UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Segurança da Informação
Aula 10 – SGSI – ISO 27001 e 27002

Prof. Dr. Eng. Fred Sauer

http://www.fredsauer.com.br

fsauer@gmail.com

Ciclo PDCA

ABNT NBR ISO/IEC 27001:2013

Partes Interessadas

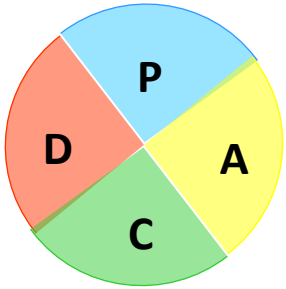
Partes Interessadas

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

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.

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 (SOA*) – Caso algum controle não seja aplicável
- ✓ Obter autorização para implantar o SGSI
- ✓ Formular um plano de ação

***SOA – Statement of Applicability**

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

- ✓ Monitorar 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 NBR ISO/IEC 27001:2013

- “Sistemas de gestão de segurança da informação – Requisitos”
  - Especifica uma série de processos voltados para garantir a 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**
  - **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**

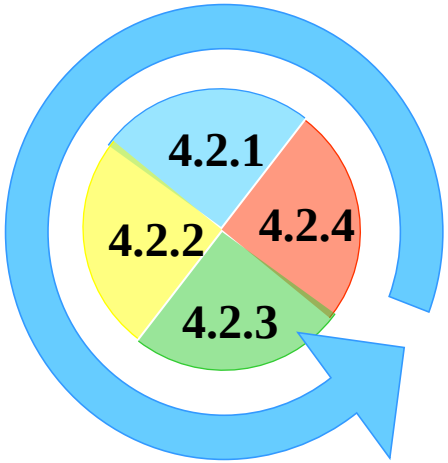
ABNT NBR ISO/IEC 27001:2013

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)



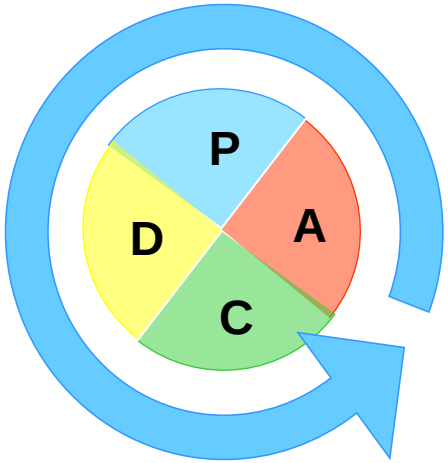
4.3. REQUISITOS DE DOCUMENTAÇÃO

- 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)

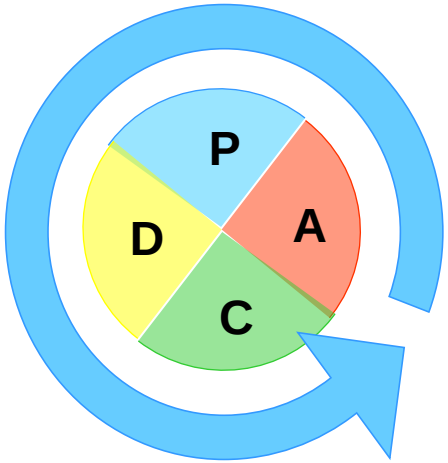
7. ANÁLISE CRÍTICA DO SGSI PELA DIREÇÃO (A)

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

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Situação atual dos certificados no mundo (seleção)

Total DEZ/2017: 39501
Japão: 9161
USA: 1517
Brasil: 170 (maior na América do Sul)
Bélgica: 127
Portugal: 112

ISO/IEC 27001 - Information Technology - Security Techniques Information Security Management Systems - Requirements

Number of certificates per country for 2017

Total	39501
Argentina	57
Australia	404
Austria	146
Belgium	127
Brazil	170
Canada	276
Chile	64
China	5069
Colombia	148
Ecuador	8
France	342
Germany	1339
Hong Kong	182
Hungary	472
India	3272
Indonesia	222
Ireland	209
Israel	345
Italy	958
Japan	9161
orea (Democratic People's Republic o	2
Korea (Republic of)	369
Lithuania	85
Mexico	315
Netherlands	913
New Zealand	28
Nigeria	54
Paraguay	2
Peru	43
Poland	705
Portugal	112
Romania	440
Russian Federation	78
Saudi Arabia	69
Serbia	133
Singapore	123
Slovakia	173
South Africa	69
Spain	803
Sweden	148
Switzerland	171
Taiwan, Province of China	994
Thailand	287
Kingdom of Great Britain and Norther	4503
United States of America	1517
Uruguay	31
Venezuela (Bolivarian Republic of)	4
Viet Nam	198

ABNT NBR ISO/IEC 27001:2013

- **Algumas empresas certificadas no Brasil**
  - Banco Matone S.A.
  - CIP Câmara Interbancária de Pagamentos
  - Fucapi – Fundação Centro de Análise
  - Módulo Security Solutions S.A.
  - Promon Engenharia LTDA
  - Promon Tecnologia LTDA
  - SAMARCO Mineração LTDA
  - Serasa, São Paulo
  - SERPRO
  - Telefonica Empresas S.A.
  - UNISYS

ABNT NBR ISO/IEC 27002:2013

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

- Entidades.
  - ISO: International Organization for Standardization
  - IEC: International Engineering Consortium
  - ABNT: Associação Brasileira de Normas Técnicas
  - BSI: British Standards Institution

ABNT NBR ISO/IEC 27002:2013

- Estrutura da Norma

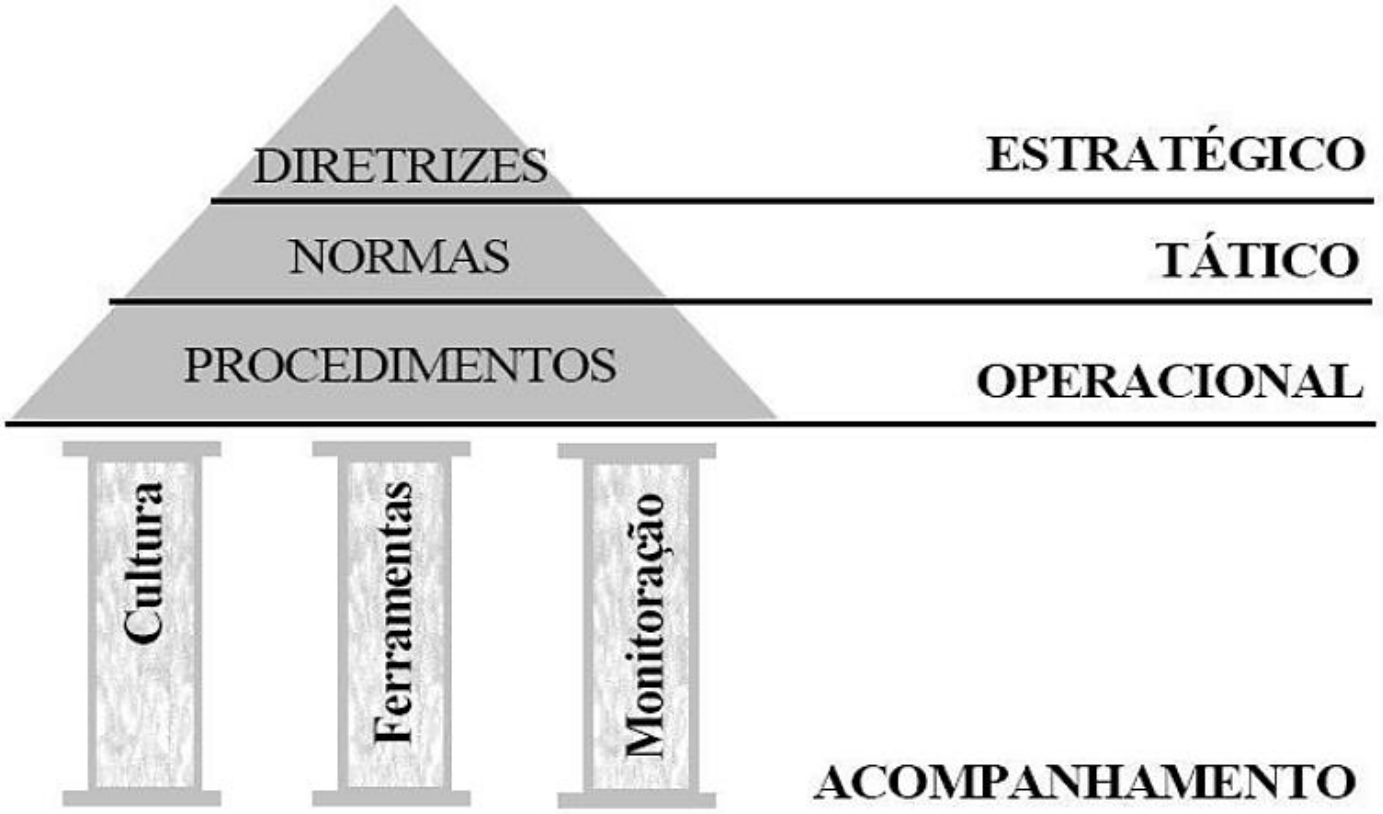
  - Objetivo do controle
  - Controle
  - Diretrizes para implementação
  - Informações adicionais

- Principal característica: **“CONVÉM”**.

ABNT NBR ISO/IEC 27002:2013

- **Organização**
  - **0. INTRODUÇÃO**
  - **1. OBJETIVO**
  - **2. TERMOS E DEFINIÇÕES**
  - **3. ESTRUTURA DA NORMA**
  - **4. ANÁLISE E AVALIAÇÃO 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 DE INFORMAÇÃO**
  - **13. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**
  - **14. GESTÃO DA CONTINUIDADE DO NEGÓCIO**
  - **15. CONFORMIDADE**

Documentos da PSI



Diretrizes

- Fundamentos estratégicos da organização.
- Correspondem a todos os ***valores*** que devem ser seguidos para que o principal patrimônio da empresa, que são as informações, tenha o nível de segurança exigido.

Normas

- ***Regras gerais da segurança*** das informações que devem ser usadas por todos os ***segmentos envolvidos*** nos processos de negócio da instituição.
- Por estarem em um nível tático (desdobramento da estratégia), podem ser específicas para o público a que se destinam.
  - Normas de segurança para técnicos
  - Normas de segurança para usuários

Procedimentos

- Orientações para realizar ***atividades operacionais*** relacionadas a segurança.
- Estas atividades operacionais envolvem procedimentos ***passo a passo*** que são detalhados, permitindo que sua execução seja padronizada, garantindo a observação de aspectos de segurança.

Exemplo: Documentos FINAIS

- ***Portaria - Comissão de Segurança***
  Portaria - Grupo de Segurança
- ***Política de Segurança da rede interna;***
- ***Norma de Segurança para a rede interna;***
- ***Norma para Utilização de Recursos Computacionais;***
- ***Norma para Uso de Correio Eletrônico;***
- ***Norma para Computadores Pessoais;***
- ***Norma de Uso de Serviços de Acesso Discado;***
- ***Norma de Uso de Serviços SSH;***
- ***Norma de Uso de Serviços Telnet;***
- ***Norma de Uso de Serviços FTP;***

- ***Norma para Utilização de Rede;***
- ***Norma de Contingência;***
- ***Norma para Uso do DNS;***
- ***Norma para Uso de Serviços e Servidores WWW;***
- ***Técnicas para Pontuação dos Ativos rede interna;***
- ***Formulário para Estabelecer Criticidade dos Ativos;***
- ***Norma para Estruturação dos Ativos;***
- ***Padrão para Criação de Documentos;***
- ***Terminologia e Glossário para a Política de Segurança;***

Fixação

- A manutenção e melhoria de um SGSI é feita na fase **Act** do ciclo de vida. Já a elaboração de uma Análise de Riscos é feita na fase **Plan**. Uma Auditoria, por sua vez, seria feita na fase **Check**.
- Enquanto na ISO 27001 a palavra-chave é **"Deve"**, na ISO 27002 a palavra é **"Convém"**. Os controles da ISO 27002 são boas práticas, e devem ser ajustados, quando necessários, à realidade da empresa. Caso algum controle não seja implementado, a empresa deverá elaborar um **"SOA"** justificando a ausência do controle.
- Uma Política é dividida em **Diretrizes**, **Normas** e **Procedimentos**, respectivamente direcionados aos setores **Estratégico**, **Tático** e **Operacional** da corporação.