Sistemas de Informação

PUC Minas

Segurança de Sistemas de Informação

Aula 6: Politicas de Segurança da Informação

Prof. Fábio Leandro Rodrigues Cordeiro.
fabio@pucminas.br

Objetivo da Aula

- Discutir os conceitos e a importância da PSI;
- Compreender a estrutura geral de uma PSI;
- Refletir sobre como implementar uma PSI:
    - destaque para o levantamento de dados da organização

Sumário

- Introdução
- A politica de Segurança da Informação (PSI)
- Documentação da PSI
- Implementação da PSI
- Considerações

Visão Geral

Politica de Segurança da Informação

- A Segurança da Informação “inicia” através da definição de uma política clara e concisa acerca da proteção das informações.

- Através de uma Política de Segurança da Informação, a empresa **formaliza suas estratégias e abordagens para a preservação de seus ativos**.

Visão Geral

Politica de Segurança da Informação

A PSI deve ser compreendida como a **tradução das expectativas da empresa em relação a segurança** considerando o alinhamento com os seus **objetivos de negócio**, **estratégias e cultura**.

Objetivos e Escopo

PSI

- 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 (ISO 17799:2005).

A PSI tem como objetivo elaborar critérios para o adequado:

- manuseio,
- Armazenamento,
- transporte e
- descarte das informações.

Objetivos e Escopo

PSI

- A Política de Segurança é um conjunto de **diretrizes, normas**, **procedimentos e instruções**, destinadas respectivamente aos **níveis estratégico, tático e operacional**, com objetivo de estabelecer, padronizar e normatizar a segurança tanto no **escopo humano como no tecnológico.**

Elaboração de PSI

PSI

- Atividades básicas do desenvolvimento de uma PSI são:
  - Estruturar o Comitê de Segurança;
  - Definir Objetivos;
  - Realizar entrevistas e Verificar a documentação existente;
  - Elaborar o glossário da Política de Segurança;
  - Estabelecer Responsabilidades e Penalidades;
  - Preparar o documento final da PSI;
  - Oficializar a Política da Segurança da Informação;
  - Sensibilizar os colaboradores.

Documentação da PSI

PSI

Algumas das Questões que a PSI deve responder:

- O que significa Segurança da Informação?
- Por que os colaboradores devem se preocupar com segurança?
- Quais são os objetivos estratégicos de Seg. Info.?
- Como é realizada a gestão da Segurança da Informação?
- O que pensa a alta administração?
- Quais são os principais papéis e responsabilidades?
- Quais as penalidades previstas?

Documentação da PSI

PSI

Algumas das Questões que a PSI deve responder:

- O que significa Segurança da Informação?
- Por que os colaboradores devem se preocupar com segurança?
- Quais são os objetivos estratégicos de Seg. Info.?
- Como é realizada a gestão da Segurança da Informação?
- O que pensa a alta administração?
- Quais são os principais papéis e responsabilidades?
- Quais as penalidades previstas?

Documentação da PSI

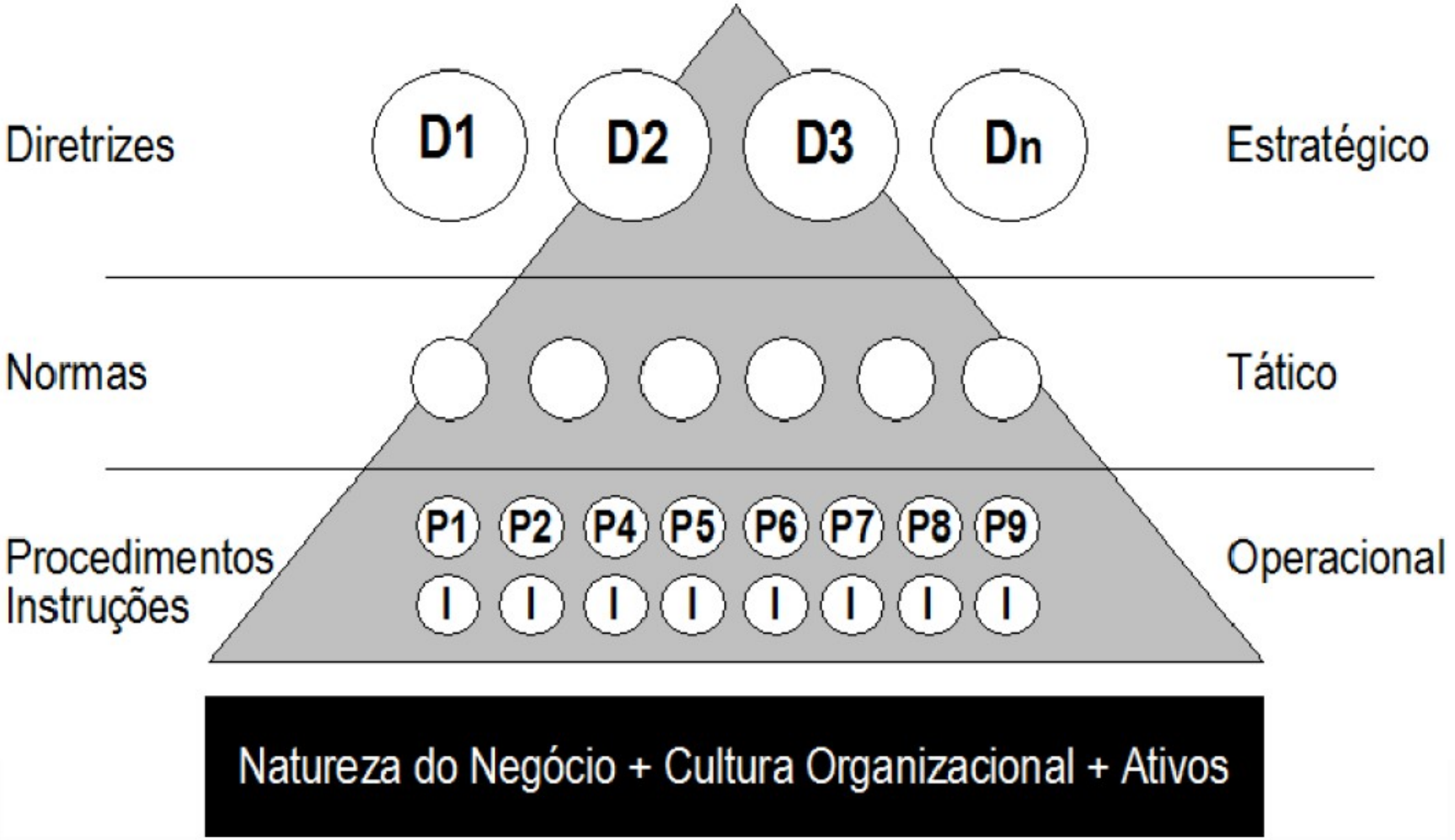
Estrutura PSI

- Um Documento da PSI deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes [**ISO 17799:2005**].

- Uma política de segurança deve ser sustentada por:
  - Diretrizes;
  - Normas;
  - Procedimentos e Instruções.

Documentação da PSI

Estrutura PSI



Documentação da PSI

Estrutura PSI

DIRETRIZES

- Conjunto de **regras gerais de nível estratégico** que tem como base a visão e a missão da empresa;
- Representam as preocupações da empresa sobre a segurança das informações;
- Correspondem a todos os valores que devem ser seguidos para que as informações tenham o nível de segurança exigido.

Documentação da PSI

Estrutura PSI

NORMAS

- Conjunto de **regras gerais segurança** que se aplicam a todos os segmentos envolvidos;
- Geralmente são elaborados com foco em **assuntos mais específicos como**: controle de acesso, uso de Internet, uso do correio eletrônico, acesso físico, instruções sobre senhas e realização de backups etc.
- Deve ser elaborada de forma mais genérica possível.

Documentação da PSI

Estrutura PSI

PROCEDIMENTOS E INSTRUÇÕES

- Conjunto de orientações para realizar atividades e **instruções operacionais** relacionadas a segurança;
- Comandos operacionais a serem executados no momento da realização de um procedimento de segurança;
- É importante que exista uma **estrutura de registro** que esses procedimentos são executados (evidências objetivas).

Documentação da PSI

Saídas

Artefatos (saídas) da Documentação da PSI

- Carta do Presidente;
- Diretrizes de Segurança da Informação;
- Normas Gerais de Segurança da Informação;
- Exemplos de Procedimentos Operacionais e Instruções Técnicas.

Documentação da PSI

Fatores críticos de sucesso

Fatores Críticos de Sucesso

- É necessário que a PSI seja analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia [ISO 17799:2005].

- **Bases de Sustentação:**

    - **Cultura + Recursos Humanos + Monitoramento**

Documentação da PSI

Fatores críticos de sucesso

Fatores Críticos de Sucesso

- A implantação da política de segurança depende de:
  - Uma boa **estratégia de divulgação e treinamento** entre os usuários, clientes e fornecedores;
  - Uma boa forma eficiente de **análise de desempenho da PSI.**

Documentação da PSI

Fatores críticos de sucesso

Fatores Críticos de Sucesso

- Barreiras à implementação da PSI

  - Falta de consciência sobre a importância da PSI;
  - Orçamento reduzido;
  - Falta de Recursos Humanos adequados;
  - Ausência de Ferramentas adequadas.

Documentação da PSI

Fatores críticos de sucesso

Fatores Críticos de Sucesso

- Para que uma PSI seja utilizada com sucesso é necessário que ela seja:

  - **Clara** – escrita com uma linguagem formal e acessível;
  - **Concisa** – não deve conter informações desnecessárias ou redundantes;
  - **Adequada** – com a realidade da empresa;
  - **Atualizada periodicamente** – mudanças no negócio, novas ameaças etc.

Considerações

Resumo

Ao elaborar uma PSI é preciso:

- Entender e definir claramente o processo de desenvolvimento;
- Estabelecer uma forma de obter dados da organização:
  - Negócio + Objetivos + Cultura.
  - O que já existe?
  - O que é necessário desenvolver?
- Definir responsabilidade e penalidades adequadas
- Como será a implementação e o monitoramento?

Referências

Notas de Aula: Prof. Prof. Leonardo Lemes Fagundes.

ISO 27001 Security. Information Security Compliance. 2011.

ABNT NBR ISO/IEC 27002:2006. Código de Prática para a Gestão da Segurança da Informação, 2006.