Segurança e Auditoria

Professor: Rodrigo Rocha

Professor

- Nome
  - Rodrigo R B Santana
- Formação Acadêmica
  - Bacharel em SI (FIR)
    - Ênfase: Engenharia de Software
  - Mestre em Ciência da Computação (UFPE)
    - Ênfase em Gestão de TI.
- E-mail:
  - rsantana4@unifavip.edu.br

PORTAL DEVRYONE

- Plano de Ensino
- Ementa
- Cronograma
- Atividades Independentes
- Metodologia de Avaliação
- Aulas
- Consultas de Faltas e Notas

Pontos importantes

- Horário das aulas
- Faltas
- Intervalo
- Tempo para entrar durante a prova
- Ausência de nome na ata de prova
- A nota do ENADE fica no histórico do aluno
- Celular embaixo da banca
- Pontuação extra

Sistema de Avaliação

- **AP1: Prova Escrita (30%)**
  - Prova abordando os assuntos vistos em sala de aula até a data da mesma.
- **AP2: Projeto (30%)**
  - Documento
  - Apresentação
  - Perguntas
- **AP3: Prova Escrita (40%) (Elaborada pelo sistema)**
- **Média para aprovação: 5,0 no mínimo**

Introdução a Segurança da Informação

Introdução Segurança a informação Agenda

- **Introdução a Segurança da Informação:**

- • Ativo de Informação
- • Ameaça
- • Vulnerabilidade
- • Incidente
- • Probabilidade
- • Impacto
- • Risco
- • Incidente

- **Como implementar um sistemas de informação seguro?**

Ativo de Informação

- **A informação**

  - Elemento essencial para todos os processos de negocio da organização, sendo, portanto, um bem ou ativo de grande valor.

Propriedades de Segurança da Informação

- A segurança da informação é garantida pela preservação de três aspectos essenciais (CID):

- • Confidencialidade
- • Integridade
- • Disponibilidade

Confidencialidade

- **O que é?**

  - O principio da confidencialidade é respeitado quando apenas as pessoas explicitamente autorizadas podem ter acesso a informação.

Integridade

- **O que é?**

  - O principio da integridade é respeitado quando a informação acessada está completa, sem alterações e, portanto, confiável.

Disponibilidade

- **O que é?**

  - O principio da disponibilidade é respeitado quando a informação está acessível, por pessoas autorizadas, sempre que necessário.

Vulnerabilidade

- **O que é?**

  - São as fraquezas presentes nos ativos de informação, que podem causar, intencionalmente ou não, a quebra de um ou mais dos três princípios de segurança da informação:

    - Confidencialidade
    - Integridade
    - Disponibilidade

Ameaça

- **O que é?**

  - É um agente externo ao ativo de informação, que aproveitando-se das vulnerabilidade deste ativo, poderá quebrar a confidencialidade, integridade ou disponibilidade da informação suportada ou utilizada por este ativo.

Probabilidade

- **O que é?**

  - A probabilidade é a chance de uma falha de segurança ocorrer levando-se em conta o grau das vulnerabilidades presentes nos ativos que sustentam o negocio e o grau das ameaças que possam explorar estas vulnerabilidades.

Impacto

- **O que é?**

  - O impacto de um incidente são as potenciais consequências que este incidente possa causar ao negocio da organização.

Risco

- **O que é?**

  - O risco é a relação entre a probabilidade e o impacto.

  - É a base para a identificação dos pontos que demandam por investimentos em segurança da informação.

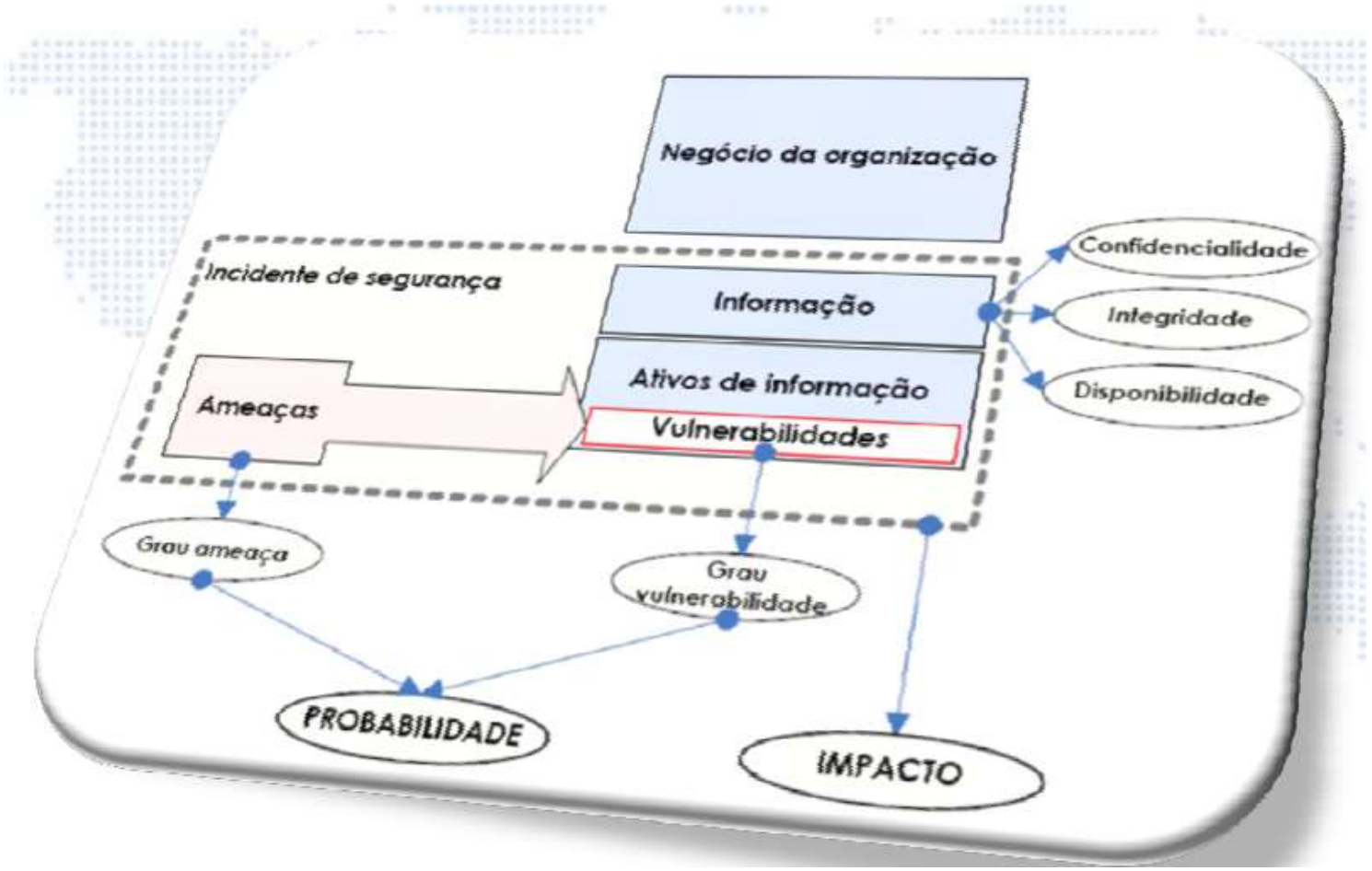
Incidente

- **O que é?**

  - Quando uma ameaça explora vulnerabilidade de um ativo de informação, violando uma das suas características de segurança (CID).

  - Este incidente tem uma chance de acontecer, e se acontecer gera um determinado impacto ou prejuízo.

Ilustrando um incidente



COMO IMPLEMENTAR UM SISTEMA DE INFORMAÇÃO SEGURO?

Como implementar um Sistema De Informação Seguro?

- **E agora? Por onde começo?**

  - Conhecer os conceitos sobre segurança da informação não significa necessariamente saber garantir a segurança.

  - Muitos experimentam esta sensação quando elaboram seus planos de segurança e acabam não atingindo os resultados desejados.

Como implementar um Sistema De Informação Seguro?

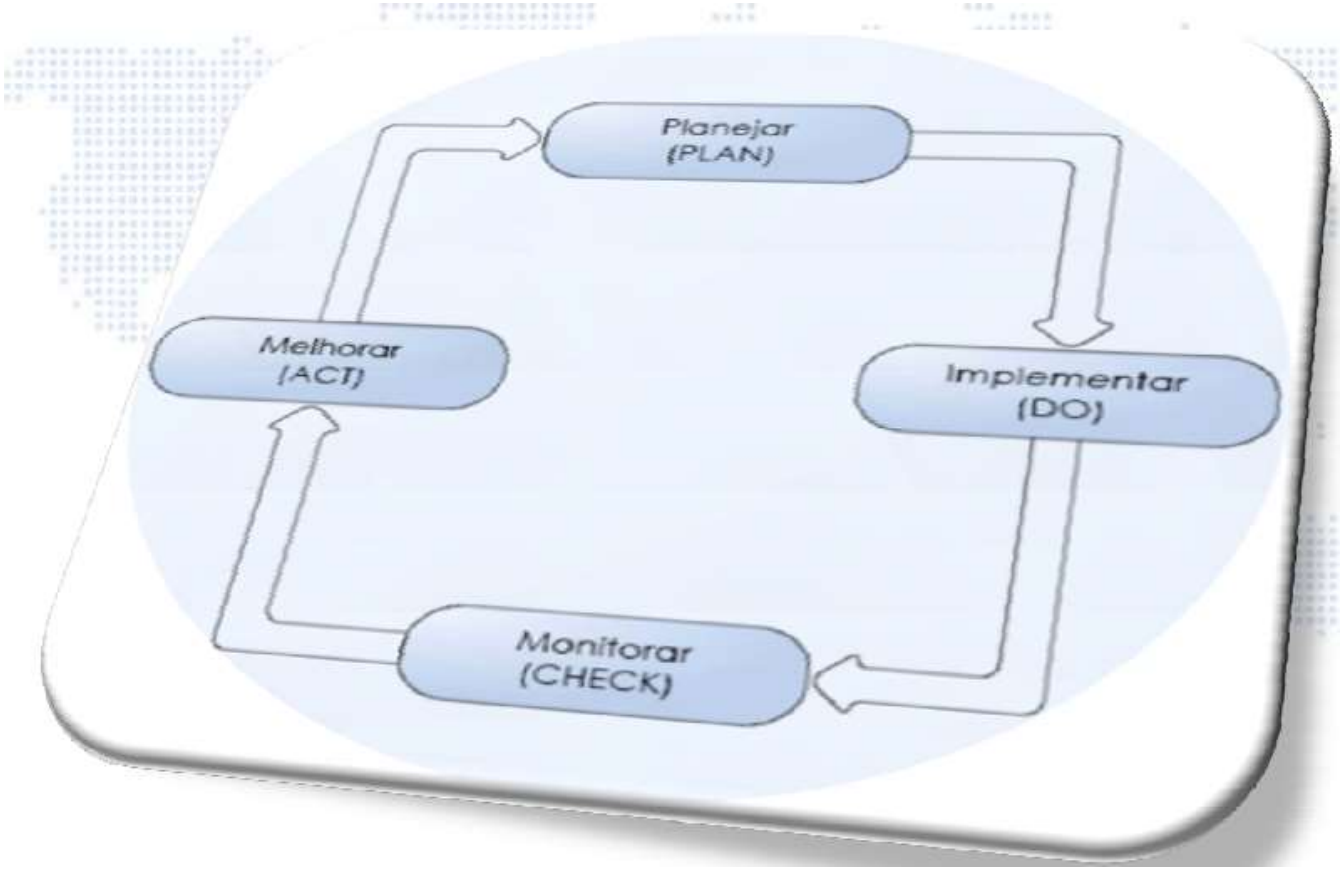
- **O inicio!**

  - A implantação de um sistema de segurança da informação não é uma tarefa trivial.

  - O modelo proposto pela qualidade (família ISO) é o caminho mais adequado para superar esse desafio.

  - Este modelo é baseado no conceito de melhoria continua (PDCA).

Modelo PDCA


Planejar
(PLAN)
Implementar
(DO)
Monitorar
(CHECK)
Melhorar
(ACT)

Como implementar um Sistema De Informação Seguro?

- **Primeira fase: Planejamento (PLAN).**

  - Nesta fase, é definido o escopo e abrangência esperada para o sistema de segurança da informação, e realizada a análise de riscos, e feito o planejamento para o tratamento do risco.

Como implementar um Sistema De Informação Seguro?

- **O que fazer com o risco?**
  - Com o risco já identificado, é importante decidir o que fazer com ele. É possível:
  - • Evitar
  - • Controlar
  - • Transferir
  - • Aceitar

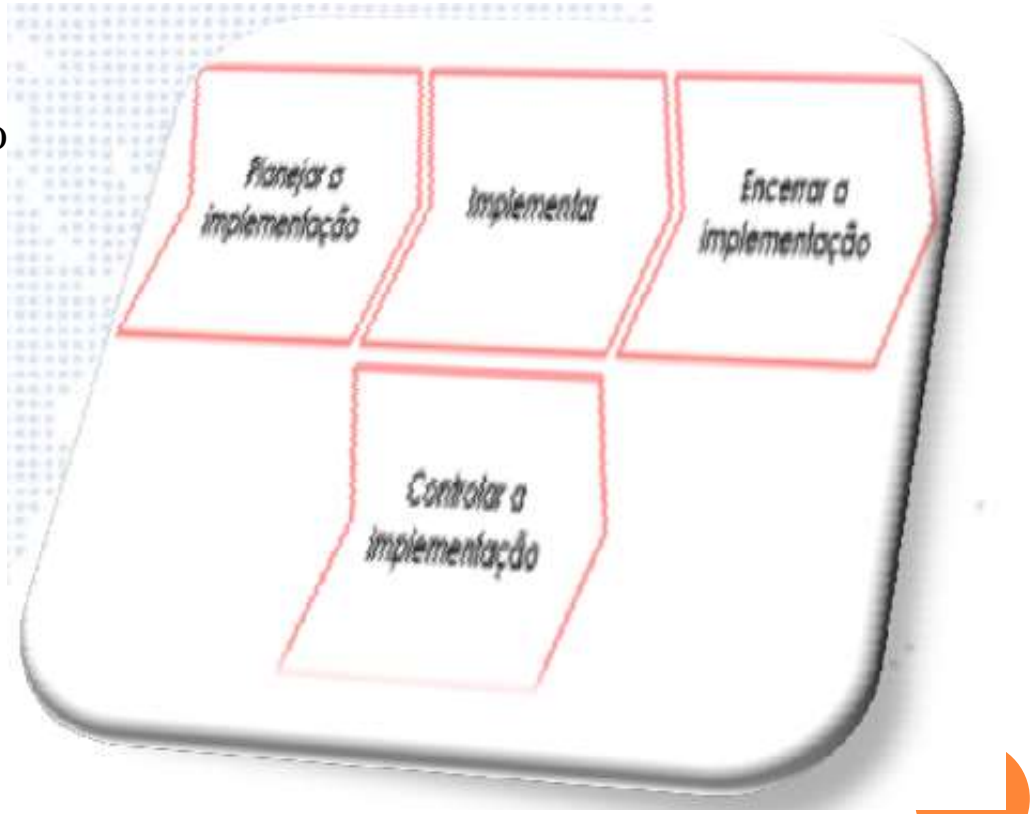
- Isto fica claro na declaração de aplicabilidade!

Como implementar um Sistema De Informação Seguro?

- **Implementando o sistema**

Após a etapa de planejamento, o próximo passo é executar o que foi planejado.

Isto envolve o planejamento da fase de implementação, a execução e o controle da implementação, e por fim, o encerramento da implementação



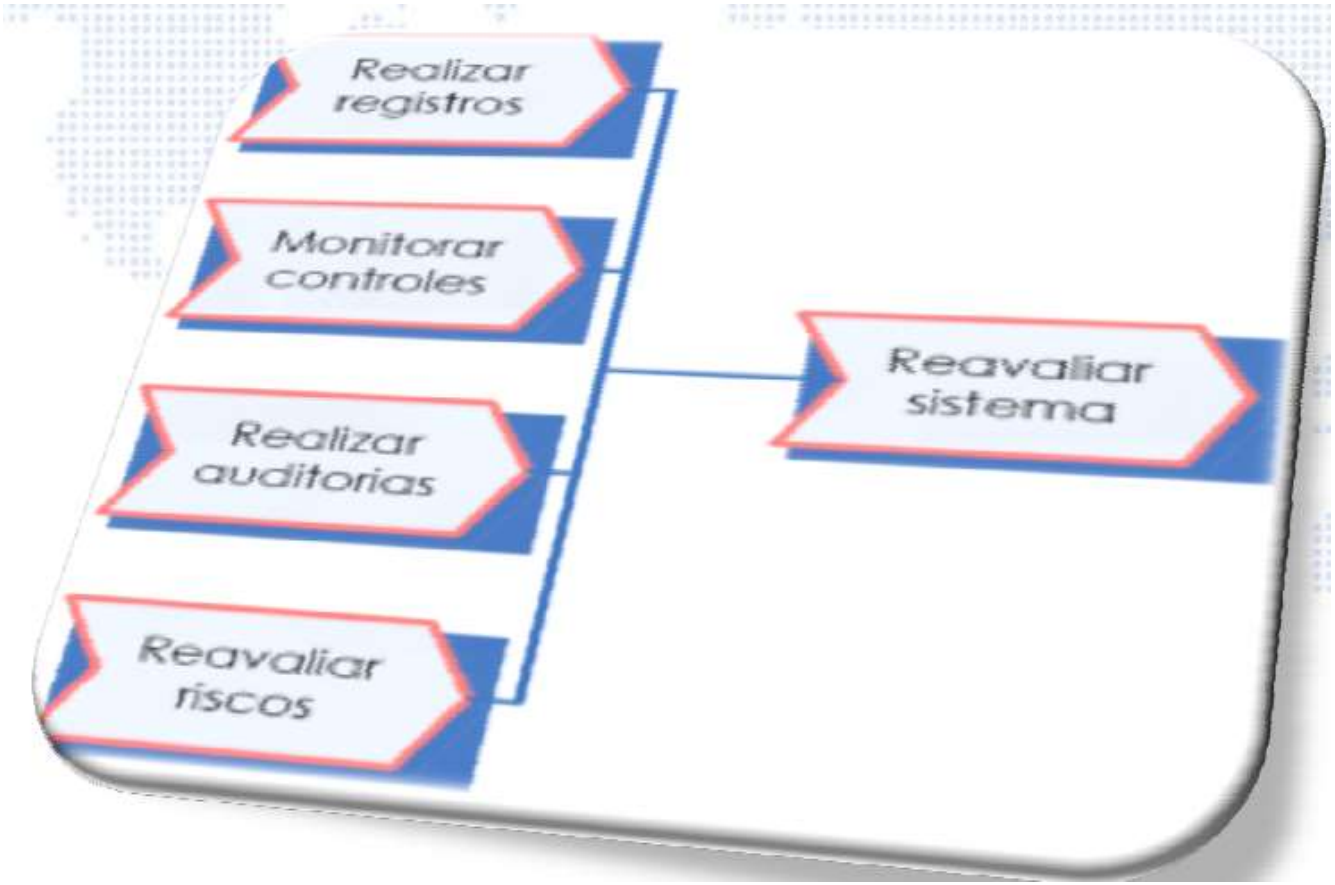
Como implementar um Sistema De Informação Seguro?

- **Monitoramento**

  - O monitoramento ou controle do sistema implica em avaliar sistematicamente se os controles implementados estão atendendo as expectativas originais.

  - Para tanto, os processos a seguir precisam ser executados com regularidade.

Como implementar um Sistema De Informação Seguro?



Controles de Segurança da Informação

- A implementação de um sistema de segurança da informação se dá pela instalação de controles específicos nas mais diversas áreas da organização, sempre pensando nas dimensões de processos, tecnologias, ambiente e pessoas.

- Política (PSI)
- Estrutura organizacional
- Controle de acesso
- Pessoas
- Segurança física
- Segurança lógica
- Desenvolvimento de sistemas
- Continuidade do negócio
- Incidentes de segurança
- Aspectos legais
- Operação de sistemas

Dúvidas... Sugestões...

Dúvidas?

Sugestões?