Organização e Políticas de Segurança da Informação

Prof. Dr. Lauro Cássio Martins de Paula

lauro.martins@ifba.edu.br

A ORGANIZAÇÃO DA SEGURANÇA

A Organização da Segurança

- Para a organização da segurança em um sistema de informação, é necessário um **Modelo de Gestão Corporativa de Segurança**

Modelo de Gestão Corporativa de Segurança

Podemos compreender que, para um **modelo de gestão cíclico e encadeado**, devemos formá-lo das seguintes etapas:

1. Comitê Corporativo da Segurança da Informação;
2. Mapeamento da Segurança;
3. Estratégia de Segurança;
4. Planejamento de Segurança;
5. Implementação de Segurança;
6. Administração de Segurança.

1. Comitê Corporativo 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.

2. Mapeamento da Segurança

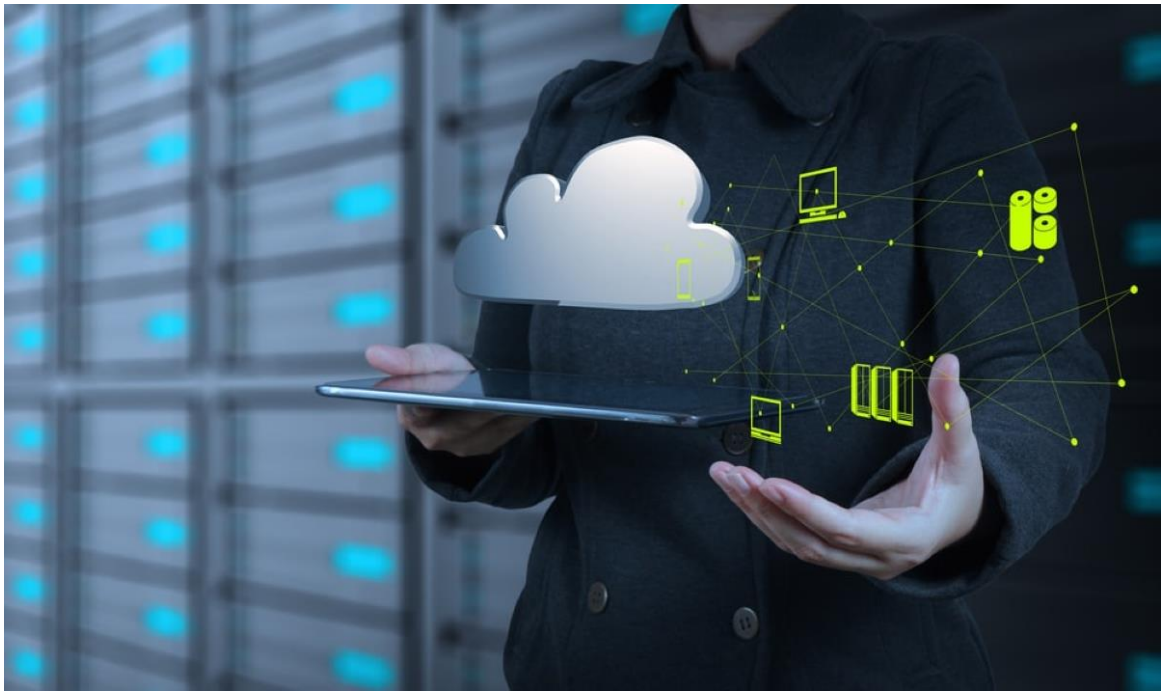
- Identificar o grau de relevância e as relações diretas entre os diversos processos de negócio, perímetros e infra-estruturas.
- Documentar os ativos físicos, tecnológicos e humanos que sustetam a operação da empresa.
- Identificar o cenário atual - ameaças, vulnerabilidades e impactos.
- Mapear as necessidades relacionadas ao armazenamento, manuseio, transporte e descarte de informações.
- Organizar as demandas de segurança do negócio.

3. Estratégia de Segurança

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

4. 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.



5. Implementação de Segurança

- Divulgar corporativamente a política de segurança.

6. Administração de Segurança

- Monitorar os diversos controles implementados;
- Garantir a adequação e conformidade do negócio;
- Administrar os controles implementados.

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Políticas de Segurança

- Plano Diretor de Segurança (PDS);
- Plano de Continuidade de Negócios (PCN ou BCP em inglês);
- Plano de Administração de Crise (PAC);
- Plano de Continuidade Operacional;
- Plano de Recuperação de Desastres (PRD ou DRP em inglês).

Plano Diretor de Segurança

- O Plano Diretor de Segurança (PDS) fornece orientações sobre como a organização deve se portar frente à 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) assegura a continuidade das atividades de cada processo dentro da organização.

Plano de Administração de Crise

- Este plano 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.

Para o Seminário

- Cada grupo deve escolher 3 etapas do modelo de gestão corporative de segurança + 3 planos de políticas de segurança;

- Cada pessoa do grupo fala de 1 etapa do modelo + 1 plano.