

Unicap

Segurança e Auditoria em Sistemas

Prof. Roque



O que veremos hoje....

- Requisitos de Segurança

Segurança da Informação

Assim, a disciplina de segurança trata de garantir a existência dos requisitos fundamentais para proporcionar um nível aceitável de segurança nos recursos de informação.

Segurança

De uma forma mais simplificada.

Proteção de informações para que sejam mantidos os **requisitos** de:

- confidencialidade,
- integridade,
- disponibilidade.

Segurança

Definir restrições aos recursos da informação.

Segurança é a gestão de tais restrições.

Para gerir restrições é preciso definir políticas de segurança.

Um conjunto de políticas de segurança define um Modelo de Segurança.

Disponibilidade (Availability)

É o requisito de segurança em que a informação deve ser entregue para a pessoa certa, no momento que ela precisar.

A informação estará disponível para acesso no momento desejado.

Proteção contra interferência como meio para acessar os recursos.

Privacidade (Privacy)

É o requisito de segurança em que a **informação deve ser fornecida para qualquer fim, mas somente com a autorização do proprietário da informação.**

Informações médicas ou financeiras.

Confidencialidade

É o requisito de segurança que visa a **proteção contra a revelação** de informação a indivíduos não autorizados.

Garante que a informação em um sistema, ou a informação transmitida são acessíveis somente a partes autorizadas.

Integridade

É o requisito de segurança que visa a **proteção da informação contra modificações não autorizadas.**

Garante que somente partes autorizadas podem modificar a informação. Modificação inclui: escrever, mudar, mudar status, apagar, criar e atrasar ou responder mensagens.

Autenticidade

É o requisito de segurança que visa validar a identidade de um usuário, dispositivo, ou outra entidade em um sistema, frequentemente como um pré-requisito a permitir o acesso aos recursos de informação no sistema.

Autenticidade

Garante que a origem da informação é corretamente identificada, assegurando que a identidade não é falsa.

Acesso (Access)

**Interação entre um usuário e o sistema
que permite a informação fluir de um
para o outro.**

Controle de Acesso -(Access Control)

Procedimentos operacionais de gerenciamento para:

- detectar e prevenir acessos não autorizados e
- permitir acessos autorizados num sistema.

Não-Repúdio

Requer que nem o transmissor nem o receptor da informação, possam negar o envio da informação.

O sistema não permite a negação, por parte do usuário, do envio de determinada informação.

Infraestrutura de Segurança (1)

O **projeto de segurança** da informação pode ser definido como segue:

Criação de uma **política de segurança corporativa** e **análise de riscos**.

Processo de **conscientização do pessoal** de informática e demais usuários.

Proteção contra **softwares maliciosos**.

Infraestrutura de Segurança (2)

Firewall ;

Sistemas de **Criptografia (Protocolos de Segurança).**

Sistemas de **Deteção de Intrusão.**

Sistemas de **Análise de Vulnerabilidades.**

Ferramentas de **Autenticação** de Usuários:
assinaturas digitais, certificação digital.

Procedimentos de **Auditoria.**

Aspectos Jurídicos .

Riscos de Segurança (1)

Risco é a possibilidade e a probabilidade da ocorrência de uma ameaça particular.

Existe, quando se permite o **acesso livre a todos os recursos** de uma rede.

Análise de Risco (2)

Análise de Risco – Identificação e avaliação dos riscos que os recursos da informação estão sujeitos.

Gerenciamento de Risco (3)

O processo total de **identificar, de controlar e minimizar os riscos** que podem afetar os recursos de informação do sistema.

Inclui a **análise de risco, a análise de custo-benefício, a avaliação de segurança das proteções** e a revisão total da segurança.

Risco Residual (4)

Riscos ainda existentes depois de terem sido aplicadas medidas de segurança.

Unicap

Dúvidas ?

Prof. Roque

