

**Curso de Sistemas de Informação – 8º período**

**Disciplina: Tópicos Especiais**

**Professor: José Maurício S. Pinheiro**

**V. 2009-1**

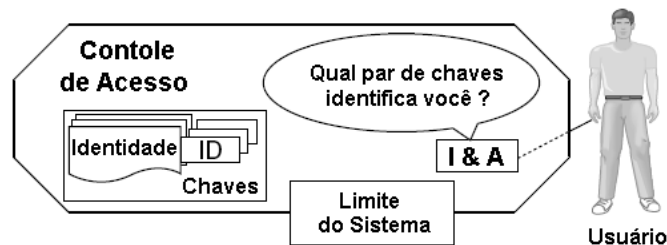
## **Aula 4 – Introdução aos Sistemas Biométricos**

### **1. Identificação, Autenticação e Controle de Acesso**

Existem duas necessidades relacionadas com a troca de dados em uma rede de comunicação: autenticação e a privacidade. Como nos sistemas eletrônicos não há a criação física da mensagem, torna-se necessário um mecanismo que garanta sua autenticidade e inviolabilidade, o que é conhecido como “autenticação”.

O roubo de identidade afeta milhões de pessoas em todo o mundo e tem sido um dos tipos de fraude mais praticados nos ambientes das redes de comunicação, especialmente a Internet. Por esse motivo, a autenticação é um item fundamental para a segurança do ambiente de uma rede de computadores ao validar a identificação dos usuários que desejam usar os recursos disponíveis.

A identificação é a função em que o usuário declara sua identidade para o sistema, enquanto que a autenticação é a função responsável pela validação dessa declaração de identidade do usuário (Fig. 1).



**Figura 1 - Identificação e Autenticação**

Somente após a autenticação e identificação do usuário é que o sistema poderá conceder (ou não) a autorização para o acesso aos recursos da rede. Muitos profissionais especializados em segurança da informação consideram que as medidas de autenticação simples, baseadas em identificador e senha precisam ser reforçadas através de uma autenticação de fator múltiplo, ou seja, associar o que o indivíduo conhece, com algo que ele possua ou com suas características individuais. Esse tipo de autenticação é conhecido como “autenticação de dois fatores”, pois são usados dois métodos e, “autenticação em três fatores”, quando três métodos são utilizados.

### 1.1. Autenticação Baseada no que se Conhece

Trata-se da autenticação baseada em algo que o usuário do sistema conheça. Nessa categoria encontramos os nomes de acesso (*login*), as senhas (*password*) e as chaves criptográficas.

Outro tipo muito utilizado é a “identificação positiva”, que requer do usuário informações pessoais (que podem ser informações previamente cadastradas em um banco de dados), além do nome e da senha pessoal.

### 1.2. Autenticação por Senhas

Define-se senha como “um dado secreto, usualmente composto por uma seqüência de caracteres, que é usado como informação para autenticar um usuário ou pessoa”. Esse dado normalmente é utilizado em conjunto com uma identificação pessoal do usuário (*login*) durante o processo de autenticação, quando da entrada deste no sistema computacional.

A autenticação é o processo de verificar a identidade declarada por uma entidade do sistema, ou seja, verificar se, quem está tentando ganhar o acesso para utilizar o sistema é realmente quem declara ser. O processo de autenticação pode ser dividido em dois passos distintos:

- **Identificação:** apresentação da identidade ao sistema de segurança através de *login* de entrada ou o nome da conta e da senha;
- **Verificação:** compara a identificação fornecida com os dados previamente armazenados. Em caso positivo, o sistema assume que a pessoa ou a entidade que requer a autorização é quem realmente declara ser, liberando o acesso às transações autorizadas. Em caso contrário, a autorização é negada e o acesso bloqueado.

A senha é uma forma de assinatura eletrônica e deve garantir que determinado indivíduo é ele mesmo, permitindo seu acesso aos vários serviços disponibilizados em um sistema de informação. Portanto, ela é pessoal, intransferível e deve ser mantida em sigilo absoluto.

### 1.3. Autenticação Baseada no que se Possui

O segundo método de autenticação é baseado em um dispositivo de posse do usuário (*token*), o qual pode ser dotado de memória (*memory token*), que apenas armazena informações, ou dotado de algum tipo de processamento (*smart token*).

Os *memory tokens* são sempre usados em conjunto com as senhas. Um exemplo de sua aplicação está nos cartões bancários (cartões com chip). Estes cartões contêm informações para a autenticação e são usados em conjunto com a senha no momento que o usuário utiliza o sistema do banco.

Já os *smart tokens* apresentam-se na forma de dispositivos eletrônicos e possibilitam o processamento de algumas informações. Eles podem ser divididos em três categorias básicas, a saber:

- **Quanto à característica física** – podem ser divididos em *Smart Cards* e outros dispositivos semelhantes a chaves, chaveiros, bastões e outros objetos portáteis;
- **Quanto à interface** – podem funcionar como interfaces eletrônicas, que requerem um dispositivo de leitura (como os *Smart Cards*), ou manuais, que utilizam um dispositivo de entrada de dados dotado de teclas ou visores, para a interação entre o usuário e a máquina;
- **Quanto ao protocolo** – os protocolos usados para autenticação podem ser divididos em três categorias:
  - **Senhas estáticas** – o usuário do sistema se autentica no *token* e o *token* autentica o usuário no sistema;
  - **Senhas dinâmicas** – as senhas são alteradas automaticamente nos sistemas com interface eletrônica, mas devem ser lidas e digitadas pelos usuários que utilizam interface estática;
  - **Desafio-resposta** – protocolo baseado em criptografia, no qual o sistema envia um desafio ao usuário, que deve responder ao sistema, o qual avalia a resposta.

#### 1.4. Autenticação Baseada nas Características Individuais

A proteção de informações importantes requer um método de autenticação no qual a possibilidade de acesso indevido ao sistema seja mínima, de forma que a autenticação garanta a identificação do usuário de forma inequívoca e eficaz. Esse método é baseado em alguma característica física ou comportamental própria do usuário do sistema, conhecida como “característica biométrica”.

A autenticação eficiente dos usuários dos sistemas computacionais é um elemento essencial para a proteção da corporação como um todo. Nesse aspecto, a autenticação biométrica leva em consideração as características físicas e comportamentais do indivíduo, comparando-as com as informações armazenadas em um banco de dados organizado com essa finalidade.

Os sistemas de autenticação, utilizados na segurança computacional têm procurado aperfeiçoar o uso do identificador biométrico e da senha pessoal como formas de validar um usuário que utilize os recursos do sistema computacional. A segurança desse processo depende de alguns fatores, tais como a forma de coleta dos dados para autenticação, a forma de transmissão desses dados e a garantia de que a informação não sofrerá nenhum tipo de interceptação ou alteração. Questões de funcionalidade, disponibilidade e processos operacionais periféricos, além da avaliação de vulnerabilidades e monitoração contínua contra fraudes devem ser analisadas para o aprimoramento desses sistemas.

## 2. Controle de Acesso Físico

O controle do acesso físico às instalações é um aspecto particularmente importante da segurança física. Os acessos de visitantes, clientes e outras pessoas não diretamente envolvidas com a operação do sistema devem ser feitos com restrições e o contato com o sistema deve ser o menor possível. Um exemplo típico de controle de acesso físico é o uso de chaves. A chave foi uma das primeiras formas usadas para conseguir acesso restrito uma vez que, pela combinação única entre chave e fechadura, o seu portador tem acesso ao ambiente que os outros não têm; esta forma de autenticação é caracterizada pelo que se possui.

Os sistemas de controle são desenvolvidos visando automatizar o processo de verificação de acesso físico ou ajudar em outras tarefas relativas à proteção de patrimônios críticos. Quando usados para autenticação, consistem de uma base de dados contendo informações sobre o nível de acesso dos usuários e um esquema para garantir a identificação dos mesmos

Podemos definir três ambientes no que se refere à segurança física (Fig. 2):

- **Ambiente Global de Segurança:** área sobre a qual a organização mantém alguma forma de controle ou influência, tal como estacionamentos ou áreas vizinhas ao local da rede de computadores;
- **Ambiente Local de Segurança:** salas adjacentes ao local da rede de computadores. O controle de entrada e saída deste ambiente deve ser feito de acordo com as medidas necessárias previamente estabelecidas na política de segurança da organização. Dentro deste ambiente podem existir diferentes regiões com controles de acesso distintos;
- **Ambiente Eletrônico de Segurança:** sala onde se localiza efetivamente a instalação computacional e seus equipamentos periféricos. Os recursos a serem protegidos e que se encontram no ambiente eletrônico de segurança são servidores, impressoras, terminais, roteadores, scanners, etc. O acesso aos ambientes pode ser feito por intermédio de controles explícitos e de controles de regulamentação de acesso. Os controles explícitos são representados por fechaduras mecânicas e eletrônicas, câmeras de vídeo, alarmes e guardas de segurança. Os controles de regulamentação ao acesso são constituídos por senhas, cartões magnéticos ou sistemas biométricos.

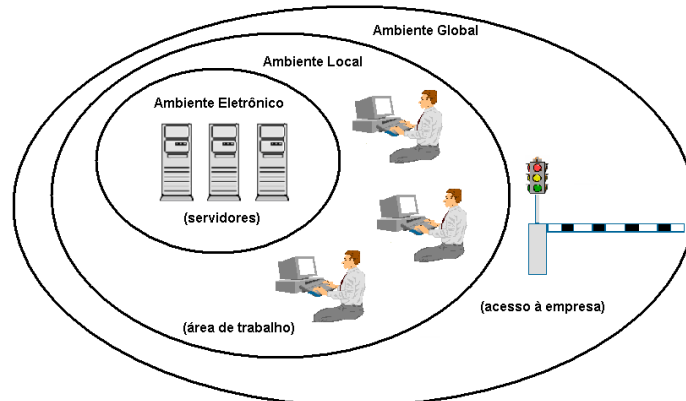


Figura 2 - Ambiente de segurança física

### 3. Controle de Acesso Lógico

Considerando que o controle de acesso físico não é suficiente para garantir a segurança das informações de um sistema computacional, serão necessários controles de acesso lógico, representados por medidas de segurança baseadas em *hardware* e *software* com a finalidade de impedir acessos não autorizados ao sistema (Fig. 3).

Os controles de acesso lógico envolvem o fornecimento da identificação do usuário e de uma senha que serve de autenticação, provando ao sistema que o indivíduo é realmente quem diz ser. O identificador deve ser único, ou seja, cada usuário deve ter sua identidade própria. O principal objetivo do controle de acesso lógico é que apenas usuários autorizados tenham acesso aos recursos da rede realmente necessários à execução de suas tarefas. Isto significa a existência de dispositivos que impeçam os usuários de executar transações incompatíveis com suas funções ou além de suas responsabilidades.

Para cumprir esse objetivo, os controles de acesso lógico devem atender a procedimentos formais que contemplem todo o ciclo de vida do acesso do usuário, desde seu registro inicial, o gerenciamento dos privilégios e senhas, até sua exclusão. Estes procedimentos devem estar em conformidade com a política de disseminação da informação.

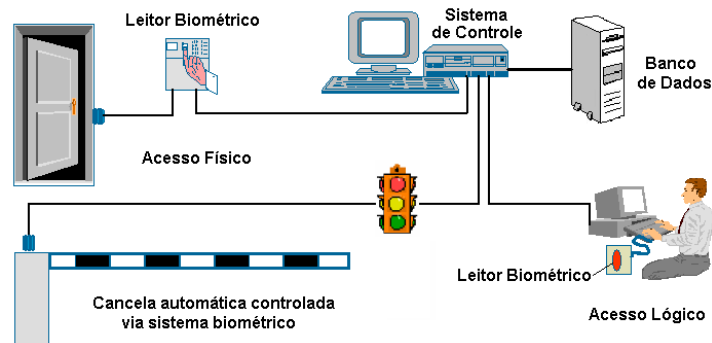


Figura 3 - Controles de acesso físico e lógico utilizando biometria

Como formas de autenticação para os sistemas de controle de acesso lógico são usadas senhas, cartões inteligentes (*Smart Cards*), dispositivos eletrônicos (*tokens*), identificação por radiofrequência (RFID), características físicas como impressão digital, face, voz, retina, entre outras.

#### 4. Definindo Biometria

A biometria pode ser formalmente definida como a ciência da aplicação de métodos de estatística quantitativa a fatos biológicos, ou seja, é o ramo da ciência que se ocupa da medida dos seres vivos (do grego bio = vida e métron = medida). Resumindo, a biometria reconhece um indivíduo pelas suas características biológicas e comportamentais. Em outras palavras, usa características humanas mensuráveis (físicas ou comportamentais) para autenticar a identidade de um indivíduo.

O primeiro método de identificação biométrica foi desenvolvido pelo francês Alphonse Bertillon no final do século XIX. O método, chamado de antropometria ou Bertillonage, em homenagem ao seu criador, confiava na combinação de medidas físicas coletadas por procedimentos cuidadosamente elaborados.

No universo das redes de computadores, biometria refere-se ao conjunto de métodos automatizados que permitem autenticar, identificar ou verificar automaticamente a identidade de um indivíduo baseando-se em suas características físicas ou comportamentais. Esses processos são realizados usando sistemas computacionais de forma a comparar, em tempo real, os padrões tomados do indivíduo, um modelo biométrico, com informações previamente armazenadas. A biometria pode ser usada para incrementar a segurança em redes de computadores, proteção de transações financeiras, controle de acesso a instalações de alta segurança, prevenir fraudes, entre outras aplicações.

Do ponto de vista da segurança dos sistemas computacionais, a biometria permite a verificação da identidade de uma pessoa através de uma característica única, inerente a ela. Essa característica pode ser fisiológica, também conhecida como “característica estática”, representada por traços fisiológicos, originários da carga genética do indivíduo, que essencialmente variam pouco ao longo do tempo (impressão digital ou características faciais, por exemplo) ou uma característica comportamental, também conhecida como dinâmica, aprendida ou desenvolvida ao longo da utilização constante, e que pode variar fortemente ao longo do tempo. Além disso, pode ser facilmente alterada pela vontade ou estado do usuário (assinatura manuscrita ou uma amostra de voz, por exemplo).

Os sistemas biométricos estão em constante processo de desenvolvimento atualmente, sendo considerados como uma das formas mais eficazes para comprovar a identidade de um indivíduo. Por exemplo, a identificação pela íris é uma realidade na Holanda, onde a polícia de imigração implantou um projeto piloto para identificar imigrantes ilegais no país. Outro exemplo de aplicação dos sistemas biométricos, agora nas redes de comunicação, está no seu emprego em combinação com outros procedimentos, visando o aumento do grau de segurança para o uso de dispositivos móveis, mais sujeitos a perdas e roubos.



As impressões digitais são talvez o identificador mais usado no campo da identificação forense. Por sinal, durante um século, as aplicações forenses foram o foco primário das técnicas de identificação de impressão digital. Forense são a ciência e a tecnologia de usar e interpretar uma evidência física para propósitos legais. Está relacionada ao processamento e interpretação dos dados coletados através das aplicações biométricas (reconhecimento de imagens, descoberta de marcas características, monitoração e vigilância, análise e interpretação de movimentos, etc.) A ciência forense não só é usada para relacionar os suspeitos a cenas de um crime, mas também busca associar outros acontecimentos anteriores que podem ter ligação com o fato.

Os agentes motivadores para desenvolvimento dos sistemas biométricos na atualidade são o aumento de fraudes causadas por *hacker's*, o crescimento da Internet e do comércio eletrônico (*e-commerce*), preocupação das empresas com relação à segurança física e lógica de funcionários, equipamentos, custos de operação e manutenção dos sistemas, entre outros.