Segurança da Informação

Competências:

- Implementar práticas e condutas de segurança da informação no ambiente de TI.

Bases Tecnológicas, científicas e instrumentais (conteúdos):

- Gestão de Segurança da Informação Segundo a NBR ISO/IEC 27001;
- NBR ISO/IEC 27001:2006: Processo de Certificação;
- Certificação de Segurança da Informação;
- Principais Normas;

Situação de Aprendizagem:

- SGSI.

NORMAS

O que é a NBR?

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Senac

- ✓ Normas nacionais são normas técnicas estabelecidas por um organismo nacional de normalização para aplicação num dado país. No Brasil, as normas brasileiras (NBR) são elaboradas pela ABNT , e em cada país, normalmente, existe um organismo nacional de normalização.

- ✓ A ABNT é reconhecida pelo Estado brasileiro como o Fórum Nacional de Normalização, o que significa que as normas elaboradas pela ABNT - as NBR - são reconhecidas formalmente como as normas brasileiras.

O que é a ISO?

- ISO é o nome usual com o qual é conhecida a International Organization for Standardization (Organização Internacional de Padronização).

- É uma entidade fundada em 1947, sediada na Suiça. Congrega organismos de normalização nacionais, cuja principal atividade é a de elaborar padrões para especificações e métodos de trabalho nas mais diversas áreas da sociedade, exceto no setor eletro-eletrônico onde a responsabilidade fica a cargo da International Electrotechical Comission (IEC).

- O Brasil é representado na ISO através da ABNT - Associação Brasileira de Normas Técnicas.

ABNT ISO/IEC 27.000

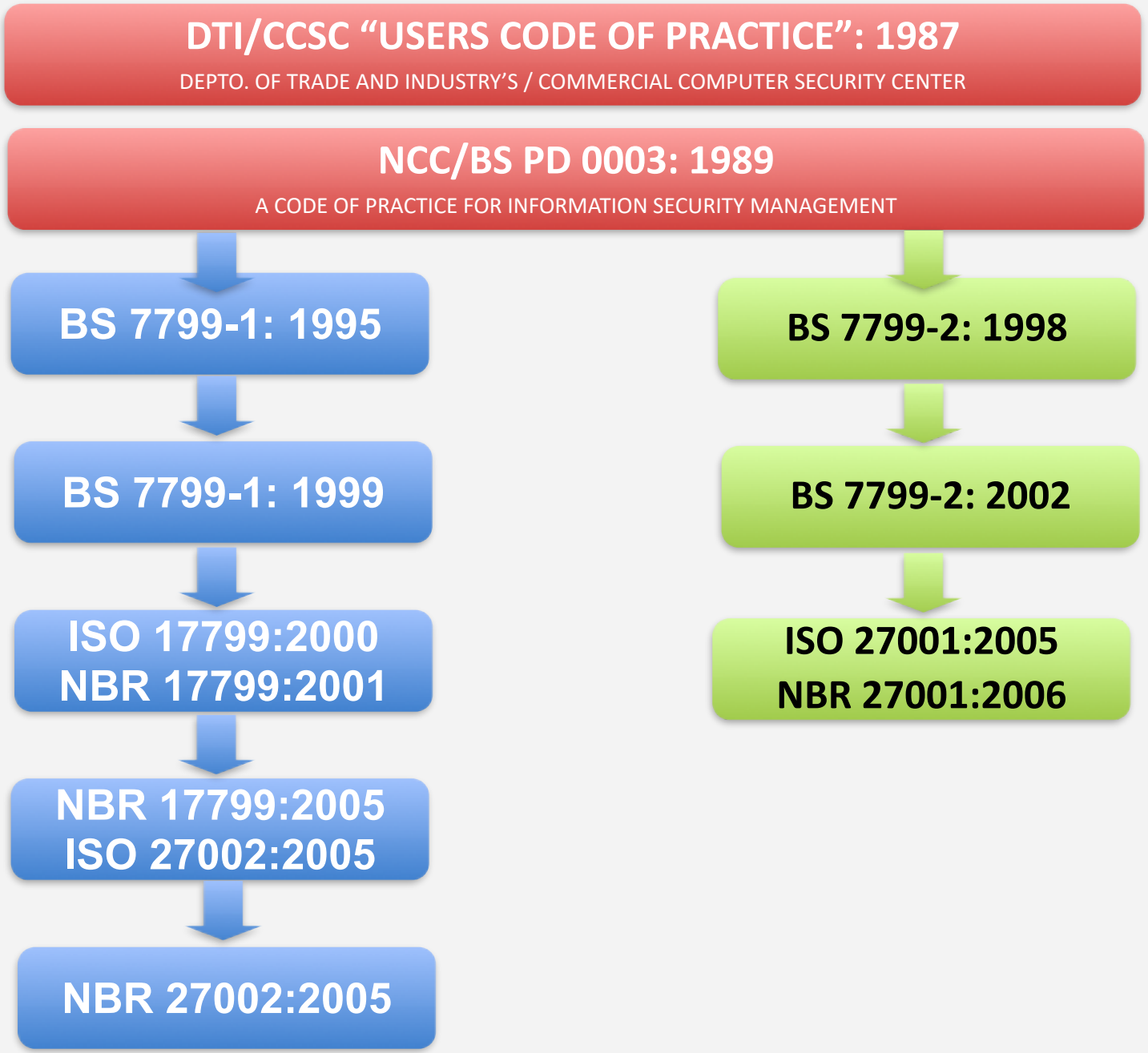
Família ISO 27000

Família 27000		
Número	Ano	Descrição
27000	ISO: 2009	Fundamentos e vocabulário
27001	ABNT: 2013	Requisitos
27002	ABNT: 2022	Código de prática para a gestão de segurança da informação
27003	ISO: 2009	Guia de implementação
27004	ISO: 2009	Métricas e medidas
27005	ABNT: 2008	Gestão de riscos
27006	ISO: 2007	Requisitos de acreditação para a certificação
27007	Em desenv.	Orientações para gestão de auditorias
27008	Em desenv.	Orientações para auditores
27011	ABNT: 2009	Técnicas de segurança - Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002
Outras normas não publicadas no Brasil e/ou em fase de desenvolvimento: 27010, 27031, 27032, 27033-X, 27034-X, 27036, 27037.		

Família ISO 27000

Família 27000		
Número	Ano	Descrição
27000	ISO: 2009	Fundamentos e vocabulário
27001	**ABNT: 2013**	**Requisitos**
27002	**ABNT: 2022**	**Código de prática para a gestão de segurança da informação**
27003	ISO: 2009	Guia de implementação
27004	ISO: 2009	Métricas e medidas
27005	ABNT: 2008	Gestão de riscos
27006	ISO: 2007	Requisitos de acreditação para a certificação
27007	Em desenv.	Orientações para gestão de auditorias
27008	Em desenv.	Orientações para auditores
27011	ABNT: 2009	Técnicas de segurança - Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002
Outras normas não publicadas no Brasil e/ou em fase de desenvolvimento: 27010, 27031, 27032, 27033-X, 27034-X, 27036, 27037.		

Família ISO 27000



Família ISO 27000

5ª

27.001:2013

3ª

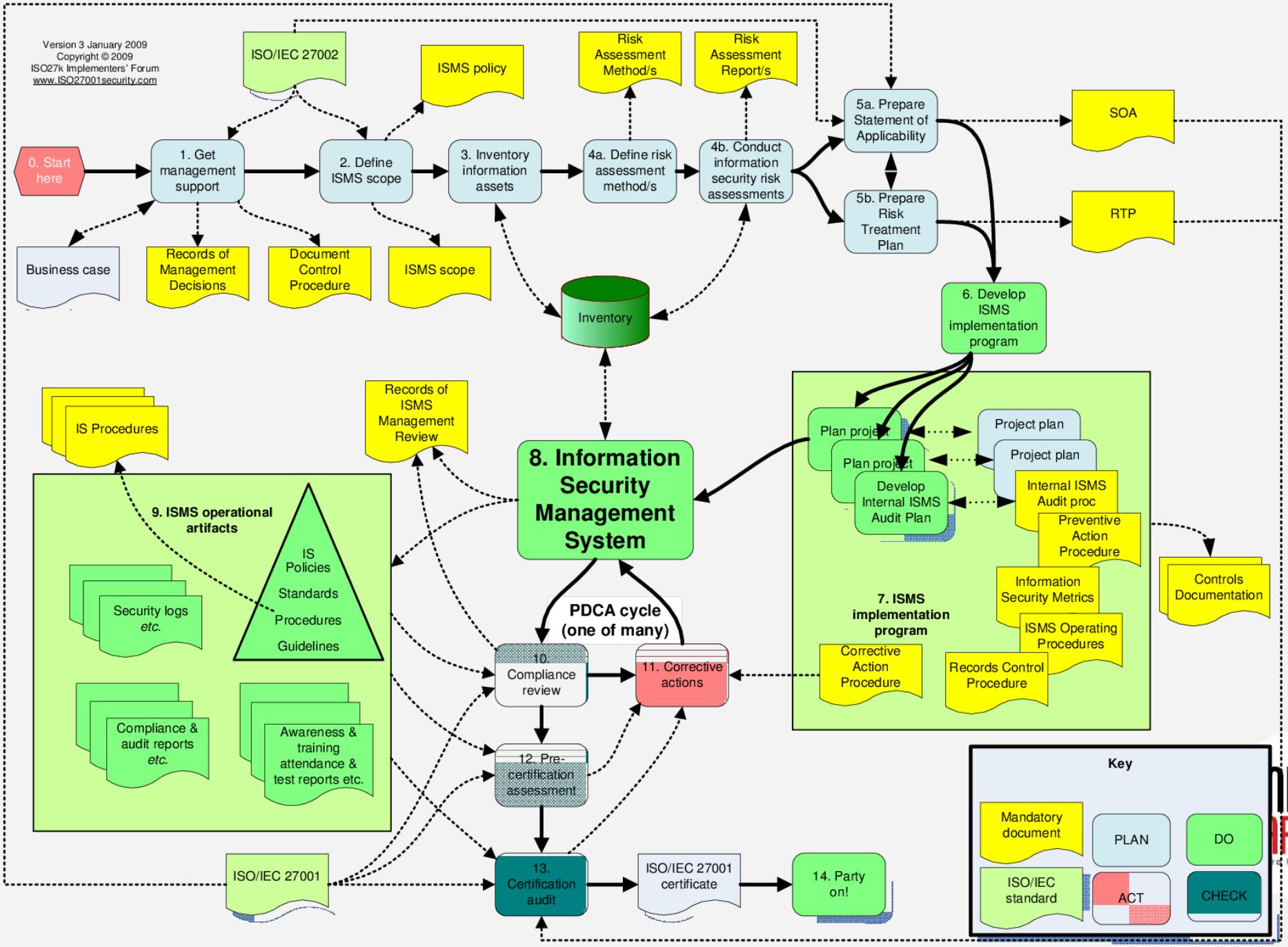
27.002:2022

ABNT NBR ISO/IEC 27001

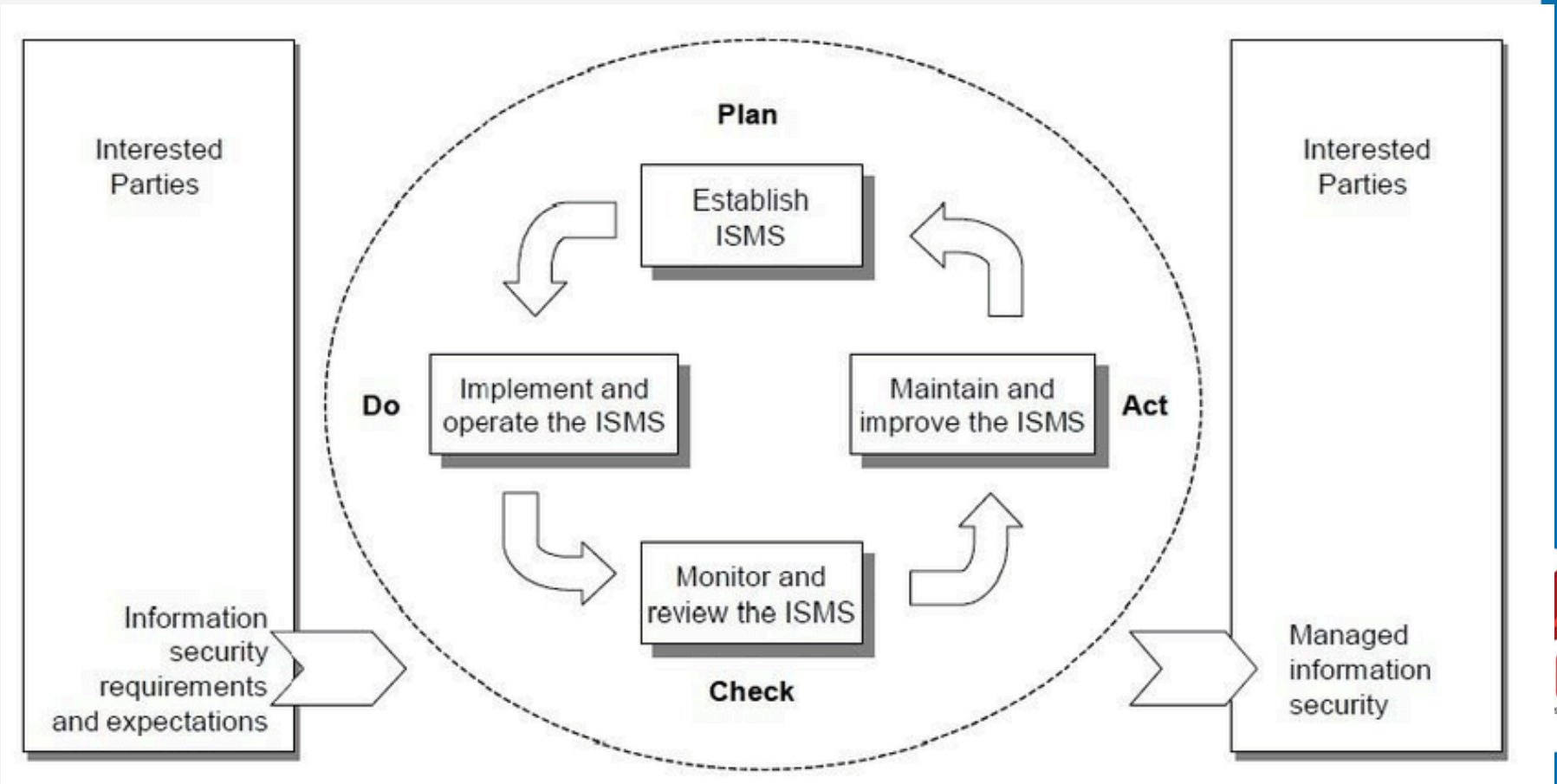
- Sistema de gestão;

- PDCA;

ABNT NBR ISO/IEC 27001



ABNT NBR ISO/IEC 27001



ABNT NBR ISO/IEC 27001

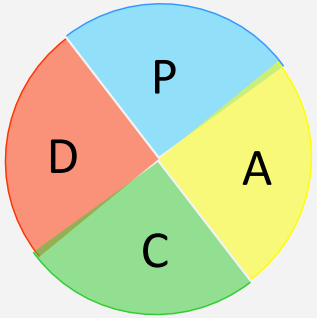
Partes Interessadas

Plan

Estabelecimento do Sistema de Gestão

Implementação e Operação do Sistema de Gestão

Do



Manutenção e Melhoria do Sistema de Gestão

Act

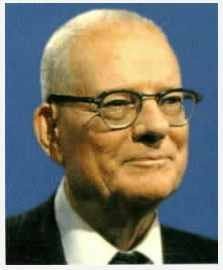
Monitoramento e Análise Crítica do Sistema de Gestão

Check

Partes Interessadas

Expectativas e requisitos de segurança da informação

Segurança da informação gerenciada



O QUE É O CICLO PDCA?

O Ciclo PDCA foi idealizado por Shewhart mais tarde aplicado por Demingno uso de estatísticas e métodos de amostragem.

O Ciclo PDCA nasceu no escopo da tecnologia TQC (*Total QualityControl) como uma ferramenta que melhor representava o ciclo de gerenciamentode uma atividade.*

Carioca Centro Universitário

PLAN

- ✓ Definir Escopo e Limites do SGSI
- ✓ Definir a Política Geral de Segurança da Informação
- ✓ Definir a metodologia para a avaliação e tratamento de riscos
- ✓ Identificar e classificar os riscos
- ✓ Identificar e classificar as alternativas para tratamento dos riscos
- ✓ Selecionar objetivos de controle e controles específicos a implementar
- ✓ Identificar riscos residuais não cobertos
- ✓ Preparar uma Declaração de Aplicabilidade (DDA) - Sumário
- ✓ Obter autorização para implantar o SGSI
- ✓ Formular um plano de ação

DO

- ✓ Implantar o plano de tratamento de riscos
- ✓ Implantar os controles definidos
- ✓ Implantar os programas de treinamento e conscientização dos usuários
- ✓ Gerenciar o SGSI

CHECK

- ✓Monitar controles existentes
- ✓Realizar revisões periódicas (Auditoria Interna)
- ✓Analisar efetividade dos controles existentes
- ✓Verificar novos riscos e nível dos riscos residuais

ACT

- ✓Implementar melhorias necessárias
- ✓Comunicar ações
- ✓Garantir que as mudanças atingiram resultado esperado

ABNT ISO/IEC 27.001:2013

ABNT NBR ISO/IEC 27001:2013

- "Sistemas de gestão de segurança da informação – Requisitos"
  - Especifica uma série de processos voltados para garantira revisão e melhoria do Sistema de Gestão.

ABNT NBR ISO/IEC 27001:2013

- Principal característica: “DEVE”.
  - Esta Norma adota o modelo conhecido como ‘Plan-Do-Check-Act’, que é aplicado para estruturar todos os processos do SGSI (Sistema de Gestão da Segurança da Informação).

ABNT NBR ISO/IEC 27001:2013

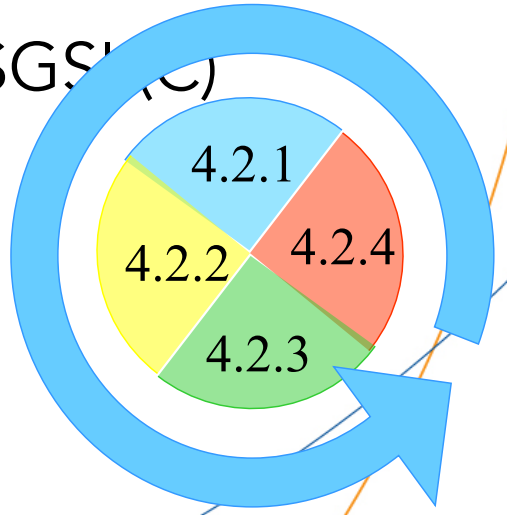
- Organização
  - 1. ESCOPO
  - 2. REFERÊNCIAS NORMATIVAS
  - 3. TERMOS E DEFINIÇÕES
  - 4. SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

ABNT NBR ISO/IEC 27001:2013

- 5. RESPONSABILIDADE DA DIREÇÃO
- 6. AUDITORIAS INTERNAS DO SGSI
- 7. ANÁLISE CRÍTICA PELA DIREÇÃO DO SGSI
- 8. MELHORIAS DO SGSI ANEXOS A, B e C

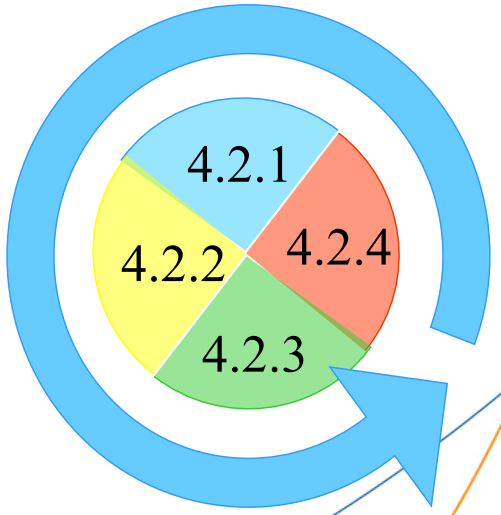
ABNT NBR ISO/IEC 27001:2013

- 4. SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO
  - 4.1. REQUISITOS GERAIS
  - 4.2. ESTABELECENDO E GERENCIANDO O SGSI
    - 4.2.1. Estabelecer o SGI (P)
    - 4.2.2. Implementar e operar o SGSI (D)
    - 4.2.3. Monitorar e analisar criticamente o SGSI (C)
    - 4.2.4. Manter e melhorar o SGSI (A)



ABNT NBR ISO/IEC 27001:2013

- 4.3. REQUISITOS DE DOCUMENTAÇÃO
  - 4.3.1. Geral (P)
  - 4.3.2. Controle de documentos (P)
  - 4.3.3. Controle de registros (P,D,C e A)



ABNT NBR ISO/IEC 27001:2013

- 5. RESPONSABILIDADE DA DIREÇÃO
  - 5.1. COMPROMETIMENTO DA DIREÇÃO (P)
  - 5.2. GESTÃO DE RECURSOS (D)
    - 5.2.1. Provisão de recursos
    - 5.2.2. Treinamento, conscientização e competência
- 6. AUDITORIAS INTERNAS DO SGSI (C)

ABNT NBR ISO/IEC 27001:2013

- 7. ANÁLISE CRÍTICA DO SGSI PELA DIREÇÃO (A)
  - 7.1. GERAL
  - 7.2. ENTRADAS PARA A ANÁLISE CRÍTICA
  - 7.3. SAÍDAS DA ANÁLISE CRÍTICA

ABNT NBR ISO/IEC 27001:2013

- 8. MELHORIA DO SGSI (A)
  - 8.1. MELHORIA CONTÍNUA
  - 8.2. AÇÃO CORRETIVA
  - 8.3. AÇÃO PREVENTIVA

Alguns Benefícios da Certificação ISO 27001

- Responsabilidade reduzida devido às políticas e aos procedimentos não implementados ou reforçados
- Oportunidade de identificar e eliminar fraquezas
- A Gerência participa da Segurança da Informação

Alguns Benefícios da Certificação ISO 27001

- Revisão independente do seu SGSI
- Fornece segurança a todas as partes interessadas
- Melhor consciência da segurança
- Une recursos com outros sistemas de gerenciamento
- Mecanismo para medir o sucesso do sistema

Algumas Razões para adotar o ISO 27001

- Eficácia melhorada da Segurança da Informação
- Diferenciação do Mercado
- Satisfazer exigências dos clientes
- Único padrão com aceitação global

Algumas Razões para adotar o ISO 27001

- Responsabilidades focadas na equipe de trabalho
- A Tecnologia da Informação cobre padrões tão bem quanto a organização, pessoal e facilidades
- Mandatos e leis

ABNT ISO/IEC 27.002:2022

ABNT NBR ISO/IEC 27002

- "CÓDIGO DE PRÁTICA PARA A GESTÃO DA SEGURANÇA DA INFORMAÇÃO"
  - Apresenta "as melhores práticas" a serem utilizadas na gestão da segurança da informação.

Estrutura da Norma

» 5. Política de Segurança da Informação (1)

Seção

Estrutura da Norma

» 5. Política de Segurança da Informação (1)

– 5.1 Política de Segurança da Informação
  - Objetivo: "Prover uma orientação de apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes".

Categoria

Estrutura da Norma

5.1.1 Documento da Política de Segurança da Informação

- "Convém que um documento da política de SI seja aprovado pela direção ..."

5.1.2 Análise Crítica da Política de Segurança da Informação

- "Convém que a política de SI seja analisada criticamente a intervalos planejados ou quando mudanças ...

Controles

Estrutura da Norma

- Objetivo do controle
- Controle
- Diretrizes para implementação
- Informações adicionais

- Principal característica: “CONVÉM”.

Seções (Categorias)

- Política de Segurança da Informação (1)
- Organizando a Segurança da Informação (2)
- Gestão de Ativos (2)
- Segurança em Recursos Humanos (3)
- Segurança Física e do Ambiente (2)

Seções (Categorias)

- Gestão de Operações e Comunicações (10)
- Controle de Acesso (7)
- Aquisição, Desenvolvimento e Manutenção de SI (6)
- Gestão de Incidentes de SI (2)
- Gestão da Continuidade do Negócio (1)
- Conformidade (3)

5.POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

» 5.1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

– Prover uma orientação e apoio da direção para a segurança da informação, com base nos requisitos do negócio, leis e regulamentações relevantes.

5.POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- Estabelecimento e manutenção de uma política clara e alinhada com os objetivos do negócio.
- Demonstrar o comprometimento da direção.
- Conscientização e treinamento.
- Análise crítica documentada e realizada em intervalos planejados.

6.ORGANIZANDO A SEGURANÇA DA INFORMAÇÃO

- 6.1. INFRA-ESTRUTURA DA SEGURANÇA DA INFORMAÇÃO
  - Gerenciar a segurança da informação dentro da organização
- 6.2. PARTES EXTERNAS
  - Manter a segurança dos recursos de processamento e da informação da organização que são acessados, processados, comunicados ou gerenciados por partes externas.

7. GESTÃO DE ATIVOS

» 7.1. RESPONSABILIDADE PELOS ATIVOS

– Alcançar e manter a proteção adequada dos ativos da organização.

• Ativos identificados claramente e inventariados constantemente.

7. GESTÃO DE ATIVOS

» 7.2. CLASSIFICAÇÃO DA INFORMAÇÃO

– Assegurar que a informação receba um nível adequado de proteção

- A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.

8. SEGURANÇA EM RECURSOS HUMANOS

- 8.1. ANTES DA CONTRATAÇÃO
- 8.2. DURANTE A CONTRATAÇÃO
- 8.3. ENCERRAMENTO OU MUDANÇA DA CONTRATAÇÃO

8. SEGURANÇA EM RECURSOS HUMANOS

» Funcionários, fornecedores e terceiros:
  - Entendam suas responsabilidades e obrigações;
  - Estejam de acordo com os seus papéis;
  - Estejam conscientes das ameaças;
  - Estejam preparados para apoiar a Política; e
  - Deixem a organização (ou mudem de trabalho) de forma ordenada.

9. SEGURANÇA FÍSICA E DO AMBIENTE

- 9.1. ÁREAS SEGURAS
- 9.2. SEGURANÇA DE EQUIPAMENTOS
  - Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.
    - Controles de entrada física; e
    - Proteção contra ameaças externas e do meio ambiente.

9. SEGURANÇA FÍSICA E DO AMBIENTE

- Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.
  - Segurança do cabeamento; e
  - Reutilização e alienação segura de equipamentos.

10. GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

- 10.1. DOCUMENTAÇÃO DOS PROCEDIMENTOS DE OPERAÇÃO
  - Garantir a operação segura e correta dos recursos de processamento de dados.
- 10.2. GERENCIAMENTO DE SERVIÇOS TERCEIRIZADOS
  - Implementar e manter o nível apropriado

10. GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

- 10.3. PLANEJAMENTO E ACEITAÇÃO DE SISTEMAS
  - Minimizar o risco de falhas nos sistemas
- 10.4. PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS E CÓDIGOS MÓVEIS
  - Proteger a integridade do software e da informação.

10. GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

- 10.5. CÓPIAS DE SEGURANÇA DAS INFORMAÇÕES
  - Manter a integridade e disponibilidade da informação e dos recursos de processamento da informação.
- 10.6. GERENCIAMENTO DA SEGURANÇA EM REDES
  - Garantir a segurança das informações em redes e a proteção da infraestrutura de suporte.

10. GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

- 10.7. MANUSEIO DE MÍDIAS
  - Prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos e interrupções das atividades do negócio.
- 10.8. TROCA DE INFORMAÇÕES
  - Manter a segurança na troca de informações e softwares à organização e com quaisquer entidades externas.

10. GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

- 10.9. SERVIÇO DE COMÉRCIO ELETRÔNICO
  - Garantir a segurança de serviços de comércio eletrônico e sua utilização segura.
- 10.10. MONITORAMENTO
  - Detectar atividades não autorizadas de processamento da informação.

11. CONTROLE DE ACESSOS

- 11.1. REQUISITOS DE NEGÓCIO PARA CONTROLE DE ACESSO
  - Controlar o acesso à informação
- 11.2. GERENCIAMENTO DE ACESSO DO USUÁRIO
  - Assegurar o acesso do usuário autorizado e prevenir o acesso não autorizado a sistemas de informação.
- 11.3. RESPONSABILIDADES DOS USUÁRIOS
  - Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação.

11. CONTROLE DE ACESSOS

- 11.4. CONTROLE DE ACESSO À REDE
  - Prevenir o acesso não autorizado aos serviços de rede.
- 11.5. CONTROLE DE ACESSO AO SISTEMA OPERACIONAL
  - Prevenir o acesso não autorizado aos sistemas operacionais.

11. CONTROLE DE ACESSOS

- 11.6. CONTROLE DE ACESSO À APLICAÇÃO E À INFORMAÇÃO
  - Prevenir o acesso não autorizadoà informação contida nos sistemas de aplicação.
- 11.7. COMPUTAÇÃO MÓVEL E TRABALHO REMOTO
  - Garantir a segurança da informação e recursos de trabalho remoto.

12. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

- 12.1. REQUISITOS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO
  - Garantir que a segurança é parte integrante de sistemas de informação.
- 12.2. PROCESSAMENTO CORRETO NAS APLICAÇÕES
  - Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.

12. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

» 12.3. CONTROLES CRIPTOGRÁFICOS
  – Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.
» 12.4. SEGURANÇA DOS ARQUIVOS DO SISTEMA
  – Garantir a segurança de arquivos de sistema.

12. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

- 12.5. SEGURANÇA EM PROCESSOS DE DESENVOLVIMENTO E DE SUPORTE
  - Manter a segurança de sistemas aplicativos e da informação.
- 12.6. GESTÃO DE VULNERABILIDADES TÉCNICAS
  - Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.

13. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

» 13.1. NOTIFICAÇÃO DE FRAGILIDADES E EVENTOS DE SEGURANÇA DA INFORMAÇÃO

– Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

13. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

» 13.2. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E MELHORIAS

– Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.

14. GESTÃO DA CONTINUIDADE DO NEGÓCIO

» 14.1. ASPECTOS DA GESTÃO DA CONTINUIDADE DO NEGÓCIO, RELATIVOS À SEGURANÇA DA INFORMAÇÃO

– 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.

15. CONFORMIDADE

» 15.1. CONFORMIDADE COM REQUISITOS LEGAIS

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

15. CONFORMIDADE

» 15.2. CONFORMIDADE COM NORMAS E POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E CONFORMIDADE TÉCNICA

– Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.

15. CONFORMIDADE

» 15.3. CONSIDERAÇÕES QUANTO À AUDITORIA DE SISTEMAS DE INFORMAÇÃO

– Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.

RELAÇÃO 27001 E 27002

27.001

A.10.4 Proteção contra códigos maliciosos e códigos móveis

Objetivo: Proteger a integridade do *software* e da informação.

A.10.4.1	Controle contra códigos maliciosos	*Controle* Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

27.002

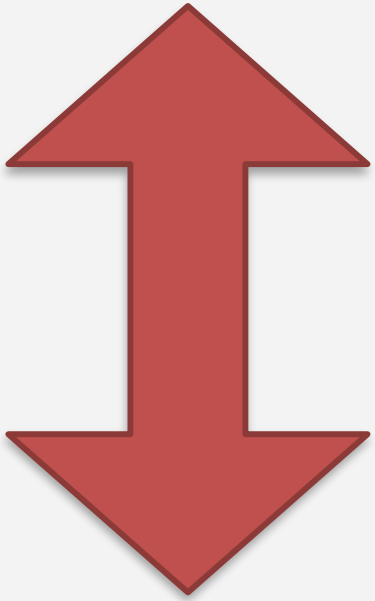
10.4 Proteção contra códigos maliciosos e códigos móveis

Objetivo: Proteger a integridade do *software* e da informação.

Precauções são requeridas para prevenir e detectar a introdução de códigos maliciosos e códigos móveis não autorizados.

Os recursos de processamento da informação e os *softwares* são vulneráveis à introdução de código malicioso, tais como vírus de computador, *worms* de rede, cavalos de Tróia e bombas lógicas. Convém que os usuários estejam conscientes dos perigos do código malicioso. Convém que os gestores, onde apropriado, implantem controles para prevenir, detectar e remover código malicioso e controlar códigos móveis.

Anexo A da 27.001



Artigos da 27.002

27.001

A.10.4 Proteção contra códigos maliciosos e códigos móveis

Objetivo: Proteger a integridade do *software* e da informação.

A.10.4.1	Controle contra códigos maliciosos	*Controle* Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

27.002

10.4 Proteção contra códigos maliciosos e códigos móveis

Objetivo: Proteger a integridade do *software* e da informação.

Precauções são requeridas para prevenir e detectar a introdução de códigos maliciosos e códigos móveis não autorizados.

Os recursos de processamento da informação e os *softwares* são vulneráveis à introdução de código malicioso, tais como vírus de computador, *worms* de rede, cavalos de Tróia e bombas lógicas. Convém que os usuários estejam conscientes dos perigos do código malicioso. Convém que os gestores, onde apropriado, implantem controles para prevenir, detectar e remover código malicioso e controlar códigos móveis.

A.10.4 Proteção contra códigos maliciosos e códigos móveis

27.001

Objetivo: Proteger a integridade do *software* e da informação.

A.10.4.1	Controle contra códigos maliciosos	*Controle* Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

10.4 Proteção contra códigos maliciosos e códigos móveis

Objetivo: Proteger a integridade do *software* e da informação.

Precauções são requeridas para prevenir e detectar a introdução de códigos maliciosos e códigos móveis não autorizados.

Os recursos de processamento da informação e os *softwares* são vulneráveis à introdução de código malicioso, tais como vírus de computador, *worms* de rede, cavalos de Tróia e bombas lógicas. Convém que os usuários estejam conscientes dos perigos do código malicioso. Convém que os gestores, onde apropriado, implantem controles para prevenir, detectar e remover código malicioso e controlar códigos móveis.

10.4.1 Controles contra códigos maliciosos

Controle

Convém que sejam implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

Diretrizes para implementação

Convém que a proteção contra códigos maliciosos seja baseada em *softwares* de detecção de códigos maliciosos e reparo, na conscientização da segurança da informação, no controle de acesso adequado e nos controles de gerenciamento de mudanças. Convém que as seguintes diretrizes sejam consideradas:

27.002

a) estabelecer uma política formal proibindo o uso [illegible] autorizad[illegible] 15[illegible]

b) estabelecer uma política formal para proteção c[illegible]ra os r[illegible]cos asso[illegible]dos [illegible]r[illegible]a im[illegible]rtaçã[illegible]de arquivos e *softwares*, seja de redes externas, [illegible]por qual[illegible]er outro m[illegible], im[illegible]ca[illegible]o q[illegible]s m[illegible]didas preventivas devem ser adotadas;

A.10.4 Proteção contra códigos maliciosos e códigos móveis

27.001

Objetivo: Proteger a integridade do *software* e da informação.

A.10.4.1	Controle contra códigos maliciosos	*Controle* Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

10.4 Proteção contra códigos maliciosos e códigos móveis

Objetivo: Proteger a integridade do *software* e da informação.

Precauções são requeridas para prevenir e detectar a introdução de códigos maliciosos e códigos móveis não autorizados.

Os recursos de processamento da informação e os *softwares* são vulneráveis à introdução de código malicioso, tais como vírus de computador, *worms* de rede, cavalos de Tróia e bombas lógicas. Convém que os usuários estejam conscientes dos perigos do código malicioso. Convém que os gestores, onde apropriado, implantem controles para prevenir, detectar e remover código malicioso e controlar códigos móveis.

10.4.1 Controles contra códigos maliciosos

Controle

Convém que sejam implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

Diretrizes para implementação

Convém que a proteção contra códigos maliciosos seja baseada em *softwares* de detecção de códigos maliciosos e reparo, na conscientização da segurança da informação, no controle de acesso adequado e nos controles de gerenciamento de mudanças. Convém que as seguintes diretrizes sejam consideradas:

a) estabelecer uma política formal proibindo o uso [illegible] utorizad[illegible] 15[illegible]

b) estabelecer uma política formal para proteção c[illegible]ra os r[illegible]cos asso[illegible]dos [illegible]r[illegible]a im[illegible]rtaçã[illegible]de arquivos e *softwares*, seja de redes externas, [illegible]por qual[illegible]er outro m[illegible], in[illegible]ca[illegible]o q[illegible]s m[illegible]didas preventivas devem ser adotadas;

27.002

27.001

A.10.4 Proteção contra códigos maliciosos e códigos móveis

Objetivo: Proteger a integridade do *software* e da informação.

A.10.4.1	Controle contra códigos maliciosos	*Controle* Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

27.002

10.4.1 Controles contra códigos maliciosos

Controle

Convém que sejam implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

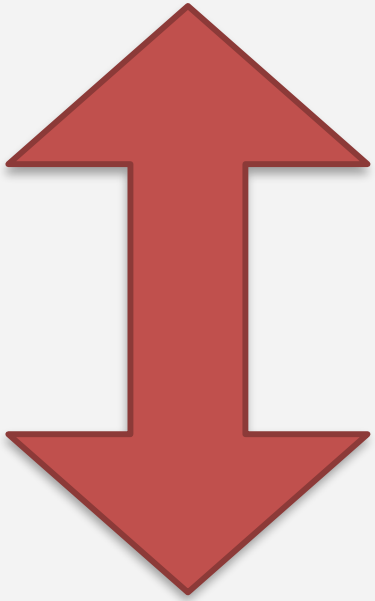
Diretrizes para implementação

Convém que a proteção contra códigos maliciosos seja baseada em *softwares* de detecção de códigos maliciosos e reparo, na conscientização da segurança da informação, no controle de acesso adequado e nos controles de gerenciamento de mudanças. Convém que as seguintes diretrizes sejam consideradas:

a) estabelecer uma política formal proibindo o uso de *softwares* não autorizados (ver 15.1.2);

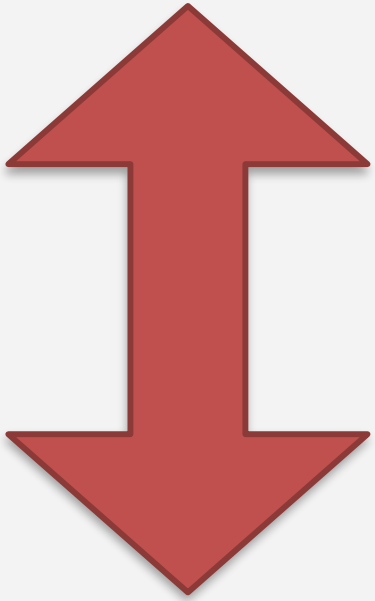
b) estabelecer uma política formal para proteção contra os riscos associados com a importação de arquivos e *softwares*, seja de redes externas, ou por qualquer outro meio, indicando quais medidas preventivas devem ser adotadas;

27.001: **DEVE**



27.002: **CONVÉM**

27.001: **DEVE**



27.002: **CONVÉM**

27.001

A.10.4 Proteção contra códigos maliciosos e códigos móveis

Objetivo: Proteger a integridade do *software* e da informação.

A.10.4.1	Controle contra códigos maliciosos	*Controle* Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

27.002

10.4.1 Controles contra códigos maliciosos

Controle

Convém que sejam implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

Diretrizes para implementação

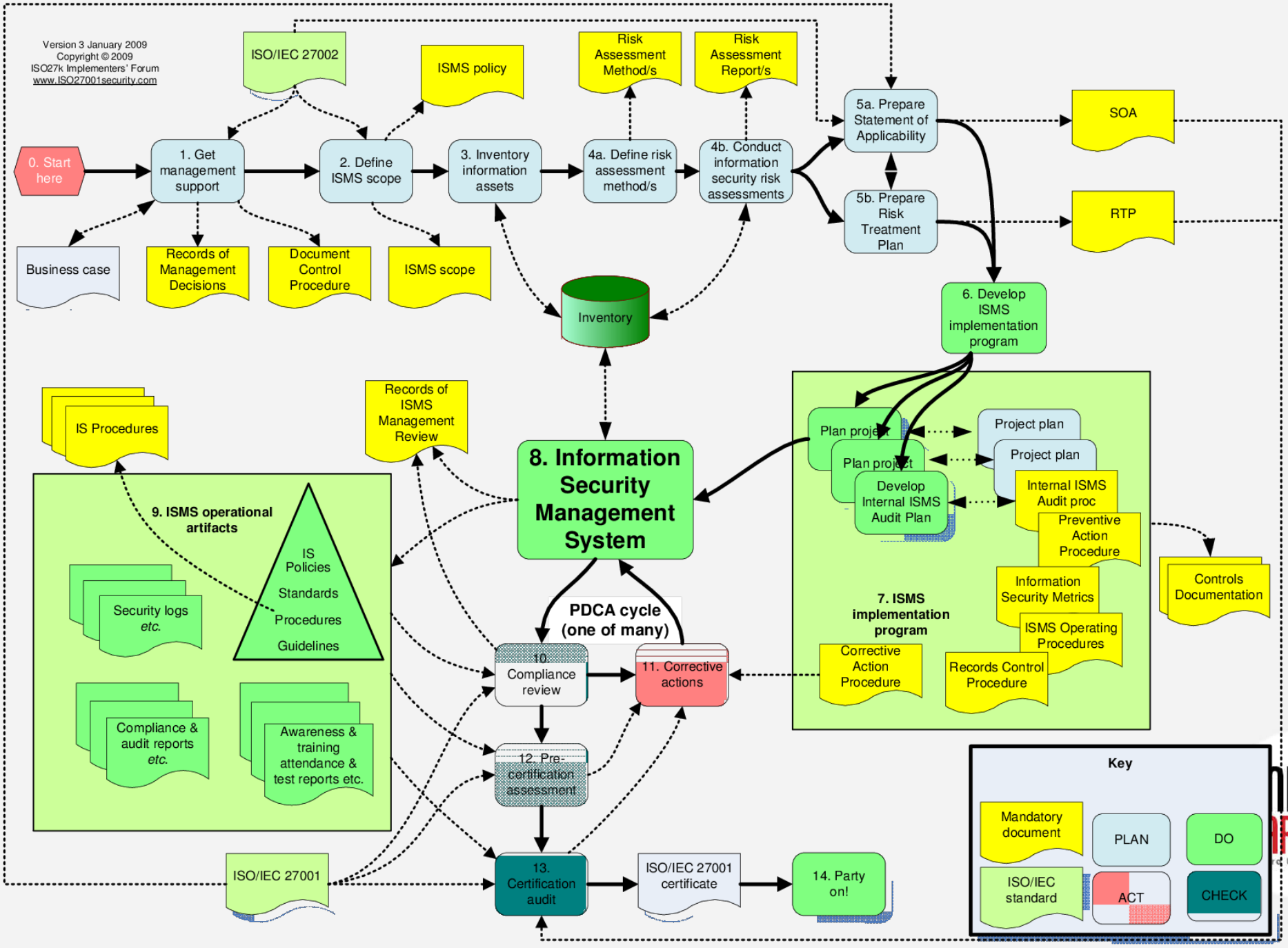
Convém que a proteção contra códigos maliciosos seja baseada em *softwares* de detecção de códigos maliciosos e reparo, na conscientização da segurança da informação, no controle de acesso adequado e nos controles de gerenciamento de mudanças. Convém que as seguintes diretrizes sejam consideradas:

a) estabelecer uma política formal proibindo o uso de *softwares* não autorizados (ver 15.1.2);

b) estabelecer uma política formal para proteção contra os riscos associados com a importação de arquivos e *softwares*, seja de redes externas, ou por qualquer outro meio, indicando quais medidas preventivas devem ser adotadas;

SGSI

SGSI


Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com
ISO/IEC 27002
ISMS policy
Risk Assessment Method/s
Risk Assessment Report/s
0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4a. Define risk assessment method/s
4b. Conduct information security risk assessments
5a. Prepare Statement of Applicability
5b. Prepare Risk Treatment Plan
SOA
RTP
Business case
Records of Management Decisions
Document Control Procedure
ISMS scope
Inventory
6. Develop ISMS implementation program
IS Procedures
Records of ISMS Management Review
8. Information Security Management System
9. ISMS operational artifacts
IS Policies
Standards
Procedures
Guidelines
Security logs etc.
Compliance & audit reports etc.
Awareness & training attendance & test reports etc.
PDCA cycle (one of many)
10. Compliance review
11. Corrective actions
12. Pre-certification assessment
13. Certification audit
ISO/IEC 27001
ISO/IEC 27001 certificate
14. Party on!
7. ISMS implementation program
Plan project
Plan project
Develop Internal ISMS Audit Plan
Project plan
Project plan
Internal ISMS Audit proc
Preventive Action Procedure
Information Security Metrics
ISMS Operating Procedures
Records Control Procedure
Corrective Action Procedure
Controls Documentation
Key
Mandatory document
PLAN
DO
ISO/IEC standard
ACT
CHECK

SGSI

Partes Interessadas

Plan

Estabelecimento do Sistema de Gestão

Implementação e Operação do Sistema de Gestão

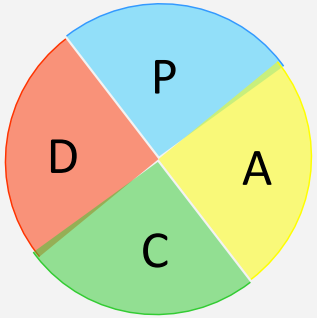
Do

Monitoramento e Análise Crítica do Sistema de Gestão

Check

Manutenção e Melhoria do Sistema de Gestão

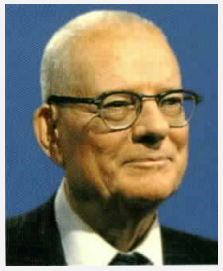
Act



Partes Interessadas

Expectativas e requisitos de segurança da informação

Segurança da informação gerenciada



O QUE É O CICLO PDCA?

O Ciclo PDCA foi idealizado por Shewhart mais tarde aplicado por Demingno uso de estatísticas e métodos de amostragem.

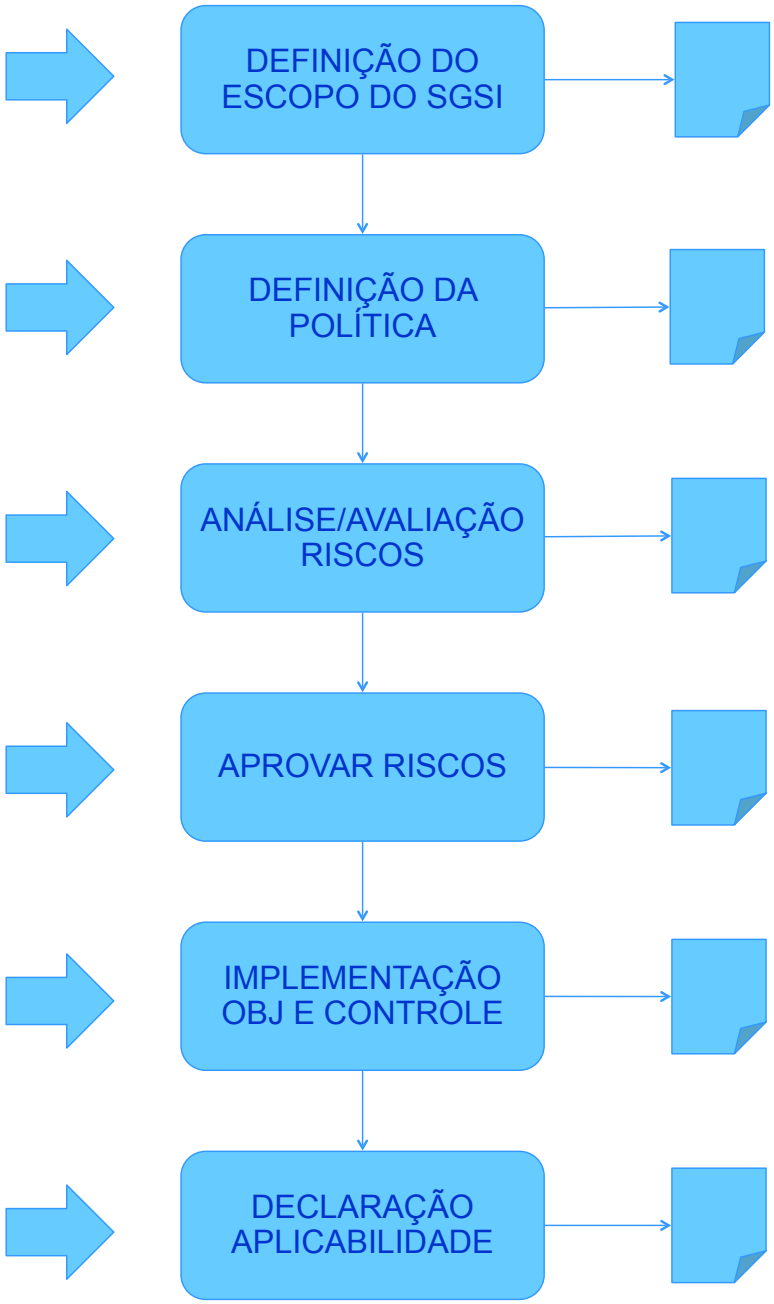
O Ciclo PDCA nasceu no escopo da tecnologia TQC (*Total QualityControl) como uma ferramenta que melhor representava o ciclo de gerenciamentode uma atividade.*

Carioca Centro Universitário

Implementação o SGSI

INPUTS

- Estabelecendo os limites de cobertura e proteção
- Diretrizes da Organização
- Ameaças, vulnerabilidades e impactos
- Abordagem do risco
- Anexo A da ISO 27001
- Justificativa da aplicação dos controles do Anexo A



OUTPUTS

- Documento de Escopo do SGSI
- Documento da Política de Segurança da Informação
- Rel An e Avaliação de Riscos
- Nível de risco aceitável definido e aprovado
- Plano de Tratamento de Riscos
- Declaração de Aplicabilidade

EXERCÍCIO

EXERCÍCIO

Sua equipe foi contratada para apresentar ao Diretor Presidente de um estabelecimento de ensino sobre a implantação do Sistema de Gestão de Segurança da Informação.

Este estabelecimento de ensino possui cursos online ministrados na modalidade EaD. A solução adotada para prover esta modalidade de ensino é o **Moodle**.

EXERCÍCIO

Este estabelecimento de ensino possui a seguinte infraestrutura:

- 02 (dois) laboratórios de 30 (trinta) computadores utilizados pelos alunos;

- 10 (dez) computadores utilizados pela área administrativa que contemplam todos os funcionários que não são professores;

- 30 (trinta) equipamentos que são itens pessoas dos professores. O estabelecimento incentiva o BYOD. Estes equipamentos correspondem a smartphones, tablets e laptops;

EXERCÍCIO

Este estabelecimento de ensino possui a seguinte infraestrutura (continuação):

- (01) uma rede cabeada ethernet cat 6;

- (02) duas redes wifi, sendo uma utilizada pelos alunos e professores e outra sendo utilizada apenas pelos professores e alunos;

- O estabelecimento de ensino possui uma sala de servidores com:

    - (05) computadores que compõe: servidor web, servidor de banco de dados, servidor moodle, servidor de arquivos e um servidor de backup que possui numa solução de storage.

    - Acesso de internet de alta velocidade de um provedor externo.

EXERCÍCIO

Considerando o escopo escolhido e a sua equipe, preencha e apresente e declaração de aplicabilidade.