Organização e Políticas de Segurança da Informação

Resumo didático baseado nos materiais fornecidos.

Modelo de Gestão Corporativa de Segurança

Este modelo é um ciclo de etapas para proteger uma organização:

Comitê Corporativo de Segurança da Informação: A equipe que orienta as ações de segurança e garante a implantação do modelo de gestão.

Mapeamento de Segurança: Identifica a relação entre os processos, perímetros e infraestruturas, além de inventariar ativos (físicos, tecnológicos e humanos) e as vulnerabilidades.

Estratégia de Segurança: Define um plano de ação de longo prazo para a segurança, alinhado com a estratégia do negócio.

Planejamento de Segurança: Prepara a organização com capacitação de pessoal, elaboração da Política de Segurança da Informação e ações corretivas emergenciais.

Implementação de Segurança: Onde a Política de Segurança é divulgada para todos na empresa.

Administração de Segurança: Foca no monitoramento dos controles de segurança para garantir a conformidade.

A Segurança no Contexto da Governança de TI

O documento utiliza o modelo CobIT para relacionar os objetivos de negócio, os recursos de TI e a informação. O ciclo de vida da TI se divide em quatro fases principais:

Planejamento e Organização

Aquisição e Implementação

Entrega e Suporte

Controle e Avaliação

Plano Diretor de Segurança (PDS)

É o documento que orienta a organização sobre a segurança da informação. Sua elaboração envolve:

Identificação e mapeamento de Processos de Negócio.

Estudo de impactos e prioridades.

Estudo dos perímetros e atividades de segurança.

Planos de Contingência
Esses planos são ferramentas para lidar com crises:

Plano de Continuidade de Negócios (PCN): Garante a continuidade das atividades essenciais da organização.

Plano de Administração de Crise (PAC): Define o funcionamento das equipes de contingência antes, durante e após um incidente. A elaboração do PCO e do PRD está incluída nele.

Plano de Continuidade Operacional (PCO): Estabelece procedimentos para gerenciar ativos, visando reduzir a indisponibilidade.

Plano de Recuperação de Desastres (PRD): Define os procedimentos para restaurar as funcionalidades dos ativos afetados e retornar ao estado original de operação.