**MINISTÉRIO DA EDUCAÇÃO**

**SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA**

**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PARÁ**

**CAMPUS ALTAMIRA**

# Disciplina

Segurança da Informação para o Desenvolvimento de Sistemas

**CH:** 33h (40h/a)

Prof.: *Pauloalbert C. S. Fernandes*

# Ementa

1. Introdução à Segurança;
2. Conceitos básicos;
3. Técnicas clássicas de criptografia;
4. Criptografia Simétrica;
5. Acordo de chave de Diffie-Hellman;
6. Criptografia de Chave Pública;
7. Gerenciamento de chaves públicas;
8. Funções Hash;
9. Assinaturas Digitais;
10. Certificação Digital;

# Ementa

11. Protocolos de Autenticação;
12. Protocolos Criptográficos;
13. Segurança de aplicações;
14. Redes Privadas Virtuais;
15. Tecnologias disponíveis para defesa;
16. Gestão da Segurança da Informação.

# Plano de ensino

# 1. Conceitos

- É a disciplina que envolve um conjunto de medidas necessárias por garantir que a ***confidencialidade, integridade e disponibilidade*** das informações de uma organização ou indivíduo de forma a preservar esta informação de acordo com necessidades específicas.
- Visa proteger a informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios.
- É uma proteção das informações contra uma ampla gama de ameaças para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidade comerciais

# 2. Princípios de Segurança

- Buscando a proteção da informação, as medidas de segurança devem minimizar os riscos de perda de critérios como confidencialidade, integridade e disponibilidade, que são definidos e exemplificados a seguir:

# 2. Princípios de Segurança

## *2.1 Confidencialidade:*

- Princípio de segurança que requer que dados devam somente ser acessados por pessoas autorizadas;
- Garante que somente pessoas autorizadas poderão acessar as informações;
- Trata-se da não permissão da divulgação de uma informação sem prévia autorização.

# 2. Princípios de Segurança

## *2.2 Integridade:*

- Princípio de segurança que garante que dados e itens de configuração somente sejam modificados por pessoas e atividades autorizadas;
- A integridade considera todas as possíveis causas de modificação, incluindo falhas de hardware e software, eventos ambientais e intervenção humana;
- Garante que a exatidão e completeza das informações não sejam alteradas ou violadas.

*Um exemplo: vamos supor que um gerente de uma empresa determina aumento de salário de 2% aos funcionários, para isso, utilizou seu e-mail para o departamento financeiro. Alguém interceptou e alterou de 2% para 20% o aumento!!!*

# 2. Princípios de Segurança

## *2.3 Disponibilidade:*

- Princípio de segurança que que garante que a informação que requer que dados devam ser acessados por pessoas autorizadas, no momento que requisitados;
- Garante acesso a uma informação no momento desejado;
- Isso implica no perfeito funcionamento da rede e do sistema;

*Imagine você necessitando de umas informações para concluir um relatório e o sistema não está funcionando!*

# 2. Princípios de Segurança

Além da trilogia CID, citados anteriormente, Sêmola (2003) acrescenta outros aspectos da segurança da informação, são eles:

## *2.4 Legalidade:*

- Garantia de que a informação foi produzida em conformidade com a lei;

## *2.5 Autenticidade:*

- Garantia de que num processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação.

# 3. Principais problemas de segurança

## *Ativos:*

- Ativo refere-se a tudo que representa valor para a organização. Caso esse ativo seja violado, poderá trazer impactos negativos para o prosseguimento das atividades da organização.

## *Exemplos de ativos:*

- As pessoas, os programas, os equipamentos, enfim, tudo que na sua ausência gera transtornos, implicando no bom funcionamento dos negócios.

# 3. Principais problemas de segurança

## *3.1 Ameaças*

- Quando um ativo da informação sofre um ataque potencial, podemos entender como ameaça. Este ataque poderá ser efetuado por agentes externos (empresas, pessoas que não são funcionários da organização) ou internos (pessoas pertencentes à organização), se prevalecendo das vulnerabilidades apresentadas no sistema empresa.

# 3. Principais problemas de segurança

## *3.1 Ameaças - exemplos*

Existem diversos tipos de ameaças, Sêmola (2003) classifica-as em categorias, a saber:

- **Naturais:** decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, poluição.
- **Involuntárias:** são inconscientes, podendo ser causadas por acidentes, erros, falta de energia etc.
- **Voluntárias:** são propositais, causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de malwares, incendiários etc.

# 3. Principais problemas de segurança

## *3.2 Riscos*

- Ao acessar a Internet, sua máquina já está exposta na rede;
- Você poderá ter seus dados pessoais expostos;
- Caso sejam acessados por alguém mal intencionado, isso poderá lhe proporcionar grandes transtornos.

# 3. Principais problemas de segurança

## *3.2 Riscos - prevenção*

- instalando um bom antivírus e claro atualizando-o diariamente;
- não acessando qualquer site;
- saber exatamente a procedência dos dados;
- utilizar softwares originais, evitando a pirataria;
- cuidado com os e-mail´s;
- evitar arquivos executáveis;

# 3. Principais problemas de segurança

## *3.3 Vulnerabilidades*

- Podemos entender por vulnerabilidades as falhas que um sistema possui, podendo provocar a indisponibilidade das informações, ou até mesmo a quebra do sigilo e alteração sem autorização.

# 3. Principais problemas de segurança

## *3.3 Vulnerabilidades – causas possíveis*

- falta de treinamento;
- falta de manutenção;
- falha nos controles de acesso;
- ausência de proteção de uma determinada área ameaçada;
- a criação de contas no sistema sem especificar as restrições e permissões.

# 3. Principais problemas de segurança

## *3.3 Vulnerabilidades – categorias*

Podemos classificar as vulnerabilidades em três categorias:

• ***Tecnológicas*:** compreendem as redes de computadores, os computadores, ameaças por vírus, hacker, enfim, todas as atividades que envolvem tecnologia.

• ***Físicas*:** representadas pelo ambiente em que se encontram os computadores e periféricos.
Exemplo: ausência de gerador de energia, normas para senhas, entre outros.

# 3. Principais problemas de segurança

## *3.3 Vulnerabilidades – categorias*

• ***Humanas*:** esta categoria envolve o fator humano, considerada a mais difícil de avaliar, por envolver características psicológicas, emocionais, socioculturais, que variam de pessoa para pessoa. Exemplos: falta de treinamento, qualificação, ambiente organizacional inapropriado para desenvolvimento das atividades etc.

# 3. Principais problemas de segurança

## *3.4 Falhas*

- É quando um sistema permite a quebra de alguns dos princípios da segurança da informação;
- A maioria dos problemas de segurança da informação está basicamente relacionada às falhas oriundas das fases de implantação e desenvolvimento de uma política de segurança.

# 3. Principais problemas de segurança

## *3.4 Falhas - exemplos*

- inexistência de uma política de segurança formalizada;
- gerenciamento dos acessos efetuados no sistema;
- backups atualizados;
- treinamentos e informativos aos usuários sobre como explorar com segurança os recursos tecnológicos;
- definição de uma gerência de Tecnologia da Informação – TI para implementar as regras e fazê-las vivas na empresa.

# 4. Mecanismos e tecnologias de segurança

## *4.1 Controles de pessoal*

- o funcionário deve conhecer seus deveres na empresa;
- treinamento adequado aos funcionários, deixando claras
- as diretrizes de segurança da empresa.

# 4. Mecanismos e tecnologias de segurança

## *4.2 Controles físicos*

- são necessários cuidados para prevenir, detectar e solucionar problemas, caso ocorra algum incidente de segurança;
- Identificar quem entra nas dependências da empresa;
- os trabalhadores da segurança também devem suas regras de trabalho;
- os locais de carga e descarga também merecem vigilância, para saber quem entrou e como entrou na empresa.

# 4. Mecanismos e tecnologias de segurança

## *4.3 Segurança de equipamentos*

- Localização e disposição física;
- proteção contra acessos não autorizados;
- guarda e descartes de arquivos;
- manutenção e aquisição de novos equipamentos;
- falhas de energia;
- além do cabeamento e toda infraestrutura utilizada.

# 4. Mecanismos e tecnologias de segurança

## *4.4 Controles de acessos lógicos*

- são que barreiras que tentam restringir ou limitar o acesso de pessoas não autorizadas ao sistema da empresa;

*Exemplos: arquivos-fontes, sistemas operacionais e os aplicativos instalados na máquina, sendo definidos pela ISO/IEC 17799.*

# 4. Mecanismos e tecnologias de segurança

## *4.4 Identificação dos usuários*

- o usuário terá uma identidade para cada serviço;
- O ***modelo centralizado*** é o que libera o acesso ao sistema ao usuário uma única vez no servidor, o qual utilizará seus privilégios por tempo determinado;
- o ***modelo federado*** permite o acesso dos usuários pela autenticação única, ou seja, uma vez cadastrado em um servidor, o cliente poderá ter sua identidade distribuída a outros servidores;
- ***modelo centrado*** no usuário, no qual quem gerencia a identidadedo usuário é o próprio usuário, permitindo ou restringindo determinada informação a um servidor.

# 4. Mecanismos e tecnologias de segurança

## *4.5 Autorização e controle de acesso*

- geralmente inspecionam o que o usuário vai fazer, desde que devidamente autorizado;
- os ***mecanismos*** mais conhecidos são os logins e senhas;
- biometria;
- certificados digitais
- ***Firewall – fora da empresa***

# 4. Mecanismos e tecnologias de segurança

## *4.6 Antivírus*

- utilizam os dois métodos para identificar infecções, sendo denominados híbridos, além de sua atualização diária, pois todos os dias são criados novos vírus;

*ps.: É importante que o usuário seja devidamente treinado para prevenir e reconhecer possíveis ataques, não bastando apenas a instalação dessas ferramentas de segurança.*

# 4. Mecanismos e tecnologias de segurança

## *4.7 Proteção de dados em curso na internet*

- ***CRIPTOGRAFIA***

# 4. Mecanismos e tecnologias de segurança

## *4.8 Detecção de intrusos*

- tem por função analisar os acessos efetuados na rede, observando as inúmeras ***linhas de logs*** e diagnosticando em tempo real possíveis ataques;
- os administradores da rede de computadores sabem sobre as invasões que estão ocorrendo ou mesmo as tentativas de invasão ao sistema de computadores, sendo capazes também de identificar possíveis ataques feitos internamente.

# 4. Mecanismos e tecnologias de segurança

## *4.9 Sistema de backup*

- refere-se à criação de cópias de segurança das informações
- importantes para os negócios que estão gravados nos servidores e computadores dos usuários;
- é necessário instalação de ferramentas específicas para essa tarefa, além disso, é importantíssimo ter certeza de que as cópias
- agendadas tenham sido realizadas corretamente e que as informações estejam íntegras;

# 4. Mecanismos e tecnologias de segurança

## *4.9 Sistema de backup*

- deve ser feito periodicamente (diário, semanal, quinzenal, mensal) de forma que, se algum incidente de segurança ocorrer, as informações possam ser recuperadas sem nenhum dano imediatamente.

# 4. Mecanismos e tecnologias de segurança

## *4.10 Firewall*

- junção de hardware e software aplicados em uma política de segurança que gerencia o tráfego de pacotes entre a rede local e a Internet em tempo real.

# 4. Mecanismos e tecnologias de segurança

## *4.11 Atualização de S.O. e aplicativos*

- minimizam os riscos e vulnerabilidades, pois os mesmos possuem atualizações que corrigem falhas apresentadas nesses aplicativos depois de comercializados;
- Caso seu aplicativo não seja original ou mesmo de uso livre, você pode estar correndo sérios riscos.

# 4. Mecanismos e tecnologias de segurança

## *4.12 Honeypot*

- tem por função impedir ou mesmo identificar a ação de um invasor, ou qualquer ação estranha ao sistema.

# 4. Mecanismos e tecnologias de segurança

## *4.13 Sistemas de autenticação*

- uso da combinação de logins e senhas;
- Certificação digital;
- cartões inteligentes;
- biometria.

*biometria é uma técnica que utiliza características biológicas como recurso de identificação, como a digital de um dedo ou mesmo da mão, ler a íris, reconhecer a voz.*

# 4. Mecanismos e tecnologias de segurança

## *4.14 Assinatura digital*

- garante que a mensagem realmente veio do remetente, confirmando sua autenticidade;
- utiliza técnicas de criptografia;
- Tem como característica provar quem foi o emissor da mensagem;
- gera um resumo criptografado da mensagem utilizando algoritmos complexos, minimizando a mensagem em tamanhos menores, que é denominado hashing ou checagem.

# 4. Mecanismos e tecnologias de segurança

## *4.15 Auditoria e acesso às informações*

- recurso de controle bastante usado principalmente nas empresas que trabalham com transações financeiras diariamente;
- pode perfeitamente ser aplicada nos recursos computacionais;
- é importante por possibilitar visualizar as atividades
- efetuadas no computador, assim como identificar quem executou a ação a partir da ID de usuário;
- tem por função, basicamente, registrar todos os acessos efetuadas nas redes de computadores, possibilitando identificar o usuário que acessou a máquina, assim como os recursos utilizados;

# 4. Mecanismos e tecnologias de segurança

## *4.15 Auditoria e acesso às informações*

Esse mecanismo de segurança auxilia na tomada de decisão para uma reformulação da política de segurança, caso a empresa já tenha, ou mesmo dar subsídios na criação de uma política de segurança eficiente.

# REFERÊNCIAS