Auditoria e Análise de Segurança da Informação

Padrões de Segurança

Prof. José Maurício S. Pinheiro - UGB - 2009

Padrões de Segurança

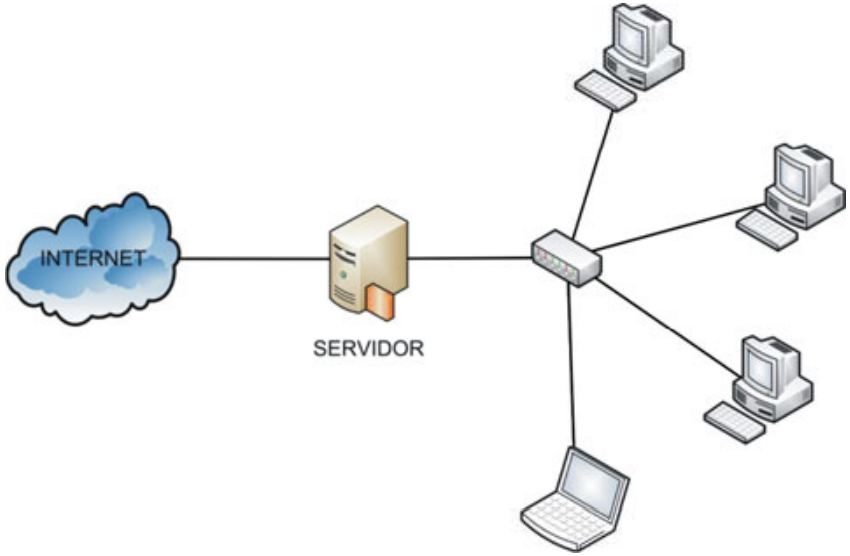
A avaliação de padrões de segurança de computadores define vários níveis de segurança.

Estes níveis descrevem diferentes tipos de segurança física, autenticação de usuário, confiabilidade do sistema operacional, e aplicações de usuário.

Controles de Acesso

Os controles de acesso, físicos ou lógicos, têm como objetivo proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.

Controle de acesso físico



Controle de acesso lógico

Controles de Acesso

A proteção aos recursos computacionais baseia-se nas necessidades de acesso de cada usuário.

A identificação e autenticação do usuário são feitas por meio de um identificador de usuário (ID) e por uma senha durante o processo de entrada (*logon*) no sistema.

Níveis de Segurança

Os SO estão classificados em quatro categorias: A, B, C, D, ordenados de maneira hierárquica crescente, com a maior divisão (A) reservada aos sistemas que oferecem maior nível de segurança.

Nas divisões C e B existem subdivisões conhecidas como classes as quais também estão ordenadas hierarquicamente.

Nível A (Desempenho Verificado)

Trata-se do nível mais alto especificado nos padrões de segurança das redes de computadores.

Inclui projeto e controle rígidos e processo de verificação.

Atribuído aos sistemas operacionais que possuem ferramentas ou capacidades de garantir a segurança total, não apresentando falhas de segurança.

Nível B1 (Segurança Criptografada)

Suporta segurança de múltiplos níveis, estabelecendo que um objeto sob controle de acesso obrigatório não pode ter suas permissões mudadas pelo proprietário do objeto.

Este nível é atribuído aos sistemas operacionais que também possuem ferramentas ou capacidades de garantir a segurança em um nível médio.

Nível B2 (Proteção Estruturada)

Atribuído aos sistemas operacionais que também possuem ferramentas ou capacidades de garantir a segurança em um nível médio.

O aspecto que o diferencia do nível B1 é a sua capacidade de armazenamento de todos os *logins* de acesso ao sistema por um tempo mínimo de 7 anos.

Nível B3 (Domínios de Segurança)

Nível atribuído aos sistemas operacionais que possuem ferramentas ou capacidades de garantir a segurança em um nível bastante alto.

O custo do projeto deve satisfazer as exigências do sistema monitor de segurança e ser razoavelmente imune às invasões e pequeno para que possa ser submetido a análises e testes.

Nível C1 (Proteção Arbitrária)

Nível atribuído aos sistemas operacionais que possuem ferramentas ou capacidade de garantir a segurança sob aspectos mínimos, sem grandes valores de segurança.

O custo do projeto de segurança satisfaz as exigências de segurança discricionária, separando os usuários dos dados.

Nível C2 (Acesso Controlado)

Além das características especificadas para o Nível de segurança C1, o Nível C2 soma características de segurança que criam um ambiente de acesso controlado.

Especifica que o sistema pode ser auditado (registro de auditoria para cada evento de sistema).

Nível D

Aplica-se aos sistemas operacionais que não distinguem um usuário de outro e não tem nenhum método definido de determinar quem está usando o sistema.

Este tipo de sistema é muito encontrado em ambientes e plataformas monousuário.

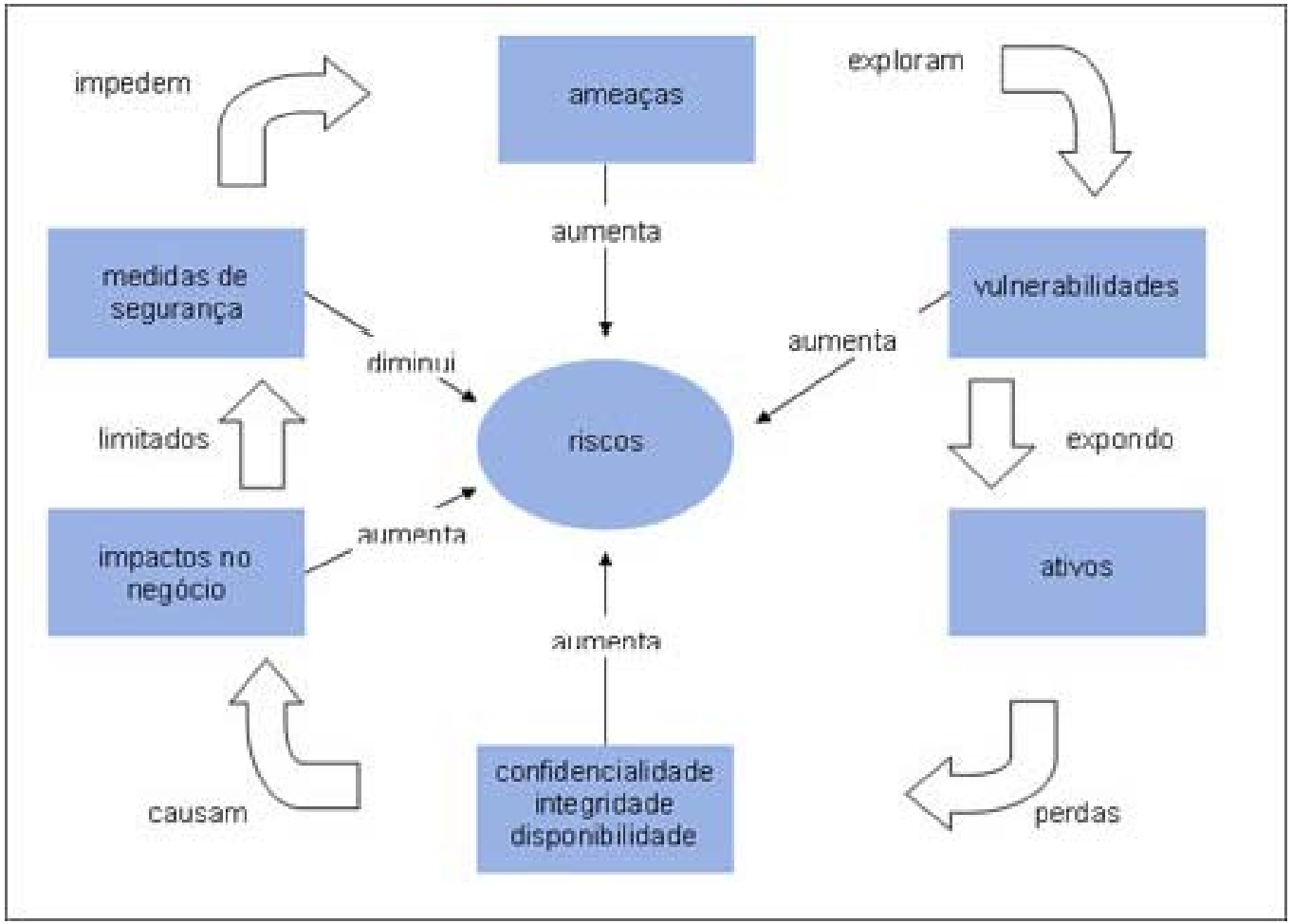
Gerenciamento de Riscos

O risco é definido como a expectativa de perda expressiva ou a probabilidade de uma ameaça explorar uma falha de segurança, causando algum resultado prejudicial.

O que não se conhece não se pode controlar.
O que não se controla não se pode mensurar.
O que não se mensura não se pode gerenciar.
O que não se gerencia não se pode aprimorar.

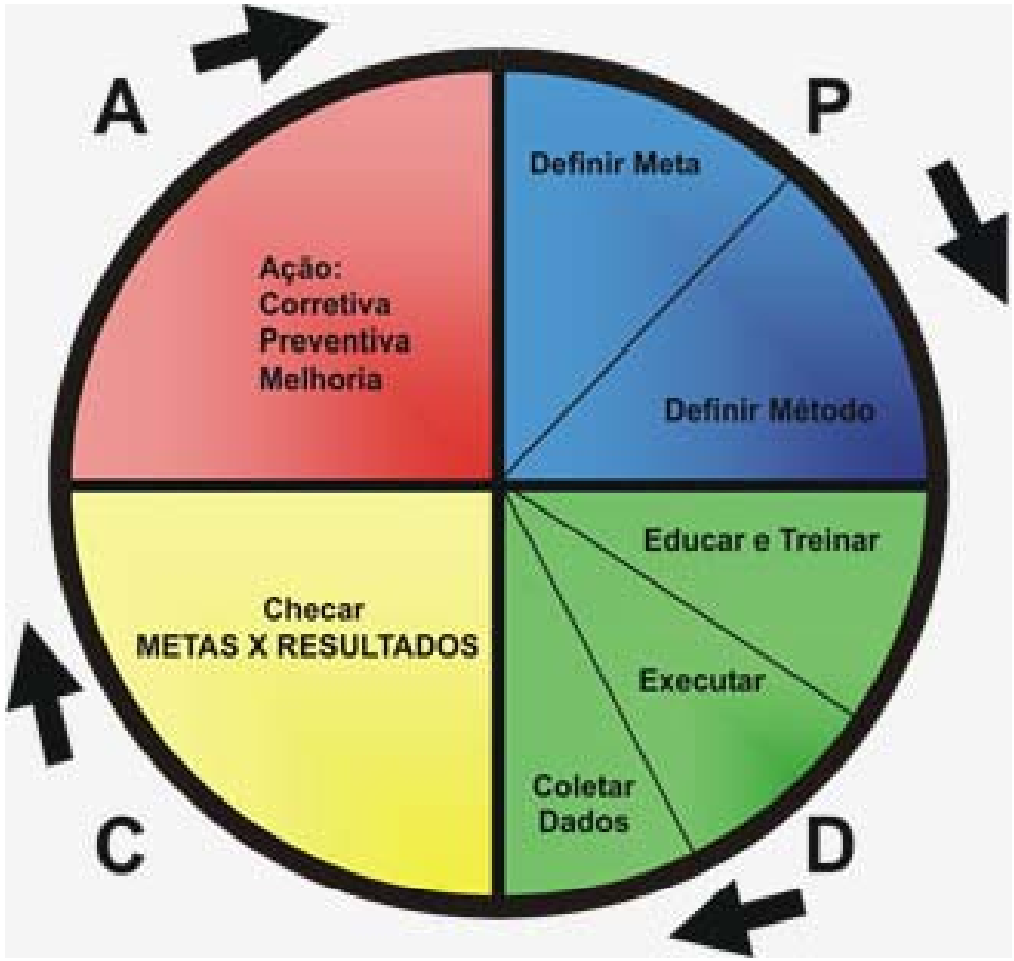
Gerenciamento de Riscos

Ciclo de Segurança da Informação



Gerenciamento de Riscos

PDCA



Gerenciamento de Riscos

GERENCIAMENTO E MAPEAMENTO DE PROCESSO

1 passo - Levante os processos / atividades;

Levante em conjunto com os colaboradores que executam estes processos / atividades, neste momento não se preocupe com o seqüencial dos processos / atividades, só identifique os processos e quais atividades estão ligadas a este processo;

Processo: Dentro de processo existe um conjunto de atividades seqüenciais (conectadas), relacionadas e lógicas, que tem entradas, processamento e produzem uma saída para um cliente interno ou externo;

Atividades: são ações que ocorrem dentro do processo. São geralmente desempenhadas por uma unidade (pessoa ou departamento) para produzir um resultado particular. Elas constituem a maior parte dos fluxogramas;

Gerenciamento de Riscos

GERENCIAMENTO E MAPEAMENTO DE PROCESSO (cont.)

2 passo - Ordenar em forma seqüencial;

É muito importante que todos os envolvidos no processo tenham a clara compreensão de sua natureza (começo / meio e fim), dê preferência utilize fluxogramas, pois facilitam os colaboradores a entenderem melhor o funcionamento de seus processos. Tenha bom senso em determinar qual o nível do detalhamento, para isso análise o resultado que você espera com este trabalho;

3 passo - Definir a documentação necessária para operação e controle;

Identifique os recursos incluindo infra-estrutura, Insumos, matéria-prima. Defina os tipos de documento que serão necessários para controlar os processos (manual, procedimento, formulários,...) utilize formatos padronizados, tenha controle de aprovação e de alteração deste documentos;

Gerenciamento de Riscos

GERENCIAMENTO E MAPEAMENTO DE PROCESSO (cont.)

4 passo - Estabelecer as características do produto / serviço, com parâmetro de aceitação;

Defina claramente o que o cliente espera, com isso defina os parâmetros de aceitação de seus produtos / serviços, em periodicidade definida consulte seu cliente para revalidar estes parâmetros;

5 passo - Definir os responsáveis pelos processos;

Diferente dos departamentos de uma organização que tem seus limites definidos (inclusive responsabilidades), um processo pode “atravessar” diversos departamentos, sendo necessário designar um “dono do processo” que tenha a visão e coordene o processo;

Gerenciamento de Riscos

GERENCIAMENTO E MAPEAMENTO DE PROCESSO (cont.)

6 passo - Estabelecer os indicadores que demonstrem a eficácia de cada processo;

Traduza os requisitos dos clientes em medidas de desempenho. Ligar diretamente as medidas de desempenho do processo às necessidades dos clientes é um dos aspectos mais eficazes da gestão do processo;

7 passo - Identificar os registros necessários para demonstrar a conformidade do produto / serviço e que os processos são capazes;

Ter uma banco de dados confiável é importantíssimo para analisarmos os indicadores, por isso, é de extrema importância, além de definirmos os indicadores, termos devidos registros de onde vamos retirar as informações para análise.

Gerenciamento de Riscos

Métodos de Avaliação de Riscos

- **Árvore de Decisão de Risco**
- **OCTAVE**
- **Grau de Proteção de Recursos (GPR)**