PROJETO DE REDES
www.projetoderedes.com.br

Auditoria e Análise de Segurança da Informação

Segurança e Confiabilidade

Prof. José Maurício S. Pinheiro - UGB - 2009

Dados e Informação

Dado é a unidade básica do conhecimento humano

Informação é o conhecimento adquirido a partir do processamento de um conjunto de dados

Dados e Informação

• Dados são fatos objetivos apresentados sem qualquer critério ou contexto;

• A informação são os dados transformados quando classificados, analisados, sumariados ou inseridos em um contexto.

Segurança e Confiabilidade

A segurança de uma rede de computadores é uma relação de confiança onde os esforços são direcionados para protegê-la do perigo ou do risco da perda de informações ou dados.

A segurança envolve a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulações não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança.

Investimentos em Segurança

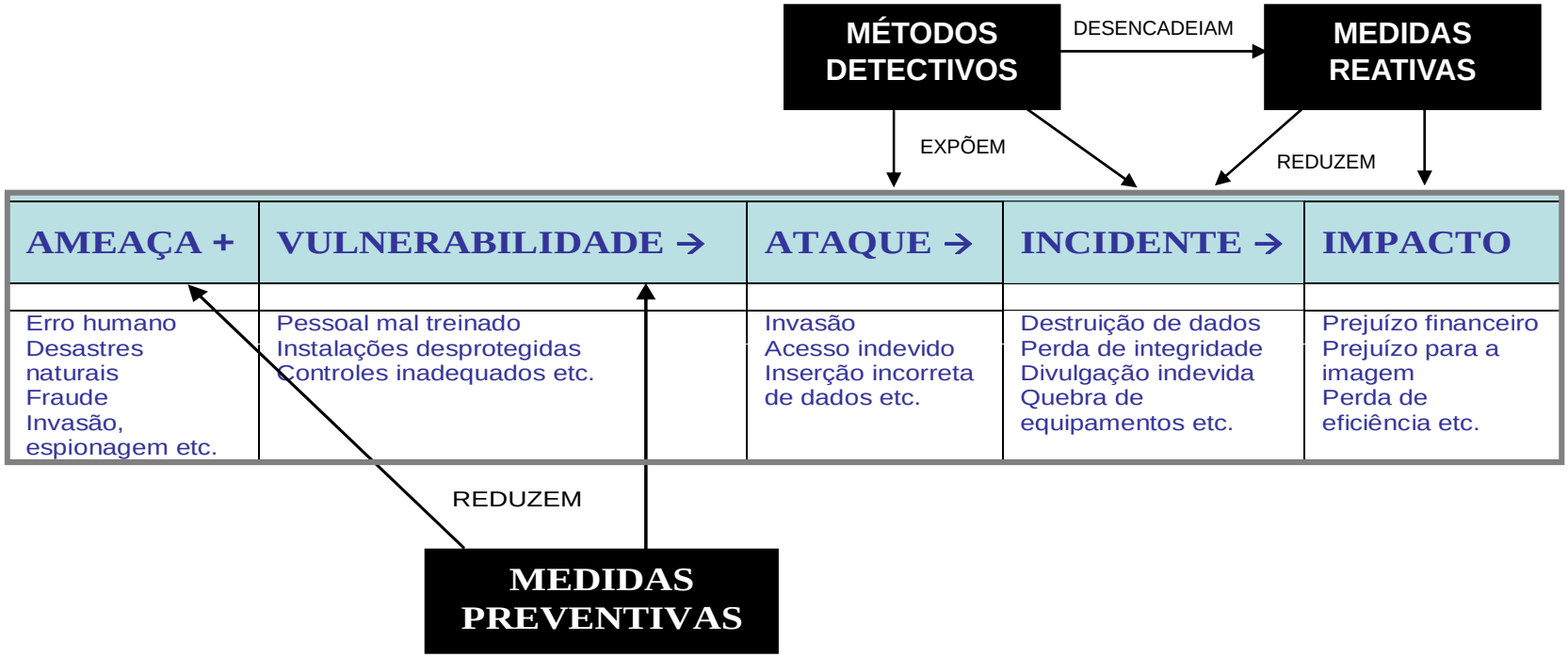
- Proteção das informações e dos conhecimentos sensíveis para a garantia de continuidade do negócio da empresa.

- Pontos Importantes:

  – O que deve ser protegido?
  – Contra o que será necessário proteger?
  – Como será feita a proteção?

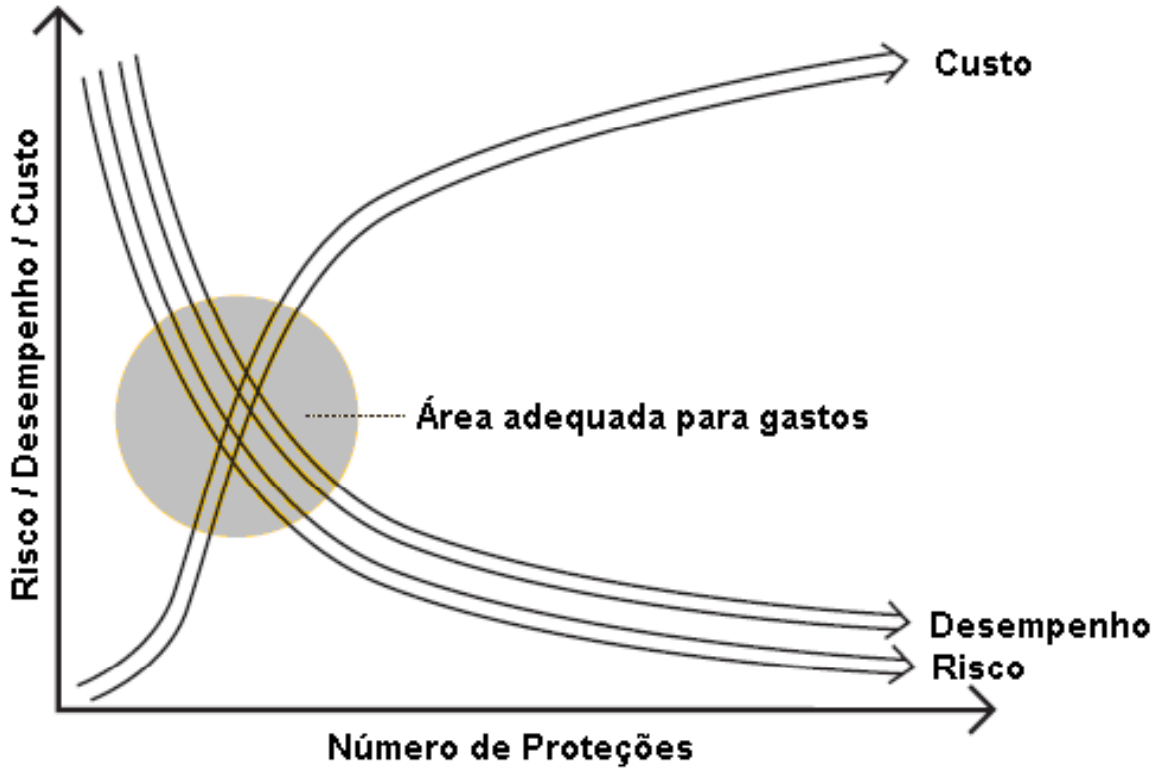
Investimentos em Segurança

RISCO = VULNERABILIDADES x AMEAÇAS x IMPACTOS
MEDIDAS DE SEGURANÇA

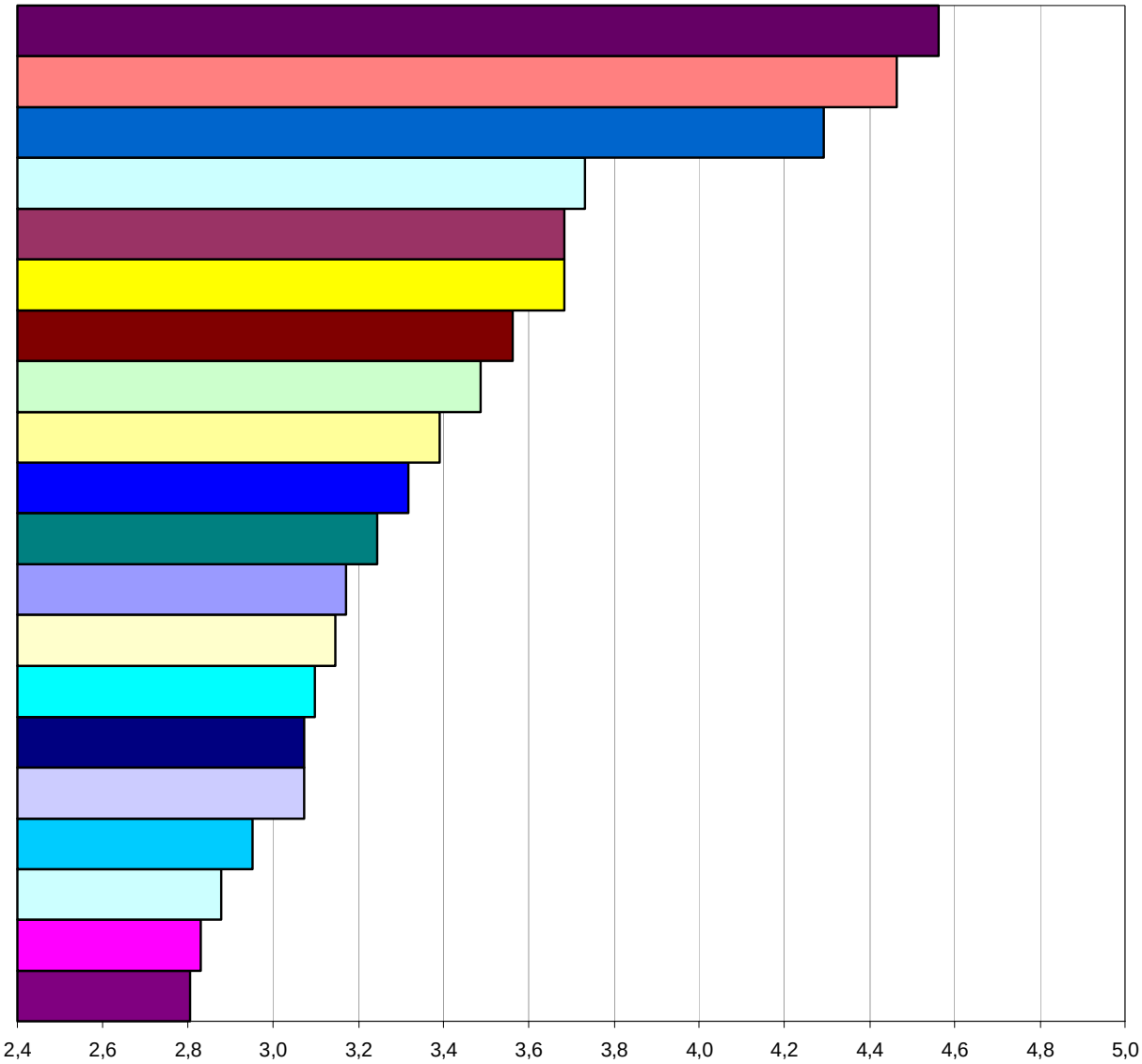


Investimentos em Segurança

O usuário espera que suas informações estejam disponíveis no momento e local que ele determinar, que sejam confiáveis , corretas e mantidas fora do alcance e das vistas de pessoas não autorizadas.



Grau de Importância das Ferramentas e Técnicas para Gestão da Segurança



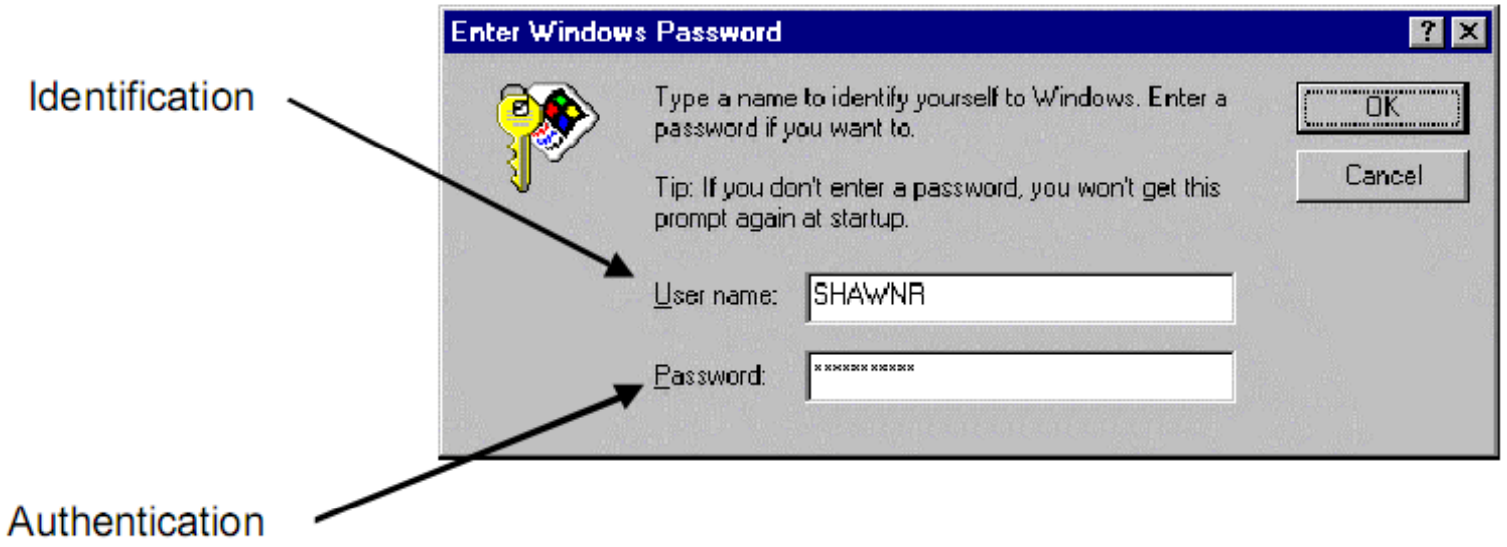
- Antivírus
- Sistema de backup
- Firewall
- Equipamento para proteção de falhas na energia elétrica
- Regras para uso da informação e dos recursos de TI
- Nome de usuário, senha individual e secreta para acesso a rede
- Atualização de software para correção de falhas de segurança
- Controle dos direitos de propriedade intelectual
- Aviso aos usuários sobre o monitoramento dos recursos de TI
- Contratos com terceiros com termos claros relativos a segurança
- Política de segurança da informação
- Classificação da informação
- Sala de servidores protegida e em local restrito
- Criptografia em banco de dados e/ou para troca de informações
- Monitoramento e análise crítica dos registros (logs)
- Descarte seguro da mídia removível
- Conscientização, educação e treinamento em segurança
- Plano de recuperação de desastres e contingência
- Canais de comunicação para registro de eventos de segurança
- Supervisão do desenvolvimento terceirizado de software com requisitos para controles de segurança da informação

Objetivos da Segurança

- **Confidencialidade** – proteger as informações contra acesso de qualquer pessoa não explicitamente autorizada pelo dono da informação;
- **Integridade** – evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação;
- **Disponibilidade** – proteger os sistemas de tal forma que não sejam degradados ou tornados indisponíveis sem a devida autorização.

Identificação e Autenticação

Identificação - método para estabelecer a identidade do usuário no sistema;
Autenticação - meio para verificar a veracidade da identidade do usuário.



Autenticação

Autenticação de usuário — Ocorre durante a seqüência de *login* no sistema, normalmente caracterizada como:

- Algo que o usuário sabe;
- Algo que o usuário possui;
- Algo que o usuário é.

Autenticação

Autenticação host-to-host — Ocorre durante a operação do sistema, normalmente caracterizada como:

- Criptografada;
- Não criptografada.

Controle de Acesso

Controle de acesso discreto

Restringe o acesso para arquivos ou diretórios baseados na identidade do usuário. Eles são discretos de modo que o dono de um arquivo (ou qualquer usuário com direitos suficientes) é livre para permitir ou revogar o acesso corrente de outros usuários àquele arquivo

Controle de Acesso

Controle de acesso obrigatório

Restringe acesso por meio de atributos especiais que são fixados pelo administrador da rede e estabelecidos pelo sistema operacional. Estes controles não podem ser evitados ou mudados por usuários não-privilegiados.

Obrigado!