UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Segurança Estratégica da Informação
ISO 27001, 27002 e 27005
Primeira Aula: ISO 27001

Prof. Dr. Eng. Fred Sauer

fsauer@gmail.com

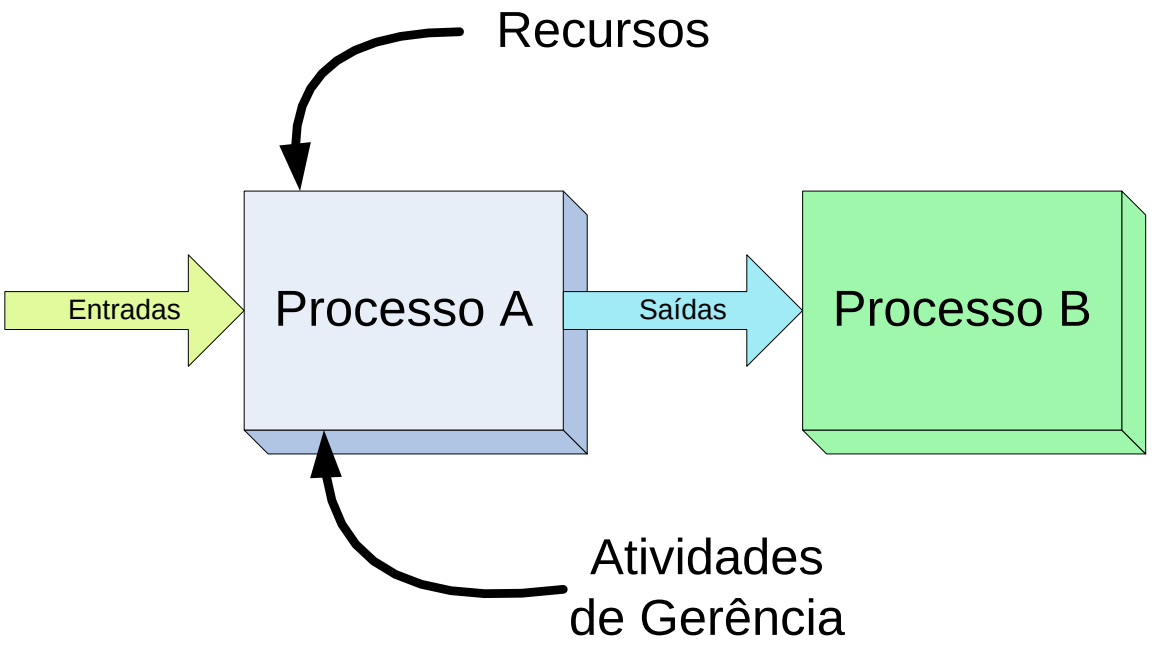
http://www.fredsauer.com.br

Documentos Normativos Básicos

- ISO 27001:2006 – SGSI (Sistemas de Gestão da Seginfo)
- ISO 27002:2007 – Boas práticas de Gestão da Segurança da Informação
- ISO 27005:2008 – Gestão de Risco em SegInfo

ISO 27001 - SGSI

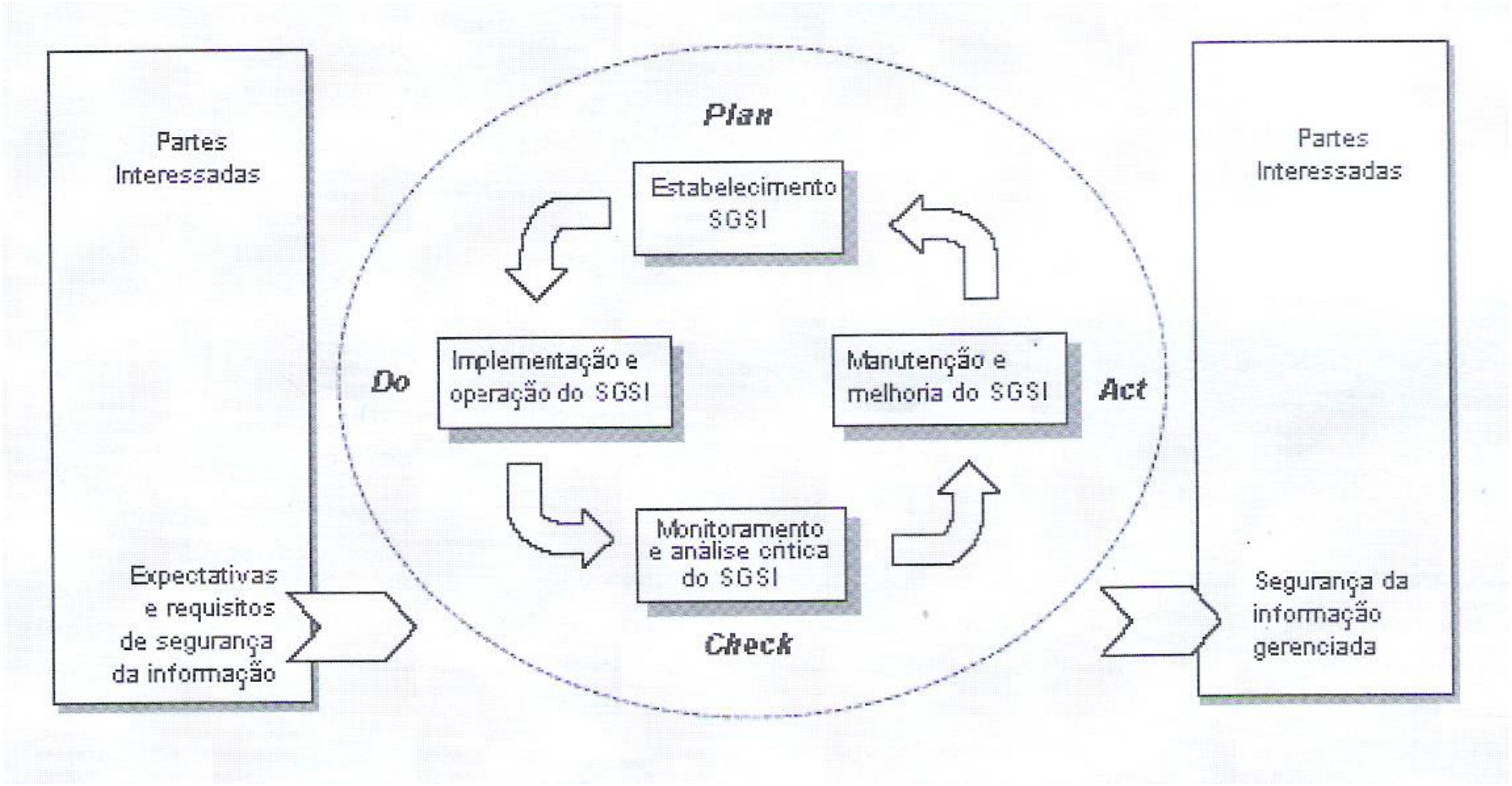
- Abordagem de Processo
- Estabelecer → Implementar → Operar → Monitorar → Analisar Criticamente → Manter → Melhorar



Abordagem de Processo

- Requisitos plenamente compreendidos
- Estabelecimento de uma Política de Segurança
- Controles para Gerência de Riscos ao Negócio
- Melhoria contínua baseada em medições efetivas e auditorias

PDCA – Estrutura dos Processos do SGSI



Exemplos de Entradas

- Requisitos
  - "*Incidentes de SegInfo não devem comprometer significativamente a situação financeira nem a imagem da corporação*"
- Expectativas
  - "*Se um incidente ocorrer, deve haver uma equipe de resposta à Incidentes pronta e apta a minimizar os impactos decorrentes*"

PDCA - Objetivos

- *Plan* – Elaboração do PDS
  - Política, objetivos, processos e procedimentos do SGSI
  - Foco na Gestão do nível de risco
  - Atendimento das políticas e objetivos globais da organização

PDCA - Objetivos

- Do – Implementar e Operar
  - Política
  - Controles
  - Processos
  - Procedimentos

PDCA - Objetivos

- Check – Avaliar e Mensurar desempenho
  - Métrica – política e objetivos dos controles
  - Resultados criticamente analisados pela Direção
- Act – Ações de Correção e Prevenção
  - Orientação por resultados
  - Reação por informações de impropriedade do SGSI com os objetivos e expectativas definidos

Requisitos de um SGSI

- Assegurar a seleção de controles adequados à proteção dos ativos da informação
- Termos relevantes:
  - **Ativo**
  - **Atributos da Informação**
  - **Atributos Adicionais**
  - **Evento de SegInfo**
  - **Incidente de SegInfo**
  - **Declaração de Aplicabilidade**

Ativo

- Elemento de valor para a organização
  - Físicos
  - Tecnológicos
  - Humanos
  - Informação !!!!

Atributos da Informação

- Disponibilidade – Acessível sob demanda por alguém autorizado
- Confidencialidade – Vedar acesso a alguém não-autorizado
- Integridade – Exatidão e completeza da informação

Atributos Adicionais

- Autenticidade - genuinidade da informação, ligada a sua origem
- Responsabilidade – identificação de autoria e credenciamento para criação e modificação
- Não-repúdio – garantia de não negação da criação ou alteração da informação, durante o ciclo de vida da informação
- Confiabilidade – grau de certeza da veracidade e precisão de uma informação
- Legalidade – grau de conformidade da informação com aspectos legais e do negócio

Evento de Seginfo

- Ocorrência identificada de um estado de sistema, serviço ou rede, indicando:
  - **Uma possível violação da política de Segurança** ;
  - **Falha de controles** ; ou
  - **Uma situação previamente desconhecida**, que possa ser relevante para a segurança da informação

Incidente de SegInfo

- **Um ou mais eventos** de segurança indesejados ou inesperados, que tenham uma **grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação**

Aspectos do Risco

- **Risco** – Probabilidade da ocorrência de um Incidente de segurança (Vulnerabilidade + Ameaça) com o impacto decorrente
- Análise de Riscos
  - **Avaliação de Riscos**
  - **Tratamento de Riscos**
  - **Gestão de Riscos**

Análise de Riscos

- Procedimento sistemático para **identificar riscos** e sua **probabilidade de tornar-se um incidente** de SegInfo

Avaliação de Riscos

- **Comparação** dos riscos estimados com parâmetros pré-definidos pela direção para aceitação de riscos

Tratamento de Riscos

- Seleção e implementação de medidas para administrar o nível de risco (**mitigar, manter, evitar, transferir**)
- Após a análise, Riscos residuais devem ser ACEITOS pela Direção

Gestão do Risco

- Análise, tratamento, aceitação e comunicação do risco

Características do SGSI

1. Definir Escopo
2. Definir Política que:
   a. Inclua uma Estrutura para SegInfo
   b. Esteja alinhada com o negócio
   c. Estabeleça critérios para avaliação de riscos
   d. Seja aprovada pela Direção
3. Definir abordagem de análise/avaliação de riscos
4. Identificar/analisar/avaliar/tratar riscos

Características do SGSI (cont)

5. Selecionar Objetivos de Controles e Controles
6. Obter aceitação da Direção para os riscos residuais
7. Obter aprovação da Direção para operar o SGSI
8. Elaborar a Declaração de Aplicabilidade

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

QUESTÃO 35

Julgue os itens a seguir acerca dos conceitos de segurança de informação.

I Uma solução de proteção adequada é aquela que combina o máximo de confidencialidade com o mínimo de disponibilidade.

II A gerência de riscos qualitativa é, em geral, mais fácil de ser implantada, quando comparada a uma gerência de riscos quantitativa.

III A estimativa de riscos de segurança para um ativo independe da existência de ameaças sobre o ativo.

IV A seleção de salvaguardas ou controles possui uma relação mais direta com os riscos de segurança sobre os ativos do que com as vulnerabilidades sobre os ativos.

V O objetivo principal de um ataque do tipo negação de serviço é a redução da integridade de um sistema de informação.

Estão certos apenas os itens

Falsa

Certa

Falsa

Certa

Falsa

Ⓐ I e III.
Ⓑ II e IV.
Ⓒ III e V.
Ⓓ IV e V.

Certa Letra B

Respostas

- I – Não. A proteção dos ativos quanto a sensibilidade CID deve ser feita de acordo com o nível de risco admissível
- II – Certo. A avaliação quantitativa depende de métricas mais precisas, que prescindem de um profundo conhecimento do negócio
- III – Errado. Os riscos são diretamente proporcionais às ameaças, vulnerabilidades e Impactos, e inversamente proporcional aos mecanismos usados para mitigar o risco
- IV – Certo, porque além das vulnerabilidades, as ameaças e os impactos também entram na escolha dos controles
- V – Errado, é a redução ou eliminação da disponibilidade

Exercícios

68

Muitas empresas cometem erros ao lidar com as questões da segurança da informação. Para que o negócio não seja impactado negativamente com esse aspecto, é importante

(A) posicionar a equipe de segurança da informação abaixo da diretoria de TI. — Falsa

(B) adotar ferramentas pontuais como medida paliativa de segurança. — Falsa

(C) elaborar ações de segurança que priorizem a reatividade. — Falsa

(D) eleger a área de TI como responsável pela segurança da informação corporativa. — Falsa

(E) investir em segurança e tratá-la como um processo contínuo. — Certa

Respostas

- A – Incorreta – O CGSI deve estar diretamente ligado à Direção Executiva (estratégico)
- B – Incorreta – São necessárias ações globais, holísticas
- C – Incorreta. A melhor ação é proativa
- D – Incorreta – Um CGSI é o mais indicado
- E – Correta – Com orientação a um PDCA

Próximo Tópico

- Norma 27002 – Controles (Boas Práticas)