Organização e Políticas de Segurança da Informação

Prof. Mauricio Pitangueira

INF 025 – AUDITORIA E SEGURANÇA DE SISTEMAS

antoniomauricio@ifba.edu.br

A Organização da Segurança

- **Modelo de Gestão Coporativa de Segurança**
  - Para a criação de um modelo de segurança não basta criar um comitê uma unidade administrativa, um novo comitê ou um ***Comitê Corporativo de Segurança da Informação.***

  - Podemos compreender que para um **modelo gestão cíclico e encadeado**, devemos formá-lo das seguintes etapas:
    - Comitê Corporativo da Segurança da Informação;
    - Mapeamento da Segurança;
    - Estratégia de Segurança;
    - Planejamento de Segurança;
    - Implementação de Segurança;
    - Administração de Segurança;
    - Segurança na Cadeia Produtiva.

A Organização da Segurança

- **Comitê Coporativo de Segurança da Informação**
  - Orientar as ações corporativas de segurança;
  - Alinhar o plano de ação às diretrizes do negócio;
  - Garantir a implantação do modelo de Gestão Corporativo de Segurança da Informação;
  - Promover a consolidação do modelo de Gestão Corporativo de Segurança da Informação.

A Organização da Segurança

- **Mapeamento de Segurança**

  - Identificar o grau de relevância e as relações diretas e indiretas entre os diversos processos de negócio, perímetros e infra-estruturas.

  - Inventaria os ativos físicos, tecnológicos e humanos que sustetam a operação da empresa.

  - Identificar o cenário atual - ameaças, vulnerabilidades e impactos.

  - Mapear as necessidades relacionadas ao armazenamento, manuseio, transporte e descarte de informações.

  - Organizar as demandas de segurança do negócio.

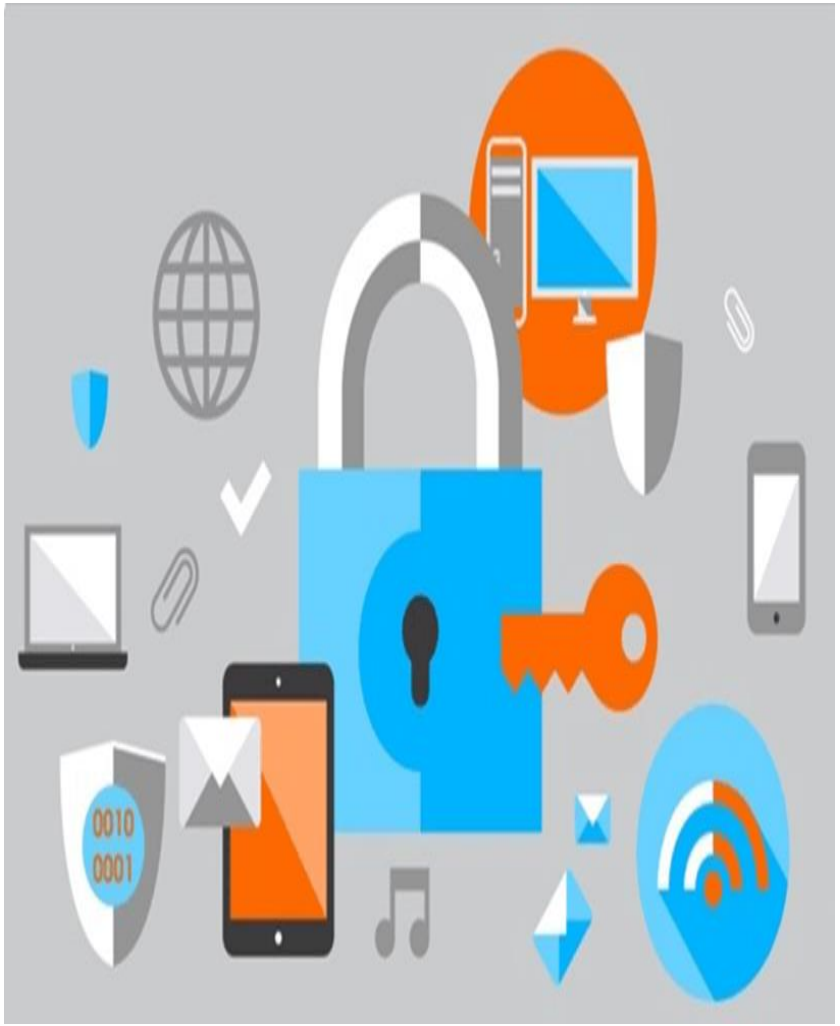
A Organização da Segurança

- **Estratégia de Segurança**
  - Definir um plano de ação, comumente plurianual, que considere todas as particularidades estratégicas, tática e operacionais do negócio;

- **Planejamento de Segurança**
  - Iniciar ações preliminares de capacitação dos executivos e técnicos.
  - Elaborar Política da Segurança da Informação sólida;
  - Realizar ações corretivas emergenciais em função do risco iminente.

A Organização da Segurança

- **Implementação de Segurança**
  - Divulgar corporativamente a Política de Segurança;
- **Administração de Segurança**
  - Monitorar os diversos controles implementados;
  - Garantia a adequação e conformidade do negócio;
  - Administrar os controles implementados.



A Segurança no Contexto da Governança de TI

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Plano Diretor de Segurança

- O **Plano Diretor de Segurança (PDS)** deve fornecer orientações sobre como a organização se portará frente a segurança da informação.

- Objetiva a montar um mapa de relacionamento e dependência entre **processos de negócio, aplicações e infra-estrutura física, tecnológica e humana**.

Plano Diretor de Segurança

- **Quais são as etapas que devemos adotar para elaboração do Plano Diretor de Segurança?**
  - Identificação dos Processos de Negócio;
  - Mapeamento da Relevância;
  - Estudo de Impactos;
  - Estudo de Prioridades;
  - Estudo de Perímetros;
  - Estudo de Atividades.

Plano de Continuidade de Negócios

- O **Plano de Continuidade de Negócios (PCN)**: o principal objetivo deste plano é de **assegurar a continuidade das atividades por cada processo dentro da organização**.

Plano de Administração de Crise

- Este documento tem o propósito de definir, passo a passo, o funcionamento das equipes envolvidas com o acionamento de contingência antes, durante e depois da ocorrência do incidente.

Plano de Continuidade Operacional

- Tem o propósito de definir os procedimentos para contigência dos ativos que suportam cada processo de negócio objetivando:
  - Reduzir os impactos de negócio; e
  - Os impactos potenciais ao negócio.

.

Plano de Recuperação de Desastres

- Define um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais de operação.

- **Por exemplo:**
  - Podemos exemplificar o caso da remoção de uma tabela do banco de dados acidentalmente parando vários sistemas e, em seguida, executando a sua recriação e verificação de todos os sistemas impactados.

Referências

Kim & Solomon. Fundamentos de Segurança de Sistemas de Informação. Ed. LTC, 2012