

**Curso de Tecnologia em Redes de Computadores**  
**Disciplina: Tópicos Avançados II – 5º período**  
**Professor: José Maurício S. Pinheiro**

## **AULA 8: Projeto de Sistema Biométrico**

### **1. Definição de Metas**

A primeira etapa no projeto de um sistema biométrico é estabelecer e documentar as metas. Essas metas variam conforme a organização envolvida ou situação particular dos usuários. Entretanto, alguns requisitos básicos têm presença garantida:

- **Escalabilidade** – O sistema deve ser capaz de crescer junto com a organização e o projeto inicial deve garantir este crescimento, ou seja, o sistema pode ser redimensionado no futuro ainda que uma expansão não seja considerada na atualidade;
- **Funcionalidade** – O sistema deve permitir aos usuários plena satisfação de suas necessidades, proporcionando uma disponibilidade de aplicação fim a fim em algum nível específico de serviço;
- **Adaptabilidade** – O sistema deve suportar as tecnologias atuais e futuras e não deve possuir nenhum componente que possa limitar a utilização de novas tecnologias disponíveis;
- **Gerenciamento** – O projeto deve permitir facilidade de monitoramento e gerenciamento da rede para garantir a operação contínua do sistema e disponibilidade de recursos;
- **Custos** – O retorno em benefícios proporcionado pelo sistema deve ser quantificado, devendo pagar ou superar o investimento feito no projeto. O custo de execução deve ser compatível com o orçamento estabelecido.

### **2. Definição dos Requerimentos**

O primeiro passo é identificar e descrever claramente o problema. Ao considerar o uso da biometria no sistema computacional, deve-se ter em mente que parte do problema presumivelmente está na definição da tecnologia para a verificação da identidade pessoal. Neste caso, é interessante conhecer e compreender como funciona o processo atual de verificação de identidade (caso este exista) e documentar isto adequadamente. Deste modo é possível examinar o processo com mais detalhes para identificar precisamente onde e como o projeto poderá integrar a biometria ao sistema existente, ou se realmente será necessário redesenhar todo o processo utilizando uma metodologia de projeto apropriada.

É importante salientar a necessidade de iniciar o projeto com a definição e documentação clara dos requerimentos. É surpreendentemente fácil perder a visão do objetivo original ao avaliar tecnologias interessantes e terminar com um sistema habilmente projetado, mas que não atende as exigências fundamentais dos seus usuários. Um aspecto para considerar neste contexto é exatamente como são descritos e documentados tais requerimentos. Isto é importante ao emitir um Pedido para Informação - RFI (*Request for Information*) ou um Pedido para Proposta - RFP

(*Request for Proposal*) aos fabricantes ou integradores dos sistemas biométricos para aquela aplicação.

Quando estas exigências são atendidas, chega o momento de considerar os processos operacionais necessários para a aplicação da tecnologia biométrica. É necessário analisar os procedimentos envolvidos em todos os níveis antes de decidir qual tecnologia é mais adequada para atender as necessidades dos usuários. Esta análise permite a coleta de informações que serão extremamente úteis no entendimento e no modelo do fluxo lógico de atividades do sistema.

### **3. Integração com o Sistema Existente**

Um importante aspecto do projeto de um sistema biométrico é determinar como a nova funcionalidade será integrada à arquitetura do sistema computacional existente. Esta é uma consideração importante, mesmo que a aplicação biométrica seja concebida como uma entidade totalmente auto-suficiente, com suas próprias listas de controle de acesso, destinadas à comparação dos modelos biométricos. Mesmo nesta situação (pouco comum), ainda é necessário definir onde o Banco de Dados da aplicação será configurado (em qual servidor) e analisar as exigências de desempenho da nova aplicação sobre a rede como um todo.

É mais conveniente que a aplicação biométrica seja configurada como parte integrante da estrutura do sistema existente, como um diretório central e separar o aplicativo responsável pelo processo de comparação do modelo biométrico da aplicação principal. Neste caso, é preciso considerar onde os aplicativos são instalados, quais protocolos são utilizados e a melhor forma de distribuir os elementos da aplicação para obter um desempenho global otimizado. A chave para o sucesso dessa etapa é envolver os administradores da rede na fase inicial do projeto para assegurar que o sistema estará de acordo com a infra-estrutura existente e será projetado conforme a política de informatização da organização.

Também é preciso definir a localização do Servidor do Banco de Dados biométrico, como serão acessadas as informações e como se dará a integração com a aplicação principal. Semelhantemente, como os dados biométricos trafegarão pela rede (capacidade de banda, se os dados serão criptografados, etc.). Nesse caso, é preciso definir protocolos de rede, qual o tipo de criptografia que deverá ser utilizado (se chave privada ou chave pública) e avaliar qual será o impacto sobre o sistema em termos de desempenho transacional.

### **4. Ajustes e Testes**

Como qualquer projeto de um novo sistema, a implementação original pode requerer ajustes subseqüentes para obter um melhor desempenho. Com respeito aos sistemas biométricos, há vários modos para efetuar tais ajustes a partir do momento em que o sistema é colocado em uso, para daí analisar as transações e o desempenho global.

Alguns destes ajustes são simples e incluem a configuração do hardware, alterações no código do software e outros podem estar relacionados ao treinamento dos usuários. Talvez o ajuste mais óbvio diga respeito ao limiar de operação do algoritmo de comparação. Muitos sistemas têm uma faixa de tolerância dentro da qual é possível ajustar adequadamente o sistema tendo em vista a probabilidade de ocorrência de falsa aceitação ou falsa rejeição.

Considera-se inicialmente o desejo da mais alta precisão disponível no sistema (alta probabilidade de rejeição dos impostores), mas o ajuste do limiar de comparação para esta característica (falsa aceitação) pode resultar em níveis inaceitáveis de falsa

rejeição, com usuários válidos que são rejeitados pelo sistema. Supondo o número de usuários válidos que tentam acessar o sistema maior que o número de impostores ocasionais, o ideal é reduzir o limiar para falsa aceitação com o objetivo de garantir um número menor de usuários válidos rejeitados, especialmente na fase inicial de operação do sistema (fase de treinamento do algoritmo de comparação). Isto permitirá que os usuários possam interagir positivamente com o novo procedimento de autenticação e construir um nível de confiança adequado com o sistema. Posteriormente pode-se ajustar o limiar de comparação para alcançar um melhor equilíbrio entre a probabilidade de falsa aceitação e a falsa rejeição.

Ajustar o limiar de comparação do sistema biométrico representa uma oportunidade para a afinação global da infra-estrutura computacional. O resultado dos ajustes poderá ser monitorado pelo sistema de gerenciamento da rede, que poderá verificar em tempo real o desempenho, detectar a carga dos sistemas, picos de tráfego, largura de banda disponível e assim por diante, como também identificar qualquer ponto de gargalo devido a componentes específicos ou ao uso de serviços comuns.

Outra área relacionada (e menos óbvia) é a distribuição física dos pontos de serviço biométrico e o processamento associado em termos de transações. Se forem detectados pontos de gargalo nos segmentos da rede, em determinados momentos, devido ao número de usuários que requerem acesso aos recursos computacionais, deve-se considerar a instalação de pontos adicionais para distribuir melhor a carga nesses segmentos. Esse balanceamento de carga beneficiará o sistema como um todo, desde diretórios, bancos de dados, sistema de comparação e servidores, demonstrando que a infra-estrutura do sistema foi projetada corretamente.

O funcionamento do software após o ajuste dependerá das aplicações em questão e de suas arquiteturas específicas. Se a aplicação foi desenvolvida localmente, então naturalmente haverá um grupo de suporte local para administrar e aperfeiçoar os códigos. Podem ser necessárias alterações na interface do usuário, tornando uma operação de registro mais simples e intuitiva, por exemplo. O ponto chave é conhecer a arquitetura dos sistemas, a estrutura funcional do software e entender como funcionam os equipamentos. Sem estas informações fica difícil estabelecer parâmetros seguros para definir se as alterações subseqüentes proporcionam melhorias ou, ao contrário, trazem novos problemas ao funcionamento do sistema.

## **5. Documentação**

A etapa final do projeto do sistema biométrico envolve a elaboração da documentação, que inclui a descrição dos requisitos dos usuários e explica como o projeto atende a esses requisitos. Também se documentam a estrutura da rede proposta para suportar as aplicações, a estrutura lógica e física, o orçamento e despesas associadas com o projeto. A criação de uma rede bem documentada também oferece um formulário de referência usado no treinamento dos usuários, solução de problemas e atualização do sistema computacional após o encerramento do projeto.

A documentação pode abranger a execução de diagramas lógicos e topologia, plantas de arquitetura refletindo o esquema de infra-estrutura implantado, tabelas de identificação e conexão de segmentos, tabelas de caracterização de estações e qualquer outro tipo de documentação técnica pertinente. Também é importante que a documentação de projeto contenha planos para implementar o sistema, medir o sucesso da implementação e desenvolver o projeto à medida que surgirem novos requisitos de aplicativos.

## 6. Aplicações Biométricas

Existem diferentes formas de aplicação dos sistemas biométricos em redes de computadores. Para implantá-las são necessários equipamentos apropriados e software que trate os dados capturados. De forma generalizada, todos funcionam sobre os mesmos princípios, mas, para cada caso, o hardware e o software devem ser adequados para o sistema biométrico escolhido.

Tradicionalmente, as aplicações biométricas são divididas em três categorias:

- Aplicações para acesso lógico a dados ou informações;
- Aplicações para acesso físico a locais controlados;
- Aplicações nas quais a biometria identifica ou verifica a identidade individual em um banco de dados, ou através de um dispositivo físico (*token*).

Enquanto as categorias mencionadas anteriormente indicam as aplicações mais genéricas nas quais a biometria pode ser desdobrada, outros fatores críticos para aplicações específicas dos sistemas biométricos compreendem:

- A interação do indivíduo com o sistema biométrico;
- Supervisão da operação pelos usuários;  
Cadastramento do usuário antes de interagir com o sistema;
- As exigências da aplicação em termos de precisão, registro e tempo de resposta;
- Formas de uso do sistema pelo usuário e que sanções estão previstas nos casos de abusos;
- O valor para o negócio das informações, instalações ou equipamentos que a biometria está protegendo;
- Quais tecnologias de reconhecimento são compatíveis para aplicação juntamente com a biometria.

## 7. Segmentos de Aplicação da Biometria

Podemos classificar uma série de prováveis aplicações para a biometria na sociedade atual, a saber:

- **Identificação Criminal** - Refere-se ao uso de tecnologias biométricas para identificar ou verificar a identidade de uma vítima, um suspeito ou um indivíduo qualquer em uma aplicação da lei. Neste caso, o papel primário da biometria é identificar um indivíduo para dar andamento a um processo de investigação, por exemplo;
- **Instituições Financeiras** - Os sistemas biométricos são utilizados em máquinas de auto-atendimento, nas transações bancárias via Internet, compra de bens e serviços, Pontos-De-Venda (PDV). A utilização de sistemas biométricos como *Smart Cards* e *Tokens*, por exemplo, complementa ou pode substituir os mecanismos de autenticação tradicionais como cartões de plástico, assinatura de punho e até mesmo números de identificação pessoais (PIN) associados com senhas;

- **Comércio Eletrônico** - Aplicações de comércio eletrônico envolvem a autenticação remota do usuário e freqüentemente requer verificação transacional. Além disso, necessitam que seja efetivado o registro da característica para processos de verificação. A biometria é usada em comércio eletrônico (*e-commerce*) para identificar e verificar a identidade de indivíduos que realizam transações remotas de bens ou serviços. O sistema biométrico pode ser usado para complementar ou substituir mecanismos de autenticação como senhas, PIN, e interação de desafio-e-resposta;
- **Acesso aos Sistemas de Informação** - Aplicação biométrica intimamente relacionada ao controle de acesso. Neste caso, a biometria pode ser usada no controle de acesso a computadores individuais ou às redes de computadores. Aplicações desse tipo normalmente não necessitam de autenticação para uma transação específica, mas para acesso a um recurso ou funcionalidade do sistema computacional;
- **Edifícios Inteligentes** - A biometria pode ser usada nos edifícios de alta tecnologia, conhecidos como “edifícios inteligentes” para identificar ou verificar a identidade de indivíduos que entram ou saem do prédio ou de uma área específica, tipicamente lojas, andares e salas, em um determinado momento. O sistema biométrico é usado para complementar ou substituir mecanismos de autenticação como chaves e outros dispositivos físicos;
- **Segurança Eletrônica** - A biometria é usada para identificar ou verificar a identidade dos indivíduos presentes em um determinado espaço ou área. O sistema biométrico é usado para complementar ou substituir métodos de autenticação como monitoração convencional através de câmeras;
- **Sistemas Governamentais** - Sistemas de benefícios (aposentadoria, assistência médica, vale-refeição, vale-transporte, etc.) são particularmente vulneráveis à fraude. Os sistemas biométricos podem ser usados para identificar ou verificar a identidade de indivíduos na interação destes com órgãos do governo com a finalidade de emissão de documentos, voto, imigração, serviços sociais, ou seguro desemprego, por exemplo;
- **Sistema Penitenciário** - O sistema penitenciário utiliza a biometria na captura de criminosos, bem como o controle de acesso (entrada / saída) e administrativo dos prisioneiros (distribuição de comida, etc.);
- **Telecomunicações** - Com o rápido crescimento das comunicações globais, os serviços de telecomunicações estão sendo vítimas de fraudes diversas. Sistemas biométricos de identificação pela voz têm sido bem recebidos no estudo de segurança deste mercado;
- **Portos e Aeroportos** - Os portos e aeroportos são regidos por legislações específicas e por leis internacionais que versam sobre a segurança da navegação e aviação civil contra atos ilícitos. Os sistemas biométricos podem ser usados para identificar as pessoas durante o embarque, a fim de garantir que sejam as mesmas que realizaram o *check-in*;
- **Instituições Médico-Hospitais** - Controle do acesso às instalações restritas (UTI, salas de cirurgia), movimentação de pacientes e também na identificação de médicos e demais funcionários;
- **Condomínios e Lazer** - Identificação de moradores/sócios, controle de estacionamento, identificação de funcionários e vigilância em condomínios fechados, clubes, etc.;
- **Instituições de Ensino** - Identificação de professores, estudantes, funcionários, controle de acesso em áreas restritas, laboratórios, biblioteca, refeitórios, etc.;

- **Aplicações Militares** - Identificação e controle de acesso em áreas restritas, portos, aeroportos e outras áreas de Segurança Máxima;
- **Assinatura Digital** - É possível a obtenção de características físicas dos usuários através de um leitor biométrico, que após o processamento adequado, transforma essa característica em um modelo. Com a inclusão deste modelo na assinatura digital é possível atribuir aos documentos eletrônicos uma marca pessoal do emissor, criando a ligação física do signatário com o documento assinado.