UNINOVE
Universidade Nove de Julho

PPGI

Disciplina
Segurança da Informação

Aula 03 – Políticas de Segurança da Informação

Professor: João Rafael
Email: joao.rafael@uni9.pro.br

São Paulo
2025

Políticas de Segurança da Informação e Seus Desafios

Políticas de Segurança da Informação

- O Objetivo de implantar **Políticas de Segurança da Informação** é inserir em uma organização: um conjunto de ***leis, regras*** e ***práticas***; que torne-as capazes de proteger os seus ativos de informação.

- A **Política de Segurança da informação** define um conjunto de ***normas***, ***métodos*** e ***procedimentos*** utilizados para a manutenção da segurança da informação, devendo ser **formalizada e divulgada** a todos os colaboradores que fazem uso dos ativos de informação.

Principais Objetivos de Políticas de Segurança da Informação

- Eliminar e administrar as vulnerabilidades;
- Minimizar os riscos;
- Reduzir os impactos no negócio;
- Proteger os ***segredos*** do Negócio;
- Proteger a infraestrutura tecnológica;
- Proteger os recursos humanos;
- Proteger o "***Know-how***" técnico;
- Proteger as Informações dos clientes.

Principais Desafios para Implantar Políticas de Segurança da Informação

- Falta de Conscientização do Corpo Executivo da Organização;
- Ausência de Responsáveis e Profissionais Capacitados;
- Escopo Muito Abrangente;
- Falta de Orçamento;
- Falta de Prioridade;

Parâmetros Essenciais para o Desenvolvimento de Políticas de Segurança da Informação

- Nível de Decisão dos Colaboradores;
- Nível Técnico dos Colaboradores;
- Hierarquia dentro da Organização;
- Abrangência da Organização;
- Tamanho da organização;
- ***Outsourcing***;

Estratégia Geral da Organização e as Políticas de Segurança da Informação

Planejamento de uma Política de Segurança da Informação

Planejamento de Políticas de Segurança da Informação

- Para planejar, construir e aplicar uma **Política de Segurança da Informação** em uma organização, devem ser considerados os aspectos:

  - Objetivo Estratégico;
  - Tecnológicos;
  - Humanos;
  - Culturais;
  - Legais.

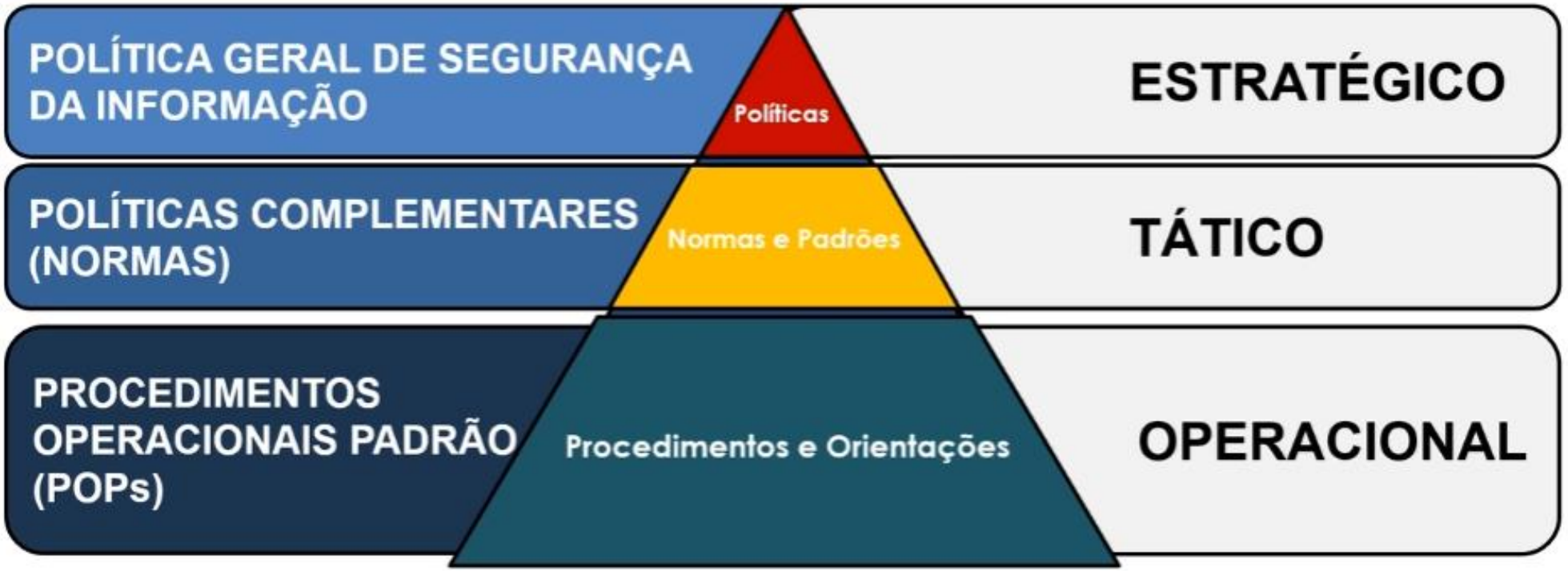
Planejamento de Políticas de Segurança da Informação

- O planejamento de uma Política de Segurança da Informação deve estar alinhada com os **3 níveis de uma organização**: ***Estratégico***, ***Tático*** e ***Operacional***, considerando suas **Diretrizes**, **Normas** e **Procedimentos**.

  - **Nível Estratégico:** Definido por diretrizes (Políticas);
  - **Nível Tático:** Padronização para toda a organização (Normas);
  - **Nível Operacional:** Padrões e Procedimentos da organização (Tarefas, Processos).

Políticas de Segurança da Informação

3 Níveis de Uma Organização



Como Desenvolver Políticas de Segurança da Informação

UNINOVE
Universidade Nove de Julho

Etapas Para o Desenvolvimento de Políticas de Segurança da Informação

- O Sucesso para implantar **Políticas de Segurança da Informação** depende do **comprometimento da alta administração**, ou seja, seu **total apoio e participação**. Ao obtê-lo, todos os colaboradores devem **aceitar e respeitar** o que foi definido nas políticas de segurança da informação implantadas.

- As Principais etapas para desenvolver uma Políticas de Segurança da Informação são:
  - **Levantamento de Informações;**
  - **Desenvolvimento de Conteúdo;**
  - **Formato do Documento;**

Etapa - Levantamento de Informações (Escopo)

- Identificação do Perfil da Organização;
- Atual status de Segurança da Informação;
- Iniciativas de Segurança Existentes ou em Desenvolvimento na Organização;
- Quais são os ativos de informação da Organização;
- Manuais e Documentações Existentes sobre os Processos Internos da Organização;
- Normas, Controles e Procedimentos que a organização segue;
- Backlog e Históricos de Projetos Anteriores de Segurança;
- Lista de Vulnerabilidades já mapeadas;
- Deficiências e Fatores de Risco (Numerado e catalogado);

Etapa - Desenvolvimento de Conteúdo (Escrita da Política)

- Definição de responsabilidades;
- Definição da Gestão de Segurança da Informação;
- Principais objetivos a serem alcançados;
- Integrantes do comitê de Segurança da Informação (Aprova / Reprova novas solicitações);
- Quem serão os proprietários da Informação;
- Quais serão os critérios para classificar a Informação em Secreta, Sigilosa, Pública;
- Normas de Segurança da Informação que serão afetadas / implantadas / implementadas;
- Lista de Diretrizes e suas formas de divulgação;

Etapa - Formato do Documento (Refinamento da Política)

- Deve ser formal, escrito de forma clara e objetiva;
- Deve ser aprovado pela alta gestão da organização;
- Eleger o responsável pela atualização e manutenção deste documento;
- Detalhar o nível de segurança considerado o mínimo aceitável;
- Ser flexível para se adaptar às mudanças tecnológicas e de negócios/legislação;
- Serem Factíveis;
- Descrever as punições que serão aplicadas, caso haja algum descumprimento do documento;

Rotina de Manutenção de Políticas de Segurança da Informação

Manutenção de Políticas de Segurança da Informação

- Há 5 estágios principais para realizar a manutenção de Políticas de Segurança da Informação:

1º) Coleta das Informações

- Rotinas de Coleta;
- Resultados das Tarefas;

2º) Armazenamento / Gravação das Informações

- Rotinas de Armazenamento;
- Informações armazenadas de forma que possam ser “Pesquisadas” e “Recuperadas”;
- Interligação das fontes de armazenamento;

Manutenção de Políticas de Segurança da Informação

3º) Avaliação das Informações

- Análise e Avaliação de Riscos;
- Definição das Prioridades da Gestão da Segurança da Informação;

4º) Compartilhamento das Informações

- Avaliação de informações compartilhadas (Organização, Clientes e ***Outsourcing***);
- Avaliação dos Métodos de Entrada e Saída de Informações das organizações;

5º) Revisão das Políticas de Segurança da Informação e Suas Documentações

- Determina as tomadas de decisão a serem seguidas, com base nos riscos encontrados.
- Este processo deve ser documento para ser examinado em auditorias futuras.

Exemplos de Aplicação para Políticas de Segurança da Informação

UNINOVE
Universidade Nove de Julho

Exemplos de Aplicação
Políticas de Segurança da Informação

- Backup e Segurança Física;
- Controles de Acesso;
- Uso de Internet / Intranet / Redes Wireless;
- Uso do Email Corporativo;
- Uso da Computação Móvel;
- Classificação da Informação;
- Uso dos Equipamentos e Softwares Corporativos dentro e fora da Organização;
- Criação, Manuseio, Transporte, Armazenamento e Descarte das Informações;
- Direitos, Permissões e Acessos a recursos de informação.

Referências

Referências e Links Úteis

- COELHO, Flávia Estélia Silva, BEZERRA, Edson Kowask, ARAÚJO, Luiz Geraldo Segadas. Gestão da Segurança e da Informação: NBR 27001 e NBR 27002. Escola Superior de Redes, 2013, 212p.
- DIAS, Cláudia. Segurança e Auditoria da Tecnologia da Informação . Rio de Janeiro: Axcel Books, 2000.
- FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. Política de Segurança da Informação: guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006.
- NAKAMURA, Emílio Tissato; GEUS, Paulo. Lício de. Segurança de redes em ambientes cooperativos. São Paulo: Berkeley, 2002.
- SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva. Rio de Janeiro: Elsevier, 2003.
- VINTEN, Gerald. Auditing and Security. AS/400, NT, Unix, Networks, and Disaster Recovery Plans. Managerial Auditing Journal, v. 17, n. 5, p. 289-290, 2002.