de Segurança
* Segurança em escritórios, salas e instalações;
* Proteção contra ameaças externas e do meio ambiente;
* Trabalho em áreas seguras;
* Acesso do público, áreas de entrega e carregamento;
* Instalação e proteção do equipamento;
* Utilidades;
* Segurança do cabeamento;
* Manutenção dos equipamentos;
* Segurança de equipamentos fora das dep. da organização;
* Reutilização e alienação segura de equipamentos;
* Remoção de propriedade.

NBR ISO/IEC 27002
10. Gerenciamento de Operações e Comunicações

- Tratado com ênfase em 10 categorias

* Procedimentos e responsabilidades operacionais;
* Gerenciamento de serviços terceirizados;
* Planejamento e aceitação dos sistemas;
* Proteção contra códigos maliciosos e códigos móveis;
* Cópias de segurança;
* Gerenciamento da segurança em redes;
* Manuseio de mídias;
* Troca de informações;
* Serviços de comércio eletrônico;
* Monitoramento.

NBR ISO/IEC 27002

10. Gerenciamento de Operações e Comunicações

- Controles:
  * Documentação dos procedimentos de operação;
  * Gestão de mudanças;
  * Segregação de funções;
  * Separação dos recursos de desenv., teste e produção;
  * Entrega de serviços (de terceiros);
  * Monit. e Anál. Crítica de Serviços Terceirzados;
  * Gerenciamento de mudanças p/ serv. terceirizados;
  * Gestão da capacidade;
  * Aceitação de sistemas;
  * Controle contra códigos maliciosos;
  * Controle contra códigos móveis;

NBR ISO/IEC 27002

10. Gerenciamento de Operações e Comunicações

- Controles:

  * Cópias de segurança das informações;
  * Controle de redes;
  * Segurança dos serviços de rede;
  * Gerenciamento de mídias removíveis;
  * Descarte de mídias;
  * Procedimentos para tratamento de informação;
  * Segurança da documentação de sistemas;
  * Políticas e procedimentos para troca de informações;
  * Acordos para troca de informações;
  * Mídias em trânsito;
  * Mensagens eletrônicas;

NBR ISO/IEC 27002

10. Gerenciamento de Operações e Comunicações

- Controles:

  * Sistemas de informação do negócio;
  * Comércio eletrônico;
  * Transações online;
  * Informações publicamente disponíveis;
  * Registros de auditoria;
  * Monitoramento do uso de sistema;
  * Proteção das informações dos registros (log);
  * Registros (log) de administrador e operador;
  * Registro (log) de falhas;
  * Sincronização de relógios.

NBR ISO/IEC 27002

11. Controle de Acessos

Objetivo: Controlar acesso à informação.

Convém que o acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação.

Convém que as regras de controle de acesso levem em consideração as políticas para autorização e disseminação da informação.

NBR ISO/IEC 27002

11. Controle de Acessos

- 7 categorias:

  * Requisitos de negócio para controle de acesso;

  * Gerenciamento de acesso do usuário;

  * Responsabilidades dos usuários;

  * Controle de acesso à rede;

  * Controle de acesso ao sistema operacional;

  * Controle de acesso à aplicação e à informação;

  * Computação móvel e trabalho remoto.

NBR ISO/IEC 27002

11. Controle de Acessos

- Controles:

  * Política de controle de acesso;
  * Registro de usuário;
  * Gerenciamento de privilégios;
  * Gerenciamento de senha do usuário;
  * Análise Crítica dos direitos de acesso de usuário;
  * Uso de senhas;
  * Equipamento de usuário sem monitoração;
  * Política de mesa limpa e tela limpa;
  * Política de uso dos serviços da rede;
  * Autenticação para conexão externa do usuário;

NBR ISO/IEC 27002

11. Controle de Acessos

- Controles:

  * Identificação de equipamento em redes;
  * Proteção e configuração de portas de diagnóstico remotas;
  * Segregação de redes;
  * Controle de conexão de rede;
  * Controle de roteamento de redes;
  * Procedimentos seguros de entrada do sistema;
  * Identificação e autenticação de usuário;
  * Sistema de gerenciamento de senha;
  * Uso de utilitários de sistema;
  * Desconexão de terminal por inatividade;

NBR ISO/IEC 27002

11. Controle de Acessos

- Controles:

  * Limitação de horário de conexão;

  * Restrição de acesso à informação;

  * Isolamento de sistemas sensíveis;

  * Computação e comunicação móvel;

  * Trabalho remoto.

NBR ISO/IEC 27002

12. Aquisição, desenv. e manut. de sistemas de inf.

- Categorias:

* Requisitos de segurança de sistemas de informação;
* Processamento correto nas aplicações;
* Controles criptográficos;
* Segurança dos arquivos do sistema;
* Segurança em processos de desenvolvimento e de suporte;
* Gestão de vulnerabilidades técnicas.

NBR ISO/IEC 27002

12. Aquisição, desenv. e manut. de sistemas de inf.

- Controles:

* Análise e especificação dos requisitos de segurança;
* Validação dos dados de entrada;
* Integridade das mensagens;
* Validação dos dados de saída;
* Política para uso de controles criptográficos;
* Gerenciamento de chaves;
* Controle de software operacional;
* Proteção dos dados para teste de sistemas;
* Controle de acesso ao código fonte do programa;
* Procedimentos para controle de mudanças;

NBR ISO/IEC 27002

12. Aquisição, desenv. e manut. de sistemas de inf.

- Controles:

* Análise crítica técnica das aplicações após mudanças de SO;
* Restrições sobre mudanças em pacotes de software;
* Vazamento de informações;
* Desenvolvimento terceirizado de software;
* Controle de vulnerabilidades técnicas.

NBR ISO/IEC 27002

13. Gestão de Incidentes de SI

- 2 categorias:

* Notificação de fragilidades e eventos de segurança da informação;

* Gestão de incidentes de segurança da informação e melhorias.

- Controles:

* Notificação de eventos de segurança da informação;
* Notificação de fragilidades de segurança da informação;
* Responsabilidades e procedimentos;
* Aprendizado com os incidentes de SI;
* Coleta de evidências.

NBR ISO/IEC 27002

14. Gestão de Cont. do Negócio

Objetivo:

Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.

- Convém que o processo de gestão da continuidade do negócio seja implementado para minimizar um impacto sobre a organização e recuperar perdas de ativos da informação;

- Convém que a gestão da continuidade do negócio inclua controles para identificar e reduzir riscos, em complementação ao processo de análise/ avaliação de riscos global.

- As conseqüências de desastres, falhas de segurança, perda de serviços e disponibilidade de serviços devem estar sujeitas a uma análise de impacto nos negócios.

NBR ISO/IEC 27002

14. Gestão de Cont. do Negócio

Controles:

* Inclusão da SI no processo de gerenciamento da continuidade de negócios;
  * Continuidade de negócios e análise/avaliação de riscos;
  * Estrutura do plano de continuidade do negócio;
  * Testes, manutenção e reavaliação dos planos de continuidade do negócio.

NBR ISO/IEC 27002
15. Conformidade

Objetivos: assegurar conformidade quanto ao aparato normativo vigente, seja ele técnico, legal (civil, penal, criminal, regulamentação de setor) ou interno ao negócio.

Contempla 3 categorias:

* Conformidade com requisitos legais;

* Conformidade com normas e políticas de segurança da informação e conformidade técnica;

* Considerações quanto à auditoria de sistemas de informação.

NBR ISO/IEC 27002

15. Conformidade

Controles:

* Identificação da legislação vigente;
* Direitos de propriedade intelectual;
* Proteção de registros organizacionais;
* Proteção de dados e privacidade de inf. pessoais;
* Prevenção de mau uso de recursos de proc. da inf.;
* Regulamentação de controles e criptografia;
* Conformidade com as políticas e normas de SI;
* Verificação da conformidade técnica;
* Controles de auditoria de sistemas de informação;
* Proteção de ferramentas de auditoria de sistemas de inf.

NBR ISO/IEC 27002
Exercícios e Observações

- Dúvidas;

- Resolução de questões;

- O que vimos aqui?

NBR ISO/IEC 27005

"Mais do que de máquinas, precisamos de humanidade. Mais do que de inteligência, precisamos de afeição e doçura. Sem essas virtudes, a vida será de violência e tudo será perdido."

(Charles Chaplin - O Último discurso, do filme O Grande Ditador)

NBR ISO/IEC 27005
Estrutura

1. Introdução
2. Escopo
3. Referências Normativas
4. Termos e Definições
5. Organização da Norma
6. Contextualização
7. Visão Geral do Processo de Gestão de Riscos de Segurança da Informação
8. Definição do Contexto
9. Análise/Avaliação de Riscos de SI
10. Análise/Avaliação de Riscos de SI
11. Tratamento do Risco de SI
12. Aceitação do Risco de SI
13. Comunicação do Risco de SI
14. Monitoramento e Análise Crítica de Riscos de SI

NBR ISO/IEC 27005
Overview

- Esta norma está de acordo com os conceitos especificados na ABNT NBR ISO/IEC 27001 e foi elaborada para facilitar uma implementação satisfatória da segurança da informação tendo como base a gestão de riscos.

- Esta norma se aplica a todos os tipos de organização que pretendam gerir os riscos que poderiam comprometer a segurança da informação da organização.

NBR ISO/IEC 27005
Overview

- Apresenta diretrizes para o processo de Gestão de Riscos de Segurança da Informação (GRSI) de uma organização, em conformidade com os requisitos de um SGSI descritos na NBR ISO/IEC 27001.

- A norma não inclui uma metodologia específica para a gestão de riscos de segurança da informação.

-Cabe à organização definir sua abordagem ao processo de riscos, levando em conta, por exemplo, o escopo dos seu SGSI, o contexto da gestão de riscos e o seu setor de atividade econômica.

NBR ISO/IEC 27005
Overview

- Esta norma é do interesse de gestores e pessoal envolvidos com a gestão de riscos de segurança da informação em uma organização e, quando aplicável, em entidades externas que dão suporte a essa atividade.

- Apresenta diretrizes para o processo de Gestão de Riscos de Segurança da Informação (GRSI) de uma organização, em conformidade com os requisitos de um SGSI descritos na NBR ISO/IEC 27001.

- A norma não inclui uma metodologia específica para a gestão de riscos de segurança da informação.

-Cabe à organização definir sua abordagem ao processo de riscos, levando em conta, por exemplo, o escopo dos seu SGSI, o contexto da gestão de riscos e o seu setor de atividade econômica.

NBR ISO/IEC 27005
Overview

- A 27005 adota como referenciais normativos as normas 27001 e 27002, indispensáveis a aplicação desta.

- É necessária abordagem sistemática de gestão de riscos de segurança da informação para se identificar as necessidades da organização em relação aos requisitos de SI e para criar um SGSI eficaz.

- A gestão de riscos de SI faz parte da gestão de riscos corporativos, devendo estar alinhada a esta.

- Convém que a gestão de riscos de segurança da informação seja um processo contínuo, contemplando: definir o contexto, avaliar e tratar os riscos.

NBR ISO/IEC 27005
Overview

Termos e definições:

Impacto – mudança adversa no nível obtido dos objetivos de negócios

Riscos de segurança da informação – a possibilidade de uma ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, prejudicando a organização (medido em função da probabilidade de um evento e de sua consequência).

Ação de evitar o risco – decisão de não se envolver ou agir de forma a se retirar de uma situação de risco

Comunicação do risco – troca ou compartilhamento de informação sobre risco entre o tomador de decisão e outras partes envolvidas

NBR ISO/IEC 27005

Overview

Termos e definições:

Estimativa de riscos – processo utilizado para atribuir valores à probabilidade e consequências de um risco

Identificação de riscos – processo para localizar, listar e caracterizar elementos do risco

Redução do risco – ações tomadas para reduzir a probabilidade, as consequências negativas ou ambas associadas a um risco

Retenção do risco – aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco

Transferência do risco – compartilhamento com uma outra entidade do ônus da perda associado a um risco

NBR ISO/IEC 27005
Overview

Aplicabilidade:

O processo de GRSI pode ser aplicado à organização como um todo, a uma área específica da organização (por exemplo: um departamento, uma localidade, um serviço), a um sistema de informações, a controles já existentes, planejados ou apenas a aspectos particulares de um controle (exemplo: Plano de Continuidade de Negócios)

NBR ISO/IEC 27005
Overview

O processo de gestão de riscos de SI:

* Definição do contexto (Seção 7);
* Análise/avaliação de riscos (Seção 8);
* Tratamento do risco (Seção 9);
* Aceitação do risco (Seção 10);
* Comunicação do risco (Seção 11);
* Monitoramento e análise crítica do risco (Seção 12).

NBR ISO/IEC 27005

Exercícios e Observações

- Dúvidas;

- Resolução de questões;

- O que vimos aqui?

Obrigado!
@thiagofagury