Modelo Intencional Genérico de Sistemas Biométricos

Jacqueline Abreu do N. T. Rodrigues, Nathálea Salem, Vera Maria B. Werneck

Universidade do Estado do Rio de Janeiro (UERJ), Rio de Janeiro, Brasil

jac@jacquelineabreu.me, nathaleas@gmail.com,vera@ime.uerj.br

Abstract. *Biometric systems have been presented in various environments. These systems are widely used in many situations, with emphasis to attend security non functional requirements. The study of essential processes executed by these systems could identify which are the functional and non-functional requirements for systems that handle biometrics. This work presents an intentional model using the i* framework that covers functional and non functional requirements and the relations between the actors involved in these processes. Therefore, we have proposed a generic intentional model that can be specialized for any biometric device, composing a reusable instrument that can be refined depending on the area in which the system must be applied.*

Resumo. *Sistemas biométricos tem uma forte presença em vários ambientes, tendo ampla utilização em diversos níveis, especialmente para atender o requisito não funcional de segurança. Com o estudo dos processos essenciais executados por estes sistemas foram identificados quais são os requisitos funcionais e não funcionais essenciais de sistemas que manipulam biometria. Este trabalho usando framework i* apresenta uma modelagem dos requisitos funcionais e não funcionais de sistemas biométricos, além das relações entre os atores envolvidos nos processos abordados. Com isso, temos a proposta de um modelo intencional genérico, que pode ser especializado para qualquer biometria, sendo um instrumento reutilizável e aprimorável de acordo com as necessidades do domínio em que o sistema será aplicado.*

1. Introdução

Considerando a importância da utilização de sistemas biométricos em diversos segmentos do mercado e acreditando neste recurso como ferramenta essencial na prática do dia a dia, buscamos, a partir deste trabalho, definir uma modelagem genérica de um sistema biométrico padrão que atenda a demanda da sociedade, por sistemas que trabalhem de forma ágil, precisa, interativa e suficientemente robusta para “combater” as diversas técnicas de fraudes e ataques ao sistema.

Biometria é uma forma de reconhecer um indivíduo através de alguma verificação (muitas vezes de natureza matemática/estatística) das suas características físicas e/ou comportamentais. Esta é uma solução que tem sido adotada em diversos sistemas comerciais como uma solução para atender a demanda de segurança e/ou privacidade em transações realizadas na nossa vida diária.

Os requisitos não funcionais são fundamentais para a eficiência e eficácia dos sistemas. Além disso a reutilização da modelagem pode ser considerada uma estratégia de crescimento qualitativo na área tecnológica, na medida em que possibilita o aproveitamento de uma modelagem padrão para a especialização biométrica do modelo desejado, evitando, desta forma, o retrabalho, otimizando o tempo do profissional ou da empresa.

Este trabalho tem como objetivo apresentar uma modelagem padrão, definida no framework i*[1], [2] para que esta sirva como referência para diferentes tipos de sistemas biométricos [3]. Na seção 2 são apresentados alguns conceitos importantes relacionados à biometria, tais quais sua definição e principais propriedades. Na seção 3 o funcionamento e os fundamentos necessários para qualquer sistema biométrico são identificados. A proposta de um sistema biométrico genérico, baseadas no modelo de Woodward et al [3] é descrita com seus processos e subprocessos, além de seus requisitos não funcionais [4], [5]. Na seção 4 a modelagem genérica do framework i* do sistema biométrico proposto é apresentada, ou seja, apresentamos a modelagem dos atores envolvidos, suas dependencias e pré-requisitos entre os processos, as metas e a forma como os atores interagem para alcançar essas metas. E finalmente na Seção 6 são apresentados as conclusões e trabalhos futuros.

2. Biometria

Biometria pode ser definida através da análise dos termos de origem grega que compõe a palavra biometria: bio - vida, metrikos – medida. Em Jain et al. [6] biometria é definida como a “ciência de reconhecer um indivíduo baseado em suas características físicas e/ou comportamentais”. Podemos dizer então que biometria é uma forma de reconhecer um indivíduo através de alguma verificação (muitas vezes de natureza matemática/estatística) das suas características físicas e/ou comportamentais.

Os seres humanos têm usado características do corpo, como voz, impressão digital, face, forma de andar e assinatura, para se reconhecerem uns aos outros [7]. Essas características podem ser divididas em fisiológicas e comportamentais, sendo que a ciência que estuda essas caracteristicas é a biometria. Características fisiológicas variam pouco ao longo do tempo. Já as características comportamentais são mais difíceis de medir por causa de influências diversas, tais como stress, fadiga ou doenças, tais como simples resfriados [8], [9].

Para que uma característica possa servir como instrumento de verificação, ela deve ser “metrificável”. Existem porém outras propriedades que a característica deve atender [7], tais quais a *universalidade* – todos os seres devem possuí-la, a *unicidade* – ela deve variar entre os indivíduos, a *permanência/imutabilidade* – a característica não deve ter mudanças significativas, mesmo submetida a ação do tempo e a *coletabilidade* – o atributo estudado deve ser de fácil obtenção, além de ter *qualidade* para poder ser usada posteriormente.

Temos como exemplo de ampla utilização as características físicas: impressão digital, íris, geometria das mãos, orelhas, etc. E, também, as características comportamentais: assinatura, voz, digitação, etc. A Tabela 1 apresenta alguns tipos de Biometria e suas características. A Figura 1 mostra alguns exemplos de biometria e como estes são apresentados nos sistemas.

Tabela 1. Tipos de Biometria

Tipo de Biometria	Característica Biométrica
Impressão Digital	Linhas de dedo; Estrutura de poros
Assinatura	Pressão e velocidade da escrita
Geometria Facial	Distância de características faciais específicas (olhos, nariz, boca)
Íris	Padrão da íris
Retina	Fundo do olho (padrão da estrutura das veias)
Geometria da Mão	Medição dos dedos e da palma
Estrutura de Veias nas Mãos	Estrutura das veias do dorso ou palma da mão ou um dedo
Formato da Orelha	Dimensões da orelha visível
Voz	Tom ou timbre
Odor	Composição química do odor
Digitação	Ritmo de digitar no teclado (PC ou outro teclado)

O reconhecimento das informações passadas pelas características biométricas (denominada a partir daqui também de biometria) pode ser uma tarefa não trivial e para tornar mais fácil as atividades relacionadas ao reconhecimento biométrico e afins, temos os sistemas biométricos.

Figura 1 - Exemplos de Biometria

3. Sistemas Biométricos

Segundo Miller [8], os sistemas biométricos são métodos automatizados de verificar ou reconhecer a identidade de uma pessoa viva baseado em algumas características fisiológicas ou algum aspecto do comportamento como exemplos da Figura 1.

Jain et al [7], afirma que um sistema biométrico é essencialmente um sistema de reconhecimento de padrão que opera através da aquisição de dados biométricos de uma

pessoa, extraindo um conjunto de recursos a partir dos dados adquiridos e comparando com o modelo definido (armazenado) no banco de dados.

Um sistema biométrico possui dois processos básicos: cadastro e autenticação. Para efetuar o reconhecimento, ou seja, a autenticação, deve-se ter os dados desta já armazenados. Com isso, percebemos que o primeiro processo a ser executado é o de cadastro. No início do cadastramento, é capturado o dado biométrico da pessoa através de um leitor de dados biométricos – sensores que capturam, gravam e convertem as informações biométricas em um formato que o sistema entenda. A seguir, atributos únicos são então extraídos e convertidos pelo sistema em um código matemático e este dado é armazenado em algum dispositivo de armazenamento como o *template* biométrico daquela pessoa. Junto a este *template* é registrada uma identidade de usuário (nome, número de identificação e outros), para facilitar a posterior autenticação do indivíduo.

Alguns sistemas podem exigir que um número mínimo de coletas seja realizado para que seja construído um perfil biométrico da característica que está sendo cadastrado. A extração dos atributos ocorre de forma igual à descrita acima, assim como a formação do *template* e o armazenamento deste.

O segundo processo do sistema biométrico, a Autenticação, ocorre quando o dado biométrico do indivíduo é capturado e o sistema pode utilizá-lo para identificar quem é a pessoa no dispositivo de armazenamento (Identificação ou Autenticação1:N) ou verificar a identidade da mesma (Verificação ou Autenticação 1:1). Para que isto aconteça, a pessoa deve estar, necessariamente, cadastrada no sistema.

No modo de Autenticação 1:N (um para muitos), a autenticação é feita comparando o dado coletado com todos os modelos de todos os usuários previamente cadastrados no banco de dados. Já no modo de Autenticação 1:1 (um para um), o sistema necessita da apresentação de uma identidade da pessoa (um número de identificação pessoal, o nome de usuário, dentre outros) para que o sistema realize a comparação biométrica apenas com os modelos correspondentes à identidade.

Esses dois processos, o Cadastro e a Autenticação, são comuns a todo sistema biométrico. Entretanto a forma de implementação pode ser diferente para cada processo do sistema, ou seja, cada um destes processos é dividido em diferentes subprocessos, que podem se diferenciar de um sistema para outro.

Neste trabalho utilizou-se uma adequação da proposta de Woodward et al. [3]. Baseado nesta, o sistema proposto é dividido nos seguintes subprocessos: aquisição de dados, processamento de sinais, análise, formação de *template*, armazenamento de dados e comparação. Nas figuras 2, 3 e 4 este processo e subprocessos foram esquematizados.

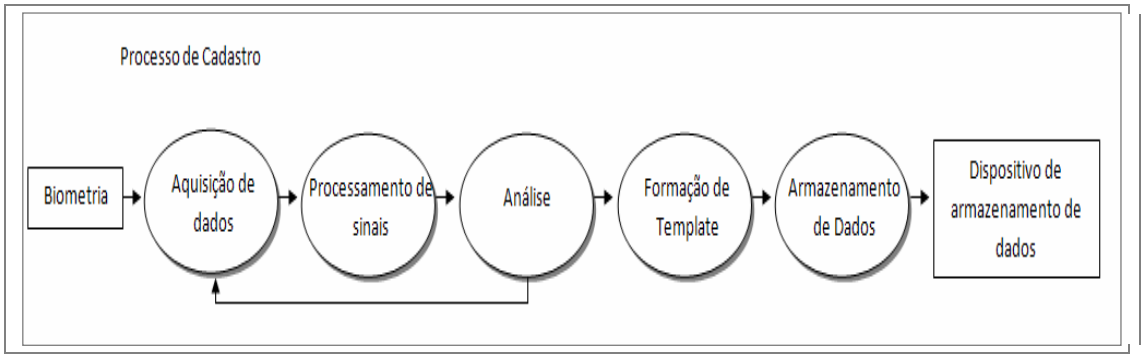

Figura 2: Processo de Cadastro no Sistema Biométrico

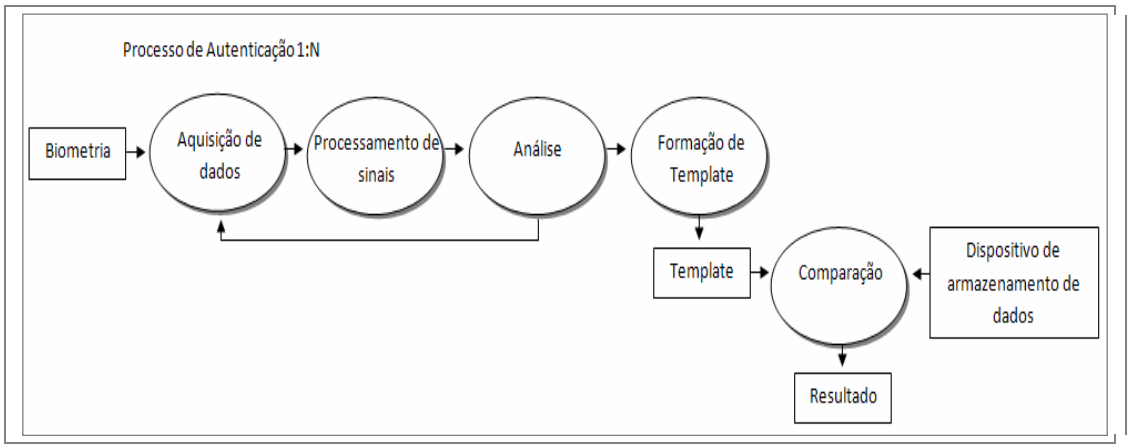

Figura 3: Processo de Autenticação 1:N (Identificação) no Sistema Biométrico

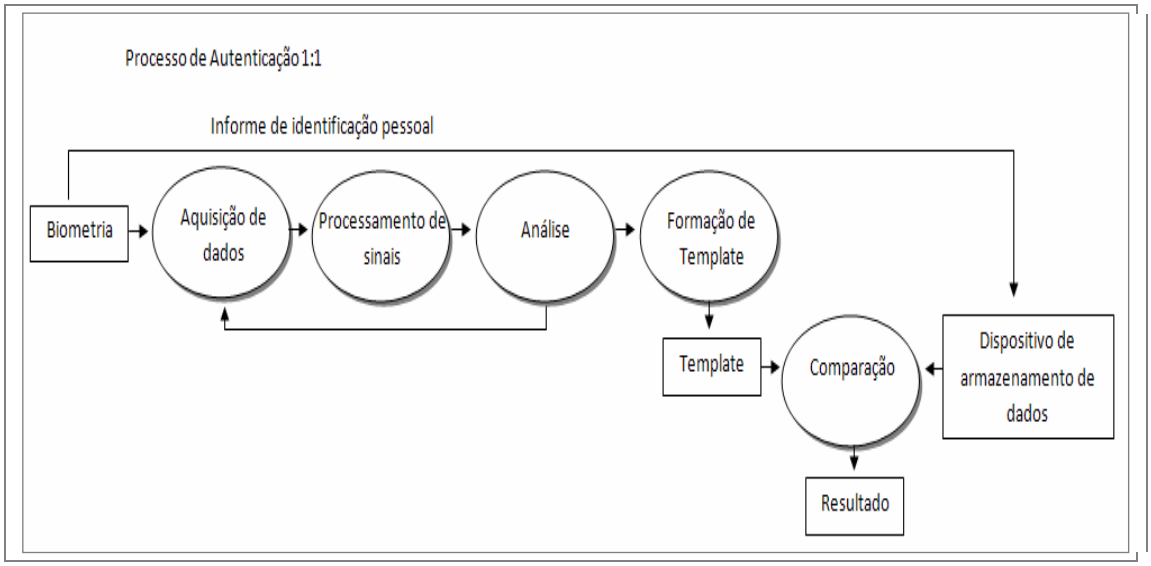

Figura 4: Processo de Autenticação 1:1 (Verificação) no Sistema Biométrico

Como observado nas figuras 2, 3 e 4, alguns subprocessos são comuns a todos os processos. Na aquisição de dados o dado biométrico é apresentado e capturado por um leitor biométrico. Isso implica na captura digital da biometria e na transferência desta para o processamento de sinais.

No segundo subprocesso, o processamento de sinais, o dado biométrico bruto é processado para o futuro armazenamento e comparação. Segundo Woodward et al. [3], o processamento consiste na segmentação da imagem, que é a limpeza dos ruídos encontrados na imagem original, através de algoritmos. Em seguida ocorre o isolamento e a extração das características (features) mais importantes.

Após o processamento de sinais, há uma análise da imagem resultante e uma comparação com o limiar mínimo de qualidade definido pelo administrador do sistema. Este subprocesso é chamado de Análise. Nele, o sistema decide se a imagem coletada tem o mínimo de qualidade requerida. Neste caso, ocorre o subprocesso de Formação do Template do sistema biométrico, que consiste no armazenamento, de forma compacta e segura, da representação matematica das características extraídas. Caso contrário, deverá ser feita uma nova captura do dado biométrico.

Após a Formação do Template os processos de Cadastro e Autenticação seguem caminhos diferentes. Até o ponto da formação do template, podem-se evidenciar esses subprocessos em um processo único, que terá seus resuldados utilizados por outro processo.

No processo de Cadastro, o último subprocesso a ser completado é o de Armazenamento de dados, onde o template é armazenado em um dispositivo de armazenamento do sistema biométrico.

Já no processo de Autenticação, o subprocesso a ser seguido é o de Comparação, onde é feita a comparação entre dois templates - um já cadastrado no sistema no processo de Cadastro e outro do dado que foi capturado no proceso de Autenticação - determinando assim o grau de correlação, isto é, o quanto eles são parecidos.

Este processo de comparação resulta numa pontuação que é comparada a um limiar de correlação, também previamente determinada pelo administrador do sistema. Dependendo da pontuação atingida, o sistema definirá se os templates são da mesma pessoa ou não.

Entretanto na Autenticação 1:1 o usuário precisa, necessariamente, apresentar uma identificação própria. Com esta informação, o sistema busca o cadastro da pessoa e compara o template do dado coletado na autenticação com o template do dado cadastrado. Enquanto que na Autenticação 1:N o template do dado coletado na autenticação é pode chegar a ser comparado com todos os templates que constam no dispositivo de armazenamento.

3.1. Requisitos do Sistema Biométrico Padrão

Os sistemas biométricos podem ser esquematizados em processos básicos, comuns às diversas implementações destes, que são a aquisição, o cadastro e a autenticação. Esses processos compõem os requisitos funcionais de um sistema biométrico padrão, já que estas são operações essenciais para o sistema abordado.

Segurança (evasão), desempenho e aceitabilidade são os requisitos não funcionais do sistema biométrico padrão (Figura 5). Eles definem características que os requisitos funcionais devem atender para que o seu funcionamento seja considerado adequado por quem fará uso deste. É esperado que um sistema biométrico seja seguro, seja aceito pelas pessoas que estarão interagindo com ele e que tenha o melhor desempenho possível. O desempenho se refere à realização do reconhecimento da característica com velocidade e precisão; a aceitabilidade indica o quanto as pessoas estão dispostas a utilizar sua biometria em seu cotidiano e a segurança o quanto o sistema fornece meios para que se tenha a menor taxa de evasão possível. Evasão indica quão suscetível o sistema é a possíveis fraudes.

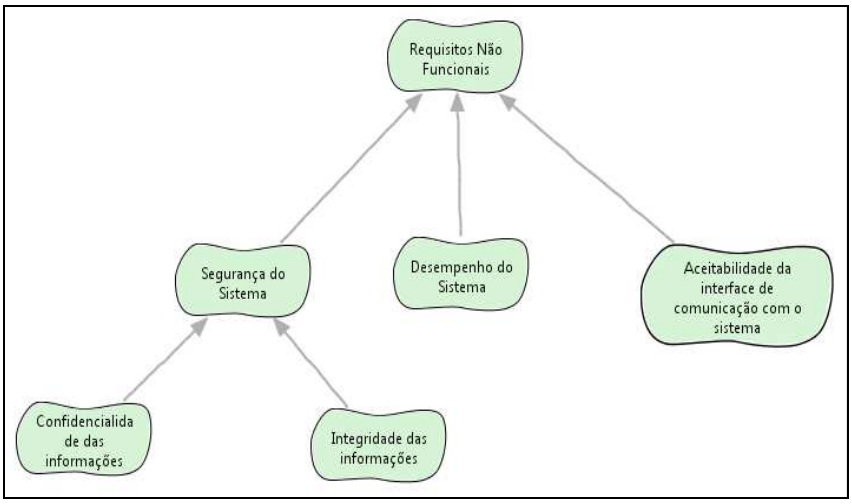

Figura 5. Requisitos Não-Funcionais do Sistema Biométrico Padrão

4. Modelagem i* para o Sistema Biométrico Padrão

O framework i* proposto por Yu [1],[2],[10], usa dois modelos: o modelo SD (*Strategic Dependency*) e o modelo SR (*Strategic Rationale*). Além desses modelos foi utilizado, também, o modelo SDSituations proposto em Oliveira [11] que permite uma melhor compreensão do domínio a ser modelado. SDSituations (Situação de dependência estratégica) representam, de forma estruturada, situações de dependência estratégica, onde cada dependência faz parte de uma situação bem definida de colaborações entre os atores envolvidos. Sua estrutura permite descrever situações que podem ou não funcionar como pré requisito de outra. Este modelo amplia a percepção das alternativas pelas quais o sistema poderá passar, refina e organiza as metas do sistema.

No estudo feito para a identificação dos atores presentes no domínio, primeiramente foram identificados os atores Pessoa e Sistema. Eles possuem relação direta de dependência para o alcance das metas definidas para ambos. O ator Sistema foi dividido em outros 3 atores: Gerenciador de Aquisição de Dados Biométricos (Aquisição Bio), Gerenciador de Cadastramento de Dados Biométricos (Cadastramento Bio) e Gerenciador de Autenticação de Dados Biométricos (Autenticador Bio). Essa

divisão foi proposta, principalmente, pela intensa interação entre eles, fornecendo e consumindo produtos do alcance de suas metas em comum.

Os *SDSituations* exibidos na figura 6 têm por objetivo relacionar as dependências e pré-requisitos entre os processos, além de explicitar as principais decisões tomadas pelo sistema. Primeiramente, para iniciar o sistema, foi definido o componente "*Adquirir Dado Biométrico*", que é a união dos subprocessos definidos de Aquisição de Sinais, Análise e Processamento de Sinais – subprocessos presentes em todos os processos pertencentes a um sistema biométrico, como pode ser visto nas Figura 2, 3 e 4.

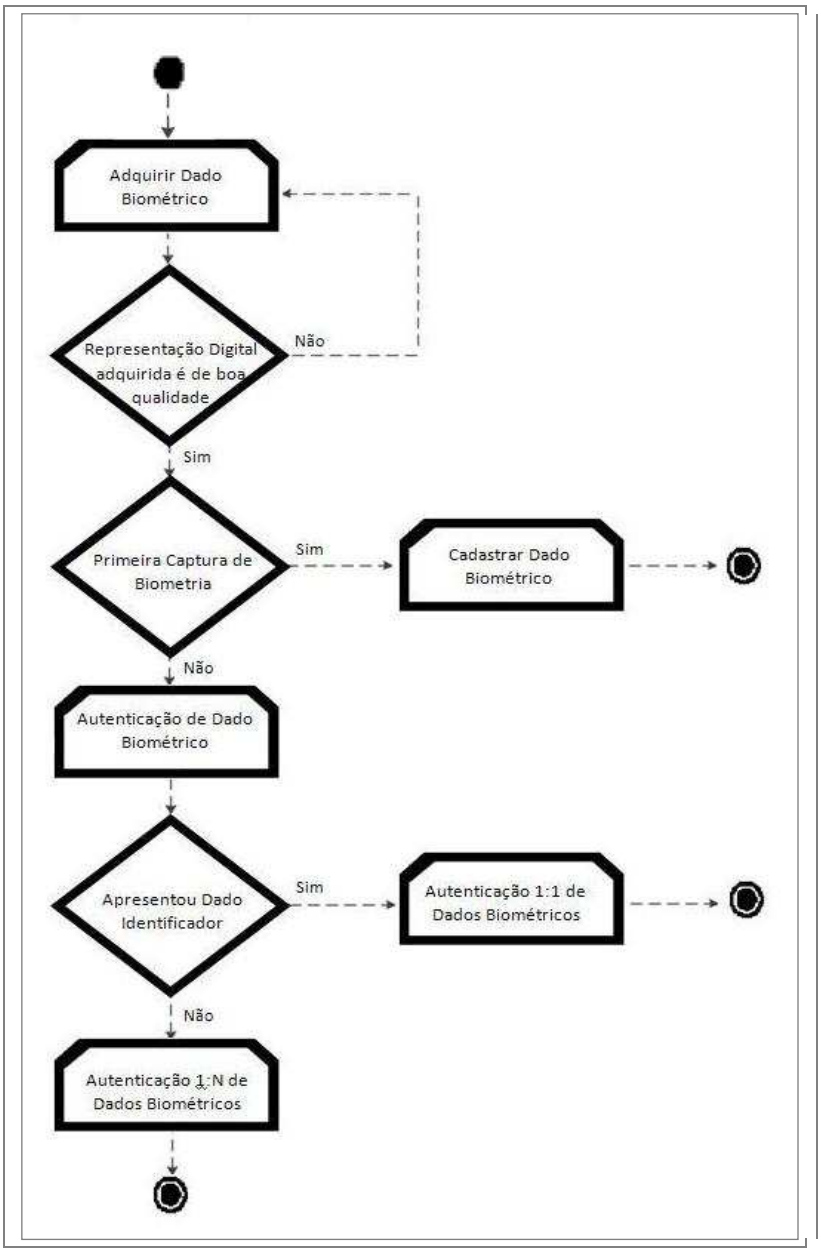

Figura 6. SDSituations do Sistema Biométrico Padrão

Além de estar presente em todos os processos, como ele também é o ponto inicial do sistema, provê a primeira condição para o fluxo do sistema: quando verifica se a representação digital adquirida possui a qualidade mínima para ser utilizada pelos componentes que dependem dela, ou seja, dos dados apresentados pela pessoa.

Desta forma, existem duas situações possíveis: *Dado Biométrico Adquirido Com Qualidade Inferior à Mínima Definida pelo Sistema* e *Dado Biométrico Adquirido Com Qualidade Superior à Mínima Definida pelo Sistema*. Após a representação digital passar pelo limiar mínimo de qualidade, o sistema verifica, no repositório de armazenamento, se aquele dado já foi cadastrado no sistema ou não: isto pode ser feito, por exemplo, através da busca por um dado pessoal cadastrado no dispositivo de armazenamento, como o nome ou algum número identificador; ou através da apresentação da biometria e da sua busca pelo dispositivo de armazenamento. Em ambos os casos, o sistema retornará a confirmação da existência ou não do cadastro da pessoa. Caso a verificação confirmar a não existência da pessoa no cadastro, tem-se a *situation Cadastrar Dado Biométrico*. Se os dados referentes à pessoa já estiverem armazenados, a *situation* é de *Autenticação dos Dados*.

O sistema deve ser capaz de autenticar a identidade de uma pessoa – seja através de uma varredura pela coleção de representações biométricas armazenadas, seja através da comparação com uma única representação. Essas duas formas de autenticação tem muitos pontos em comum, porém contem peculiaridades significativas na execução do processo. Neste momento, a principal diferença entre os mecanismos de autenticação é a apresentação de um dado identificador por parte da pessoa que está interagindo com o sistema. Os processos associados a este recurso do sistema são Autenticação 1:N, ou seja, autenticar 1 (uma) pessoa procurando no meio de muitas representações biométricas – representadas através da letra N – e a Autenticação 1:1, ou seja, autenticar 1 (uma) pessoa comparando-a com 1 (uma) única representação biométrica retornada da busca do resultado da apresentação do dado biométrico.

A seguir os modelos SD foram definidos seguindo a estrutura dos componentes contidos no SDSituation. Cada um deles é correspondente a um processo e cada processo é representado pelas dependências estratégicas dos atores. Foram definidos SD para Aquisição de Dados Biométricos, Cadastramento de Dados Biométricos, Autenticação 1:1 de Dados Biométricos e Autenticação 1:N de Dados Biométricos.

No processo de *Aquisição de Dados Biométricos*, ilustrado pela figura 7, foram identificados dois atores envolvidos: *Pessoa* e Gerenciador de Aquisição de Dado Biométrico. Os elementos que os relacionam são: recurso *Leitor Biométrico* e as metas *Biometria Seja Capturada*, *Características da Representação Digital Sejam Obtidas* e *Template Seja Formado*.

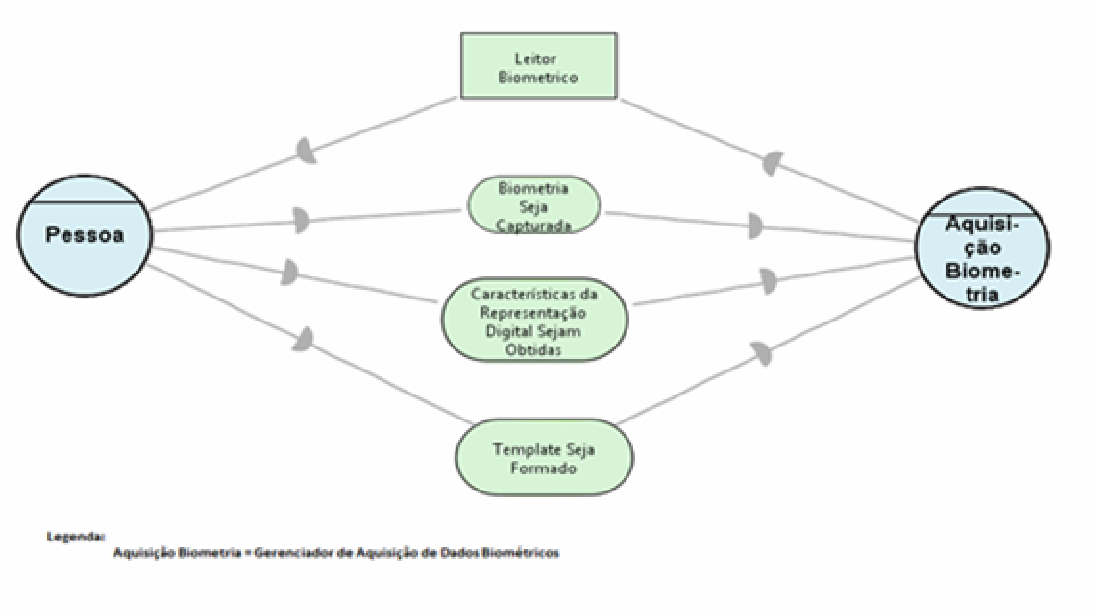

Figura 7. Modelo SD Aquisição de Dados Biométricos

Para que o objetivo deste processo seja cumprido, todas as metas devem ser satisfeitas. Primeiramente, para que a meta *Biometria seja capturada* seja obtida, o ator *Pessoa* depende que ator *Gerenciador de Aquisição de Dados Biométricos* faça a captura da biometria. Com o propósito de alcançar esta meta, o *Gerenciador de Aquisição de Dados Biométricos* depende que o ator *Pessoa* realize algumas tarefas (que foram descritas no modelo SR). Desta forma o *Gerenciador de Aquisição de Dados Biométricos* pode cumprir a meta *Características da Representação Digital Sejam Obtidas*, pois as características serão obtidas da biometria capturada. Em relação a esta meta, *Pessoa* depende do *Gerenciador de Aquisição de Dados Biométricos* extrair as informações relevantes da biometria oferecida.

A última meta a ser alcançada entre os atores *Pessoa* e *Gerenciador de Aquisição de Captura Biométrica* é *Template Seja formado*. O *template* será formado baseado nas características obtidas da representação digital. Novamente, *Pessoa* depende do *Gerenciador de Aquisição de Dados Biométricos* para que as informações sobre a biometria adquirida sejam organizadas num formato apropriado para os processos seguintes.

Após a definição dos SDs foram definidos os modelos SR correspondentes. Estes, de forma geral, se propõem a demonstrar como as dependências contidas no modelo SD serão satisfeitas, através da descrição de tarefas de cada componente existente no modelo SD referente. A modelagem completa dos SDs e SRs do sistema Biométrico padrão encontra-se em Salem e Rodrigues [12].

A Figura 8 mostra o modelo SR de *aquisição de dados biométricos* correspondente ao modelo SD da Figura 7. Para que a meta *biometria seja adquirida*, outras duas metas precisam ser realizadas: *biometria seja reconhecida*, relacionada com pessoa, e *biometria seja capturada*, relacionada a gerenciador de autenticação de dados biométricos.

A meta *Biometria seja reconhecida* para ser alcançada conta com a tarefa *apresentar dado biométrico* para ser concluída, que por sua vez se divide em duas partes: *possibilitar captura* e *encerrar apresentação*.

Já com gerenciador de aquisição de dados biométricos tem a meta *biometria seja capturada* sendo atendida pela tarefa *capturar biometria*. Esta tarefa se decompõe na tarefa *obter representação digital* e na meta *template seja formado*.

A tarefa *obter representação digital* depende do recurso *leitor biométrico*, que depende da tarefa ligada à *Pessoa*: *possibilitar captura*. Com esta tarefa concluída, o próximo passo é atingir a meta *características biométricas sejam obtidas*. Esta meta depende que a *Pessoa* execute a tarefa *possibilitar captura* para atender à dependência da meta *características da representação digital sejam capturadas*.

Características da representação digital sejam obtidas é uma meta que se divíde em três outras tarefas para ser alcançada. As três tarefas utilizam o recurso *algoritmo de processamento de representação digital*. Com a utilização deste algoritmo, sera possível *reduzir (possíveis) ruídos, isolar e extrair características mais importantes, avaliar qualidade da representação digital*. O cumprimento desta meta gera o recurso *representação digital processada*.

Outra atividade necessária para o sucesso da meta *biometria seja capturada* é a meta *template seja formado*, derivada da tarefa *capturar biometria*. Para que o *template seja formado*, a tarefa *criar template* deve ser realizada. Esta última precisa que a tarefa *recuperar representação digital processada* e *gerar template* sejam realizadas. *Recuperar representação digital* depende do recurso *representação digital processada* para ser completada. Com a representação recuperada, a tarefa *gerar template* pode ser executada. Esta gerará o recurso *template de dados biométricos adquiridos*, que dará suporte as atividades de outros atores do sistema.

No processo de aquisição de dado biométrico os requisitos não funcionais envolvidos são desempenho e aceitabilidade da interface de comunicação com o sistema. O sistema deve ser implementado de forma a oferecer a resposta para pessoa no menor tempo possível, além de não fornecer informações incorretas para nenhum receptor de dados que estão interagindo na obtenção da representação digital da biometria. Quanto à aceitabilidade, a interface com que a pessoa irá interagir com o sistema não deve oferecer dificuldades para que a biometria seja oferecida, bem como desconforto ou constrangimento. Pessoa deve aceitar interagir com o sistema para que a biometria seja capturada.

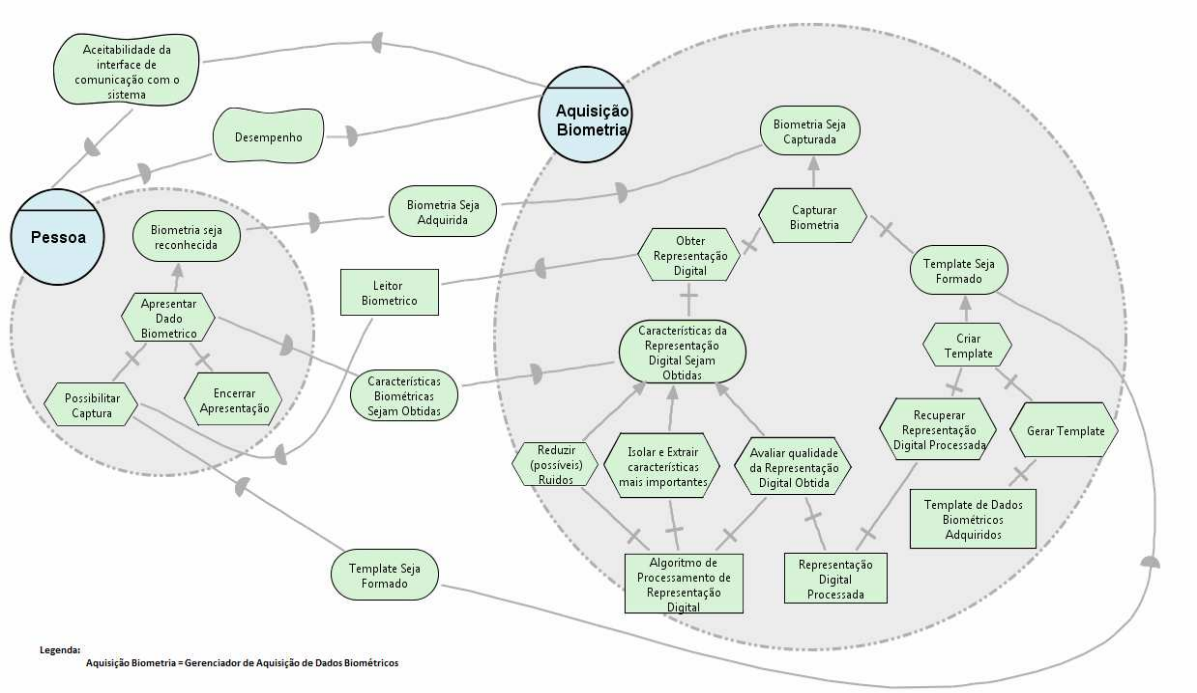

Figura 8. Modelo SD Aquisição de Dados Biométricos

5. Conclusões e Trabalhos Futuros

A cada dia que passa, sistemas biométricos estão sendo adotados como instrumento para o reconhecimento automatizado dos indivíduos, para diversos fins. A biometria é considerada uma tecnologia suficientemente segura e eficaz, na medida em que as características analisadas pelos dispositivos são únicas e estão no corpo, tornando assim as possibilidades de fraude menores. Além da segurança, outra vantagem existente neste mecanismo é a comodidade, pois o individuo se torna literalmente sua senha, não sendo necessário memorizar tantos códigos.

Considerando tais vantagens apresentamos os aspectos relacionados à utilização da biometria em sistemas computacionais e a modelagem de um sistema biométrico, para cadastro e autenticação de indivíduos, que funcione para diferentes tipos de biometria. Diferentes tipos de leitores biométricos podem ser utilizados, possibilitando uma maior conexão com outras tecnologias, inclusive móveis, como já temos visto em esboços de projetos construídos.

Por isso, neste trabalho foi proposta uma modelagem genérica de um sistema que atenda a qualquer tipo de biometria definindo os requisitos funcionais e não-funcionais de sistemas biométricos. Esta é uma atividade de suma importância no desenvolvimento de sistemas complexos.

Futuramente pretendemos aplicar esse modelo no desenvolvimento de sistemas biométricos reais para poder não só avaliar o modelo como aprimorá-lo, e analisar os benefícios dessa abordagem.

Referências

[1] Yu, E. (1995). Modeling Strategic Relationships for Process Reengineering, Ph.D. Thesis, Graduate Dept. of Comp. Science, University of Toronto.

[2] Yu, E., Giorgini, P., Maiden, N., Mylopoulos, J.. Social Modeling for Requirements Engineering, MIT Press, 2010.

[3] Woodward Jr., John D.; Orlans, Nicholas M.; Higgins, Peter T. Biometrics. McGraw-Hill / Osborne. 2003.

[4] Cysneiros,L.M. and Leite, J.C.S.P.; Non-Functional Requirements: From Elicitation to Conceptual Model" IEEE Transactions on Software Engineering – May, 2004

[5] Chung, L.; Nixon, B.; Yu, E.; Mylopoulos, J.; Non-Functional Requirements in Software Engineering – Kluwer Academic Publishers, Massachusetts, USA, (2000).

[6] Jain, Anil K.; Ross, Arun; Pankanti, Sharath; Biometrics: A Tool for Information Security. IEEE Transactions on Information Forensics and Security. Vol. 1 No. 2. June 2006.

[7] Jain, Anil K.; Ross, Arun; PRABHAKAR, Salil An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics. Vol. 14 No. 1. January 2004.

[8] Miller, Benjamin Vital signs of identity. IEEE Spectrum. February 1994.

[9] Uludag, Umut; Pankanti, Sharath; Prabhakar, Salil; Jain, Anil K. Biometric cryptosystems: Issues and challenges. 2004.

[10] Yu, Eric; Liu, Lin; Li, Ying Modelling Strategic Actor Relationships to Support Intellectual. Property Management. Trust in Cyber-Societies - Integrating the Human and Artificial Perspectives. eds. LNAI-2246. pag.175-194. 2001.

[11] Oliveira, A. P., Engenharia de Requisitos, um Método de Elicitação, Modelagem e Analise de Requisito, Tese, PUC Rio, Brasil, 2007.

[12] Salem, N. e Rodrigues, J. A. N. T., Modelagem: Um sistema Biométrico para Diferentes Tipos de Biometria utilizando o Framework i*, Projeto Final do Curso de Ciência da Computação, UERJ, 2011.