Julíbio David Ardigo

Modelo de Infra-estrutura de Chaves Públicas como Organização Virtual para Processos de Avaliação Somativa à Distância

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Santa Catarina como requisito parcial para obtenção do grau de Doutor em Engenharia de Produção.

Orientador: Prof. José Franciso Salm, Ph. D.

Florianópolis, Março de 2004

Modelo de Infra-estrutura de Chaves Públicas como Organização Virtual para Processos de Avaliação Somativa à Distância

Julíbio David Ardigo

O candidato foi julgado aprovado na Tese de Doutorado para obtenção do título de Doutor em Engenharia de Produção.

Prof. Edson Pacheco Paladini, Dr.
Coordenador do Curso

Banca Examinadora

Prof. José Francisco Salm, Ph. D.
Orientador

Prof. Carlos Roberto De Rolt, Dr.

Prof. Luis Gonzaga Mattos Monteiro, Dr.

Prof. Ricardo Felipe Custódio, Dr.

Prof. Walter Celso de Lima, Dr.

Agradecimentos

Inicio esta seção reconhecendo o apoio dispensado pelas instituições nas quais atuo, ESAG/UDESC e Funcitec, para a realização deste trabalho.

Agradeço em particular ao meu orientador, Professor José Francisco Salm, Ph. D. em administração, pela confiança demonstrada em mim ao aceitar este desafio, sem a qual este trabalho sequer teria iniciado.

No mesmo sentido faço um agradecimento especial ao meu amigo, Professor Ricardo Felipe Custódio, Doutor em ciências da computação, pelo amparo dado a este projeto, cuja participação equivaleu-se a de um co-orientador, fundamental para a consecução deste intento.

Ainda relativo a ajuda recebida para realização deste trabalho, agradeço aos Professores mestres em pedagogia Mariano Castro Neto, Vera Lúcia Silva de Souza e Alba Regina Battisti de Souza, pelas trocas de idéias e disponibilização de material sobre o tema avaliação; ao Bacharel em ciência da computação, Ricardo Barbi dos Santos, pelo seu apoio no uso de ferramentas de modelagens; aos mestres em ciências da computação, Fernando Carlos Pereira e Adriana Elissa Notoya, pelo subsídio e acaloradas discussões que refinaram esta proposta em termos de segurança da informação; e ao Professor Carlos Roberto De Rolt, Doutor em engenharia de produção, pelas suas colaborações relativas ao tema organizações virtuais e sua utilização em infra-estruturas de chaves públicas.

Igualmente importante foi o apoio recebido dos amigos e familiares, bem como sua compreensão pelas ausências, em especial de minha esposa, Leliane, e filhos, Juliane e David, que junto comigo sofreram as angústias da realização de um projeto desta envergadura.

Por fim, agradeço a todos que de alguma forma tenham contribuído para a consecução deste trabalho.

Resumo

O objetivo do presente trabalho é o de propor um modelo de infra-estrutura de chaves públicas como organização virtual para processos de avaliação somativa à distância mediada por computador que satisfaça os requisitos mínimos de segurança e diminua os custo de utilização desta tecnologia em relação ao processo apresentado com a utilização da infra-estrutura de chaves públicas convencional. Como estratégia inicial, foi modelado um processo de avaliação somativa a distância convencional, representado pela “Linguagem de Modelagem Unificada” - UML, adotando a metodologia de “Processo Unificado da Rational” - RUP. A aplicação desta metodologia iterativa incremental resultou em uma visão múltipla dos processos envolvidos e seu melhor entendimento. Após esta modelagem, agregou-se sistemas computadorizados ao processo para se obter um modelo de avaliação somativa à distancia mediada por computador. A questão da segurança de informações foi solucionada por meio de infra-estrutura de chaves públicas, que demandou a proposição de uma política para uma infra-estrutura de chaves públicas aplicada a avaliação. No intuito de minimizar os custos, oriundos da implementação desta infra-estrutura, propôs-se um modelo de infra-estrutura de chaves públicas como organização virtual aplicada a processos de avaliação somativa à distância, inspirado na disseminação de tecnologias de informação e comunicação nas organizações e do surgimento de novos modelos organizacionais. A solução proposta tende a reduzir os custos de implementação baseando-se no curto período de vida destes processos e na possibilidade de aproveitamento dos recursos disponíveis nos parceiros que os implementam. Além disto, esta proposta, mantendo o atendimento a todos os requisitos de segurança garantidos pela utilização de uma infra-estrutura de chaves públicas convencional, amplia a possibilidade de gerenciamento cooperativo entre os parceiros.

Palavras chaves: organização virtual, infra-estrutura de chaves públicas, avaliação à distância.

Abstract

The aim of this work is to consider a public key infrastructure model as virtual organization for processes of distance summative assessment aided by computer. This model meets the minimum-security requirements and reduces the usage cost of this technology compared to the process presented with the use of conventional public key infrastructure. As an initial strategy, a conventional process of distance summative assessment was modeled, noted in Unified Modeling Language - UML and adopting the methodology of Rational Unified Process - RUP. The application of this iterative incremental methodology resulted in a multiple view of the processes involved and a better understanding of them. After this modeling, computerized systems were added to the process so that a model of distance summative assessment aided by computer could be achieved. The question of the information security was addressed by a public key infrastructure, which required the proposition of a policy for a public key infrastructure applied to assessment. In order to minimize costs, deriving from the implementation of this infrastructure, a public key infrastructure model as virtual organization applied to distance summative assessment process was proposed. This approach was inspired by the dissemination of information and communication technologies in the organizations and the sprouting of new organizational models. The proposed solution tends to reduce implementation costs due to the short lifetime of these processes and the possibility of making use of these resources, which are available in the partners who implemented them. This proposal, besides meeting all security requirements through the use of a conventional public key infrastructure, extends the possibility of cooperative management among the partners.

Keys words: virtual organization, public key infrastructure, distance assessment.

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Apresentação do Tema

A evolução e disseminação da tecnologia de informação e comunicação tem revolucionado o cotidiano das pessoas de tal forma que é difícil desconsiderá-la. Esta constatação transcende o indivíduo, sendo fortemente percebida por organizações de diferentes áreas e características (DEWETT; JONES, 2001).

Uma das áreas que está sofrendo forte influência desta evolução é a do ensino. Além de facilitar o acesso à informação, estas tecnologias possibilitam a implementação de novos modelos de capacitação, sobretudo a capacitação mediada por computador, com ênfase no ensino à distância (PARIKH; VERMA, 2002).

Sob a ótica das organizações, a difusão da tecnologia de informação e comunicação incrementa a dinâmica das mudanças, atribuída à diminuição da distância e do tempo necessário para o acesso e troca de informações (PHILIP; BOOTH, 2001). Este ambiente dinâmico favorece a valorização da capacitação (ENSHER; NIELSON; GRANT-VALLONE, 2002), que demanda novos modelos de capacitação, como ilustrado na figura 1.1.

As reações a esta demanda são particulares à indivíduos, governos e organizações, em especial, instituições educacionais. No caso dos indivíduos a reação mais perceptível é a busca de capacitação em instituições com reconhecimento público ou certificação reconhecida pelo mercado (LANG, 2001). Já os governos, além de aumentarem as exigências em relação aos seus quadros de pessoal, têm regulamentado formas alternativas de capacitação e certificação, como o ensino à distância, conforme descrito pela Secretaria de Educação à Distância (SEED), do Ministério da Educação e Cultura (MEC) (BRASIL, 2003). As organizações, de forma geral,

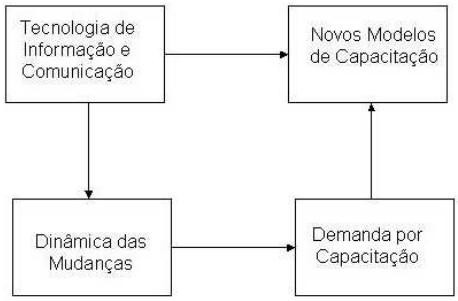

Figura 1.1: Difusão das tecnologias de informação e comunicação demanda novos modelos de capacitação

têm reagido pelo incremento do investido na capacitação de seus colaboradores (TAO; HOB; YEH, 2001) e enfatizando, nos processos de seleção e promoção de pessoal, o quesito da qualificação (ENSHER; NIELSON; GRANT-VALLONE, 2002). Esta política fica evidenciada com a disseminação das denominadas universidades corporativas (EBOLI, 2000). Já as instituições educacionais, por sua vez, têm buscado se adequar a esta nova realidade e atender esta demanda (CARSWELL, 1998).

Estas respostas à demanda imposta pela disseminação das tecnologias de informação e comunicação requerem novos processos de capacitação, certificação e seleção (ENSHER; NIELSON; GRANT-VALLONE, 2002), com formas compatíveis de avaliação (ROVAI, 2000), conforme ilustrado na figura 1.2.

O processo de avaliação, em termos gerais, possui um espectro de significados e aplicações muito amplo (VERBO, 2003). Este trabalho trata a avaliação como o método utilizado para determinar e classificar o domínio de um indivíduo sobre determinado assunto ou sua capacidade de realizar tarefas específicas, podendo ser enquadrada como avaliação somativa (LOPES; BARBOZA, 2003; SANTOS, 2002).

Porém, independentemente da definição adotada, pressupõe-se que este tipo avaliação deva ser um processo equitativo em termos de classificação, que dê igualdade de oportunidade entre os participantes, e eficaz, por determinar o real domínio ou capacidade do indivíduo (BAKER; MAYER, 1999). As características apresentadas são implícitas, ou esperadas, em processos de avaliação comuns a nossa rotina, como: provas; trabalhos; vestibulares; e concursos, que comumente, são presencias.

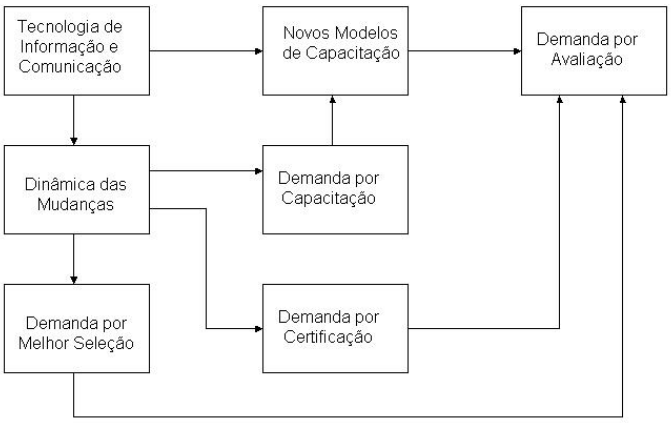

Figura 1.2: Difusão das tecnologias de informação e comunicação demanda novos modelos de avaliação

As avaliações presenciais são, em geral, aplicadas simultaneamente em um mesmo ambiente físico. Já a avaliação à distância pode ser um processo no qual o avaliado se submete a avaliação em diferentes momentos, condições e recursos, o que dificulta preservar as características de eqüidade e eficácia em todos as suas fases (ROVAI, 2000). Portanto, a avaliação somativa a distância, com objetivos de certificar e selecionar, pode ser encarada como um processo avaliativo cuja abrangência espacial foi ampliada por minimizar ou eliminar a necessidade da presença simultânea dos envolvidos em um mesmo ambiente físico.

Ocorre que, enquanto observa-se uma evolução nos processos de capacitação, em especial no ensino à distância mediado por computador, onde diferentes tipos de mídia, armazenamento, acesso e transmissão de informação, ampliaram as possibilidades de utilização desta modalidade de ensino (PARIKH; VERMA, 2002), os processos de avaliação, sobretudo os de avaliação somativa, têm-se mostrado mais conservadores (ROVAI, 2000), como ilustrado na figura 1.3.

Tem-se observado que a prática mais comum em relação a avaliação à distância é portar métodos de avaliação presencial para o mundo virtual [1] (BAKER; MAYER, 1999). Porém, esta prática compromete as características fundamentais de eqüidade e eficácia. Para contornar estas dificuldades, em alguns cursos de ensino à distância adota-se a metodologia de avaliação

[1] utilizado aqui em contraste com o mundo físico

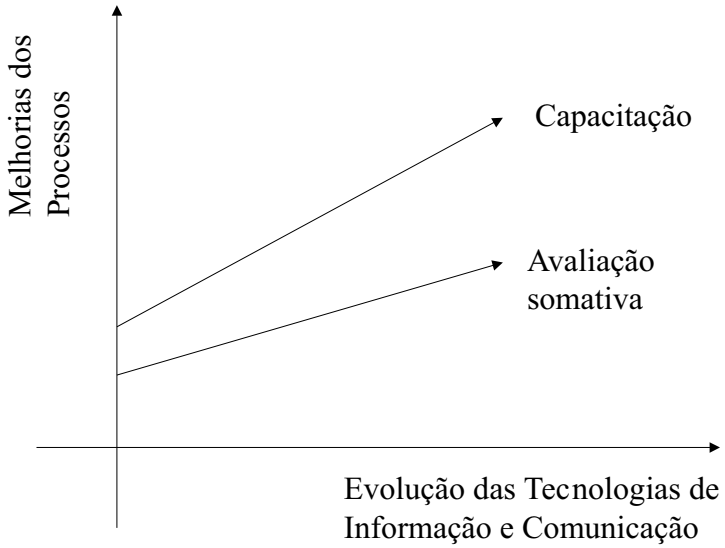

Figura 1.3: Ilustração da evolução dos processos em função das tecnologias de informação e comunicação

presencial convencional (ROVAI, 2000), enquanto em outros foca-se a avaliação à distância no processo contínuo de ensino / aprendizagem (LUCAS, 2001), minimizando os aspectos negativos de se portar os métodos presenciais para o mundo virtual. Entretanto esta última abordagem tem alcance limitado quando aplicada a processos de seleção e certificação, onde a avaliação tende a ser mais pontual.

1.1 Discussão do tema e do problema

Em resumo, pode-se constatar que a disseminação das tecnologias de informação e comunicação teve um impacto menor na avaliação somativa, aplicável a processos de certificação e seleção, do que no processo de capacitação (ROVAI, 2000).

Entretanto, o aparecimento da criptografia de chaves públicas, que é uma tecnologia de informação e comunicação, bem como sua apropriação por parte das organizações, possui o potencial de mudar este cenário. Esta tecnologia é a base para implementação de uma infraestrutura de chaves públicas que viabiliza as seguintes características à documentos eletrônicos: autenticação, que garante a autoria; integridade, que garante o conteúdo; confidencialidade, que assegura o acesso apenas as pessoas autorizadas; irretratabilidade, que torna inviável a

alguém negar o envio ou recebimento; e tempestividade, que confere data e hora ao documento eletrônico.

Um exemplo claro de onde esta tecnologia pode ser aplicada é a implementação de concursos para seleção de pessoal baseado em avaliação somativa. Facilmente pode-se presumir a aplicabilidade das características elencadas em todas as fases do processo, da elaboração e aplicação à correção.

Nesta abordagem pode-se vislumbrar as potencialidades de se implementar este processo pela parceria de várias organizações, valendo-se da disseminação dos recursos da tecnologia de informação e comunicação. Muitas delas estão utilizando estas tecnologias como suporte para mudanças no modelo organizacional (KEIL et al., 2000), como organizações de aprendizagem (ROBEY; BOUDREAU; ROSE, 2000) e organizações virtuais (PANTELI; DIBBEN, 2001), facilitando a implemetação de parcerias temporárias.

É importante destacar que as organizações virtuais estão embasadas em princípios de confiança mútua (KASPER-FUEHRERA, 2001), a qual pode ser garantida através da tecnologia de infra-estrutura de chaves públicas (LI; DAI; ZHANG, 2001), princípios estes que são intrínsecos ao processo de avaliação somativa à distância.

Pelo exposto, levanta-se a hipótese de que uma infra-estrutura de chaves públicas no contexto de organizações virtuais possa ser utilizada em um processo de avaliação somativa à distância mediada por computador, de forma a reduzir os custos em relação a utilização de infra-estrutura de chaves públicas convencional.

Assim o problema a ser resolvido é o de como implementar uma infra-estrutura de chaves públicas como organização virtual aplicável ao processo de avaliação somativa à distância, que satisfaça a hipótese formulada.

1.2 Objetivos

Os objetivos do presente trabalho são apresentados a seguir, subdivididos em objetivo geral e específicos.

1.2.1 Objetivo geral

O objetivo geral desta tese é o de propor um modelo de infra-estrutura de chaves públicas como organização virtual para processos de avaliação somativa à distância mediada por computador que satisfaça os requisitos mínimos de segurança e diminua os custo de utilização desta tecnologia em relação ao processo apresentado com a utilização da infra-estrutura de chaves públicas convencional.

1.2.2 Objetivos específicos

Para atingir o objetivo geral os seguintes objetivos específicos devem ser alcançados:

- Modelar um processo de avaliação somativa à distância;
- Modelar um processo de avaliação somativa à distância mediado por computador;
- Propor um modelo de avaliação somativa à distância, mediado por computador, que utilize uma infra-estrutura de chaves públicas; e
- Propor um modelo de infra-estrutura de chaves públicas, no contexto de organizações virtuais, para o modelo de avaliação somativa à distância proposto.

1.3 Justificativa

A motivação inicial deste estudo foi de cunho pessoal do autor. Como egresso de cursos à distância realizado na adolescência, sempre questionou a cerca da viabilidade técnica e econômica de se implementar processos de avaliação que aumentassem a aceitabilidade deste tipo de capacitação. Ainda sob a ótica pessoal, a larga experiência na utilização da tecnologia de informação e comunicação no ambiente acadêmico[2] culminou com a coordenação e o desenvolvimento de um sistema de apoio à aprendizagem, denominado POLVO, utilizado em

[2]como coordenador da área de informática da Universidade do Estado de Santa Catarina - UDESC, do projeto de internet acadêmica em Santa Catarina - RCT-SC, da capacitação e avaliação do PROINFO em Santa Catarina, do concurso CIASC 2002 e como co-orientador de dissertações de mestrado na área (Zabot, 2001) e (Bonelli, 2000).

vários cursos de extensão e pós-graduação, promovidos pelo LabTIC[3], e em disciplinas de vários cursos de graduação da UDESC. Na utilização deste sistema, novamente ficou evidenciado a carência de um processo de avaliação somativa à distância, mediada por computador, passando este a ser outro fator motivador do presente trabalho.

Em paralelo a experiência pessoal tem-se o interesse institucional da UDESC frente ao ensino e, conseqüentemente, a avaliação à distância. Atualmente, a UDESC é uma das instituições brasileiras com maior número estudantes de graduação na modalidade de ensino à distância. Seu processo de avaliação é implementado no modelo de avaliação presencial. O trabalho proposto pode configurar-se como uma alternativa adicional ao modelo imperante, mantendo a seriedadade e transparência do processo atual.

Adicionalmente, como é grande a demanda por capacitação à distância no Brasil, dado a exigências legais e geográficas (BRASIL, 2003), a aplicação da proposta poderá implicar na possibilidade de: inclusão de mais pessoas nos processos de capacitação, certificação e seleção; ampliação da abrangência geográfica do processo de avaliação; redução de custos do processo de avaliação; ampliação da oferta de processos de certificação; aumento de confiabilidade da avaliação à distância e conseqüentemente dos cursos de ensino à distância.

Por outro lado, esta pesquisa em si já deixa como legado um estudo científico da sobreposição das áreas de tecnologia de informação e comunicação nas organizações, organizações virtuais, infra-estrutura de chaves públicas, e avaliação somativa à distância mediada por computador.

1.4 Originalidade e ineditismo

Uma característica necessária ao presente trabalho é a originalidade. O termo original, do latim *originali*, implica em um trabalho de caráter próprio, que é criação do autor, não sendo cópia, imitação ou tradução (GRANDE..., 2003). O presente trabalho é fruto da experiência deste autor, da discussão deste com pesquisadores que atuam nas áreas de conhecimento envolvidas, juntamente com uma pesquisa bibliográfica ampla destas áreas de conhecimento e de como elas interagem entre si, sendo portanto original e não cópia ou tradução de outro trabalho.

[3]Laboratório de Tecnologias de Informação e Comunicação, que constitui-se em um grupo de pesquisa da ESAG/UDESC, cadastrado no CNPq e coordenado pelo autor

Entretanto, o fato deste trabalho ser original não implica na ausência de embasamento e inspiração em uma série de trabalhos disponíveis na literatura.

Dentre os trabalhos que abordam o tema de avaliação à distância mediado por computador, destaca-se o realizado por Rovai (2000), que apresenta os desafios de processos avaliativos nestas condições.

Com respeito a utilização de infra-estruturas de chaves públicas para contornar os desafios da avaliação não presencial tem-se o trabalho desenvolvido por Scheffel (2002), que foca um dos aspectos abordados por Podestá e Meinel (2000), que enfatiza a necessidade desta infra-estrutura em universidades virtuais.

Com respeito a trabalhos correlatos a montagem da infra-estruturas de chaves públicas como organizações virtuais, tem-se o realizado por Li, Dai e Zhang (2001), baseado no esquema de Takaragi, Miyazaki e Takahashi (2000).

No presente trabalho propõe-se uma infra-estruturas de chaves públicas como organização virtual, utilizando o esquema apresentado por Damgård e Koprowski (2001), aplicada a processos de avaliação somativa à distância.

Para se verificar o ineditismo da proposta foi realizada uma ampla pesquisa na literatura especializada em busca de trabalhos correlatos. Esta iniciativa foi tomada por se consider inédito (do latim *ineditu*) algo nunca visto, que acontece ou é feito pela primeira vez, ou ainda não publicado (GRANDE..., 2003). A amplitude desta pesquisa é detalhada no capítulo 2, página 22, especificamente na tabela 2.1.

Através da pesquisa mencionada, observou-se que, nem a maneira proposta para construção da infra-estrutura de chaves públicas como organizações virtuais, nem tampouco a aplicação destas a processo de avaliação à distância, foram encontradas na bibliografia científica disponível, comprovando a inediticidade desta proposta.

1.5 Limites da tese

O presente trabalho é desenvolvido com foco em um modelo de infra-estrutura de chaves públicas, no contexto das organizações virtuais, aplicada ao processo de avaliação somativa à distância mediada por computador. Apesar deste foco já restringir a abrangência do trabalho em si, é relevante enfatizar que a proposta:

- envolve a proposição de um modelo interpretativo, não tendo por objetivo explicar a teoria que o origina;
- se limita a tratar a avaliação somativa à distância dentro do contexto tecnológico atual;
- pressupõe a popularização das infra-estruturas de chaves públicas nas instituições;
- não objetiva discutir os modelos de avaliação, sob a perspectiva pedagógica;
- não visa esgotar qualquer dos tópicos envolvidos de forma individual.

1.6 Organização do documento

Após este capítulo introdutório, a exposição desta pesquisa é iniciada pela descrição da revisão realizada na literatura especializada, capítulo 2, página 22, seguida por um aprofundamento nos conceitos e serviços envolvendo criptografia, necessário para o entendimento das propostas, capítulo 3, página 50, e a descrição da metodologia empregada nesta pesquisa, capítulo 4, página 74. Os próximos capítulos focam no atendimento dos objetivos específicos, sendo apresentado um processo de avaliação somativa a distância no capítulo 5, página 92, um processo de avaliação somativa a distância mediado por computador, capítulo 6, página 104, e um processo de avaliação somativa a distância mediado por computador utilizando infra-estrutura de chaves públicas, capítulo 7, página 116. Por fim apresenta-se a proposta de uma infra-estrutura de chaves públicas aplicada a processos de avaliação somativa a distância mediada por computador, capítulo 8, página 148, e a conclusão deste trabalho, capítulo 9, página 171.

Capítulo 2

Revisão da Literatura

2.1 Introdução

Para se atingir os objetivos propostos no trabalho, fez-se necessário uma pesquisa bibliográfica ampla de várias áreas de conhecimento e de como elas interagem entre si.

As principais áreas abordadas nesta revisão envolvem:

- avaliação, em especial a avaliação somativa à distância;
- organizações, especificamente as organizações virtuais;
- infra-estrutura de chaves públicas; e
- infra-estrutura de chaves públicas no contexto das organizações virtuais.

Como estratégia para se realizar esta revisão utilizou-se como fonte de pesquisa, além de livros, teses, dissertações, recomendações, normas e legislação específica, uma série de periódicos científicos, disponíveis através do Portal da Capes, foram pesquisados para o levantamento do estado da arte sobre o tema.

A seguir é apresentado uma tabela que resume a extensão da pesquisa realizada.

Tabela 2.1: Periódicos Pesquisados

	Publicação	**TIC**[1]	**OV**[2]	**EAD**[3]	**SEG**[4]
1	Academic Exchange	0	0	4	0
2	Accounting Management and Information Technologies	1	0	0	0
3	Advances in cryptology - CRYPTO ’88 Proceedings, Springer-Verlag	0	0	0	1
4	Advances in Cryptology - CRYPTO ’98, LCNCS 1462	0	0	0	1
5	Advances in Cryptology - Proceedeings of Eurocrypt 93, LNCS 756	0	0	0	1
6	Bank Marketing	0	0	0	0
7	Card Technology Today	2	0	0	2
8	Clarkson University, Department of Math and Computer Science	0	0	0	1
9	Communications of the ACM	0	0	0	3
10	Computer Communications	0	0	0	2
11	Computer Law & Security Report	0	0	1	2
12	Computer Networks	0	0	0	2
13	Computer Standards & Interfaces	0	0	0	1
14	Computer-Aided Design	0	1	0	0
15	Computers & Education	0	0	6	0
16	Computers & Operations Research	0	1	0	0
17	Computers & Security	0	0	0	6
18	Computers and Composition	0	0	1	0
19	Computers in Human Behavior	0	0	4	0
20	Computers in Industry	1	0	0	0
21	CRYPTOBYTES	0	0	0	1
22	Decision Support Systems	2	0	1	2
23	Disponível na internet: www.mcs.le.ac.uk/ glowe/Security/Casper	0	0	0	1
24	European Management Journal	1	0	0	0
25	Expert Systems with Applications	1	0	1	0
26	Future Generation Computer System	0	0	0	1
27	Futures	0	1	0	0
28	Harvard Business Review	0	0	0	1
29	Head - School of Software Engineering and Data Communications	0	0	0	1
30	HP Laboratories Bristol	0	0	0	1
31	http://www.cs.technion.ac.il/ biham	0	0	0	1

Continua na próxima página

Tabela 2.1 – continuação da página anterior

	Publicação	**TIC**[1]	**OV**[2]	**EAD**[3]	**SEG**[4]
32	IEEE 8th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises	0	0	0	1
33	IEEE Transactions on Information Theory	0	0	0	1
34	IEEE Transactions on Software Engineering	0	0	0	1
35	Information & Management	2	1	2	0
36	Information and Organization	2	1	1	0
37	Information and Software Technology	0	0	1	0
38	Information Sciences	0	0	1	0
39	Information Security Technical Report	0	0	0	6
40	Information Systems	1	0	0	0
41	Institut für Telematik	0	0	0	1
42	Institut für Telematik e.V.,Trier	0	0	1	0
43	Int. J. Human-Computer Studies	0	0	1	0
44	Int. J. Production Economics	1	1	0	0
45	International Journal of Information Management	0	0	1	0
46	International Journal of Project Management	0	0	0	1
47	International Journal Production Economics	0	1	0	0
48	Internet and Higher Education	0	0	7	0
49	Internet Research: Electronic Networking Applications and Policy	0	1	0	0
50	ITiCSE	0	0	1	0
51	J. Systems Software	0	0	0	1
52	Journal of Business Research	1	0	0	0
53	Journal of Cryptology	0	0	0	1
54	Journal of High Technology Management Research	0	1	1	0
55	Journal of Management	2	2	0	1
56	Journal of Operations Management	2	0	0	0
57	Journal of Strategic Information Systems	2	0	0	0
58	Journal of Universal Computer Science	0	0	0	1
59	Learning and Instruction	0	0	1	0
60	Medical Education	0	0	1	0
61	National Institute of Standards and Technology	0	0	0	1
62	Network and distributed systems security	0	0	0	0
63	Network Security	0	0	0	2

Continua na próxima página

Tabela 2.1 – continuação da página anterior

	Publicação	**TIC**[1]	**OV**[2]	**EAD**[3]	**SEG**[4]
64	Organizational Dynamics	1	0	0	0
65	Proceedings of ECSCW'99 - The 6th European Conference on Computer Supported Cooperative Work	0	0	1	0
66	Proceedings of EUROCRYPT'91	0	0	0	1
67	Proceedings of Second International Workshop on Fast Software Encryption	0	0	0	1
68	Proceedings of the 35th Annual Hawaii International Conference on System Sciences	0	1	0	0
69	Proceedings of the Internet Society Symposium on Network and Distributed Security (NDSS'98)	0	0	0	1
70	Proceedings of Workshop on Fast Software Encryption	0	0	0	1
71	Public Key Cryptography '2000, LNCS 1751	1	0	0	0
72	Research Policy	0	0	0	0
73	School of Computer Science	0	0	0	1
74	Sequences'91: Methods in Communication, Security, and Computer Science	0	0	0	1
75	Technological Forecasting and Social Change	1	1	0	0
76	Technovation	1	1	0	0
77	The 1st International Conference on Information Security and Cryptology	0	0	0	1
78	The Journal of Academic Librarianship	0	0	1	0
79	The Journal of Consumer Affairs	0	0	0	1
80	The Journal of Systems and Software	1	0	0	0
81	U.S Patent	0	0	0	1
82	World Multiconference on Systemics, Cybernetics and Informatics	0	0	1	0
83	XII Simpósio Brasileiro de Informática na Educação - SBIE	0	0	1	0
84	Outras Fontes - diferentes de artigos publicados em periódicos científicos	4	1	14	51
	Total Global	30	15	55	109

Legenda:

[1] Tecnologia de Informação e Comunicação nas Organizações

[2] Organizações Virtuais

[3] Ensino e Avaliação à Distância

[4] Tecnologia de Segurança das Informações

Na seqüência deste capítulo é feita uma abordagem das principais áreas tratadas nesta revisão, subdividida nas seções: 2.2, que descreve o processo de avaliação; 2.3, que aborda as organizações virtuais; 2.4, relativa a infra-estrutura de chave pública; 2.5, que expõe a infra-estrutura de chave pública no contexto das organizações virtuais; e, por fim, na seção 2.6 é apresentada uma conclusão sobre o temas estudados.

2.2 Avaliação

Para que se possa aprofundar neste tema busca-se, na presente seção, conceituar avaliação, seus objetivos, instrumentos, etapas e características, bem como transpô-la para o contexto virtual e à distância.

2.2.1 Definição

O conceito de avaliação, em termos gerais, possui um espectro amplo de significados, porém, a partir da origem da palavra, pode-se conceituar avaliação como o ato de determinar a valia, as condições, a aptidão ou a capacidade (física ou intelectual) para realizar determinada tarefa (PORTO, 2003). Nesta mesma direção, Haydt (2002, p. 10) define que *"avaliar é interpretar dados quantitativos e qualitativos para obter um parecer ou julgamento de valor, tendo por base padrões ou critérios"*.

No presente trabalho, a avaliação é abordada no contexto da docimologia[1] (BONNIOL; VIAL, 1997). Entretanto, para que seja definida de forma ainda mais específica, é necessário se levar em consideração variáveis como o ator, a dimensão e os objetivos da avaliação. Assim,

[1] *"Estudo sistemático dos exames e da avaliação de conhecimentos"*(VERBO, 2003)

neste caso, tem-se o indivíduo como o ator a ser avaliado e seu domínio de conhecimento sobre determinado assunto, ou sua capacidade de realizar tarefas específicas, como as dimensões a serem avaliadas. Já os objetivos da avaliação merecem um tratamento a parte, o que é feito na seqüência.

2.2.2 Objetivos

Entre os objetivos básicos da avaliação pode-se destacar os de selecionar e certificar um indivíduo, bem como o de realimentar o processo ensino-aprendizagem. Segundo estes objetivos a avaliação pode ser denominada somativa, diagnóstica e formativa, além da denominação comportamental, muitas vezes utilizada.

Quando o processo de avaliação tem por objetivo a seleção, ele deve possibilitar a classificação dos participantes, ou seja, deverá possuir características discriminatórias. Um exemplo clássico deste tipo de avaliação é obtido a partir de testes padronizados. De acordo com Smith e Ragan (1999, p. 93),

> *"estes testes, após sua elaboração, são aplicados em grupos controle de forma a determinar as questões com maior e menor número de acertos, que serão eliminadas quando da aplicação final, permitindo assim uma distribuição normal dos resultados, garantindo a característica de discriminação entre os participantes"*[2].

Sob outra perspectiva, a avaliação para certificação busca determinar se um indivíduo é apto para realizar determinada tarefa, ou possui determinado nível de conhecimento sobre dado assunto. Sua principal diferença em relação à avaliação para seleção é que o objetivo discriminatório do instrumento de avaliação perde a relevância. Isto não implica que estes objetivos sejam mutuamente excludentes, entretanto, caso uma avaliação tenha por objetivos tanto a certificação quanto a classificação, uma das características se sobressairá no processo (SMITH; RAGAN, 1999).

Estas modalidades de avaliação são denominadas de avaliação somativa (SCRIVEN; STUFFLEBEAM, 1978). A avaliação somativa tem sido criticada na literatura pedagógica por colocar o objeto do conhecimento acima do indivíduo, àquele que detém o conhecimento, e avaliando mais seu equilíbrio emocional do que suas aptidões e o rendimento (LIMA, 1994). No entanto,

[2] tradução livre

este tipo de avaliação tem ganho espaço e aceitação em alguns segmentos, como os clássicos TOEFL (*Test of English as a Foreign Language*), GRE (*Graduate Record Exam*), Exame da OAB (Ordem dos Advogados do Brasil), vestibulares e concursos públicos, bem como os recentes ENEM (Exame Nacional de Ensino Médio), POSCOMP (exame que tem sido exigido para ingresso em programas *stricto sensu* em computação) e o teste da ANPAD (Associação Nacional de Programas de Pós-Graduação em Administração).

Já no processo de ensino-aprendizagem, apesar de se fazer uso da avaliação somativa para promoção dos alunos, enfoca-se mais a avaliação diagnóstica e formativa. A avaliação diagnóstica tem por objetivo determinar os conhecimentos prévios necessários para novas aprendizagens, bem como detectar dificuldades da aprendizagem. Já a avaliação formativa busca verificar se os objetivos da aprendizagem estão sendo alcançados pelos alunos e embasar melhorias no processo de ensino-aprendizagem (ROVAI, 2000).

Ainda correlato aos objetivos da avaliação, tem-se a abordagem comportamental ou *behaviorista*, cujo intuito é observar a resposta de um indivíduo a determinado treinamento, amplamente difundida no setor empresarial (LANG, 2001). Neste contexto a avaliação fica submetida a um esquema classificatório de objetivos educacionais. Um dos mais conhecidos destes esquemas aplicados a educação é a taxionomia de Bloom, que busca classificar os objetivos educacionais nas dimensões cognitiva, afetiva e psicomotora (BLOOM; HASTINGS; MADAUS, 1983), hoje, severamente criticada.

2.2.3 Instrumentos

Uma vez definido os objetivos da avaliação é necessário definir os instrumentos a serem utilizados. Para tal, deve-se levar em conta o grau de objetividade, ou subjetividade, dos dados levantados para análise do avaliador, que é uma das características marcantes do instrumento.

Segundo Smith e Ragan (1999), os instrumentos para análise de desempenho, são, em geral, mais subjetivos e de difícil aplicação em larga escala. Entre estes instrumentos destacam-se: tarefas reais, onde a avaliação se dá pela observação da realização destas tarefas; problemas, onde problemas reais são apresentados para que o avaliado resolva na forma escrita; dissertações, que permite que o avaliado exponha seu ponto de vista sobre atividades específicas; simulações, onde problemas reais são apresentados em um ambiente simulado, real ou virtual;

projetos, onde a avaliação é feita a partir de projeto a ser desenvolvido pelo avaliado; portfólio, onde os avaliadores abordam os projetos e trabalhos já realizados pelo avaliado.

Por outro lado, quando os objetivos são a classificação e certificação, os instrumentos mais comuns são testes de múltipla escolha, verdadeiro ou falso, associar, completar, ou mesmo de questões dissertativas (com respostas curtas). Sendo que sua elaboração deve levar em conta os objetivos da avaliação, conforme exposto na seção 2.2.2, página 27.

Além destes instrumentos de avaliação existem outros sendo utilizados, sobretudo na escola, como auto-avaliação e avaliação de grupo (WOS, 2002).

2.2.4 Características do processo avaliativo

Entre as características de um processo avaliativo, em especial os destinados a seleção e certificação, destacam-se sua validade, confiabilidade e praticidade (SMITH; RAGAN, 1999), bem como sua tradição, legalidade e credibilidade (BAKER; MAYER, 1999).

Segundo Haydt (2002), a validade da avaliação diz respeito ao seu poder de avaliar o que pretende avaliar. No caso de avaliações objetivas um instrumento é válido se: os itens individuais forem consistentes com as metas e objetivos a serem avaliados; os itens de cada objetivo forem representados e devidamente amostrados no espectro de perguntas; e, quando da aplicação de outros instrumentos de avaliação, igualmente válidos, na mesma turma, o resultado for semelhante.

Por outro lado a avaliação é confiável ou fidedigna se avalia consistentemente os seus objetivos. Esta característica garante que aquele que foi bem avaliado é competente e o que foi mal avaliado é incompetente naquele assunto. Isto implica que se a mesma avaliação for reaplicada na turma, sem nenhuma intervenção relacionada com o aspecto ensino-aprendizagem, o resultado deve ser semelhante. Vários fatores interferem na confiabilidade de um instrumento, entre eles detacam-se: objetividade; grau de acerto das respostas por sorte, como verdadeiro ou falso; instrumento que permite interpretações diferentes das respostas; tamanho do instrumento; clareza dos itens; qualidade das instruções; formato de prova em relação a familiaridade do avaliado; teste a partir do computador para um público não familiarizado; e, condições ambientais e emocionais (SMITH; RAGAN, 1999).

Já a praticidade ou viabilidade de um instrumento está relacionada com o custo e tempo

necessários a implementação de suas etapas. Por exemplo, pode-se considerar que uma das melhores modalidades de avaliação é a observação da execução de tarefas que envolvam o espectro de conhecimento desejado, com critérios bem definidos. Porém, o custo e o tempo necessários para aplicação deste tipo de avaliação em larga escala a torna inviável (HAYDT, 2002).

Portanto, segundo Smith e Ragan (1999), os instrumentos de avaliação devem contemplar equilibradamente suas características de validade, confiabilidade e praticidade.

Além das características mencionadas, o processo como um todo está associado a tradição, legalidade e credibilidade (BAKER; MAYER, 1999). Enquanto a tradição pode ser considerada como fator cultural, a legalidade abrange o atendimento das leis envolvidas no processo de avaliação específico. Já no que tange a credibilidade, esta pode ser associada a validade do processo, pois implica em se acreditar que foi avaliado o que se propôs avaliar.

A avaliação deve ser um processo eqüitativo em termos de classificação, ou seja, que dê igualdade de oportunidade entre os participantes, o que acaba por ser implícito a sua validade. Assim, neste trabalho, a validade da avaliação implicará não apenas no que esta sendo avaliado mas em como esta sendo avaliado, garantindo também a legalidade e credibilidade, quando presente em todas as fases do processo.

2.2.5 Etapas

Qualquer avaliação é composta por pelo menos três etapas críticas: elaboração; aplicação; e correção. Uma quarta etapa, não menos importante, porém mais relevante no processo ensino-aprendizagem, é a de interpretação da avaliação (FOWELL; SOUTHGATE; BLIGH, 1999) e (ROVAI, 2000).

Conforme Haydt (2002), a elaboração de uma avaliação envolve, em primeiro lugar, levar em consideração seus objetivos, como explanado na seção 2.2.2, página 27. A partir dos objetivos da avaliação e do conteúdo a ser avaliado pode-se escolher o instrumento a ser utilizado, conforme seção 2.2.3, página 28. Após determinar a extensão da prova e seu tempo de duração, pode-se iniciar a elaboração das questões, ou tarefas, e das instruções. Por fim, uma revisão e aperfeiçoamento são indicados, sendo que a aplicação da avaliação em grupos de controle pode ser necessária para garantir determinadas características do processo.

A etapa de aplicação da avaliação, além de ser crucial para a legalidade e credibilidade, pode influenciar o desempenho dos avaliados. Entre as variáveis que influenciam a aplicação destacam-se o tempo dado para a realização da avaliação, as condições ambientais, a percepção de seriedade e o domínio dos meios utilizados na avaliação por parte do avaliado (SMITH; RAGAN, 1999).

Já a etapa de correção é mais sensível ao tipo de instrumento utilizado. Enquanto questões objetivas requerem apenas um gabarito, as questões dissertativas, por exemplo, requerem critérios mais complexos, como uma tabela pontuando características específicas. Neste último caso é comum que mais de um avaliador corrija cada questão e que o resultado da avaliação seja comparado, sendo que uma nova correção deve ser requerida a um terceiro avaliador quando houver discrepância significativa (HAYDT, 2002).

Quanto à interpretação dos resultados, etapa mais aplicável à processos de ensino-aprendizagem, identifica lacunas de conhecimento dos alunos, requerendo reforços específicos, ou detectando falhas no processo em si (HACK, 2000).

Por fim, é importante ressaltar que uma deficiência em qualquer das fases do processo de avaliação pode comprometer o processo como um todo, sobretudo no que tange a sua validade.

2.2.6 Avaliação à distância

Em um processo de avaliação à distância o avaliado se submete a avaliação em diferentes momentos, condições e recursos, o que dificulta preservar as características de eqüidade e eficácia em todos as suas fases (ROVAI, 2000). Porém, a avaliação somativa a distância, com objetivos de certificar e selecionar, pode ser encarada como um processo avaliativo cuja abrangência espacial foi ampliada por minimizar ou eliminar a necessidade da presença simultânea dos envolvidos em um mesmo ambiente físico.

Tem-se observado que a prática mais comum em relação a avaliação à distância é portar métodos de avaliação presencial para o mundo virtual (BAKER; MAYER, 1999), como usual em cursos de ensino à distância. Porém, esta prática pode comprometer a validade do processo, sobretudo na eqüidade no mesmo. Para contornar estas dificuldades alguns cursos de ensino à distância adotam a metodologia de avaliação presencial convencional (KUMAR, 1999), enquanto outros focam a avaliação à distância no processo contínuo de ensino-aprendizagem

(LUCAS, 2001), minimizando assim os aspectos negativos de se portar os métodos presenciais para o mundo virtual. Entretanto esta última abordagem tem alcance limitado quando aplicada a processos de seleção e certificação, onde a avaliação tende a ser mais pontual.

Apesar da avaliação à distância existir como processo independente da utilização das novas tecnologias de informação e comunicação, a utilização de avaliação mediada por computador está redefinindo este processo (BULL, 1999).

2.2.7 Avaliação mediada por computador

A avaliação mediada por computador facilita a utilização de algumas formas de avaliação convencional e viabiliza diferentes abordagens, porém, traz consigo novos desafios.

A partir das facilidades implícitas à tecnologia de informação e comunicação, pode-se deduzir, de forma simplificada, que a utilização de testes objetivos é facilitada pelo uso do computador. Em realidade esta é a primeira geração de avaliação mediada por computador, que constitui-se em portar as denominadas provas convencionais para os computadores (BENNETT, 1998). Entre as vantagens técnicas deste procedimento, pode-se destacar a facilitação dos processos da: elaboração das questões, pelo incremento de comunicação entre os elaboradores e acesso à material de apoio e banco de questões; aplicação presencial, pela simplificação da logística de distribuição do material a ser aplicado, uma vez tendo-se a infra-estrutura; correção, principalmente quando as questões são objetivas (MCDONALD, 2002).

Mesmo nesta aplicação, aparentemente simples, existe o desafio de saber se a avaliação mediada por computador é equivalente a avaliação convencional. Neste sentido McDonald (2002) realizou um estudo, ilustrado na figura 2.1, no qual concluiu haver diferenças, tanto empírica quanto estatística, entre os resultados obtidos através de avaliações implementadas pelo método de convencional e as mediadas por computador. Ele menciona que apesar do rápido crescimento da avaliação mediada pelo computador estas diferenças não podem ser ignoradas. Da mesma forma Kumar (1999), que realizou um estudo com aplicação de avaliações manuais e *on-line* à alunos do curso de computação, obteve resultados equivalentes.

Uma segunda geração de avaliação mediada por computador envolve, segundo Bennett (1998), tanto a utilização dos recursos multimídia como a geração automática de perguntas. Estas perguntas são oriundas de uma base, aleatoriamente selecionadas, cobrindo adequada-

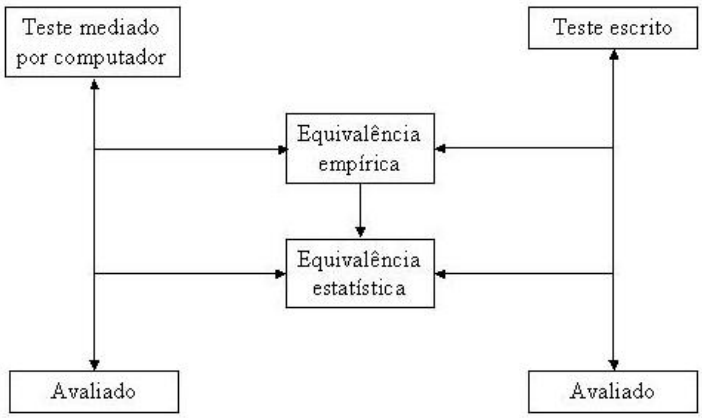

Figura 2.1: Modelo de equivalência estatística e empírica entre avaliação convencional e mediada por computador (MCDONALD, 2002, fig.1)

mente todo o espectro de conhecimento a ser avaliado e variando seu grau de dificuldade. Já a terceira geração está fortemente associada ao processo ensino-aprendizagem, sendo altamente interativo, apresentando simulações de situações reais ao avaliado.

Modelos de avaliação baseado em computador são facilmente encontrados na literatura, como o apresentado por Preston e Shackelford (1999), que implementou um protótipo para avaliação mediado por computador, utilizou-o na avaliação presencial e defende sua aplicabilidade para a avaliação à distância.

Assim, fica claro que além do desafio de buscar a validação da avaliação presencial mediada por computador frente à convencional, surge uma nova demanda que é implementá-la à distância.

2.2.8 Avaliação à distância mediada por computador

No caso da aplicação da avaliação à distância mediada por computador ficam evidentes os desafios relativos a garantia de identidade do usuário, bem como do controle das variáveis envolvidas na aplicação da avaliação, de forma a garantir sua validade (KANUKA, 2001).

Talvez, este fato contribua, não de forma exclusiva, para que a maioria dos trabalhos que

abordam a avaliação à distância mediada por computador foquem o processo ensino-aprendizagem, sob a ótica da avaliação formativa.

Neste sentido, Hack (2000) argumenta que deve-se buscar uma avaliação global, tratando-se inclusive dados informais do processo de ensino-aprendizagem. Para tal, propõe mecanismos complementares para avaliação do aluno de educação à distância embasado na avaliação de Kirkpatrick *apud* (HACK, 2000) para obtenção da reação do aluno e do nível de aprendizado alcançado.

Porém, mesmo esta técnica não dispensa a identificação do aluno, conforme indicado pelo estudo sobre ferramentas de suporte a monitoração do aluno em ambiente de ensino à distância baseado na WEB, realizado por Souto e Zanella (2001). Eles identificaram como sendo fundamental a determinação de três parâmetros básicas: identificação do aluno; rastreamento de seu "manuseio" do material didático disponibilizado; e levantamento de seu perfil cognitivo.

Ainda focado na necessidade de identificação do aluno que está se submetendo a um processo avaliativo, Fiorese (2000) propôs um modelo de autenticação de usuários para ensino à distância. Seu trabalho descreve diferentes métodos e tecnologias de autenticação de usuários buscando determinar quais se adequam a um ambiente de ensino à distância, dando preferência as de baixo custo e facilidade de utilização. O sistema proposto por ele exige uma combinação de senhas, respostas a perguntas randômicas e utilização de dispositivos biométricos, e gera histórico de cada acesso, como: data e hora; duração; e endereço fixo da máquina cliente.

Já Scheffel (2002) vale-se da proposta de Fiorese (2000) para realizar um estudo sobre o uso da Internet para aplicação de avaliações de conhecimento onde os alunos encontram-se afastados das instituições e não são supervisionados por pessoas no momento da avaliação. O modelo que propõe é aplicável tanto na avaliação formativa como na somativa, tal qual: cursos à distância; certificação profissional; proficiência em idiomas; e concursos públicos. Ele propõe uma nova arquitetura que permite o uso da Internet como meio seguro de realização de avaliações. A arquitetura proposta baseia-se em infra-estrutura de chaves públicas, conceituada na seção 2.4, página 41.

De acordo com os conceitos apresentados sobre avaliação questiona-se se a avaliação à distância mediada por computador pode se valer de novos modelos organizacionais, como organização virtual, tópico abordado na seqüência, para facilitar e otimizar sua implementação.

2.3 Organizações virtuais

Dado os objetivos do presente trabalho, faz-se necessário conceituar organização e o ambiente organizacional, abordar a relação da tecnologia de informação e comunicação com as organizações, bem como caracterizar organizações virtuais.

2.3.1 Conceitos de organização e ambiente organizacional

Apesar de ser possível definir uma organização sob vários aspectos, neste trabalho uma organização será entendida como um sistema, ou um "*dispositivo social para cumprir eficientemente, por intermédio do grupo, alguma finalidade declarada; equivale à planta para a construção de uma máquina que será criada para algum objetivo prático*"(KATZ; KAHN, 1987, p. 32).

Sob esta visão sistêmica uma organização pode ser tratada como sistema fechado ou aberto. Nos primórdios da ciência da administração as organizações foram tratadas como sistemas fechados, pois nesta, a eficácia e o sucesso dependiam exclusivamente dos processos internos, caracterizados por uma liderança autoritária com controle rígido e baseada na burocracia, não interagindo com o ambiente externo. Entretanto, com a evolução desta ciência observa-se, segundo Bowditch e Buono (1997, p.142), que as organizações passaram a ser "*encaradas como sistemas abertos, que precisam se adaptar a condições externas mutantes, para desempenharem, terem sucesso, e até sobreviverem ao longo do tempo de forma eficaz*".

Para um melhor entendimento da questão posta, é necessário fazer um aprofundamento conceitual de ambiente. Nesta abordagem, apesar de haver controvérsias em relação a sua definição, há convergência de que ambiente refere-se a fatores externos à organização. Bowditch e Buono (1997, p.143) tratam o ambiente organizacional como "*todos os elementos existentes fora dos limites da organização, e que tenham potencial para afetar a organização como um todo ou partes dela"*, ou mesmo, sob uma ótica mais ampla, afirmam que "*o ambiente é qualquer coisa que não faça parte da própria organização*".

Ainda seguindo a abordagem de Bowditch e Buono (1997, p.143), no intuito de ser mais preciso em relação a definição de ambiente, pode-se subdividi-lo em "*Ambiente Geral*" e "*Ambiente Específico*". Onde o ambiente geral "*se refere aos fatores, tendências e condições gerais que afetam a todas as organizações (condições tecnológicas, fatores sociais, ...)*", enquanto o

ambiente específico envolve "*os fatores e as condições externas que tenham relevância imediata para a organização. ... geralmente inclui os clientes, fornecedores, sindicatos, autoridades regulamentadoras, grupos de interesse público, associações de classe e outros públicos*".

A partir deste entendimento de ambiente, alguns autores afirmam que as organizações são controladas pelas contingências ambientais, como Pfeffer e Salancik *apud* Hall (1982), sendo que outros sugerem que as organizações controlam o ambiente, como McNeil e Perrow *apud* Hall (1982).

Sem entrar no mérito da discussão de causa e efeito, aborda-se na seqüência o fator externo, do ambiente geral, tecnologia de informação e comunicação, pois este viabiliza, ou causa, a implementação de novos modelos organizacionais, como organizações as virtuais.

2.3.2 Tecnologia de informação e comunicação nas organizações

A tecnologia de informação e comunicação, como fator ambiental, está relacionada as mudanças nas organizações, quer por causá-las quer por viabilizá-las (HALL, 1982). Neste sentido aborda-se este tópico em relação as dificuldades iniciais, os benefícios imediatos e as mudanças organizacionais relacionadas.

Uma das questões cruciais que envolvem sistemas de informação nas organizações é seu desenvolvimento/customização e respectiva implantação (LEEM; KIM, 2002). Stewart, Mohamed e Daet (2002) enfatizam as dificuldades de implantação das tecnologias de informação e comunicação, bem como as conseqüências negativas na produtividade e inovação devido a demora em se adotar estas tecnologias. Apesar dos dois trabalhos proporem metodologias próprias para desenvolvimento/customização e implantação de sistemas de informação empresarial, o importante é salientar que um cuidado especial deve ser dedicado a esta etapa de forma que estas tecnologias aumentem a eficácia da organização.

Outro ponto relevante é prever como as características organizacionais serão afetadas pela implementação de tecnologias de informação e comunicação, bem como a influência destas características sobre os sistemas. Dewett e Jones (2001) relacionam as características organizacionais tais como estrutura, tamanho, aprendizado, cultura e relacionamentos inter-organizacionais com os resultados em termos de eficiência e sinergia da informação.

Quanto aos benefícios da adoção destas tecnologias nas organizações, eles são, em geral,

considerados axiomáticos. Entretanto seus benefícios são mais evidentes na automação de processos operacionais do que nos processos estratégicos. Ou seja, os benefícios constatados por Gunasekarana et al. (2002) no comércio eletrônico e seus impactos na gerência de operações são mais evidentes que os obtidos por Ramos, Junco e Espinosa (2002) quando da utilização de sistemas de informação no auxílio à tomada de decisão.

No que tange as mudanças organizacionais a partir de sistemas de informação Rajagopal (2002) argumenta que as empresas implantaram ERPs (*enterprise resourse planning*) durante a década de 1990 para obter sistemas de informação uniformes e uma clara perspectiva de sua organização de modo a reprojetar seus processos de negócio. Para chegar em tal conclusão ele analisou seis indústrias e três tipos de ERP: SAP; Baan; e Oracle. Na mesma direção Keil et al. (2000) explora como as tecnologias de informação e comunicação estão influindo, ou mesmo direcionando, a transformação dos negócios.

Em função do aparecimento dos novos modelos organizacionais Chou (2002) realizou um estudo sobre os efeitos dos sistemas de computador sobre a aprendizagem organizacional. Em sua pesquisa concluiu que estes sistemas representam um vetor positivo na aprendizagem organizacional, apesar de depender de sua cultura e contexto.

Porém uma das maiores mudanças viabilizadas, ou causadas, nos modelos organizacionais referem-se as organizaçãos virtuais, tópico a ser tratado na seqüência.

2.3.3 Virtualidade

O objetivo desta seção é definir organizações virtuais, partindo da conceituação de virtual à abordagem de níveis de virtualidade nas organizações expressa por diversos autores.

Antes do advento da computação o termo virtual implicava, principalmente, no potencial para ser ou ocorrer sem de fato existir ou acontecer (VERBO, 2003).

Já com o concepção e o desenvolvimemento da informática o termo virtual passou a indicar algo que "*resulta de, ou constitui uma emulação, por programas de computador, de determinado objeto físico ou equipamento*" (FERREIRA, 1999). Dentro deste contexto, o autor do presente trabalho desenvolveu em seu mestrado um instrumento virtual como um "*sistema que realiza a aquisição e processamento de um sinal, através de um microcomputador, emulando um instrumento.*" (ARDIGO, 1994)

Outra forma corrente da utilização do termo virtual é para contrapor o real, ou seja representa um

> "*ambiente simulado por computador, muito próximo da realidade (utilizado para treinar astronautas, para jogos de vídeo, etc.), que transmite ao operador a impressão de que faz parte desse ambiente e lhe dá a possibilidade de intervir, através de um equipamento especial criado para esse fim.*" (GRANDE…, 2003)

Entretanto, nenhuma destas abordagens são aplicáveis às organizações, especificamente para definir organizações virtuais. Assim fez-se necessário uma busca na literatura especializada por uma definição apropriada. Porém, ao se realizar esta busca constata-se a dificuldade de se encontrar um definição única para o termo virtual aplicado às organizações.

Por exemplo, enquanto Davidow e Malone (1993), considerados os criadores do termo "corporação" virtual, conceituam organização virtual de forma a abranger qualquer forma organizacional nova, Byrne (1993) utiliza o mesmo termo para um conjunto de conexões através de sistemas digitais, entre entidades diferentes, que se utilizam de "*core competencie*" para uma colaboração temporária.

Até mesmo a necessidade de utilização de tecnologias de informação e comunicação não é consenso. Enquanto alguns pesquisadores, como Martin (1996), acreditam que a união através de tecnologias de informação e comunicação é necessária para que organizações virtuais existam, outros negam sua necessidade (COYLE; SCHNARR, 1997) ou não discutem explicitamente esta questão (GOLDMAN; AL, 1995).

Assim, para facilitar o entendimento deste trabalho, se convencionará organização virtual como um conjunto de indivíduos, grupos ou instituições, que, de forma temporária, auxiliado pela tecnologia de informação e comunicação, cooperem de forma a quebrar barreiras de tempo ou espaço (físico ou administrativo), para atender a determinados objetivos.

Esta definição se aproxima da apresentada por Fuehrer *apud* (BONELLI, 2001)[3]:

> "*Uma organização virtual é uma rede temporária de instituições independentes, empresas, ou indivíduos especializados que trabalham em conjunto de forma natural através de tecnologias de informação e tecnologias de comunicação sob o*

[3] trabalho orientado por este autor

> *intuito de aumentar seus potenciais individuais e obter "vantagens competitivas". Eles fazem integração vertical, unificam suas "core competencies" e trabalham como uma organização (ou unidade organizacional)*". (Fuehrer, 1997)

Entretanto, enfatiza-se que esta abordagem pode ser mais sofisticada. Neste sentido, apresenta-se a seguir várias abordagens sobre este conceito.

Watson-Manheim, Crowston e Chudoba (2002) desenvolveram uma definição mais precisa do termo virtual em relação as mudanças ou conservação de variáveis do ambiente de trabalho. As variáveis propostas para análise são a virtualidade dos: empregados, em relação ao empregador, grupo de trabalho e localização física e temporal; grupos, que mantendo o empregador quebrem a dependência de localização ou tempo; equipes, que mantendo o contratante podem variar o local de trabalho, seus membros e suas tarefas; organização, que mantendo o contratante interage com pessoas que trabalham para outros ou em outros projetos; e sociedade, que pode ter indivíduos se comunicando sobre assuntos comuns com descontinuidade de tempo e espaço.

Outra abordagem é dada por Panteli e Dibben (2001) que fazem uma revisão da natureza das organizações virtuais e de como as tecnologias de informação e comunicação podem transformar as organizações do mundo convencional para o virtual.

Já Cullen (2000) avalia as atuais características de política pública, legal e econômica, em relação a colaboração entre organizações e sugere que as empresas virtuais, como uma nova forma de consórcio, ocuparão espaços de outras modalidades de parcerias, como as *joint ventures*.

Como aplicação imediata deste modelo, Offodile e Abdel-Malek (2002) destacam que pequenas indústrias podem ganhar competitividade por adotar estratégias de manufatura virtual. Porém, para tal, segundo Hong (2002), é necessário que os sistemas inter-organizacionais facilitem tal estratégia. Assim, após destacarem que os sistemas existentes são muito complexos ou defasados, propõem uma nova de forma de classificação destes sistemas de modo a determinar sua eficácia, facilitando a formação de organizações virtuais.

Neste sentido, Khalil e Wang (2002) propõe um modelo de gerenciamento de organizações virtuais que explora as vantagens competitivas implícitas neste modelo de organização, que, pode ser traduzido por meta-gerenciamento, que consiste em atividades básicas que envol-

vem analisar e rastrear os requisitos e fazer ajustes segundo um critério ótimo. Wang (2000), também enfatiza que o gerenciamento de uma organização virtual vai além do simples suporte da tecnologia de informação. Ele propõe a modelagem orientada objeto da organização e a análise da cadeia de valor virtual para propor um modelo de gerenciamento.

Ainda para solucionar o problema de gerenciamento de organizações virtuais Zhugea et al. (2002) propôs um simulador baseado em modelo de *workflow* por agentes pertencentes a federações para o desenvolvimento de organizações virtuais. O modelo proposto consiste no *workflow* por agentes pertencentes a federações, no estabelecimento de regras para mapear o domínio da organização virtual, em um conjunto de serviços de gerência e o no desenvolvimento macro do processo. O modelo proposto unifica o domínio organizacional tradicional com o modelo de sistemas de informação resultando em um modelo de organização virtual, o que habilita o usuário a desenvolver intuitivamente organizações virtuais do ponto de vista do domínio.

Para minimizar incompatibilidades entre organizações virtuais e ajudar as organizações a colaborar entre si independente de estrutura, processos e ambiente computacional, foram propostos vários protocolos no NIIIP (National Industrial Information Infrastructure Protocols). Alguns destes foram analisados por Hardwick et al. (2000) permitindo inferir como estes afetarão o desenvolvimento de distribuição de dados em formato padrão.

Ainda quanto a abrangência das organizações virtuais, Ip *et al* (IP et al., 2001) enfatizam que alianças dinâmicas e empresas virtuais são componentes essenciais no processo de manufatura global. Entretanto salientam que para se obter sucesso neste modelo é essencial minimizar o risco de seleção de parceiros para o cumprimento dos prazos envolvidos no processo produtivo. Eles descrevem e modelam o problema do risco baseado na seleção de parceiros.

Neste sentido Kasper-Fuehrera (2001) apresenta uma teoria de confiança entre diferentes organizações virtuais que foca em como a confiabilidade pode ser construída neste tipo de ambiente. A teoria destaca três pontos para a superação dos obstáculos ao estabelecimento de confiança no contexto virtual, a saber: a confiabilidade das tecnologias de informação e comunicação; o estabelecimento de visão comum do negócio; e uma forte ética de negócio.

Estes dois últimos autores enfatizam a necessidade de confiança entre parceiros para a formação de organizações virtuais. Como a infra-estrutura de chaves públicas pode se constituir na base tecnológica de construção da confiança entre entidades, este tema será detalhado na

próxima seção.

2.4 Infra-estrutura de Chaves Públicas

Os requisitos de segurança para um processo de avaliação à distância mediada por computador podem ser satisfeitos por meio de uma Infra-estrutura de Chaves Públicas (ICP) (HUNT, 2001), que constitui-se em uma base para serviços e aplicações que utilizam conceitos e técnicas de criptografia assimétrica (ADAMS; LLOYD, 2002). Entretanto a literatura pesquisada apresenta ora um material tão sub-dividido que dificulta o entendimento do todo ora uma abordagem simplista. Para preencher estas lacunas, apresenta-se nesta seção única os principais conceitos envolvidos em uma ICP, deste o criptografia assimétrica até o conceito de criptografia temporal, reservando-se uma abordagem detalhada para o capítulo 3, página 50.

Conforme já abordado, um processo de avaliação deve ser um processo eqüitativo em termos de classificação, que dê igualdade de oportunidade entre os participantes, e eficaz, para determinar o real domínio ou capacidade do indivíduo (BAKER; MAYER, 1999).

O processo de avaliação à distância mediado por computador utiliza a tecnologia de informação e comunicação para ampliar a abrangência espacial em relação a uma avaliação covencional, por minimizar ou eliminar a necessidade da presença simultânea do avaliador e avaliado em um mesmo ambiente físico (ROVAI, 2000). Porém este processo tem de preservar as características de eqüidade e eficácia em todas as suas fases.

Para que estes objetivos sejam alcançados é imprescindível que os documentos eletrônicos utilizados em todas as fases de um processo de avaliação à distância mediada por computador tenham: autenticação, que garante a autoria; integridade, que garante o conteúdo; confidencialidade, que assegura o acesso apenas à pessoas autorizadas; irretratabilidade, que torna inviável a alguém negar o envio ou recebimento; e tempestividade, que confere data e hora aos documentos eletrônicos. Estes requisitos podem ser satisfeitos por meio de uma Infra-estrutura de Chaves Públicas (ICP) (HUNT, 2001).

O elemento básico de uma ICP é o certificado digital (HOUSLEY; POLK, 2001). Um certificado digital é um documento eletrônico, emitido por um dos componentes de uma ICP, que associa um usuário à sua chave pública.

Um certificado digital é um documento eletrônico, emitido por um dos componentes de

uma ICP, que associa um usuário à sua chave pública.

Em termos computacionais chaves são dados utilizados para permitir ou negar acesso, análogo a uma senha, que o usuário utiliza para acessar sistemas ou para gravar arquivos de forma que outros não possam lê-los (SCHNEIER, 1996).

Para gravar arquivos de forma que outros não possam lê-los são utilizadas técnicas de cifragem. Mesmo que um usuário não autorizado tenha acesso a um arquivo cifrado, não conseguirá entender as informações contidas nele, pois o processo de cifragem embaralha os dados. Se a técnica de embaralhamento utilizada for a criptografia simétrica (STINSON, 1995; MENEZES; OORSCHOT; VANSTONE, 1996; STALLINGS, 1998), o decifragem das informações contidas no arquivo necessita da utilização da chave originalmente utilizada em sua cifragem.

O exemplo anterior ilustra a confidencialidade de um documento eletrônico, pois somente o usuário autorizado (conhecedor da chave) tem acesso às informações contidas nele. Porém, se houver a necessidade de compartilhar esta chave para que diferentes usuários tenham acesso à informação, a garantia da confidencialidade fica mais complexa. Para estas situações é recomendado o uso da criptografia assimétrica.

A criptografia assimétrica, proposta por Whitfield Diffie e Martin Hellman em (DIFFIE; HELLMAN, 1976), utiliza um conceito diferente para executar a cifragem de dados. Esta técnica utiliza um par de chaves, denominadas chave pública e privada. A geração destas chaves ocorre através de um processo matemático que as torna fortemente ligadas e possibilita que as operações (cifragem/decifragem) realizadas por uma chave só possam ser revertidas pela correspondente do par.

A eficácia desta técnica é dependente da manutenção do sigilo da chave privada, que deve ser tratada como pessoal e intransferível. Já a chave pública pode estar acessível a todos, sem que isto comprometa o funcionamento do sistema, uma vez que a partir da chave pública é computacionalmente inviável obter a chave privada (MENEZES; OORSCHOT; VANSTONE, 1996).

O fato de uma chave privada ser conhecida por somente um usuário, implica que um documento cifrado utilizando-se esta chave é um documento com identificação de autoria, pois ninguém mais tem capacidade de produzir o mesmo resultado. Através da chave pública deste usuário é possível decifrar o documento, o que permite concluir que o autor detém a chave privada correspondente. Este processo está fortemente ligado ao conceito de assinatura digital (RIVEST; SHAMIR; ADLEMAN, 1978), que garante a integridade e autenticação de documentos

eletrônicos.

A garantia da integridade de um documento eletrônico pode ser alcançada de forma análoga a garantia de validade de um número do Cadastro de Pessoas Físicas (CPF). No CPF os dois últimos algarismos representam os “dígitos verificadores”, que na realidade são o resultado da aplicação de uma função matemática aos dígitos do CPF. Uma mudança em um dos números que compõem o CPF compromete os dígitos verificadores. No caso da garantia da integridade de documentos eletrônicos é utilizada uma função “resumo criptográfico” para realizar esta operação.

A função resumo criptográfico (STANDARDS; TECHNOLOGY, 1993) possui a característica de função unidirecional, ou seja, é fácil computar o resumo a partir de um documento, porém a partir do resumo é computacionalmente inviável obter o documento que o originou. Outra característica é que o resumo criptográfico identifica o documento de maneira única, análogo a uma impressão digital. Se qualquer dado no documento original, por menor que seja, for alterado, gerará um resumo completamente diferente. Desta forma, uma vez conhecido o resumo de um documento a ocorrência de qualquer alteração pode ser detectada.

O processo de conferência da integridade de um documento eletrônico consiste na repetição do processo da geração do resumo, pelo conferente, e a comparação deste com o resumo recebido. Se ambos os resumos forem idênticos, o documento pode ser considerado íntegro.

Além disso, não deve ser possível obter dois documentos distintos que tenham o mesmo resumo criptográfico. Desta forma pode-se considerar o resumo criptográfico, por si só, como a assinatura de um documento eletrônico. A título de exemplo pode-se citar o resumo criptográfico dos programas utilizados nas urnas eletrônicas que são tornados públicos meses antes de uma eleição, para que a sociedade possa constatar que o programa não foi alterado durante as eleições. Cabe salientar que esta assinatura permite somente verificar a integridade do documento eletrônico, sem estabelecer uma ligação de autoria.

Assim, no processo de assinatura digital, o resumo apenas confere integridade ao documento, a autenticação é provida através da cifragem deste resumo pelo assinante, utilizando sua chave privada.

Retornando ao conceito da confidencialidade, porém abordando a comunicação sigilosa envolvendo a troca de documentos eletrônicos, os mesmos devem ser cifrados pelo remetente utilizando a chave pública do destinatário, pois somente o destinatário, conhecedor da chave

privada correspondente, poderá ter acesso ao conteúdo dos documentos.

Diferente do que ocorre na criptografia simétrica, a troca de documentos confidenciais utilizando criptografia assimétrica reduz o grau de complexidade de gerenciamento e distribuição de chaves, pois (STALLINGS, 1999):

- na criptografia assimétrica, a comunicação sigilosa, entre vários usuários, necessita apenas de um par de chaves para cada usuário, ou seja $2n$ chaves, enquanto que utilizando-se a criptografia simétrica são necessárias $\frac{n(n-1)}{2}$ chaves, sendo n o número de usuários;
- na criptografia assimétrica não é necessário a utilização de meios sigilosos para a distribuição de chaves, uma vez que a chave a ser distribuída é pública.

Entretanto, a credibilidade da técnica de criptografia assimétrica é dependente da confiança depositada na associação do usuário à sua chave pública. Caso esta associação seja burlada, um usuário poderá acessar informações destinadas a outro, ou mesmo autenticar um documento em nome deste. Isto ocorre se um usuário gerar um par de chaves e declarar que a chave pública é de outro. Como ele conhece a chave privada deste par poderá executar diversas ações com a identidade do usuário que declarou ser. Assim, um dos maiores desafios da criptografia assimétrica é como ter certeza que determinada chave pública pertence a um usuário específico.

A forma mais utilizada para associar um usuário a uma chave pública é a utilização de certificados digitais (HOUSLEY; POLK, 2001). Estes são emitidos e gerenciados por uma ICP, que é composta pelos seguintes componentes principais:

Autoridade Certificadora (AC): responsável pela emissão, disponibilização, suspensão e revogação de certificados digitais;

Autoridade de Registro (AR): responsável pela conferência das informações prestadas pelo solicitante contidas em uma requisição de emissão ou revogação de um certificado;

Diretório Público (DP): responsável por disponibilizar em local público todos os certificados emitidos por uma AC, bem como listas de certificados revogados;

Autoridade de Datação (AD): responsável por conferir âncoras temporais à documentos eletrônicos.

A junção destes componentes permite gerenciar todo o ciclo de vida de um certificado. Este ciclo de vida envolve: requisição, validação da requisição, emissão, aceitação pelo requerente, utilização, suspensão, revogação, expiração e renovação.

Considerando este ciclo do ponto de vista do usuário, pode-se tanto fazer a requisição de um certificado como solicitar a revogação de um certificado vigente. O componente da ICP responsável por receber as requisições dos usuários é a AR.

No caso de uma requisição de certificado, são enviados à AR dados para a identificação do proprietário do certificado (sujeito), bem como a chave pública deste (BURR, 1998). Para analisar a solicitação, a AR confere as informações de cada requisição de acordo com a classificação do certificado que está sendo solicitado. A classificação determina os requisitos de confiança dos certificados. Assim, alguns procedimentos do ciclo de vida do certificado são diferentes para cada classe, como a conferência das informações da requisição e a finalidade do uso do certificado. Por exemplo, nas requisições de emissão de um certificado para autenticação de conta de e-mail, pode-se conferir apenas a posse da conta, por meio de desafios enviados a esta. Já para a emissão de certificados de autenticação de indivíduo, a AR pode exigir a presença física do usuário com a apresentação de documentos pessoais.

As requisições aprovadas pela AR são encaminhadas para AC que emite o certificado. A AC fará a conferência da requisição, apenas para verificar se o pedido está de acordo com sua política de certificação (SABO; DZAMBASOW, 2001), sendo que cada AC tem liberdade de estabelecer sua política, respeitas as políticas das ACs de hierarquia superior.

Após a conferência, a AC retorna a requisição com a informação de atendimento ou rejeição da requisição. Caso a requisição de emissão de certificado seja aceita, a AC emite o certificado, que é um conjunto de informações, baseadas nas informações da requisição e da chave pública do usuário, assinadas[4] pela AC, que em geral, a depender de sua política, o disponibiliza no DP e o envia para o usuário.

Após a emissão do certificado, a depender da política de certificação, pode haver uma etapa de aceitação do certificado pelo requerente. Esta aceitação pode ser feita pela notificação à AC, em caso de erro ou defeito em um certificado, imediatamente após seu recebimento ou publicação no DP.

Uma vez aceito pelo requerente, o certificado poderá ser utilizado durante seu período de

[4]realização do processo de assinatura digital.

vigência. Este período está definido em dois campos do próprio certificado, sendo que um indica a data de início da validade e outro indica sua data de expiração. Expirado um certificado, o usuário poderá proceder a solicitação de renovação do mesmo, o que implica na emissão de um novo certificado de forma mais simplificada. Entretanto pode ser necessário que um certificado deva deixar de ser válido dentro de seu período de vigência, temporária ou permanentemente, por suspensão ou revogação, respectivamente. Um exemplo clássico desta situação é o usuário perceber que sua chave privada foi copiada por outro.

Para solicitar suspensão ou revogação de um certificado, o usuário deve proceder de forma similar a solicitação de emissão do certificado, ou seja, deve enviar a solicitação a AR que repassa à AC. Esta verifica se o solicitante tem direito de pedir a suspensão ou revogação daquele certificado e concede ou nega o pedido.

Caso a requisição seja aceita, a AC suspende ou revoga o certificado, inclui identificadores deste em um arquivo denominado lista de certificados revogados (LCR), assina este arquivo e o disponibiliza no DP.

O diretório público tem como responsabilidade principal a obrigação de manter disponível os certificados válidos, durante sua vigência, e as LCRs, de acordo com tempo definido na política da AC que emitiu o certificado.

Cabe salientar que o procedimento de suspensão ou revogação de um certificado não invalida as assinaturas realizadas anteriormente a sua revogação, fato que pode ser comprovado em função da âncora temporal.

A âncora temporal é um atributo confiável de tempo adicionado pela Autoridade de Datação (AD) (BAYER; HABER; STORNETTA, 1991; HABER; STORNETTA, 1991) à assinatura. No momento da realização, esta é encaminhada para a AD, a qual retorna um recibo com a data de submissão. O recibo é um documento assinado pela AD que contém o resumo criptográfico do documento inicial concatenado com a informação de tempo.

2.5 Infra-estrutura de Chave Pública no contexto de Organização Virtual

A partir dos conceitos apresentados sobre ICP e sobre organizações virtuais, pretende-se abordar aspectos da ICP em relação a sua adoção dentro de uma organização, interação de várias organizações e organizações virtuais.

Do ponto de vista tecnológico, Fernandes (2001) argumenta que a implementação de uma ICP dentro de um organização implica na necessidade de mudança no modelo de segurança da área de tecnologia de informação e comunicação como um todo. Uma vez implementada, Polk e Hastings (2000) abordam que as organizações estão utilizando suas ICPs em processos internos, implementando redes virtuais privadas e garantindo a segurança de informações. Porém, muitas destas tem parcerias com outras organizações e para manter as informações com o mesmo padrão de segurança interno no comércio eletrônico entre empresas, é necessário conectar suas ICPs, que podem ser de diferentes arquiteturas e diferentes políticas de segurança. Para isto os autores sugerem a adoção de uma Autoridade de Certificação Ponte, que permita a iteração de ICPs individuais, sem que estas sofram alteração em suas políticas ou arquiteturas.

Ampliando esta abordagem, Li, Dai e Zhang (2001) argumentam que estruturas tradicionais de autoridades certificadoras, por serem hierárquicas e intrincadas, não são compatíveis com o modelo de organizações virtuais, caracterizadas pelo seu caráter temporário de existência. Dado a este fato propõem uma autoridade certificadora virtual (ACV) que representa a AC da organização virtual emitindo certificados para empresas convencionais, participantes desta organização virtual, mantendo as autoridades de certificação de cada participante o mais intacta possível. Nesta proposta a constituição da chave privada, elemento principal para emissão de certificados, é realizada por meio de esquema de compartilhamento de segredo sem autoridade central[5]. Desta forma, a constituição da chave privada é determinada por todos os participantes, e nenhum destes obtém acesso absoluto a esta chave, sendo necessário a cooperação entre um certo número de participantes para emissão dos certificados pela ACV.

No contexto educacional, Podestá e Meinel (2000) propõe a integração de uma ICP a

[5]Técnica de divisão de uma informação em n partes, de modo que a reconstrução desta só é possível através da reunião de t partes, sendo $t <= n$

uma Universidade Virtual[6] utilizando alguns conceitos abordados nesta seção. Esta proposta visa solucionar as necessidades de emissão segura de dados confidenciais sobre a rede, autoria de documentos eletrônicos e determinação de tempo de criação dos mesmos. Para isto, são utilizados certificados digitais para cifragem dos dados, assinatura e datação de documentos, entretanto, emitidos por ICPs convencionais.

2.6 Conclusão

A partir da pesquisa realizada, percebe-se o potencial benefício da utilização de novos modelos organizacionais e da evolução de novas tecnologias de informação e comunicação à processos de avaliação somativa à distância.

Com respeito a novos modelos organizacionais, abordou-se as organizações virtuais, adotando o conceito de conjunto de indivíduos, grupos ou instituições, que, temporariamente, auxiliado pela tecnologia de informação e comunicação, cooperam de forma a quebrar barreiras de tempo ou espaço (físico ou administrativo), para atender a determinados objetivos. A flexibilidade implícita destas organizações, principalmente no que tange a seu ciclo de vida, pode ser utilizada em benefício da implementação de processos de avaliação somativa à distância mediada por computador.

Entretanto, a formação de organizações virtuais demanda a confiança entre os parceiros que a compõe. Como a infra-estrutura de chaves públicas pode se constituir na base tecnológica de construção da confiança entre entidades, acredita-se que a implementação de uma infra-estrutura de chaves públicas, no contexto de organizações virtuais, pode conferir igual flexibilidade, em termos de ciclo de vida, permitindo assim sua utilização em processos da avaliação somativa à distância, envolvendo diferentes entidades.

Como visto, uma proposta de AC virtual, já foi feita por Li, Dai e Zhang (2001). Porém, este trabalho aborda apenas o ciclo de gerenciamento da chave privada da autoridade certificadora, o que não resulta no completo atendimento das necessidades para alcançar os objetivos desta tese. Assim, o estudo deve ser estendido para abranger outros aspectos, como a análise e provimento de requisitos de segurança.

Além da constatação da inexistência de trabalhos científicos com esta abrangência, não

[6] conceituada por Carswell (1998)

foi encontrado nenhum outro sobre a utilização de infra-estrutura de chaves públicas, dentro do contexto de organizações virtuais, para a implementação de avaliações somativas à distância. Assim, constata-se a necessidade de realização de estudos que contemplem este aspecto visando a criação de modelos de confiança, que atendam características específicas deste processo.

Capítulo 3

Criptografia: Conceitos e Serviços

O uso de documentos eletrônicos em aplicações críticas, tal como um concurso público, exige o atendimento de certos requisitos de segurança, fundamentais para garantir a segurança de informações envolvidas na aplicação. Estes requisitos, já citados em capítulos anteriores, referem-se a integridade, autoria, confidencialidade e não-repúdio de documentos eletrônicos.

A Criptografia permite alcançar estes requisitos através de algoritmos, protocolos e serviços criptográficos. Este capítulo apresenta conceitos ligados a criptografia e a tecnologia de segurança da informação que possuem grande relevância, pois formarão as bases das propostas deste trabalho, a serem apresentadas em capítulos subseqüentes.

A seção 3.1 apresenta em detalhes a tecnologia de Infra-estrutura de Chaves Públicas (ICP), provendo a identificação dos requisitos necessários à sua constituição e funcionamento. Na seção 3.2 são conceituados esquemas de compartilhamento de segredos, os quais representam um importante mecanismo criptográfico utilizado em situações que deseja-se aumentar a segurança de uma determinada informação, através da descentralização do controle desta. Por fim, a seção 3.3 aborda o conceito de Serviços de Criptografia Temporal, os quais permitem determinar o momento futuro em que uma informação cifrada poderá ser decifrada e ter seu conteúdo conhecido.

3.1 Infra-estrutura de Chaves Públicas

Uma ICP constitui-se de um conjunto de componentes que cooperam entre si no processo de emissão, revogação e publicação de certificados digitais e listas de certificados revogados.

Uma ICP fornece a base para serviços e aplicações que utilizam conceitos e técnicas de criptografia assimétrica (ADAMS; LLOYD, 2002).

A segurança de informações sempre foi um importante ponto no estabelecimento de comunicação entre partes, envolvendo desde a confiança entre estas, até o sigilo, integridade, autenticidade e não repúdio destas informações. Algoritmos criptográficos assimétricos proporcionam o atendimento a estes requisitos, entretanto é necessária uma forma segura de associar os elementos (chaves públicas e privadas) destes algoritmos a entidades específicas.

O certificado digital apresenta-se como a solução para a ligação confiável de uma entidade a um determinada chave pública. Um certificado digital deve atender a propriedades específicas, pois caso seja emitido de maneira inadequada, torna-se possível a ocorrência de ataques realizados por agentes maliciosos.

Assim, Polk e Hastings (2000) enumera nove propriedades que um certificado ideal deve atender:

1. deve ser um objeto puramente digital;
2. deve conter o nome do usuário que possui a chave privada correspondente a chave pública contida no certificado;
3. deve ser fácil determinar se foi emitido recentemente;
4. deve ser criado por uma entidade que o proprietário da chave privada confie;
5. deve ser fácil de verificar se o certificado é autêntico ou forjado;
6. deve possuir uma prova de violação, que não permita a alteração do conteúdo do certificado;
7. uma vez que a parte confiável pode emitir vários certificados para um mesmo usuário, deve ser fácil distinguí-los;
8. deve ser possível determinar a partir do certificado a aplicação a que se destina seu uso; e
9. deve ser possível verificar se as informações do certificado ainda são atuais.

O certificado digital que mais se aproxima do atendimento dos requisitos elencados é realizado por uma infra-estrutura de chaves públicas (ICP). Assim, descreve-se a seguir: o certificado digital provido por uma ICP, seção 3.1.1; a Lista de Certificados Revogados, seção 3.1.2, página 58; os componentes de uma ICP, seção 3.1.3, página 60; as políticas e práticas de certificação, seção 3.1.4, página 63; os modelos de confiança, seção 3.1.5, página 64; os caminhos de certificação, seção 3.1.6, página 68; e o custo de uma ICP, seção 3.1.7, página 69.

3.1.1 Certificado Digital

Certificado digital, também chamado certificado de chave pública, pode ser conceituado como um documento eletrônico que associa, de maneira segura, uma entidade a uma chave pública.

O campo de utilização de certificados digitais é amplo, abrangendo o comércio eletrônico, o ambiente coorporativo e governamental e o uso pessoal, como exemplos. Nestes contextos os certificados digitais permitem a implementação de assinaturas digitais, mecanismos de autenticação, integridade de dados, não-repúdio e confidencialidade (STALLINGS, 1999).

Estruturalmente um certificado digital é formado por uma seqüência de campos e atributos, sendo estes próprios de uma entidade específica. Estes campos contém, no mínimo, informações necessárias a identificação do seu proprietário e da entidade que o emitiu, e à verificação da sua validade e autenticidade.

O formato de certificados digitais mais aceito e adotado atualmente tem como base o modelo especificado na recomendação ITU-T X.509 Versão 3 (ITU-T, 2000), elaborado pelo *Telecommunication Standardization Sector* (ITU-T), o qual é integrante da *International Telecommunication Union* (ITU). Estas especificações permitem que diferentes aplicações que possuem mecanismos de certificação digital sejam capazes de manipular e extrair dados de certificados digitais e listas de certificados revogados, bem como interagir com os componentes de uma ICP.

Um certificado no formato X.509 consiste essencialmente de três conjuntos de campos: *conteúdo básico do certificado*, *conjunto de extensões* e *envelope de controle de integridade*.

O *conteúdo do certificado*, conforme ilustra a figura 3.1, é composto do *conteúdo básico do certificado* e *conjunto de extensões*. O *conteúdo básico do certificado* é composto por

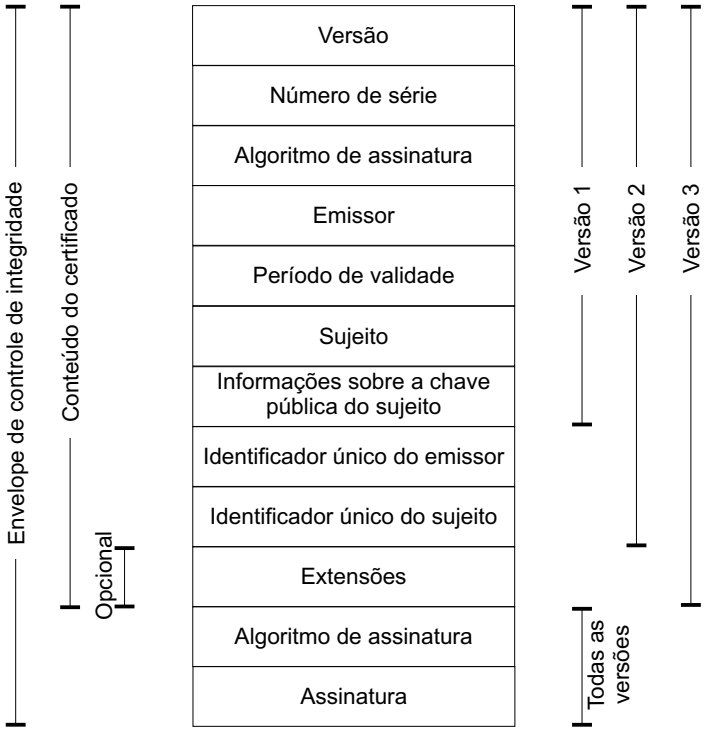

Figura 3.1: Certificado Digital X.509

campos obrigatórios e opcionais. As informações obrigatórias são constituídas por seis campos obrigatórios: número de série; identificador do algoritmo de assinatura; dados do emissor e chave pública; período de validade do certificado; dados do sujeito do certificado; e informações sobre a chave pública do sujeito do certificado. Enquanto as informações opcionais são formadas pelos campos: versão; identificador único do emissor; e identificador único do sujeito.

A omissão da informação da versão implica na codificação do certificado na versão 1, onde não constam os identificadores únicos e as extensões. A versão 2 suporta a inclusão dos indentificadores do emissor e do sujeito e a versão 3 suporta além dos identificadores, as extensões.

O *conjunto de extensões* é opcional e permite incluir no certificado informações não suportadas pelos demais campos. Embora existam campos de extensões padrão, é possível a definição de outros campos de extensão, podendo estes serem criados a fim de suprir necessidades específicas de uma ou mais aplicações. Um exemplo destas necessidades ocorre em um cenário onde um Banco emitirá certificados para todos os seus clientes, e estes certificados

devem conter o número da agência e da conta corrente do respectivo cliente. Os campos básicos do certificado não suportam tais informações, portanto a solução é criar dois campos de extensão para conter as informações.

O *envelope de controle de integridade* permite verificar a autenticidade e integridade de um certificado. Sobre os campos do *conteúdo do certificado* é calculado o resumo criptográfico e realizado a assinatura digital da AC emissora, garantindo que nenhum deles foi alterado. A identificação dos algoritmos utilizados para gerar o resumo e a assinatura são armazenados nos campos *algorítimo de assinatura* e a assinatura propriamente dita, no campo *assinatura*. O processo de validação de um certificado se utiliza destes campos e constitui-se na verificação da integridade do certificado e da verificação da autenticidade da assinatura da AC emissora. Qualquer erro encontrado em algum destes dois procedimentos, invalida o certificado.

Os campos que a recomentação X.509 contempla são especificados na tabela 3.1, já a organização estrutural e classificação destes campos é apresentada na figura 3.1

Tabela 3.1: Campos de um certificado de chave pública no padrão X.509.

Campo	**Descrição**
version	Versão do padrão em que o certificado foi emitido, podendo ser versão 1, 2 ou 3.
serialNumber	Identificador único do certificado, determinado pela AC emissora.
signature	Identificação do algoritmo utilizado pela AC para assinar o certificado.
issuer	Nome da AC emissora.
validity	Período de validade do certificado. Este campo é composto por dois atributos, a data em que o certificado tornou-se válido e a data da sua expiração.
subject	Nome da entidade detentora da chave privada correspondente a chave pública do certificado.
subjectPublicKeyInfo	Chave pública do sujeito e identificador do algoritmo ao qual a chave é aplicável .
issuerUniqueID	Número identificador da AC emissora do certificado.
subjectUniqueID	Número identificador do sujeito do certificado.
extensions	Contém informações opcionais.
signatureAlgorithm	Identificação do algoritmo utilizado pela AC para assinar o certificado.
signatureValue	Assinatura da AC no certificado.

Em relação ao certificado ainda é necessário detalhar suas extensões, o que é feito na seção 3.1.1.1, e seu ciclo de vida, conforme seção 3.1.1.2, página 56.

3.1.1.1 Extensões do Certificado

As extensões são campos adicionais dos certificados, que permitem incluir informações nos certificados não suportadas pelo conteúdo básico. Dentre as vantagens da utilização das extensões estão a possibilidade de restrição o uso do certificado, facilidade na construção de caminhos de certificação, direcionamento do certificado para aplicações específicas. Abaixo são apresentadas algumas das principais extensões:

Restrições Básicas *(Basic Constrainsts)*: A versão 1 do certificado digital não possui campo onde possa ser informado se o certificado pertence a uma Autoridade Certificado ou a um usuário final. Assim, o uso das restrições básicas permite identificar esta característica facilitando a construção do caminho de certificação, detalhado na seção 3.1.6.

Esta extensão também permite incluir restringir o comprimento do caminho, ou seja, um número inteiro que indica a quantidade máxima de ACs que poderão estar abaixo no caminho de certificação. Por exemplo, se o valor especificado for igual a zero, a AC não poderá emitir certificados para outras ACs; se não especificado valor, a quantidade de ACs que constituem o caminho de certificação não sofre restrição.

Uso da Chave *(Key Usage)*: Os campos básicos de um certificado não permitem definir a finalidade de uso do certificado, afim de restrigir o uso da chave para determinadas funções. A extensão *Uso da Chave*, dispõem de nove opções de especificação do uso da chave pública, que podem ser combinados entre si:

- *keyCertSign:* a chave pública pode ser utilizada para verificar assinaturas nos certificados;
- *cRLSign:* chave pública pode ser usada para verificar assinaturas nas LCRs;
- *non-Repudiation:* a chave pública pode ser usada para verificar a assinatura digital para prover o não repúdio de um serviço;
- *digitalSignature:* a chave pública pode verificar assinaturas quando o serviço não é coberto por nenhuma das três opções do uso de chave anteriores;
- *keyEncipherment:* a chave pública pode ser utilizada para cifrar chaves criptográficas;

- *dataEncipherment:* a chave pública pode ser usada para cifrar dados diretamente, exceto chaves criptográficas;
- *keyAgreement:* a chave pública pode ser usada no obtenção de chaves de sessão;
- *encipherOnly:* usado somente em conjunto com a opção *keyAgreement* e indica que a chave de sessão obtida somente pode ser usada para cifrar dados; e
- *decipherOnly:* semelhante ao *encipherOnly*, porém a chave de sessão obtida somente pode executar a operação de decifrar.

Uso Estendido da Chave *(Extended Key Usage)*: Esta extensão permite inserir uma aplicações específicas para uso da chave, sendo composta pelo OID da aplicação em que a chave pública pode ser utilizada.

Identificador da Chave da Autoridade *(Authority Key Identifier)*: O *Identificador da Chave da Autoridade* é utilizado para distinguir uma chave pública de outra quando uma AC tem múltiplas chaves de assinatura, ou seja, possui vários certificados digitais com o mesmo nome distinto, porém cada um com o par de chaves diferentes.

Identificador do Sujeito da Chave *(Subject Key Identifier)*: Esta extensão permite identificar o certificado que contém uma chave pública específica.

A figura 3.2 apresenta a estrutura do certificado com suporte a extensões.

3.1.1.2 Ciclo de Vida do Certificado Digital

Um certificado digital possui um tempo de vida finito. O seu ciclo de vida tem início na sua requisição e é continuado pelas fases de validação da requisição, emissão, aceitação pelo requerente, uso, suspensão, revogação e expiração. A figura 3.3 ilustra este ciclo.

A fase inicial compreende a criação da requisição e o seu envio para a entidade validadora. Estas ações são, usualmente, realizadas pelo próprio requerente do certificado.

A requisição de um certificado corresponde a um documento eletrônico assinado, que contém dados relacionados ao requerente, tais como o seu nome e a organização a que pertence, e a chave pública que será certificada. A assinatura constante neste documento é realizada através da chave privada correspondente a chave pública nele contida.

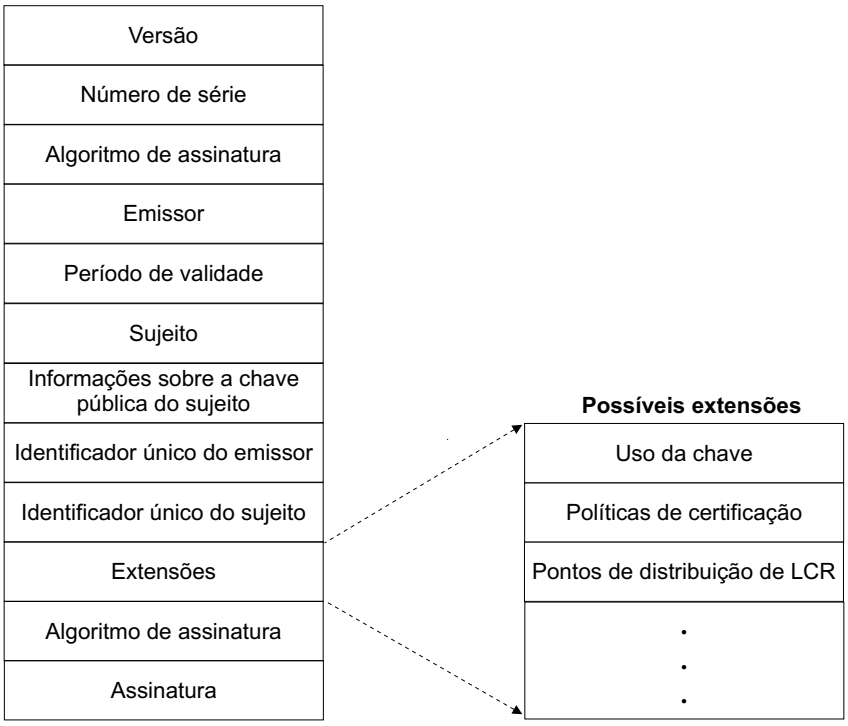

Figura 3.2: Extensões de um Certificado Digital

A validação da requisição é feita por uma Autoridade de Registro ou pela própria Autoridade Certificadora que emitirá o certificado, seguindo uma política previamente estabelecida. A entidade validadora é determinada pela política que rege a ICP.

Após a validação da requisição, a Autoridade Certificadora emite, com base nesta, o certificado digital e posteriormente o disponibiliza ao requerente para que este possa avaliá-lo. Caso o requerente aprove o certificado, inicia-se a fase de uso deste.

A suspensão de um certificado é uma ação preventiva que visa impedir o uso do certificado durante um determinado período de tempo, ou até que uma determinada situação seja resolvida, como como por exemplo durante a tramitação de um processo administrativo em que o funcionário deve ficar impedido de executar ações utilizando o certificado emitido pela empresa.

A revogação de um certificado pode ser motivada por um situação específica, por exemplo, por uma solicitação do proprietário do certificado sob a alegação de que sua chave privada foi comprometida.

Figura 3.3: Ciclo de vida de um certificado digital

A fase final do ciclo de vida corresponde a expiração do certificado, a qual ocorre quando o período de tempo indicado no seu campo de validade é transcorrido.

3.1.2 Lista de Certificados Revogados

O mecanismo utilizado por uma AC para revogar um certificado antes que este tenha seu período de validade expirado, consiste na inserção do número serial deste certificado em um documento eletrônico chamado *Lista de Certificados Revogados (LCR)*. Portanto, uma LCR contém uma relação de todos os certificados revogados que uma AC emitiu e que ainda não tenham expirado (VIEGA; MESSIER; CHANDRA, 2002).

As LCR são públicas, e sua finalidade é permitir que usuários verifiquem se um certificado específico está ou não revogado. A sua distribuição ocorre através dos chamados *pontos de distribuição*, cujas identificações estão presentes em um campo de extensão dos certificados e são definidos pela AC emissora do certificado.

Devido a importância da sua função, é essencial que as LCR sejam regularmente atua-

lizadas, a fim de evitar que certificados revogados sejam considerados válidos por motivos de desatualização de uma LCR. Entretanto são necessárias políticas e mecanismos de atualização e distribuição eficazes que levem em consideração fatores como a disponibilidade de servidores, largura de banda em redes de comunicação, desempenho de aplicações, dentre outros. Pois uma alta taxa de atualização em LCRs podem ocasionar prejuízos, tais como o aumento do tráfego em redes de comunicação e o comprometimento do desempenho de aplicações e servidores envolvidos. Portanto, há a necessidade de que uma AC estabeleça períodos regulares para a atualização e disponibilização de suas LCRs, que não impliquem em prejuízos para as partes envolvidas.

A estrutura de uma LCR é composta basicamente por campos que identificam o seu emissor, a sua data de emissão e expiração, os identificadores dos certificados revogados e a assinatura da entidade emissora da LCR, a qual assegura a integridade da LCR.

O formato da estrutura de LCRs foi definido na recomendação ITU-T X.509. Existem duas versões para tal estrutura, versão 1 e versão 2, sendo que a primeira versão caiu em desuso em virtude de diversas limitações que possuía, solucionadas na segunda versão. A figura 3.4 apresenta a organização estrutural e classificação dos campos de uma LCR versão 2.

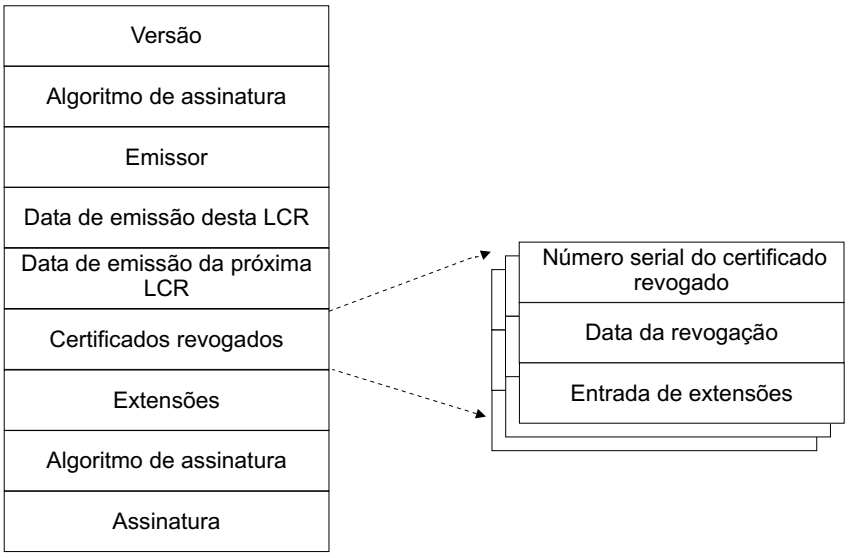

Figura 3.4: Lista de Certificados Revogados

3.1.3 Componentes de uma ICP

Uma infra-estrutura de chaves públicas é constituída pelo ambiente físico, equipamentos, programas e pessoas, que em conjunto são responsáveis por criar e gerir a infra-estrutura que provê serviços ligados a emissão e manutenção de certificados de chave pública.

Entre seus componentes destacam-se a Autoridade Certificadora, descrita a seguir, a Autoridade de Registro, descrita na seção 3.1.3.2, página 61, o Diretório Público, descrito na seção 3.1.3.3, página 62, e a Autoridade de Datação, descrita na seção 3.1.3.4, página 62.

3.1.3.1 Autoridade Certificadora

A Autoridade Certificadora é o componente principal de uma ICP e é ela que detém a confiança de seus usuários. Constituem suas funções (HOUSLEY; POLK, 2001):

- Emitir certificados digitais;
- Emitir LCR;
- Publicar certificados válidos e LCR; e
- Manter informações relativas a certificados expirados e revogados, emitidos por ela.

Uma AC pode emitir certificados para qualquer tipo de entidade, seja ela uma pessoa, equipamento, ou mesmo outra AC. O mecanismo de emissão de um certificado consiste no recebimento, análise e validação dos dados contidos em uma requisição criada e enviada por uma entidade. A validação deste dados visa constatar a sua veracidade, uma vez que, quando emitido, o certificado digital ligará estes dados a um determinado sujeito. A assinatura da AC sobre o certificado confere a ele validade perante a comunidade de usuários que confiam, direta ou indiretamente, naquela AC em particular.

Com exceção a emissão de certificados, que constitui função exclusiva da AC, as demais funções podem ser delegadas pela AC para outros componentes da ICP. Desta maneira, a AC pode direcionar seus esforços para a execução de sua função exclusiva e manutenção da sua própria segurança.

Devido a natureza crítica dos serviços prestados pela AC, torna-se necessária a implantação de políticas de segurança rígidas e eficazes, principalmente no que concerne a proteção da

sua chave privada, uma vez que é com ela que a AC assina os certificados e as LCR que emite. Estas políticas devem prever a criação de um perímetro seguro em torno da AC, utilizando barreiras físicas, lógicas e humanas.

O item mais crítico de uma ICP é a manutenção da chave privada da AC, em maior grau de criticidade, a da AC raiz. O eventual comprometimento da chave privada de uma AC, implica na destruição da confiança depositada sobre todos os documentos que ela emitiu, e conseqüentemente na invalidação destes, uma vez que eles serão passíveis de fraude.

Em virtude deste fato, as ACs podem adotar mecanismos que incrementem o grau de segurança das chaves através do uso de módulos criptográficos de hardware que seguem o padrão FIPS[1] 140-2 (NIST, 2001). Estes equipamentos são responsáveis pela geração do par de chaves e a manutenção da chave privada.

Outras medidas importantes que visam a segurança da AC e a disponibilidade dos seus serviços são: redundância de equipamentos e sistemas, cópias de segurança de sistemas e dados, controles físicos em ambientes que abrigam componentes da infra-estrutura (salas cofres) e controles lógicos que evitem ataques através de sistemas informatizados.

3.1.3.2 Autoridade de Registro

A Autoridade de Registro (AR) é um componente opcional e cabe a ela assumir funções administrativas delegadas por uma AC e necessárias à emissão de certificados digitais. Estas funções constituem na análise e validação de dados constantes em requisições de certificados enviadas por usuários.

A averiguação e comprovação dos dados obedece a políticas e procedimentos previamente estabelecidos. Alguns destes constituem na verificação de documentos, a solicitação da presença física do solicitante e comprovação de posse da chave privada correspondente à chave pública informada na requisição (FORD; BAUM, 1997).

As políticas e procedimentos de análise e validação são estabelecidos de maneira particular para cada classe de certificados, cujas requisições serão analisadas pela AR.

As ARs normalmente são geograficamente separadas uma das outras, visando facilitar o acesso aos seus serviços pelos usuários.

[1] Federal Information Processing Standards Publication

Ao receber uma requisição a AR procede com análise dos dados contidos nesta, utilizando nestes processos as políticas e procedimentos cabíveis para o tipo de certificado solicitado na requisição. Se validados os dados, a AR assina digitalmente a requisição, o que comprova a sua validade, e a envia a AC que emitirá o certificado. Cabe à AC a emissão do certificado digital.

3.1.3.3 Diretório Público

O Diretório Público (DP) é a entidade responsável pela publicação e distribuição de certificados digitais e LCR.

Embora responsável pela distribuição de certificados e LCR, o DP não é responsável pela integridade destes documentos. Suas funções são armazenar e maximizar a disponibilidade e o desempenho no acesso a estes. A integridade dos documentos armazenados no DP é garantida pela assinatura digital neles constante, de autoria da AC que os emitiu.

A obtenção de um certificado digital ou de uma LCR ocorre, normalmente, através de um DP, onde deve-se localizar o documento desejado através de mecanismos de busca próprios do sistema. Na busca devem ser informados determinados parâmetros que permitam a localização do documento específico ou um pequeno grupo de documentos, dentre os quais está o desejado. Um exemplo destes parâmetros é o nome do sujeito de um certificado digital.

No contexto atual, os serviços de Diretório Público mais difundidos são os estruturados com base no modelo definido na recomendação ITU-T X.500 (ITU, 1997) e que possuem seus mecanismos de acesso baseados no protocolo *Lightweight Directory Access Protocol (LDAP)* Versão 2 (YEONG; HOWES; KILLE, 1995) ou Versão 3 (WAHL; HOWES; KILLE, 1997).

3.1.3.4 Autoridade de Datação

A Autoridade de Datação (AD) é responsável por ancorar no tempo documentos eletrônicos ou ações ligadas a eles, tal como uma assinatura digital.

Segundo Bayer, Haber e Stornetta (1991), um método eficiente de datação deve atender os seguintes requisitos de segurança:

- **Privacidade:** somente o cliente pode ter acesso ao conteúdo do documento;
- **Canal de comunicação e armazenamento:** provimento de praticidade independentemente do tamanho do documento;

- **Erro na comunicação:** garantia da integridade dos dados e operação ininterrupta do serviço de datação;
- **Anonimato:** garantia de anonimato ao cliente; e
- **Confiança:** certeza da consistência dos dados de temporalidade.

Os métodos de datação podem ser absolutos ou relativos (ROOS, 1999). A autenticação temporal absoluta contém informações de data e hora igual a usada no mundo real, enquanto relativa contém informações que verificam se um documento foi datado antes ou depois de um outro documento. O esquema absoluto pressupõe que a AD seja uma entidade confiável, e o esquema relativo não necessita desta propriedade, pois existem mecanismos que garantem que o documento sempre seja datado com data e hora corretas. Este problema pode ser tratado através da utilização do encadeamento dos resumos dos documentos protocolados, proposto por (PASQUAL, 2002).

Autoridades de Datação devem prover mecanismos que permitam, através de processos de auditoria, a constatação da sua correta operação.

3.1.4 Políticas de Certificação e Práticas de Certificação

Políticas de Certificação e Práticas de Certificação são diferentes documentos que descrevem um conjunto de regras e procedimentos associados a operação e aos produtos de uma ICP.

Políticas de Certificação descreve quais são os requisitos de segurança que devem ser atendidos pelas ACs na emissão dos seus certificados, bem como a aplicabilidade destes dentro de uma determinada comunidade de usuários (CHOKHANI; FORD, 1999).

Em uma Política de Certificação, além de serem estabelecidos, de maneira detalhada, requisitos e restrições de emissão e uso de um certificado digital emitido através da ICP, também são estabelecidas as responsabilidades dos usuários quanto a requisição, ao uso e a manipulação de certificados e chaves criptográficas.

Nesta política também estão especificados as classes possíveis de certificados e a finalidade de uso destes, restringindo desta maneira a aplicação de determinado certificado. Um

certificado, por exemplo, pode ter seu uso restrito a assinatura de e-mails ou a autenticação em um determinado sistema.

Já nas Práticas de Certificação é declarado o conjunto de práticas empregadas pelas ACs da ICP na emissão dos certificados digitais (CHOKHANI; FORD, 1999).

3.1.5 Modelos de confiança

A constituição de uma ICP pode conter várias ACs, e estas necessitam estabelecer relações de confiança entre si (HOUSLEY; POLK, 2001; LLOYD et al., 2001). Esta necessidade também existe no relacionamento entre ACs de ICPs distintas. A importância destes relacionamentos está ligada ao fato da AC ser a "terceira parte", na qual o usuário deposita sua confiança.

As relações de confiança entre ACs podem ser constituídas de diversas maneiras, sendo estas classificadas em modelos de confiança (PERLMAN, 1999).

Modelos de confiança estabelecem uma cadeia de confiança[2] entre ACs, denominada caminho certificação (LLOYD, 2002). Através deste é possível verificar se uma AC é confiável, partindo de um ponto de confiança[3]. Estes modelos são úteis para permitir que um certificado emitido por uma AC, possa ser aceito e validado por outra, bem como, possibilitar que uma ICP seja escalável[4].

Os modelos de confiança podem ser estabelecidos de duas formas: relacionamentos hierárquicos ou relacionamentos ponto-a-ponto. As seções subseqüentes abordarão os modelos de confiança estudados, a saber: hierárquico; em malha; e em ponte.

3.1.5.1 Modelo Hierárquico

Este modelo apresenta a organização das ACs relacionadas entre si de forma hierárquica. A relação de confiança entre as ACs é estabelecido automaticamente na emissão dos seus certificados. ACs superiores emitem os certificados para as ACs inferiores, que, por sua vez, os utilizam para assinar os certificados que emitem. Este fato, implica diretamente na confiança da AC inferior na AC superior.

[2] constituída por relacionamentos de confiança entre entidades ordenados por uma seqüência.

[3] AC em que o usuário confia, sendo normalmente a entidade emissora do seu certificado.

[4] funcionamento de uma solução a medida que o problema cresce.

Uma AC superior, localizada no topo da hierarquia, possui seu certificado auto-assinado, ou seja, na geração do seu certificado, a própria AC realiza a assinatura (HUNT, 2001). Estas ACs são denominadas *AC raiz*.

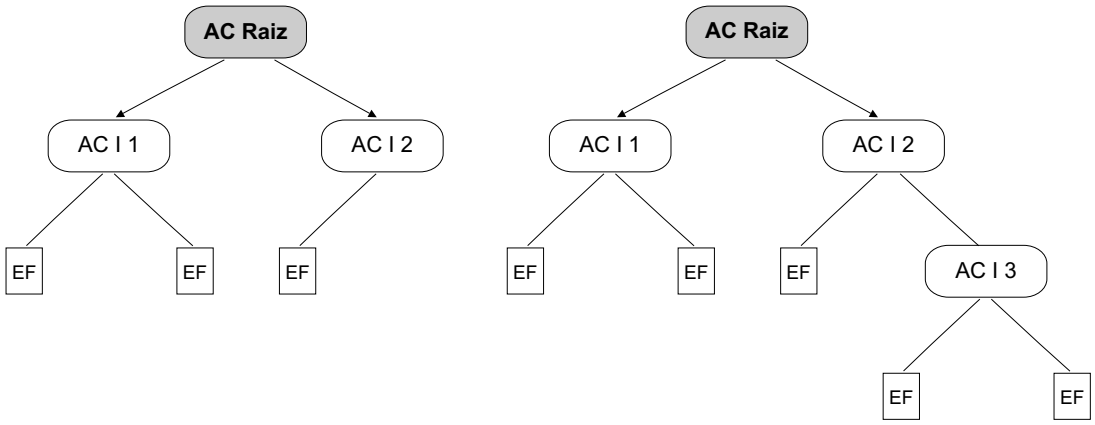

Figura 3.5: Modelos de confiança hierárquicos

Como ilustrado na figura 3.5, uma ICP pode ser constituída por várias ACs raiz, sendo que estas podem emitir certificados para entidades ou usuários finais (EF), ou para outras ACs, isto depende da política adotada. Normalmente as ACs raiz emitem certificados apenas para ACs inferiores, as chamadas ACs intermediárias (ACI) ou finais. As intermediárias são as que possuem ACs subordinadas a ela, enquanto as finais emitem certificados apenas para usuários(MOSES, 2002). Esta organização estabelece o caminho de certificação.

Este modelo possui quatro propriedades atrativas. A primeira se refere a escalabilidade, pois é fácil a inserção de uma nova AC dentro da hierarquia. A segunda propriedade, é a facilidade de construção do caminho de certificação, pois a confiança é unidirecional. A terceira é por possuir caminhos de certificação relativamente curtos, uma vez, que o maior caminho é igual a profundidade da árvore mais um. A quarta propriedade diz respeito a facilidade do usuário conhecer qual aplicação dos certificados emitidos por uma AC, dado sua localização hierarquia (POLK; HASTINGS, 2000).

A desvantagem deste modelo, é que o comprometimento da AC raiz, implica no comprometimento da hierarquia inteira, pois a característica deste modelo está na concentração da confiança nas ACs raiz (PERLMAN, 1999; POLK; HASTINGS, 2000).

3.1.5.2 Modelo em Malha

O modelo de confiança em malha, conecta as ACs através de relacionamentos ponto-a-ponto, conforme ilustra a figura 3.6. Estes relacionamentos são criados através da emissão mútua de certificados, onde cada AC emite o certificado para outra, estabelecendo um relacionamento bi-direcional, também chamada de certificação cruzada[5](LLOYD et al., 2001).

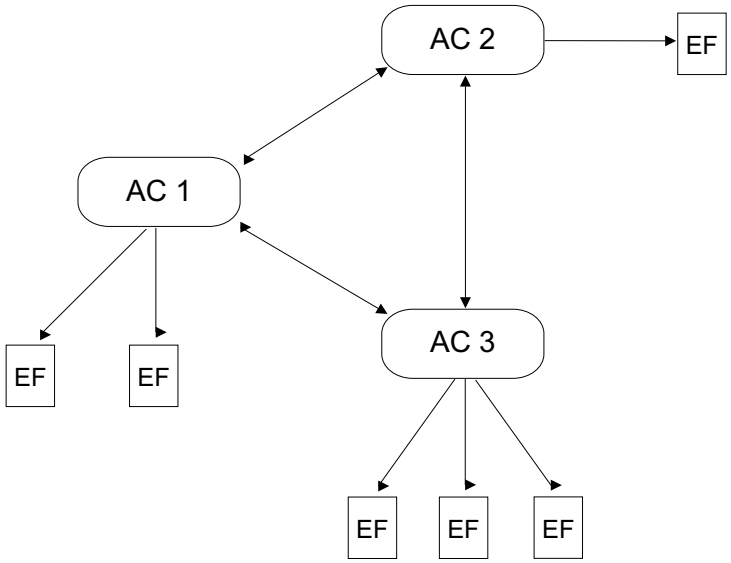

Figura 3.6: Modelo de confiança em Malha

Porém, a forma do estabelecimento destes relacionamentos não permitem que ACs imponham condições para gerenciar os tipos de certificados que outra AC pode emitir. Entretanto, a relação de confiança pode ser condicionada através da sua especificação nas extensões[6] do certificado emitido (POLK; HASTINGS, 2000).

Uma ICP em malha tem como propriedade atrativa a facilidade de incorporar uma AC de outra ICP, bastando estabelecer um relacionamento ponto-a-ponto entre ACs de ambas ICPs. Outra característica atrativa, é que neste modelo o comprometimento de qualquer AC não se

[5]A certificação cruzada também pode ser unilateral, neste caso ocorre apenas a emissão do certificado de uma AC para outra.

[6]além dos campos de informação obrigatórios de um certificado, como identificação do proprietário do certificado (sujeito), sua chave pública, dados e assinatura da AC, um certificado contém campos adicionais que podem ser utilizados para diversos propósitos, por exemplo, informar a política sob a qual o certificado foi emitido. Estas informações são colocadas em uma área do certificado denominada extensões.

propaga para a cadeia inteira, como ocorre na hierárquica.

Entretanto o modelo em malha possui algumas propriedades indesejáveis, as quais estão relacionadas ao modelo de confiança bi-direcional. Neste, o caminho de certificação é não determinístico, e assim, mais complexo que o hierárquico, sendo que o número máximo de uma caminho de certificação é igual ao número de ACs pertencentes a cadeia de confiança.

3.1.5.3 Modelo em Ponte

O modelo em ponte permite ligar ICPs que implementam diferentes modelos de confiança através de uma entidade denominada ponte (ALTERMAN, 2001).

Conforme ilustrado na figura 3.7, a ponte é utilizada como um ponto central de confiança, o qual as autoridades ceritificadoras estabelecem confiança através da certificação cruzada. Este modelo reduz a quantidade de relacionamentos de confiança entre ACs, pois a confiança em uma ponte resulta na confiança em todas as entidades que estabeleceram relacionamento com a ponte, não necessitando constituir confiança com cada AC individualmente.

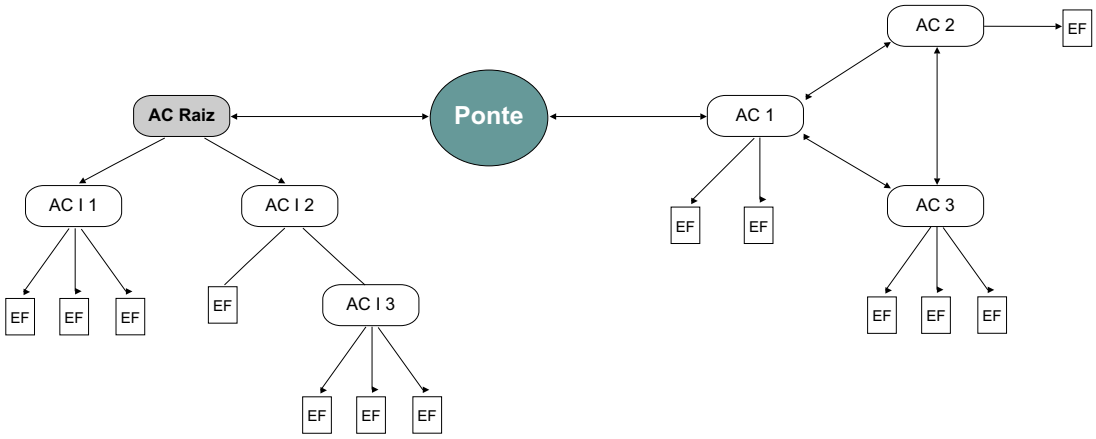

Figura 3.7: Modelo de confiança em Ponte

A ponte é um ponto de confiança apenas para ACs, pois esta não emite certificados diretamente a usuários. Estes alcançam a confiança em uma determinada AC se seu ponto de confiança (sua AC) confiar em uma ponte que mantém relacionamento com a AC desejada (POLK; HASTINGS, 2000).

A ponte permite que instituições com infra-estruturas de chave pública próprias intero-

perem através de uma arquitetura simplificada, que minimiza o gerenciamento da certificação cruzada e melhora a interoperabilidade técnica Alterman (2001).

3.1.6 Caminho de Certificação

A comunicação entre duas partes que utilizam certificados digitais emitidos por Autoridades Certificadoras distintas necessitam ser validados entre as partes. A validação consiste na verificação do caminho de certificação, ou seja, uma cadeia de certificados entre o certificado e o ponto de confiança devem ser estabelecido, e cada certificado dentro do caminho deve ser checado.

O caminho de certificação é um processo complexo e está sujeito a um grau de tentativa e erro. O caminho de certificação abrange duas fases: caminho de construção e caminho de validação (LLOYD, 2002).

A fase de caminho de construção consiste na determinação de um ou mais caminhos de certificação candidatos. Um caminho de certificação ser candidato se deve ao fato de que a cadeia de certificados pode alcançar a AC alvo, porém a cadeia pode ser inválida por outros motivos como o comprimento do caminho, nome ou restrições da política de certificado.

A fase de caminho de validação inclui a verificação de cada certificado no caminho. Esta verificação inclui a confirmação do período de validade, a existência de revogação, integridade e a análise da política.

A análise da política consiste no atendimento das restrições do comprimento do caminho, extensões e política de restrições contidas nas política da AC que emitiram o certificado das ACs que encontram-se no caminho de construção.

O nível mais básico do candidato ao caminho de certificação é a “corrente conhecida”, na qual o caminho é constituído entre a âncora de confiança e o certificado alvo.

A âncora de confiança será sempre uma autoridade certificadora, pois é considerada uma “terceira parte confiável”, ou seja, um agente ou entidade na qual é depositada a confiança nos serviços prestados. Já o certificado alvo é um certificado de uma entidade final.

A figura 3.8 apresenta a construção de um caminho de certificação utilizando as informações constantes nas três versões do certificado digital. A construção é realizada através das informações do Emissor do Certificado e do Sujeito.

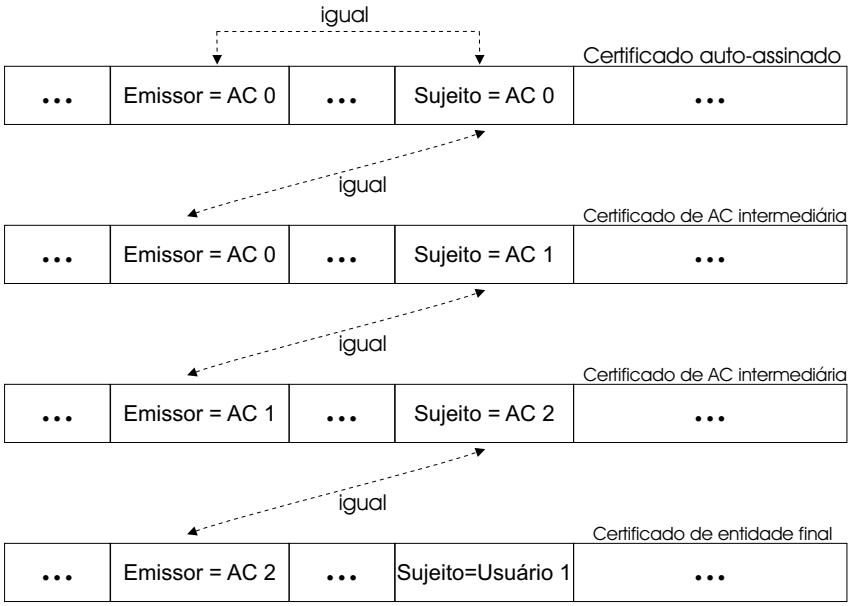

Figura 3.8: Construção do caminho de certificação

Se a construção seguir no sentido da âncora de confiança para baixo, o sujeito da AC0 é igual ao emissor, pois é um certificado auto-assinado. O certificado seguinte possui como o emissor o sujeito do certificado anterior. Esta operação se repete até alcançar o certificado alvo.

Esta operação pode ocorrer no sentido inverso, partindo do certificado alvo e verificando se este alcança a âncora de confiança.

3.1.7 Custo Total de Propriedade de uma ICP

Uma análise realizada pela empresa americana *VeriSign, Inc.*, uma das maiores empresas da área de certificação digital, avaliou o Custo Total de Propriedade (CTP) de uma ICP (VERISIGN, 2002). Esta análise envolveu diversos elementos, os quais são em parte listados abaixo:

1. Infra-estrutura física do ambiente que abrigará os componentes da ICP;
2. Equipamentos;
3. Programas;
4. Equipamentos e equipe profissionais responsáveis pela segurança física da ICP;

5. Equipe de profissionais da área de tecnologia de informação;

6. Procedimentos de registro e autenticação; e

7. Serviços de consultoria.

A análise de CTP visa quantificar custos de aquisição, operação e gerenciamento de serviços ou produtos, durante um determinado período de tempo.

Alguns dos valores levantados em (VERISIGN, 2002) são apresentados, a título informativo, na tabela 3.2.

Tabela 3.2: Alguns dos itens avaliados na análise de Custo Total de Propriedade de uma ICP realizada pela VeriSign, Inc.: Valores considerando o custo anual em dólares.

Item avaliado	**Custo**	**Fator multiplicativo**
Servidor (equipamento)	U$ 50.000,00	por servidor, com capacidade para 10.000 usuários
Programa para servidor	U$ 27.000,00	por servidor
Programa para estação de trabalho	U$ 30,00	por usuário
Serviços de consultoria	U$ 2.500,00	por dia durante 30 dias
Infra-estrutura de um Centro de Controle de Operações	U$ 300.000,00	por ano

3.2 Compartilhamento de Segredos

Esquemas de compartilhamento de segredos são mecanismos criptográficos que permitem dividir um segredo em partes, de modo que ele somente possa ser reconstruído a partir da união de um número, previamente determinado, destas partes. Após a divisão do segredo, as partes obtidas são distribuídas entre os membros de um grupo de entidades.

Em essência, estes esquemas permitem distribuir o controle de uma certa informação entre as entidades de um grupo, provendo, assim, uma maior segurança para a informação representada pelo segredo, uma vez que o controle desta não estará entregue a uma única entidade.

Comumente, esquemas de compartilhamento de segredos são utilizados no compartilhamento de chaves criptográficas, entretanto o segredo a ser compartilhado pode possuir diversas naturezas, o que assegura a utilização destes esquemas em um grande número de aplicações.

O compartilhamento de um determinado segredo entre entidades pode ocorrer de forma heterogênea, permitindo cada uma destas possua um nível diferente de controle sob o segredo em relação as demais. Isto pode ser provido através da divisão do segredo em um número maior de partes que a quantidade de entidades do grupo e posterior entrega destas partes, em diferentes quantidades, a cada uma das entidades. Desta maneira, terá maior controle sobre o segredo a entidade que possuir maior número das suas partes.

Esquemas de compartilhamento de segredos são baseados em técnicas matemáticas e dividem-se em dois grupos, a saber:

1. Esquema de Divisão do Segredo; e
2. Esquema de Limiar.

Em esquemas de Divisão do Segredo (SCHNEIER, 1996), o segredo é dividido entre os membros de um grupo de forma que o ele somente possa ser reconstruído se todos os detentores das suas partes cooperarem, entregando-as no processo de reconstrução. Estes esquemas possuem uma desvantagem, a qual recai sobre a necessidade de cooperação de todos aqueles que receberam inicialmente uma parte do segredo, pois caso uma das partes não seja entregue, por algum motivo, o segredo não poderá mais ser recuperado. Formalmente estes esquemas permitem dividir um segredo s entre um grupo de n entidades, de forma que sua reconstrução é possível através da cooperação de t destas entidades, sendo $t = n$.

Esquemas de limiar foram propostos independentemente por George R. Blakley e Adi Shamir (SHAMIR, 1979). Ao contrário de esquemas de Divisão do Segredo, neste o segredo pode ser dividido de maneira que, para viabilizar a sua reconstrução, somente sejam necessária um número mínimo de entidades detentoras das partes do segredo. A desvantagem encontrada nos esquemas de divisão do segredo não ocorre aqui, pois o número de entidades que devem cooperar para reconstruir o segredo não é, necessariamente, igual ao número total de entidades do grupo. Formalmente estes esquemas permitem dividir um segredo s entre um grupo de n entidades, de forma que sua reconstrução é possível através da cooperação de t destas entidades, sendo $t \leq n$.

Os elementos existentes em esquema de compartilhamento de segredo são:

- Grupo de entidades;

- Terceira entidade confiável (opcional); e
- Estrutura de acesso.

O **grupo de entidades** é formado pelos n portadores das parcelas do segredo divido. São eles, portanto, que possuem o controle compartilhado sobre este segredo.

A **terceira entidade confiável** (TEC) é a responsável por dividir o segredo e entregar as partes aos membros do grupo de entidades. Sendo a TEC a responsável pela divisão do segredo, ele conseqüentemente é conhecedor da informação representada pelo segredo. Entretanto, existem aplicações que exigem que ninguém conheça previamente o segredo e tampouco tenha controle total sobre ele, o que torna a figura da TEC indesejável. Este requisito é suprido por protocolos de compartilhamento de segredos que não utilizam uma TEC (INGEMARSSON; SIMMONS, 1991; PEDERSEN, 1991; JACKSON; MARTIN; O'KEEFE, 1995; STINSON; WEI, 1999). Nestes protocolos o segredo é construído e compartilhado de maneira cooperativa entre os membros do grupo e somente é conhecido no momento em que houver a cooperação entre um certo número de entidades do grupo.

A **estrutura de acesso** determina todos os subgrupos autorizados capazes de reconstruir o segredo. Um subgrupo é considerado autorizado, uma vez que ele possua um mínimo de t, das n entidades detentoras das parcelas do segredo. Portanto, t, normalmente referenciado por *limiar*, representa o número de entidades necessárias para viabilizar a reconstrução do segredo. O subgrupo que possuir um número de entidades menor que t, é incapaz de obter qualquer informação sobre o segredo, sendo, por este motivo, denominado subgrupo não autorizado.

3.3 Serviço de Criptografia Temporal

Um Serviço de Criptografia Temporal (SCT) fornece mecanismos que permitem determinar o momento futuro em que uma informação deixará de ser confidencial. Este serviço fundamenta-se no conceito de criptografia temporal proposto por Timothy C. May (MAY, 1993) e aprofundado por de Ronald L. Rivest, Adi Shamir e David A. Wagner (RIVEST; SHAMIR; WAGNER, 1996). Após estes, outros trabalhos foram publicados abordando este conceito.

A criptografia temporal permite determinar o tempo futuro em que uma informação cifrada poderá ser decifrada. Através de métodos específicos, a confidencialidade da informação

é assegurada durante todo o período que antecede ao momento previamente determinado para a sua divulgação. Os métodos utilizados podem basear-se em (RIVEST; SHAMIR; WAGNER, 1996):

1. **Entidades confiáveis:** a informação a ser protegida é entregue a uma terceira entidade, considerada confiável, a qual compromete-se em manter segura e confidencial a informação durante o período de tempo estabelecido; e

2. **Complexidade computacional:** os meios que permitirão o acesso a informação confidencial somente podem ser obtidos através da solução de um problema. Este é construído de maneira que sua solução somente seja encontrada após transcorrido o período de tempo em que a informação deve permanecer confidencial e mediante o emprego contínuo de um determinado esforço computacional.

Marco Casassa Mont, Keith Harrison e Martin Sadler apresentaram em (MONT; HARRISON; SADLER, 2003) um SCT baseado em entidades confiáveis, denominado *HP Time Vault Service (HP-TVS)*. O funcionamento do HP-TVS baseia-se em criptografia assimétrica e consiste, inicialmente, em emitir e publicar várias chaves públicas. Através destas chaves é possível determinar o momento futuro em que as respectivas chaves privadas serão tornadas públicas. No momento especificado em cada chave pública, o HP-TVS constrói e divulga a respectiva chave privada. Desta maneira, ao usuário deste serviço basta selecionar dentre as chaves públicas disponíveis, a que terá sua chave privada divulgada na data em que deseja-se que determinado documento deixe de ser confidencial. A confidencialidade deste documento, que deve ser cifrado com a chave pública escolhida, estará assegurada até a divulgação da respectiva chave privada.

3.4 Conclusão

Os detalhamentos apresentados referente a tecnologia de infra-estrutura de chaves públicas, provendo a identificação dos requisitos necessários à sua constituição e funcionamento, aos esquemas de compartilhamento de segredos, e aos serviços de criptografia temporal, são fundamentais para o entendimento das propostas apresentadas nos capítulos 7 e 8.

Capítulo 4

Procedimentos Metodológicos

A descrição dos procedimentos metodológicos adotados nesta pesquisa tem por objetivo facilitar tanto seu entendimento como sua eventual replicação. Este raciocínio é coerente com o exposto por Santos (2000, p. 25): "*os pesquisadores são freqüentemente solicitados a caracterizar seus trabalhos, especialmente por ocasião da leitura por terceiros de qualquer etapa dos resultados*".

Assim, na seqüência deste documento é apresentado a caracterização desta pesquisa, método de pesquisa, análise e interpretação dos dados e a metodologia de modelagem utilizada.

4.1 Caracterização da pesquisa

Dado as diversas formas de classificação de pesquisas adotadas por diferentes autores de estudos metodológicos (GUERRA, 1996), exige-se uma análise da pesquisa proposta sob a luz de diferentes óticas de forma a dar-lhe uma caracterização consistente.

Na seqüência a pesquisa proposta é caracterizada em relação à(ao):

4.1.1 Natureza

Alguns autores iniciam a classificação da pesquisa em relação a sua natureza, se básica ou aplicada.

Segundo Silva e Menezes (2001, p. 20), uma pesquisa de natureza aplicada é aquela capaz de "*gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos.*"

Este entendimento é reforçado por Guerra (1996) que menciona que a pesquisa aplicada "... *se caracteriza pelo interesse na aplicação, utilização e conseqüências práticas dos conhecimentos. A pesquisa aplicada busca o conhecimento para fazer, atuar, construir ou modificar.*" [1]

Como a proposta de pesquisa satisfaz as definições apresentadas ela pode ser classificada como uma pesquisa de natureza aplicada.

4.1.2 Objetivo

Outra forma de classificar a pesquisa, é fazê-lo de acordo com seus objetivos, subdividindo-a em: exploratória; descritiva; ou explicativa.

Como descrito no início do presente capítulo a definição do tema de pesquisa proposto envolveu várias discussões com pesquisadores que atuam nas áreas de conhecimento específicas, juntamente com uma pesquisa bibliográfica ampla de várias áreas de conhecimento e de como elas interagem entre si.

O procedimento descrito enquadra-se no tipo de pesquisa dito exploratório, pois, de acordo com Santos (2000, p. 26) este tipo de pesquisa busca

> "*informar ao pesquisador a real importância do problema, o estágio em que se encontram as informações já disponíveis a respeito do assunto, e até mesmo, revelar ao pesquisador novas fontes de informação. Por isso, a pesquisa exploratória é quase sempre feita como levantamento bibliográfico, entrevistas com profissionais que estudam/atuam na área, visitas a web sites, etc.*"

Entretanto, por se estar descrevendo as possíveis influências no processo de avaliação somativa da evolução tecnológica dentro do modelo de organizações virtuais, a pesquisa proposta pode ser enquadrada como do tipo descritiva. Pois, atende a definição expressa por Gil (2002, p. 42) de que pesquisas descritivas "*tem como objetivo primordial a descrição de determinada população ou fenômeno, ou, então, o estabelecimento de relação entre variáveis.*"

Em resumo, sob a ótica do tipo de pesquisa no que diz respeito aos seus objetivos, a proposta pode ser classificada como exploratória e descritiva.

[1] tradução livre

4.1.3 Tempo

Uma pesquisa pode ser classificada em função de sua abordagem em relação ao tempo. A pesquisa horizontal, ou longitudinal, é aquela cujo fenômeno é observado durante um período de tempo. A pesquisa vertical, ou transversal, é aquela cujo fenômeno é observado em um determinado instante de tempo (GUERRA, 1996).

Sob esta perspectiva, a pesquisa proposta pode ser classificada como vertical, ou transversal, pois foca uma realidade atual dada uma evolução tecnológica e organizacional.

4.1.4 Procedimento de coleta de dados

Com respeito aos procedimentos de coleta de dados Santos (2000, p. 25) classifica a pesquisa como bibliográfica, documental, experimento, levantamento e estudo de caso.

Comparando-se a definição dada pelos autores a pesquisa proposta, segundo o procedimento de coleta de dados, pode ser considerada:

- bibliográfica, pois é desenvolvida com base em livros, teses, dissertações, artigos científicos, normas e legislação específica; e
- experimental, pois envolve a proposição de um modelo, sua representação e análise.

Ainda no que tange a pesquisa bibliográfica, a utilização de um modelo de desenvolvimento deve ser vista apenas como um roteiro, que pode ser alterado no decorrer do trabalho (GIL, 2002). Lakatos e Marconi (2001), no intuito de auxiliar a identificar as informações, apresenta o seguinte modelo de roteiro, utilizado neste trabalho:

- Leitura preliminar, que permite uma familiarização com o tema;
- Leitura seletiva, que identifica os principais eventos/atividades ocorridos no período considerado para análise;
- Leitura reflexiva, que incrementa o entendimento do assunto; e
- Leitura interpretativa, que compara as abordagens teóricas e empíricas discutidas pelos autores pesquisados em relação a realidade tratada no presente estudo.

Gil (2002, p. 42), acresce à classificação inicial as pesquisas a *ex-post facto*, o estudo de coorte, a pesquisa-ação e a pesquisa participante. Santos (2000, p. 30), por outro lado, considera estas outras classificações segundo o procedimento de coleta, inclusive o da pesquisa qualitativa ou quantitativa, como "*modalidades de aplicação dos procedimentos anteriores*".

Em resumo, do ponto de vista de coleta de dados a pesquisa proposta pode ser caracterizada como bibliográfica e experimental.

4.1.5 Abordagem

A classificação da pesquisa como quantitativa ou qualitativa não é trivial, tanto do ponto de vista teórico, quando da classificação deste trabalho específico.

A dificuldade teórica se dá pelas diferentes convenções e abordagens dada por diversos autores, conforme destacado no trabalho de Falconer e Mackay (1999). Inclusive Santos (2000, p. 30), considera a classificação da pesquisa em qualitativa ou quantitativa, como "*modalidades de aplicação dos procedimentos anteriores*" de coleta de dados.

Do ponto de vista prático, como a pesquisa proposta adota como procedimento para coleta os dados a pesquisa bibliográfica e a experimentação, a classificação em termos qualitativos ou quantitativos se torna mais complexa. Já esta classificação aplicada a trabalhos que envolvem pesquisa de campo, através de formulários, é mais simples.

Para facilitar pode-se considerar que a classificação como qualitativa ou quantitativa sejam "*abordagens do problema*", conforme definido por Silva e Menezes (2001, p. 20). Neste sentido Silva e Menezes (*idem*) definem que a "*interpretação dos fenômenos e a atribuição de significados são básicas no processo de pesquisa qualitativa*".

Sob esta ótica a pesquisa proposta pode ser classificada como qualitativa.

4.1.6 Fonte de informação

A classificação da pesquisa em função da fonte de informação, de onde se extraem os dados ou do local onde ocorre a investigação (GUERRA, 1996), pode ser dividida como de: documentos; de campo; laboratório; ou simulação (HELLENS, 2001).

Como descrito no início deste capítulo a pesquisa proposta envolve uma ampla pesquisa bibliográfica e a proposição de modelos. Sendo assim, no que diz respeito a fonte de infor-

mação, a fonte de informação para a pesquisa proposta são documentos e a análise do modelo proposto.

4.2 Método de pesquisa

Em relação a definição de método de pesquisa Lakatos e Marconi (2000, p. 46) dão a seguinte definição resumida:

> "*O método é o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo - conhecimentos válidos e verdadeiros -, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista.*"

Com respeito ao enquadramento da pesquisa proposta em relação ao método de pesquisa, pode-se concluir que o método utilizado é o hipotético-dedutivo, pois "*...defendo o aparecimento, em primeiro lugar, do problema e da conjectura, que serão testados pela observação e experimentação*" (*idem*, p. 72).

4.3 Análise e interpretação dos dados

Esta pesquisa é fruto de várias discussões com pesquisadores que atuam nas áreas de conhecimento específicas, juntamente com uma pesquisa bibliográfica ampla de várias áreas de conhecimento e de como elas interagem entre si. A pesquisa envolve ainda a proposição de um modelo computacional para tratar o problema, sua representação e análise de forma teórica.

Pelo exposto pode-se aplicar o sugerido por Alves-Mazzotti e Gewandsznajder (2001, 171): "a análise será desenvolvida durante toda a investigação, através de teorizações progressivas...".

Por sua vez o modelo proposto será, "sob o ponto de vista epistemológico", uma "interpretação das teorias obtidas dos dados documentais", conforme Vera (1976, 153).

Assim, em resumo, a pesquisa proposta pode ser classificada como: aplicada, pela sua natureza; exploratória e descritiva, em relação a seus objetivos; transversal, sob a perspectiva do tempo; bibliográfica e experimental, em relação aos procedimentos de coleta de dados; de

documentos e análise dos modelos, como fonte dos dados; e qualitativa, em relação a abordagem.

Entretanto, como esta pesquisa culmina na apresentação de modelos é necessário ainda a descrição da metodologia de modelagem.

4.4 Modelagem

As propostas apresentadas neste trabalho baseiam-se na descrição e depuração de modelos computacionais. Portanto, é fundamental conceituá-los, apresentar as bases da engenharia de software, descrever a linguagem de representação e metodologia a ser utilizada.

4.4.1 Modelos

Os modelos propostos neste trabalho podem ser entendidos como a "representação simplificada e abstrata de fenômeno ou situação concreta, e que serve de referência para a observação, estudo ou análise" e "descrição formal de objetos, relações e processos, e que permite, variando parâmetros, simular os efeitos de mudanças de fenômeno que representa", conforme definição dada por Aurélio (FERREIRA, 1999).

De forma precisa, serão utilizados para modelos computacionais, que são representações formais de processos, com visão tanto estática como dinâmica, envolvendo representações através de textos, diagramas e fórmulas matemáticas. Buscar-se-á através da descrição destes modelos formais apresentar as idéias propostas.

A área da ciência da computação que aborda o uso de modelos computacionais é a engenharia de software.

4.4.2 Engenharia de Software

A engenharia de software possui basicamente o mesmo princípio da engenharia de sistemas e de hardware, ou seja, ela existe para fazer com que o produto final antes de ser construído seja analisado e discutido para aumentar as possibilidades de sucesso em sua criação. Este produto pode ser um programa de computador, sistema computacional ou mesmo um periférico de hardware. A engenharia de software abrange um conjunto de três elementos fundamentais: os

métodos; as ferramentas; e os procedimentos, que possibilitam ao gerente o controle do processo de desenvolvimento do programa e oferece ao profissional uma base para sua construção com alta qualidade e produtividade (PRESSMAN, 1995).

Dentro da engenharia de software encontramos o conceito do desenvolvimento de programa, que Larman (2000, p. 40) afirma ser um método para organizar as atividades relacionadas com a criação, entrega e manutenção de sistemas de software.

No mesmo sentido Bezerra (2002, p. 19) conceitua desenvolvimento de programa para computador como o processo que "compreende todas as atividades necessárias para definir, desenvolver, testar e manter um produto de software".

Como este processo é uma atividade bastante complexa, grande números de projetos não atingem as metas do planejamento em relação a tempo e custo. Porém a utilização de ferramentas de engenharia de software tem sido um dos fatores para a melhora deste cenário, conforme relatório feito pelo Standish Group (EXTREME..., 2000), que compara o sucesso de projetos realizados entre 1994 e 2000, conforme figura 4.1.

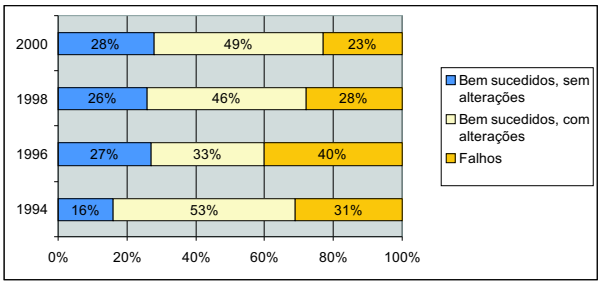

Figura 4.1: Taxa de sucesso de projetos

Há quase uma década Pressman (1995) já salientava que o desenvolvimento de programas de computador não dava a necessária ênfase à análise e planejamento, focando o desenvolvimento para a solução do problema. Assim, salientava a necessidade do uso de técnicas de engenharia de software para resolver problemas no desenvolvimento de sistemas.

A aplicação da engenharia de software se dá, segundo Bezerra (2002), pela execução das seguintes tarefas: levantamento e análise de requisitos, o projeto, a implementação, os testes e a implantação. A seqüência com que estas tarefas são implementadas determinam o modelo de ciclo de vida.

Dentre os modelos de ciclo de vida mais difundidos destacam-se o modelo em cascata, espiral e o modelo iterativo incremental (PRESSMAN, 1995).

Neste trabalho adota-se o modelo iterativo incremental, no qual, segundo Quatrany (2001), o desenvolvimento se dá como uma série de iterações que evoluem para o sistema final. Cada iteração consiste de um ou mais dos seguintes componentes de processo: modelagem de negócios; requisitos; análise; design; implementação; teste; e distribuição.

Este modelo é considerado iterativo porque permite a possibilidade de voltar nas decisões e corrigir erros anteriormente não percebidos. Assim várias iterações são feitas em cada ciclo, até que se atinja um resultado satisfatório. Também é considerado incremental porque permite a adequação de novos recursos ou novas idéias ao sistema.

Neste tipo de modelo riscos técnicos são estimados e têm sua prioridade avaliada no estágio inicial do ciclo de vida, sendo revistos durante o desenvolvimento de cada iteração. Assim garante-se que riscos maiores sejam tratados antes, o que minimiza os riscos totais do sistema (QUATRANY, 2001). Tanto Bezerra (2002) como Larman (2000) argumentam que este método diminui os riscos dos projetos. Porém destaca-se a afirmação de Larman (2000, p. 44) que salienta que neste modelo “a complexidade nunca se torna incontrolável..., porque a implementação ocorre rapidamente para um pequeno subconjunto do sistema”.

4.4.3 Linguagem de Modelagem Unificada - UML

Para se modelar um sistema é necessário utilizar uma notação. Uma linguagem de modelagem possui vocabulário e regras voltados para a representação conceitual e física de um sistema. A linguagem adotada para representar os modelos desta pesquisa foi a Linguagem de Modelagem Unificada (*Unified Modeling Language* - UML). Assim, é fundamental descrever seus fundamentos e notações.

Um dos fundamentos desta linguagem é sua representação visual, sobretudo diagramática, de um problema. Este fundamento baseia-se no fato de que “conjuntos complexos de dados, quando graficamente visualizados, apresentam muito mais informações ao leitor do que os próprios dados brutos” (BOOCH; JACOBSON, 2000). Assim, segundo Booch e Jacobson (2000, p. 12-15), a UML é uma abstração gráfica para visualizar, especificar, construir e documentar sistemas de software complexos, e “é perfeitamente utilizada em processos orientado a casos de

usos, centrado na arquitetura, iterativo e incremental".

Outro aspecto fundamental é o fato desta linguagem ser utilizada para representar múltiplas visões de um mesmo problema, facilitanto assim a percepção de imperfeições no modelo e iterações para a melhora do mesmo. Assim no desenvolvimento de programas computacionais, para desenvolver sistemas complexos, o projetista precisa abstrair diferentes visões do sistema, montar modelos usando notações precisas, verificar que os modelos satisfaçam as exigências do sistema e acrescentar, gradativamente, detalhes para transformar os modelos em uma implementação (SANTOS, 2002).

A UML representa a unificação das notações Booch, OMY e Objectory, bem como as melhores idéias de uma quantidade de outros teóricos de metodologia em objeto. Ela oferece um padrão de facto no domínio de análise e design baseado em objeto, apoiada em uma ampla base de experiência de usuário. Além disso a UML, segundo Bezerra (2002, p. 14), é "independente tanto de linguagem de programação quanto de processos de desenvolvimento", sendo assim um fator importante para a sua utilização.

A UML divide-se em três blocos de construção: os itens; os relacionamentos; e os diagramas. Os itens são abstrações identificadas como cidadãos de primeira classe em um modelo; os relacionamentos reúnem esses itens; e os diagramas agrupam coleções relevantes de itens (BOOCH; JACOBSON, 2000).

Neste trabalho serão abordados apenas itens, relacionamentos e diagramas, que são utilizados na implementação do projeto nos capítulos vindouros. Assim, a seguir, apresenta-se o conceitos de classes, casos de uso, ator, interação, e os diagramas da UML.

4.4.3.1 Classes

As classes são descrições de atributos e métodos de um conjunto de objetos. Graficamente, as classes são representadas por retângulos, geralmente incluindo seu nome, atributos e métodos (ou operações) conforme mostra a figura 4.2.

A classe apresentada na figura anterior é uma representação genérica, pois uma classe pode ser diferenciada pela sua atuação. Por exemplo, uma classe utilizada para criar uma interface com o usuário será uma classe de interface, uma classe que representa ações do sistema é denominada classe controle e uma classe que representa uma tabela de um banco de dados

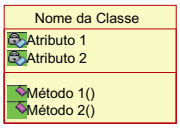

Figura 4.2: Representação de uma classe

será uma classe persistente denominada entidade. As representações de classes por sua atuação são denominadas “esteriótipos”. A figura 4.3 representa os esteriótipos das classes interface, controle e entidade.

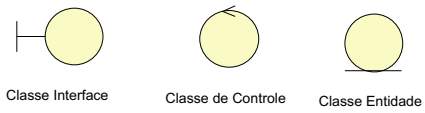

Figura 4.3: Representação dos esteriótipos das classes interface, controle e entidade

Uma classe Interface descreve o comportamento externamente visível de um elemento, ou seja o que um usuário ou componente consegue visualizar do sistema que esta sendo modelado. A classe de controle representa a realização das opções disponíveis na classe de interface e por fim a classe entidade representa um elemento persistente que pode ser caracterizado por um documento em papel, uma tabela em um banco de dados ou mesmo um arquivo digital.

4.4.3.2 Casos de uso

Conforme Booch e Jacobson (2000), um caso de uso (*use case*) é a descrição de um conjunto de seqüência de ações realizadas pelo sistema que proporciona resultados observáveis e de valor para um determinado ator. Um caso de uso é utilizado para estruturar o comportamento de itens em um modelo. A figura 4.4 apresenta sua representação gráfica.

Figura 4.4: Representação gráfica de um caso de uso

4.4.3.3 Ator

Existe ainda a representação dos atores do sistema. Segundo Larman (2000), o ator é uma entidade externa ao sistema que estimula o sistema com eventos de entrada ou recebe algo dele, podendo representar uma pessoa ou outro sistema que interage com o projeto que esta sendo desenvolvido. Ele corresponde ao que não se criará/implementará no sistema, na etapa de implementação. Em outras palavras, um usuário chamado candidato não será implementado pelo programador, pois ele já existe e é apenas um ator que interage com o sistema. Sua representação é apresentada na figura 4.5.

Figura 4.5: Representação gráfica de um ator

4.4.3.4 Interação

Segundo Booch e Jacobson (2000), a interação representa as mensagens trocadas entre um conjunto de objetos de determinado contexto para a realização de propósitos específicos. As interações envolvem mensagens, seqüências de ações e ligações. A representação das interações é apresentada na figura 4.6.

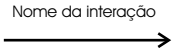

Figura 4.6: Representação gráfica de uma interação

4.4.3.5 Diagramas da UML

A representação gráfica de um conjunto de elementos, denomina-se diagrama. Geralmente eles são representados como gráficos de vértices e arcos, desenhadas para permitir a visualização de um sistema sob diferentes perspectivas. Nesse sentido, um diagrama constitui uma projeção de um determinado sistema. Dentre os diagramas da UML abordados nesta

tese estão os diagramas de casos de uso, atividade, classes participantes, seqüências, e estados (BOOCH; JACOBSON, 2000).

Diagrama de caso de uso exibe um conjunto de casos de uso, atores e seus relacionamentos. Diagrama de caso de uso abrangem a visão estática de uso do sistema. Esses diagramas são importantes principalmente para a organização e a modelagem de comportamentos do sistema. Um exemplo deste diagrama é apresentado na figura 4.7.

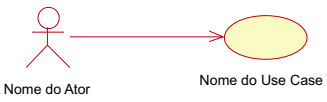

Figura 4.7: Diagrama de caso de uso

Diagrama de atividades é um tipo especial de diagrama de gráfico de estado, exibindo o fluxo de uma atividade para outra no sistema. Um exemplo deste diagrama é apresentado na figura 4.8.

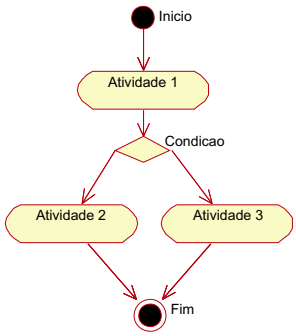

Figura 4.8: Diagrama de atividades

Diagrama de classes participantes exibe um conjunto de classes, interfaces e colobora-ções, bem como seus relacionamentos. Um exemplo deste diagrama é apresentado na figura 4.9.

O diagrama de seqüência corresponde a um diagrama que representa uma interação entre um conjunto de objetos ou classes e seus relacionamentos, incluindo as mensagens que podem ser trocadas entre eles. O diagrama de seqüência dá ênfase a ordenação dos tempos das mensagens trocadas entre classes ou objetos. Um exemplo deste diagrama é apresentado na figura

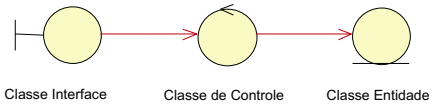

Figura 4.9: Diagrama de classes participantes

4.10.

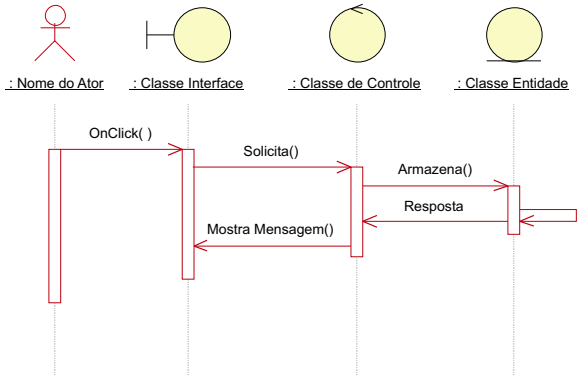

Figura 4.10: Diagrama de seqüência

Diagrama de gráficos de estados (Diagrama de estados) exibe uma máquina de estados, formada por estados, transições, eventos e atividades. O diagrama de gráfico de estados abrange a visão dinâmica do sistema. Um exemplo deste diagrama é apresentado na figura 4.11.

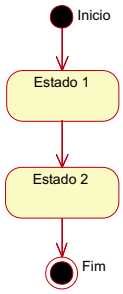

Figura 4.11: Diagrama de estados

4.4.4 Processo Unificado da Rational - RUP

Um processo é um conjunto de passos parcialmente ordenados com a intenção de atingir uma meta. Na engenharia de software, sua meta é entregar, de maneira eficiente e previsível, um produto de software capaz de atender as necessidades do negócio (BOOCH; JACOBSON, 2000). Segundo Bezerra (2002) o Processo Unificado da Rational (*Rational Unified Process* - RUP) é o principal representante da abordagem de desenvolvimento iterativo incremental, e é patenteado pela empresa Rational Software Corporation. Além desta abordagem ele contempla a orientação a objeto e é um modelo que traz as melhores técnicas do desenvolvimento moderno de programas de computador, focando a criação de uma arquitetura robusta, análise de risco e utilização de casos de uso para o desenvolvimento (KRUCHTEN, 2000). O Processo Unificado da Rational, consiste em uma abordagem de um ciclo de vida, especialmente adequada a UML (*Unified Markup Language*).

Segundo Rational... (2003), a estrutura de projeto do RUP envolve duas dimensões, a saber: estática, que denota as atividades a serem abordadas em cada fase; e dinâmica, que representa as fases no tempo e suas iterações. Sua representação gráfica é apresentada na figura 4.12.

A dimensão estática está subdividida nas seguintes atividades:

- Modelagem de negócio
  - é a identificação de capacidades do sistema e necessidades do usuário;
  - desenha-se o modelo de negócio.
- Requisitos
  - são levantadas as exigências funcionais e não funcionais do sistema;
  - definem-se os requisitos de funcionamento do programa e as atribuições do cliente.
- Análise e Design
  - nesta atividade é descrito como o sistema será realizado na implementação;
  - transforma-se os requisitos do sistema em um sistema propriamente dito.
- Implementação

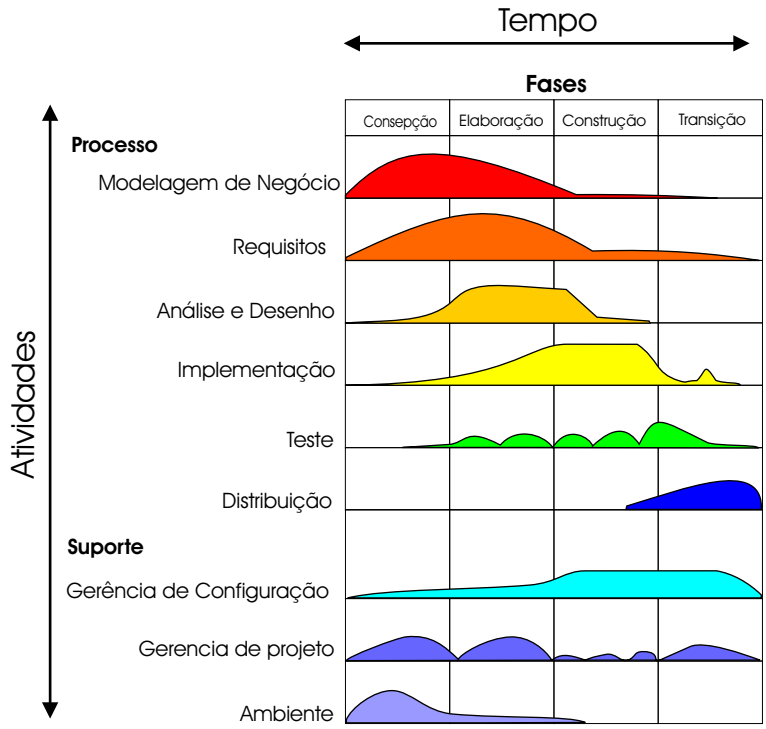

Figura 4.12: Metodologia RUP (adaptada de Rational... (2003))

  - é a programação, escrita do código;
  - codificam-se as especificações levantadas, transformando-as em um sistema executável.

- Testes
  - consiste em testar o sistema, garantindo o seu funcionamento ao usuário final.
- Distribuição
  - é a entrega do sistema e treinamento de usuários.
- Gerencia de configuração
  - controla as alterações ocorridas durante todo o projeto do programa de computador.
- Gerencia de projeto

  - procura garantir o sucesso do produto atendendo as necessidades levantadas, gerenciando os riscos do projeto.

- Ambiente

  - configura uma organização para ajustar o tempo de desenvolvimento do projeto, descrevendo as atividades necessárias para tal.

Segundo Quatrany (2001, p. 6), a dimensão dinâmica está subdividida nas seguintes fases:

- Concepção

  - Nesta fase existe a modelagem e a decisão de como será o projeto, visto que algo é necessário para apresentar ao cliente. Nesta etapa são revistas as regras de negócios, ou seja, os requisitos que o programa deve abordar para resolver o problema de um cliente, por exemplo. Uma fase de concepção adequada estabelece as exigências de alto nível para um sistema desejável e possível, tanto tecnológica quanto sociologicamente. Uma fase de Concepção inadequada leva a sistemas tão indesejáveis, caros, impossíveis e maus definidos que provavelmente nunca serão terminados ou usados.

- Elaboração

  - Depois de aprovado o projeto pelo cliente, começa a elaboração, verificando a fundo as necessidades do cliente e adaptando o sistema a elas. As regras de negócios são alteradas se necessário e começa aqui a criação de modelos de negócio para melhor visualização dos problemas abordados pelas regras.

- Construção

  - O RUP utiliza-se de um modelo chamado de “Modelo Iterativo e Incremental”. É importante dizer que este modelo é aplicado desde a elaboração do projeto até a fase de testes do sistema.

- Transição

– Nesta fase o programa desenvolvido é mostrado ao usuário que o requisitou para utiliza-lo e testa-lo a fim de descobrir se ele satisfaz as exigências e descobrir bugs que não foram encontrados na fase de testes, ou fazer modificações para torna-lo mais satisfatório.

4.4.5 Modelagem de negócios

A modelagem de negócios é uma técnica para modelar os processos envolvidos, determinando formas de expressar as suas atividades e seus comportamentos colaborativos. Ela não implica em mudanças nos processos e sim em uma técnica para visualizá-los e documentá-los de forma a identificar os riscos, cabendo ao analista tomar as decisões pertinentes às alterações, quando houver necessidade.

Neste contexto a UML pode ser usada para especificar, visualizar, construir e documentar modelos de negócios e associá-los a sistemas computacionais. Segundo Business... (2003), ela estabelece meios de encontrar problemas, procurar soluções e melhorar sistemas através de uma linguagem de modelagem facilmente entendida e auto-intuitiva. Wilcox e Gurau (2003) destacam que a comunicação entre os analistas de sistema, de negócio e outros membros da equipe de projetos melhoram consideravelmente sua comunicação e entendimento, com o uso da UML como linguagem padrão de modelagem. Apesar de existirem abordagens específicas para a implementação de modelos de negócio com UML, com a feita por SALM (2003), a linguagem padrão será utilizada nesta abordagem.

Com respeito a metodologia a ser utilizada no levantamento destes modelos, optou-se pela RUP. Segundo Booch e Jacobson (2000), a metodologia RUP aborda a modelagem de negócio, o levantamento de requisitos a análise do problema em questão, além de outras atividades. Neste trabalho, para se levantar os modelos desejados, se utilizará a as fases de concepção e elaboração da RUP de forma iterativa incremental.

Assim a fase de concepção envolve o levantamento dos requisitos e a especificação do caso de uso, que abrange a determinação dos: objetivos; pré-condições; iniciador; fluxos de atividades principais, alternativas e de exceção; pós-condições; e atores envolvidos. Esta fase envolve ainda a construção dos diagramas de caso de uso, que descreve o contexto do negócio, e o de atividades, que descreve o comportamento em um negócio ou os seus fluxos.

A fase de elaboração envolve a construção dos diagramas de diagramas classes participantes, seqüência e de estados. O diagrama de classe descreve uma estrutura estática do negócio; o diagrama de seqüência descreve as interações dinâmicas entre os funcionários(atores) e o que eles estão manipulando, desta forma demonstra de que modo o comportamento descrito nas atividades esta se concretizando; e o diagrama de estado, que permite uma análise dos estados de espera do sistema.

4.4.6 Modelagem utilizada neste trabalho

A modelagem a ser utilizada neste trabalho envolve, em momentos diferentes, a apresentação de descrições textuais, visuais ou matemáticas, de forma a representar uma situação ou proposta.

Nos capítulos 5, 6 e 7, optou-se por uma descrição majoritariamente textual sobre os processos apresentados. Entretanto, estas descrições estão embasadas nas modelagens de negócios modeladas nos apêndices A, B e C, respectivamente. Já no capítulo 8, optou-se por descrever a proposta, ou modelo, através de descrição textual e matemática.

Através do uso desta metodologia busca-se descrever as propostas de forma a possibilitar uma inferência sobre sua validade.

Capítulo 5

Modelo de avaliação somativa à distância

Um modelo de avaliação somativa à distância deve satisfazer os principais conceitos abordados na literatura especializada, apresentados na seção 2.2, do capítulo 2. Analisando-os, percebe-se que um concurso para contratação de mão de obra, que constitui-se em umas das modalidades de avaliação somativa que é aplicada em vários lugares simultaneamente, é um de seus exemplos mais completos. Outros modelos de avaliação somativa podem ser obtidos pela sua simplificação.

Assim, o modelo de avaliação somativa à distância apresentado neste trabalho tem como base um concurso com o objetivo de certificar e classificar candidatos, modalidade de avaliação em que o autor tem experiência em participação como elaborador de questões, coordenador de aplicação e coordenação geral.

O modelo formal é apresentado no apêndice A, onde adota-se a representação através da *Unified Modeling Language* e a metodologia *Rational Unified Process*, detalhadas na seção 4.4, do capítulo 4.

Neste capítulo, com o objetivo de facilitar o entendimento, o modelo proposto é descrito de forma textual e simplificada. Entretanto, deve-se ter em mente que a descrição textual apresentada deverá manter coerência e até mesmo vocábulos característicos da modelagem formal para manter a proposta coesa.

Inicialmente, descreve-se o processo como um todo, seção 5.1, passando à exposição de cada fase individual, a partir da fase de definições iniciais, seção 5.2, passando pelas fases de elaboração das questões a serem utiizadas no instrumento de avaliação, item5.3, de inscrição

dos candidatos ao processo, seção 5.4, de aplicação do instrumento de avaliação, seção 5.5, e da fase de correção e divulgação dos resultados, seção 5.6, finalizando com uma conclusão apresentada na seção 5.7.

5.1 Fases do processo

O primeiro passo para explicar o modelo é identificar seus principais processos, o que é detalhado na seção A.3, do apêndice A.

Este processos ou fases são denominados casos de uso para efeito da metodologia adotada. Assim, o caso de uso geral, envolvendo todos os casos de uso do sistema, é apresentado na figura 5.1, onde os atores foram suprimidos para facilitar a visualização.

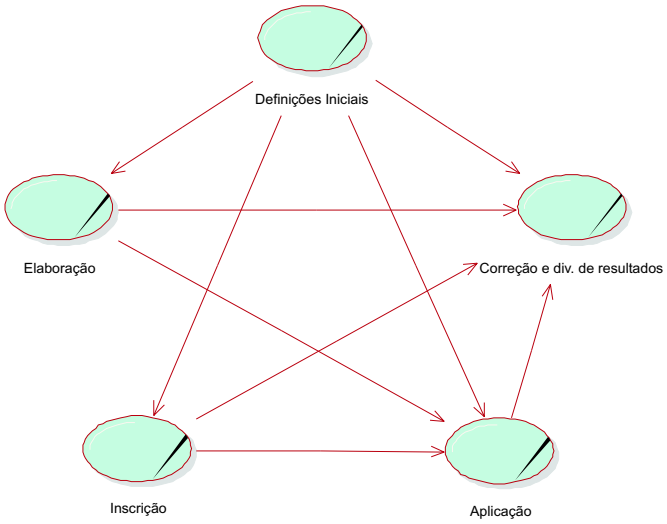

Figura 5.1: Diagrama do caso de uso da avaliação somativa à distância

O diagrama exposto nesta figura revela as fases do processo de avaliação modelado e suas inter-relações. Por ora é sufuciente ter contado com a denominação das fases, definições iniciais, elaboração, inscrição, aplicação e cooreção e divulgação dos resultado, pois elas são detalhados na seqüência deste documento.

5.2 Definições iniciais

Neste item descreve-se a fase de definições iniciais, cujo objetivo é definir as regras para o processo de avaliação e publicá-las. Para atingir o objetivo desta fase é necessário executar as atividades elencadas no diagrama de atividades principais apresentado na figura 5.2, a saber: contratar o elaborador de edital; elaborar o edital; contratar o receptor de inscrição; contratar o coordenador do concurso; contratar a equipe de tratamento de recursos; contratar a equipe de tratamento de dados; e publicar edital.

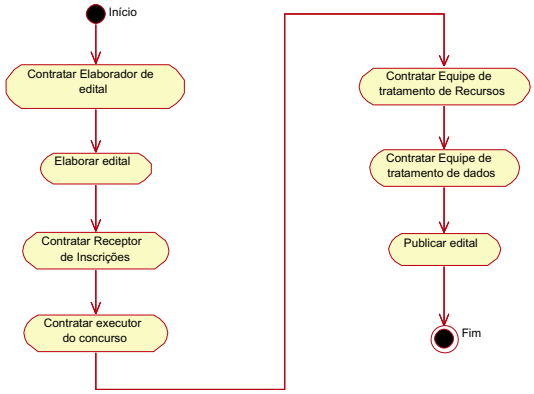

Figura 5.2: Diagrama de atividades de negociação e definições iniciais

Assim, inicialmente, a partir da necessidade de seleção de pessoal, o contratante deverá decidir por um elaborador de edital, que após selecionado deverá ser contratado. Ao final desta ação tem-se um contrato que deve ser armazenado. Note-se que o elaborador de edital é em geral uma pessoa física, um especialista que pode contar com cooperação de equipe própria ou outros atores.

A segunda atividade consiste na elaboração do edital. O elaborador do edital decide iniciar a elaboração, que resulta em várias versões produzidas até que o elaborador decida escolher uma versão final. A escolha da versão final implica em seu armazenamento.

Esta versão deverá contemplar, entre outros fatores, os objetivos da avaliação, seu conteúdo programático, a definição de um instrumento de avaliação viável de ser aplicado, procedimentos legais e definição do processo de recepção de inscrição (HAYDT, 2002).

Apesar desta atividade ser apresentada como realizada apenas pelo elaborador de edital pode haver interação com o contratante e com os atores ainda a serem contratados, como o

coordenador do concurso e o receptor de inscrição, para subsidiar a elaboração do mesmo.

A terceira e quarta atividades envolvem a contratação do receptor de inscrição e do coordenador do concurso, respectivamente. Estas atividades envolvem dois atores, pois a decisão de escolher o receptor de inscrição e o coordenador do concurso é do elaborador do edital, tendo em vista que estes atores podem ser necessários para a elaboração precisa do edital, porém a decisão de contratá-los é do contratante do concurso. Ao final de cada uma destas atividades a ação de contratar implica em um contrato que deve ser armazenado. Destaca-se que estes dois atores devem ser encarados como pessoas jurídicas, o primeiro responsável pela operacionalização de todo o concurso e o segundo responsável pela recepção de todas as inscrições.

A quinta e sexta atividades envolvem a contratação de equipe de tratamento de recurso e de tratamento de dados, respectivamente. Note que a esta altura o coordenador do concurso já foi contratado para a execução do mesmo, assim este ator decide escolher estas equipes e as contrata, o que resulta em contratos a serem armazenados.

A última atividade envolve a publicação do edital. A partir de sua versão final, o coordenador do concurso decide pela publicação. Assim, este é enviado para o ator imprensa, cujo contrato não é detalhado por ser considerado serviço público baseado em contrato por adesão.

Note-se que o diagrama apresentado na figura 5.2 exibe o fluxo principal de atividades, não sendo apresentado atividades alternativas ou de exceção. A modelagem formal desta fase é apresentada nos ítens A.7.1 e A.8.1, do apêndice A.

5.3 Elaboração

Com a publicação do edital, na fase de definições iniciais, pode-se dar início a fase de elaboração, que consiste em montar o instrumento de avaliação a ser aplicado aos candidatos, a partir da construção de um banco de questões. Como expresso no diagrama de atividades apresentado na figura 5.3, para se realizar esta fase é necessário: escolher o coordenador de elaboração; escolher os elaboradores; escolher os revisores; elaborar as questões; revisar as questões elaboradas; escolher as questões que comporão o instrumento de avaliação; e montar o instrumento de avaliação.

A primeira atividade a ser desempenhada nesta fase é a contratação do coordenador de elaboração. Para tal, o coordenador do concurso deverá procurar por um coordenador de ela-

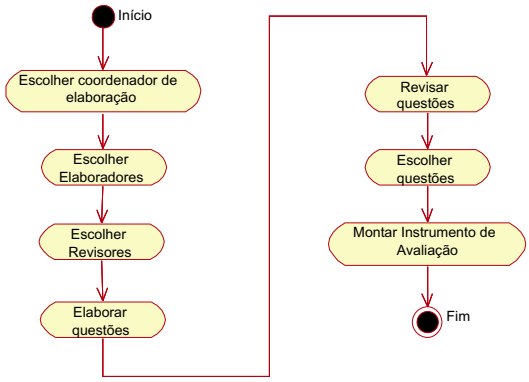

Figura 5.3: Diagrama de atividades da fase de elaboração

boração. Com os possíveis coordenadores de elaboração encontrados, deverá selecionar qual deles será contratado. A partir desta decisão o contrato é efetivado e armazenado.

Uma vez contratado, o coordenador de elaboração deverá buscar colaboradores do processo de elaboração do instrumento de avaliação, que envolvem elaboradores de questões e revisores. Os indivíduos selecionados deverão ser submetidos ao coordenador do concurso para contratação.

Neste ponto o coordenador da elaboração solicita aos elaboradores comporem um dado número de questões, com grau de dificuldade definido, sobre determinado assunto de seu domínio, constante do programa da avaliação.

Estas solicitações são armazenadas e os elaboradores ficam com a responsabilidade de compôr as questões de acordo com os parâmetros solicitados e submetê-las para armazenamento e revisão. Assim, após armazenadas, as questões devem ficar acessíveis apenas aos revisores específicos e ao coordenador de elaboração.

No momento seguinte entra em ação o revisor, que deverá avaliar a questão em si: se está correta; se corresponde ao assunto solicitado; e se apresenta o grau de dificuldade desejado. O resultado de sua revisão deverá ficar acessível apenas ao coordenador de elaboração.

Certamente a tarefa de maior responsabilidade é montar o instrumento de avaliação. A montagem deste envolve a escolha das questões elaboradas, que devem garantir que aqueles considerados aprovados sejam aptos a executar as tarefas exigidas para o cargo, o que é característico de processos de certificação. Por outro lado, as questões devem ser escolhidas de forma

a permitir um suficiente grau de discriminação entre os candidatos, em geral obtido pela equilibrada composição do grau de dificuldade das questões, característica de processos de seleção ou classificação (SMITH; RAGAN, 1999). Outro fator relevante é garantir equalização das questões em relação ao programa, tanto por questões de seleção como por razões legais (BAKER; MAYER, 1999).

Porém, as características mais difíceis de serem garantidas em relação ao instrumento de avaliação montado é sua validade e confiabilidade. A validade implica em garantir que se fosse aplicado uma avaliação com outro instrumento, ao mesmo público, sem intervenção formativa, o resultado obtido seria semelhante (HAYDT, 2002). Já a confiabilidade implica que, se fosse possível aplicar outra avaliação, com o mesmo instrumento, ao mesmo público, sem intervenção formativa, o resultado seria semelhante (SMITH; RAGAN, 1999). Como estas característica só poderiam ser provadas pela aplicação em pequena escala do instrumento em si, sua comprovação em um concurso para seleção de pessoal fica prejudicada, devendo-se valer da experiência do coordenador de elaboração para que o instrumento montado possua estas características.

Com estas necessidades em mente o coordenador da fase de elaboração pode selecionar as questões que comporão o instrumento de avaliação, que deverá ser armazenado com as respostas às questões objetivas aleatoriamente dispostas.

Cabe salientar que o sigilo é característica intrínseca a esta fase do processo de avaliação, o que não implica na ausência de rastreabilidade, que é fundamental para o caso de haver recurso contra as questões elaboradas.

A modelagem formal desta fase é apresentada nos ítens A.7.2 e A.8.2, do apêndice A.

5.4 Inscrição

Análogo ao que ocorre com a fase de elaboração, à fase de inscrição dos candidatos pode ser iniciada a partir da publicação do edital na fase de definições iniciais. Seu objetivo é promover e permitir inscrição por parte dos candidatos, resultando em uma base de dados de candidatos homologados com seus respectivos locais de avaliação. Para atingir este objetivo, deve-se executar as atividades elencadas no diagrama apresentado na figura 5.4, que são: contratar o homologador de inscrição; contratar campanha publicitária; receber inscrições do receptor de

inscrições; homologar inscrições; contratar locais de aplicação; divulgar homologação e local de aplicação aos candidatos.

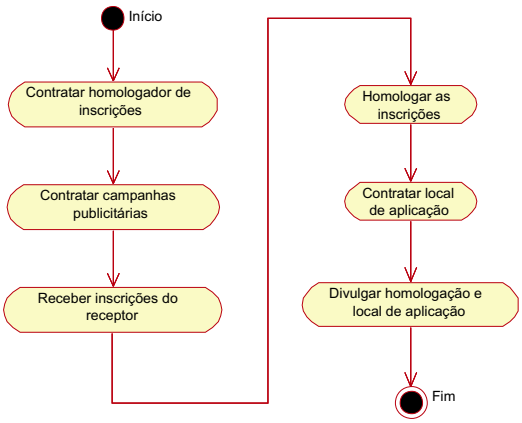

Figura 5.4: Diagrama de atividades da fase de inscrição

Vale ressaltar que a recepção das inscrições é feita pelo receptor de inscrição, ator contratado na fase de definições iniciais. Assim, como este ator representa um ente externo ao modelo, as atividades por ele executadas que não tenham interface direta com o processo detalhado.

A atividade que inicia a fase de inscrição é a contratação do homologador de inscrições, feita pelo coordenador do concurso. Quando este decide contratar um homologador de inscrições, é feita uma busca, seleção e contratação de um homologador, entre os disponíveis, o que implica em um documento a ser adequadamente armazenado.

Em seguida o coordenador pode iniciar a divulgação do concurso. Para tal, deve buscar, selecionar e contratar, uma equipe de publicidade, cuja campanha proposta seja escolhida dentre as apresentadas. A divulgação deverá encerrar quando findar o prazo de inscrição.

Em paralelo à campanha publicitária, como mencionado, o receptor de inscrição deverá estar recebendo inscrições baseado nas regras estabelecidas no edital. Ao finalizar o prazo para que potenciais candidatos realizem a inscrição, o homologador de inscrições deverá solicitar ao receptor de inscrições que as disponibilize. Ao fazê-lo, os documentos destas inscrições ficarão acessíveis para análise.

A partir deste ponto o homologador de inscrição poderá homologá-las. Para tal deverá analisar se as inscrições atendem aos requisitos de inscrição. A sua conclusão deverá ser adequadamente armazenada.

Conhecendo os dados dos homologados, o homologador de inscrições deve buscar e analisar os locais específicos de aplicação do instrumento de avaliação, restrito às localidades previstas no edital, e submetê-las ao coordenador do concurso para contratação.

Com a decisão sobre os locais de aplicação do instrumento de avaliação tomada e com acesso aos dados dos homologados, o homologador deve relacionar os candidatos com o local de aplicação.

Por fim, os candidatos devem ser informados da situação de sua inscrição, bem como o local e data precisos da realização da avaliação. Para fazê-lo, além de mensagem enviada aos candidatos, optou-se por uma confirmação de inscrição em data e locais pré-definidos no edital, onde o candidato deva pegar sua confirmação de inscrição. Esta confirmação pode ser feita via internet.

A modelagem formal da fase de inscrições é apresentada nos ítens A.7.3 e A.8.3, do apêndice A.

5.5 Aplicação

Com as fases de elaboração e inscrição concluídas pode-se dar início a fase de aplicação do instrumento de avaliação aos candidatos homologados, que é finalizada com as respostas dos candidatos ao instrumento de avaliação entregues ao coordenador de aplicação. Uma série de atividades tem de ser executadas para que se implemente esta fase, conforme expresso pelo diagrama apresentado na figura 5.5. Estas atividades são: contratar um coordenador da aplicação; contratar coordenadores locais e fiscais; capacitar da equipe de campo; transportar e distribuir os instrumentos de aplicação aos coordenadores de aplicação local; preparar locais de aplicação; transportar e distribuir os instrumentos de aplicação aos fiscais; controlar acesso dos candidatos; controlar aplicação do instrumento de avaliação; receber respostas ao instrumento de avaliação; conferir material de respostas entregues pelo candidato; preencher ata de aplicação; enviar respostas e atas ao coordenador local; conferir material entregue pelos fiscais; enviar respostas e atas ao coordenador de aplicação; e conferir material entregue pelos coordenadores locais.

A primeira atividade é exercida pelo coordenador do concurso e implica na contratação do ator coordenador de aplicação. Por sua vez, o coordenador desta fase faz um levantamento

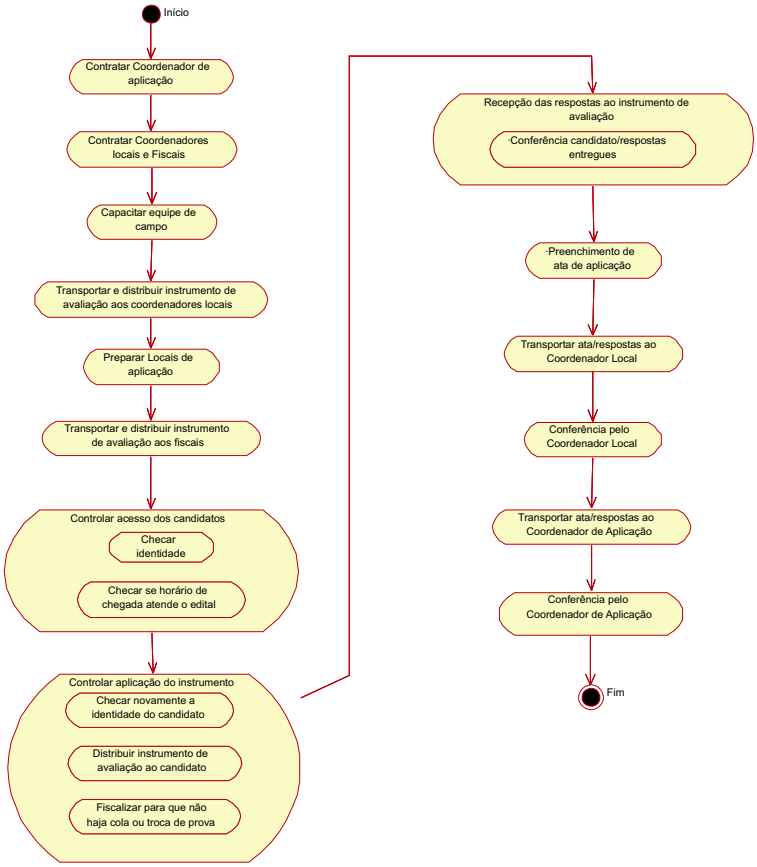

Figura 5.5: Diagrama de atividades da fase de aplicação

de possíveis coordenadores locais e fiscais, e os encaminha ao coordenador do concurso para contratação. Cabe destacar que estas ações podem iniciar antes do final das fases de inscrição e elaboração concluídas.

Após estas contratações deve ser realizada a capacitação da equipe de campo, que deverá ser iniciada pelo coordenador de aplicação. Esta atividade é fundamental para o correto andamento de um processo que exige tratamento igual em diferentes locais.

Próximo à data de realização da aplicação, o coordenador de aplicação deverá distribuir os instrumentos de aplicação aos coordenadores de aplicação local, tomando cuidados especiais quanto a segurança, como a utilização de identificação e lacres.

Antes de implementar a aplicação do instrumento, os coordenadores locais deverão preparar os locais para aplicação da avaliação com a ajuda dos fiscais. Esta atividade envolve principalmente a definição e indicação das posições dos candidatos.

Imediatamente antes da aplicação os coordenadores locais deverão distribuir os instrumentos de avaliação, ainda lacrados, aos fiscais que ficarão nas salas.

Alguns fiscais deverão controlar o acesso dos candidatos ao local de aplicação do instrumento de avaliação, o que envolve a confirmação da identidade via documento definido no edital e encaminhamento do candidato que chegou em tempo. A seguir, os fiscais de sala deverão confirmar os candidatos em suas posições e distribuir o instrumento de avaliação.

Esta seqüência de passos devem ser feitas de forma a garantir a simultaneidade e iguais condições de aplicação. A garantia de iguais condições aos candidatos envolve, além das atividades prévias de escolha do local, manutenção do sigilo do instrumento de avaliação e aplicação de igual instrumento a todos os candidatos que disputam uma mesma vaga, evitar que um candidato seja ajudado ou perturbado por outrém, ou que tenha acesso a algum tratamento ou informação que lhe confira vantagem (SMITH; RAGAN, 1999).

O fiscal deverá ainda receber as respostas ao instrumento de avaliação de cada candidato sob sua responsabilidade e conferir se o material corresponde ao documento de respostas. Ao final deverá preencher ata de aplicação e entregar o documento de respostas e ata ao coordenador local de aplicação.

O coordenador local de aplicação deverá conferir material entregue pelos fiscais e entregá-lo ao coordenador de aplicação, que deverá proceder nova conferência. Esta sucessiva conferência tem por objetivo detectar e corrigir, o mais rápido possível, qualquer irreguralidade que tenha ocorrido.

A modelagem formal da fase de definições iniciais é apresentada nos ítens A.7.4 e A.8.4, do apêndice A.

5.6 Correção e divulgação dos resultados

Após a etapa de aplicação pode-se proceder a fase de correção e divulgação dos resultados, cujo objetivo é certificar (aprovar) e classificar os candidatos segundo suas respostas ao instrumento de avaliação e vagas disponíveis. Para atingir este objetivo é necessário implementar as atividade apresentadas no diagrama da figura 5.6, que são: contratar coordenação de correção; contratar avaliadores de respostas; atribuir nota às respostas das questões objetivas; distribuir cópias das respostas às questões discursivas para dois avaliadores; receber avaliações

dadas para cada resposta das questões discursivas; atribuir nota às respostas das questões discursivas; atribuir nota para cada candidato; identificar e classificar candidatos aprovados; identificar candidatos classificados em relação às vagas disponíveis; divulgar resultado preliminar; e divulgar resultado final.

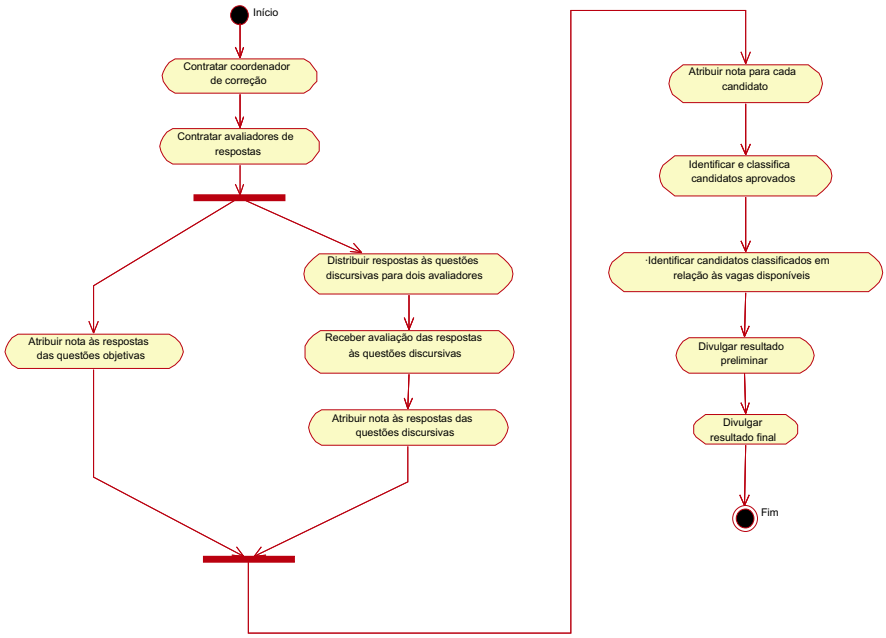

Figura 5.6: Diagrama de atividades da fase de correção e divulgação dos resultados

Inicialmente o coordenador do concurso deverá contratar o coordenador de correção, selecionado por ele, e avaliadores de respostas, levantados pelo coodenador de correção.

Em seguida o coordenador de correção iniciar o processo de atribuir nota às respostas dadas às questões objetivas, cujo gabarito já foi entregue junto com as questões, tarefa a ser realizada pela equipe de tratamento de dados.

A seguir o coordenador de correção deverá distribuir as respostas descritivas a pelo menos dois avaliadores, com supressão da identificação dos candidatos, para manter tratamento igual aos candidatos (HAYDT, 2002). Estes deverão atribuir sua nota as respostas das questões. Na seqüência é solicitado à equipe de tratamento de dados que atribui nota às questões subjetivas, tarefa feita pelo cálculo da média da nota dos avaliadores.

Com as notas de cada questão de cada candidato já atribuídas, a equipe de tratamento de dados deve atribuir nota aos candidatos, identificar os aprovados e classificá-los, dando destaque

aos classificados dentro do número de vagas disponíveis.

O cordenador desta fase pode então enviar para publicação o resultado preliminar e, após decorrido o prazo de recursos, o resultado final.

A modelagem formal da fase de definições iniciais é apresentada nos ítens A.7.5 e A.8.5, do apêndice A.

5.7 Conclusão

Neste capítulo descreveu-se um modelo de concurso como um processo de avaliação somativa à distância, atingindo-se, em conjunto com o apêndice A, o primeiro objetivo estabelecido neste trabalho.

Entretanto, deve-se ter em mente que existem outras avaliações que poderiam ser descritas, bem como outra formas de se implementar um concurso. Mesmo a modalidade a distância apresentada, pode ser considerada como uma avaliação descentralizada, visto que ela é implementada na presença de fiscais.

Porém, o entendimento deste processo é fundamental para se atingir outros objetivos propostos, de modelar o processo de avaliação à distância mediado por computador e com infraestrutura de chaves públicas, a serem descritos nos capítulos 6 e 7, respectivamente.

Capítulo 6

Modelo de avaliação somativa à distância mediada por computador

No capítulo 5 foi descrito um modelo de avaliação somativa à distância. No presente capítulo apresenta-se um modelo que engloba o anterior, alterando-o pela utilização de sistema computadorizado no processo.

A utilização de sistemas computadorizados na avaliação somativa a distância apresenta uma série de vantagens em relação a abordagem convencional, porém acarreta em vários desafios.

Desconsiderando o uso de sistemas computacionais apenas como ferramenta de apoio, sua primeira aplicação no processo de avaliação em si ocorre ao porta-se as denominadas provas convencionais para os computadores. Entre as vantagens técnicas deste procedimento, pode-se destacar a facilitação dos processos de: elaboração das questões, pelo incremento de comunicação entre os elaboradores e acesso à material de apoio e banco de questões; aplicação presencial, pela simplificação da logística de distribuição do material a ser aplicado, uma vez tendo-se a infra-estrutura; correção, principalmente quando as questões são objetivas (MCDONALD, 2002).

Outra vantagem envolve a possibilidade de geração automática de perguntas, a partir de uma base, variando seu grau de dificuldade de forma a cobrir adequadamente todo o espectro de conhecimentos a ser avaliado, culminando na possibilidade de avaliar o candidato frente a simulações de situações reais que irá enfrentar (BENNETT, 1998).

Quanto aos desafios, em primeiro lugar destaca-se a necessidade de comprovar que a

avaliação mediada por computador é equivalente a avaliação convencional, sobretudo no caso de uma avaliação aplicada parcialmente no formato convencional e parcialmente utilizando sistema computadorizado (MCDONALD, 2002).

Outro importante desafio diz respeito a garantir as características de segurança das informações. Apesar de ser necessária em todas as fases do processo, sua necessidade é mais visível na fase de aplicação da avaliação. No caso de haver necessidade de comprovar que todos tiveram acesso a mesma avaliação e de apresentar as respostas dos candidatos, a tecnologia computacional convencional pode ser manipulada, podendo ser questionada. Além disto, no caso de aplicação à distância são adicionados os desafios relativos a garantia de identidade do usuário, bem como do controle das variáveis envolvidas na aplicação da avaliação, de forma a garantir sua validade (KANUKA, 2001).

Apesar desta limitações, descreve-se na seqüência deste documento um modelo de avaliação somativa à distância mediada por computador. Esta descrição é iniciando pela apresentação da proposta em si, seção 6.1, passando a descrever o caso de uso controle de acesso, seção 6.1.1, e definições iniciais, seção 6.1.2, que são diretamente afetados por esta abordagem. A seguir apresenta-se alterações comuns ao casos de uso restantes, seção 6.1.3, e como são afetados individualmente os casos de uso de elaboração, inscrição, aplicação e correção e divulgação dos resultados, seções 6.1.4, 6.1.5, 6.1.6, e 6.1.7, respectivamente. Por fim é apresentado uma conclusão na seção 6.2. Como esta proposta envolve um sistema computacional, em alguns momentos, além da descrição do negócio, abordar-se-á detalhes específicos do sistema.

6.1 O modelo proposto

O modelo proposto é descrito de forma textual e simplificada, com o objetivo de facilitar o entendimento, porém esta descrição é baseada no modelo formal apresentado no apêndice B, onde o modelo é representado através da *Unified Modeling Language* e desenvolvido adotando-se a metodologia *Rational Unified Process*.

Com a mediação do computador, que envolve a utilização de um sistema computadorizado, foi acrescido ao diagrama de caso de uso geral apresentado na figura 5.1, página 93, o caso de uso controle de acesso. O novo diagrama de caso de uso geral é apresentado na figura 6.1, onde os atores, como no caso anterior, foram suprimidos para facilitar a visualização.

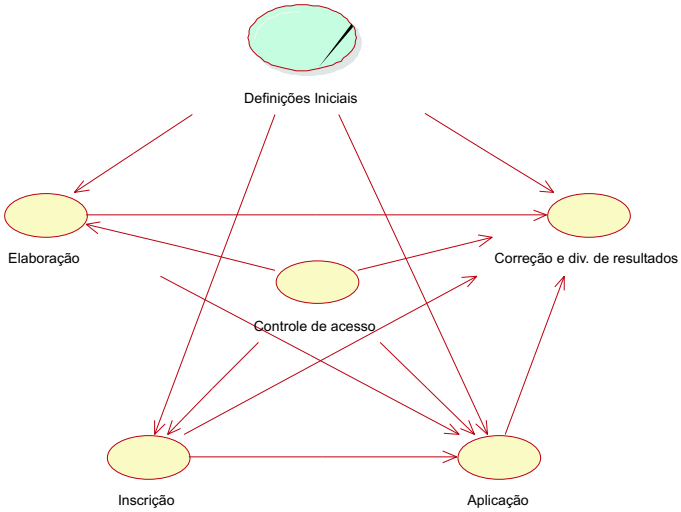

Figura 6.1: Diagrama do caso de uso da avaliação somativa à distância mediada por computador

O diagrama exibido nesta figura mostra as fases do processo modelado e suas inter-relações. Percebe-se que o acesso ao sistema é apresentado como um processo à parte, o que minimiza as alterações nos casos de uso já modelados. Este caso de uso é apresentado a seguir.

6.1.1 O acesso ao sistema

O caso de uso controle de acesso tem por objetivo permitir o acesso dos usuários ao sistema, dentro de suas funções no processo de avaliação. Para tal, os papéis devem ter sido previamente definidos e atribuídos aos usuários que da mesma forma já devem ter sido cadastrados no sistema. Para realizar tal função o sistema deverá executar as atividades elencadas no diagrama apresentado na figura 6.2, a saber: mostrar tela de entrada do sistema; solicitar conta/senha; conferir dados informados; verificar níveis de acesso; registrar acesso do usuário; e permitir o acesso ao sistema.

Inicialmente, o usuário deve preencher os campos disponibilizados na interface específica para conta e senha e submetê-las ao sistema. Este, por sua vez, verificará a conta e senha junto aos dados dos usuários. Caso os dados confiram, o sistema permitirá o acesso de acordo com o papel registrado obtido na base de dados e o armazenará o registro de acesso.

Caso o usuário seja candidato e esteja no momento de aplicação da avaliação, antes de permitir o acesso, o sistema solicitará que o candidato se sujeite a uma leitura biométrica que

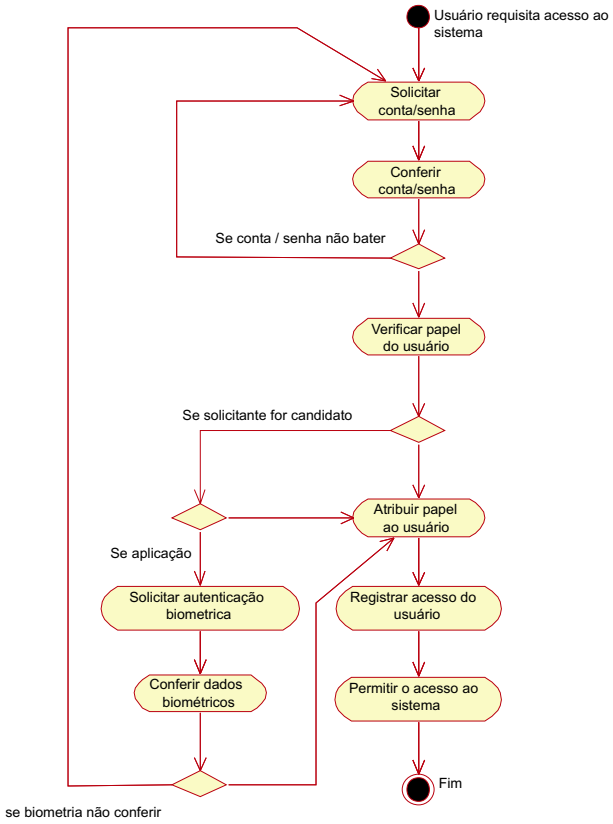

Figura 6.2: Diagrama de atividades do controle de acesso com computador

será comparada com os dados da inscrição do candidato. Neste caso, somente se esta última comparação conferir é que será concedido acesso ao sistema, com o correspondente registro.

A modelagem formal deste caso de uso é apresentada no apêndice B, seção B.4.

6.1.2 A fase de definições iniciais

O caso de uso definições iniciais, apesar de já ter sido descrito no capítulo anterior, merece uma abordagem a parte, pois é a partir dele que o sistema será disponibilizado, afetando todos os outros casos de uso.

As principais alterações em relação ao modelo manual são o acréscimo das atividades disponibilizar sistema e cadastrar usuários, conforme diagrama apresentado na figura 6.3, o que implica na adição do ator usuário, da interface sistema e das tabelas usuários e papéis no banco de dados.

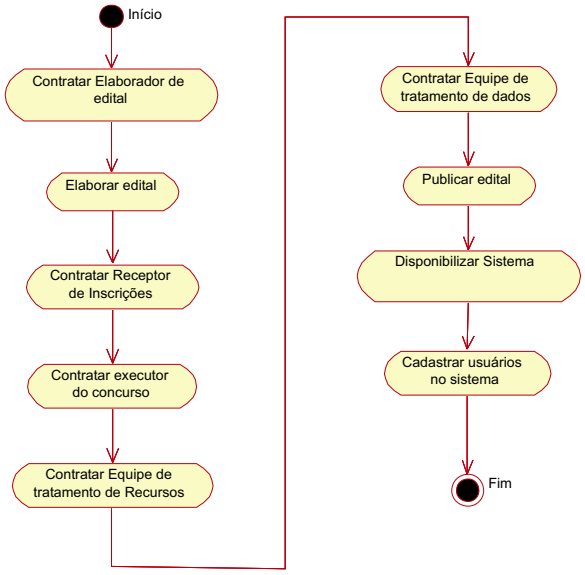

Figura 6.3: Diagrama de atividades do controle de acesso por computador

Observando este diagrama percebe-se que a realização das primeiras atividades permanecem as descritas na seção 5.2, do capítulo 5, entretanto as atividades de disponibilizar sistema e cadastrar usuários são novas.

A atividade de disponibilizar sistema demanda decisão do coordenador do concurso, cuja ordem deverá ser enviada à equipe de tratamento de dados.

Esta equipe deverá escolher disponibilizar, parametrizar e inicializar o sistema. Para parametrizar o sistema deve-se consultar o edital e os contratos já firmados de forma a ter os elementos de escolha para parametrização. Tendo estes elementos a mão, a equipe de tratamento de dados poderá definir papéis a serem desempenhados pelos atores do sistema, suas atribuições e prazos envolvidos. Ao final da execução desta atividade, o coordenador do concurso deve ser informado que o sistema foi disponibilizado.

Com o sistema disponível, a equipe de tratamento de dados deve cadastrar os usuários. Esta atividade implica em buscar informações dos contratados e criar conta e senha para os mesmos. Para tal o sistema deverá checar a existência prévia das contas e, em caso negativo, criá-las e enviar mensagem ao usuário informando sua conta e senha.

A partir deste ponto, ainda dentro da atividade cadastrar usuário, a equipe de tratamento de dados já pode atribuir-lhes papéis. Esta ação implica na consulta às entidades persistentes

usuários, contratos e papéis, para que possa-se decidir que papéis atribuir a cada usuário, que em seguida deverá ser informado através do envio de uma mensagem, finalizando a atividade de cadastramento.

Cabe salientar que esta última atividade descrita, de cadastrar usuários, será assumida como implícita à atividade de armazenar contrato nos próximos casos de uso. Desta forma, diminui-se as alterações em relação aos casos de uso já descritos no capítulo anterior.

A modelagem formal deste caso de uso é apresentada na seção B.5.1, do apêndice B.

6.1.3 Atividades comuns aos demais casos de uso

Os casos de usos já modelados neste capítulo contém atividades comuns aos demais casos de uso, permitindo sua análise sem grandes modificações em seus modelos.

Por exemplo, quando da atividade de armazenar contratos dos próximos casos de uso, conforme detalhado no final do caso de uso definições iniciais, seção 6.1.2, deve-se considerar que implicará no cadastramento dos contratados como usuários do sistema. Desta forma os contratados terão meios de acessar o sistema através do caso de uso de controle de acesso, conforme detalhado na seção 6.1.1.

Estas ações passam a ser assumidas como implícitas e transparentes aos modelos dos casos de uso elaboração, inscrição, aplicação e correção e divulgação dos resultados, apresentados nos capítulo 5.

Entretanto, a forma como estas atividades são implementadas é substancialmente afetada. Isto implica em alteração nas possibilidades de aplicação destes modelos, como apresentado a seguir.

6.1.4 A fase de elaboração

Os objetivos e as atividades do caso de uso elaboração permanecem os descritos na seção 5.3, do capítulo 5, apesar de sistema computadorizado. Entretanto, a forma e os resultados da execução destas atividades sofrem alteração.

Em relação a contratação do coordenador de elaboração, dos elaboradores de questões e dos revisores, a mudança ocorre no armazenamento do contrato, que, como descrito no na seção 6.1.3, implica no cadastramento dos contratados no sistema.

Com os interlocutores tendo acesso ao sistema o coordenador de elaboração pode solicitar a elaboração de questões. Como o acesso ao sistema é baseado no papel do usuário no processo de avaliação, as questões elaboradas são disponibilizadas para revisão e, posteriormente, liberadas para serem utilizadas no instrumento de avaliação.

Uma grande vantagem da utilização de um sistema nesta fase do processo e a agilidade da troca de informações entre o s interlocutores e a possibilidade de recrutar elaboradores e revisores com formação e que trabalhe especificamente no objeto, mesmo que distante fisicamente.

No que tange a montagem do instrumento de avaliação, como o processo é de certificação e classificação, deverá ser prévia ao início da aplicação. Entretanto, caso o objetivo da avaliação fosse somente a certificação, o instrumento de avaliação poderia ser montado durante a aplicação, através da seleção aleatória em um banco de questões, mantendo a representatividade dos assuntos e variando o grau de dificuldade. Ainda relativo ao potencial do uso desta tecnologia, destaca-se a possibilidade de simulação de situações onde o domínio avaliado seria necessário.

Certamente o grande desafio desta proposta é referente ao sigilo, característica intrínseca a esta fase do processo de avaliação.

A modelagem formal da fase de elaboração é apresentada no apêndice A, com sua especificação detalhada na seção A.7.2 e sua realização mostrada na seção A.8.2. As alterações advindas da adição do computador são modeladas na seção B.5.2, do apêndice B.

6.1.5 Alterações na fase de inscrição

A adição da adição do computador no processo de inscrição não modifica os objetivos e as atividades deste caso de uso, descritos na seção 5.4, do capítulo 5. Porém, a execução destas atividades e seus resultados sofrem alteração.

Cabe destacar que a recepção das inscrições é feita pelo receptor de inscrição, ator já contratado na fase de definições iniciais. Assim, como este ator representa um ente externo ao modelo, as atividades por ele executadas que não tenham interface direta com o processo detalhado.

A atividade de contratar o homologador de inscrições e a equipe de publicidade, feita pelo coordenador do concurso, análogo ao realizado no caso de uso elaboração, como descrito no na seção 6.1.3, implica no cadastramento dos contratados no sistema.

Como os usuários do sistema já estão cadastrados, a solicitação para disponibilização dos dados do inscritos, por parte do homologador de inscrição, bem como seu atendimento por parte do receptor de inscrição, ocorrerão via sistema. Entretanto, por tratar-se de um sistema computacional convencional os documentos físicos também deverão ficar acessíveis para análise.

A análise das inscrições ficará facilitada, uma vez que os dados necessários estarão acessíveis digitalmente. Com a definição dos dos homologados via sistema, a logística de levantamento das necessidades de espaço físico fica trivial.

Após a contratação dos locais de aplicação da avaliação nas localidades previstas no edital, o homologador deve relacionar cada candidato com um local de aplicação. Tarefa igualmente otimizada pelo sistema.

Quanto a informar os candidatos sobre sua situação de inscrição, bem como do local e data precisos da realização da avaliação, manteve-se a estratégia de, além de mensagem enviada aos candidatos, exigir que o mesmo confirme sua inscrição em data e locais pré-definidos no edital, onde o candidato deva pegar sua confirmação de inscrição. A mensagem disponibilizada para o candidato deverá conter conta e senha a ser utilizada tanto na confirmação via internet, como na aplicação do instrumento de avaliação. Deve ser observado que este processo não garante a identidade do inscrito, devendo esta atribuição ser exercida em outra fase.

A modelagem formal da fase de inscrição é apresentada no apêndice A, com sua especificação detalhada na seção A.7.3 e sua realização mostrada na seção A.8.3. As alterações advindas da adição do computador são modeladas na seção B.5.2, do apêndice B.

6.1.6 A fase de aplicação

Na fase de aplicação do instrumento de avaliação o uso de sistemas computacionais oferece os maiores benefícios e conseqüentemente, os desafios associados. Basicamente, os objetivos e tarefas a serem realizados permanecem os descritos na seção 5.5, do capítulo 5, porém as opções de sua operacionalização são ampliadas.

As contratações do coordenador de aplicação, dos coordenadores locais e fiscais, culminam com a disponibilização de suas contas e senhas.

A capacitação do pessoal de campo é a primeira atividade desta fase facilitada pelo uso do sistema, pois poderá envolver capacitação a distância no sentido de garantir procedimentos

padrões nos diferentes locais de aplicação.

A distribuição do instrumento de avaliação é uma tarefa crítica para este tipo de sistema. Como a segurança não pode ser garantida opta-se por disponibilizar o instrumento somente durante a aplicação do processo, mesmo que dificulte a adoção de estratégias de contingência por parte dos coordenadores locais e fiscais.

A preparação do locais de aplicação envolve principalmente a identificação geral dos locais, a disponibilização dos equipamentos e por em condições a execução de estratégias de contingência. Esta atividade envolve ainda a definição e indicação das posições individuais dos candidatos.

A atividade de recepção dos candidatos permanece inalterada no conceito. Ou seja, o acesso dos candidatos deverá ser controlados por fiscais que consultarão listas de candidatos, manual ou automaticamente, e confirmação sua identidade via documento definido no edital, encaminhando o candidato que chegou em tempo. A seguir, os fiscais de sala deverão confirmar a identidade dos candidatos em suas posições de avaliação, novamente com consulta a listas manuais ou digitais, pois conhecimento de conta e senha por parte do candidato não garante sua identidade.

A garantia de iguais condições aos candidatos envolve, além das atividades prévias de escolha do local, manutenção do sigilo do instrumento de avaliação e aplicação de igual instrumento a todos os candidatos que disputam uma mesma vaga, evitar que um candidato seja ajudado ou perturbado por outrém, ou que tenha acesso a algum tratamento ou informação que lhe confira vantagem (SMITH; RAGAN, 1999). Isto implica que, além da fiscalização visual dos fiscais, o sistema deverá impedir que outro processo seja executado na máquina de forma a favorecer ou prejudicar um candidato.

Certamente o instrumento de avaliação em si abre várias abordagens não viáveis de forma manuscrita, como a montagem instantânea do instrumento de avaliação e a apresentação de questões que são simulações das atividades a serem desempenhadas pelos candidatos.

Cada resposta dada pelo candidato deve ser instantaneamente armazenada na máquina local, no servidor local e, se as condições de infra-estrutura permitirem, no servidor central, de forma a possibilitar a substituição do equipamento cliente, ou troca de posição em caso de pane. Ao final da avaliação a mesma deverá ser enviada via sistema e seu resumo criptográfico, junto como o do instrumento de avaliação, devem ser impressos em duas vias e assinados pelo can-

didato e pelo fiscal. Desta forma garante-se ao candidato que suas respostas não serão trocadas e ao fiscal que o candidato submeteu-se ao instrumento de avaliação padrão. No caso de haver falha de comunicação, este processo deverá ser feito junto a um dispositivo de armazenamento do fiscal, para manter-se pelo menos duas cópias das respostas, contando a máquina local.

Ao final o fiscal deverá preencher e enviar a ata via sistema, além de imprimi-la, assiná-la e entregá-la com protocolação manual ao coordenador local de aplicação, junto com os documentos assinados pelos candidatos.

O coordenador local de aplicação deverá conferir material entregue pelos fiscais, tomar as providências necessários e reportar-se ao coordenador de aplicação, enviando os documentos assinados pelos candidatos e fiscais, adotando um processo de protocolação manual.

Como mencionado, esta sucessiva conferência tem por objetivo detectar e corrigir, o mais rápido possível, qualquer irreguralidade que tenha ocorrido.

A modelagem formal da fase de inscrição é apresentada no apêndice A, com sua especificação detalhada na seção A.7.4 e sua realização mostrada na seção A.8.4. As alterações advindas da adição do computador são modeladas na seção B.5.2, do apêndice B.

6.1.7 A fase de correção e divulgação dos resultados

Dado que as atividades apresentadas no diagrama mostrado na figura 5.6, página 102, sofrem apenas alterações de forma de execução, faz-se a seguir sua abordagem descritiva.

Como nas outras fases a atividade de contratação envolve a disponibilização de conta e senha para acesso ao sistema aos contratados, neste caso o coordenador de correção e avaliadores de respostas.

A atividade de atribuir nota às respostas dadas às questões objetivas, é automática ao sistema, pois restringe-se a comparação de dados disponíveis no sistema.

Quanto às respostas descritivas, o coordenador de correção, via sistema, as disponibilizará a pelo menos dois avaliadores, com supressão da identificação dos candidatos, para manter tratamento igual aos candidatos (HAYDT, 2002). Estes deverão atribuir sua nota as respostas das questões. Com o retorno dos avaliadores, o próprio sistema atribui nota às questões subjetivas, tarefa feita pelo cálculo da média da nota dos avaliadores. Por questão de segurança as avaliações feitas deverão ser entregues também no formato impresso, assinados e protocoladas.

Com as notas de cada questão de cada candidato já atribuídas, a equipe de tratamento de dados deve atribuir nota aos candidatos, identificar os aprovados e classificá-los, dando destaque aos classificados dentro do número de vagas disponíveis. Apesar destas informações estarem disponíveis no sistema, deve-se estabelecer procedimentos de verificação padrões para evitar a divulgação de resultados inconsistentes.

O cordenador desta fase pode então enviar para publicação o resultado preliminar e, após decorrido o prazo de recursos, o resultado final, ainda utilizando métodos convencionais de assinatura e protocolação.

A modelagem formal da fase de inscrição é apresentada no apêndice A, com sua especificação detalhada na seção A.7.5 e sua realização mostrada na seção A.8.5. As alterações advindas da adição do computador são modeladas na seção B.5.2, do apêndice B.

6.2 Conclusão

Neste capítulo descreveu-se um processo de avaliação somativa à distância mediado por computador, atingindo-se, em conjunto com o apêndice A, o segundo objetivo específico estabelecido neste trabalho.

O modelo apresentado utiliza um sistema computacional convencional, cuja identificação dos usuários se dá através de conta e senha. Apesar de ter adicionado uma série de potencialidades ao processo, este modelo apresenta dificuldades técnicas quanto aos dados transacionados e armazenados digitalmente.

Dentre estas destacam-se as dificuldades para manter o sigilo e a integridade, comprovar a autoria, inviabilizar o repúdio, comprovar a tempestividade, bem como a demanda por conectividade e limitações quanto aos locais de aplicação da avaliação.

Neste modelo computacional convencional, a dificuldade na manutenção do sigilo quando da transmissão de dados se dá em função da necessidade de partilhar uma senha (em realidade uma chave) de acesso entre os interlocutores. Esta operação é complexa e de difícil gerência e uma vez comprometida pode invalidar todo o processo. Já a manutenção do sigilo dos dados armazenados é mais simples de ser implementada, desde que os mesmos sejam armazenados de forma cifrada no banco de dados impossibilitando até mesmo o acesso por parte do administrador técnico do sistema. Porém, como a chave para cifrar os dados a serem armazenados é um

arquivo que vai transitar no sistema, o processo pode ser igualmente comprometido.

No que tange a autoria e integridade de um documento eletrônico, dado que para abri-lo é necessário conhecer a senha utilizada para cifrá-lo, aquele que tem direito de abrir o documento pode se passar pelo autor ou trocar seu conteúdo. Este fato compromete as características de integridade e identificação do autor do documento eletrônico no modelo computacional convencional.

Sendo assim, não se pode garantir a autoria e a integridade de um documento, pois existe a possibilidade de repúdio tanto da autoria como do envio ou recebimento do mesmo. No caso de envio e recebimento, mesmo que se utilize resumos dos documentos como recibos, a possibilidade de repúdio de autoria torna o processo pouco eficaz.

Igual raciocínio pode ser aplicado em relação a tempestividade dos documentos eletrônicos. Mesmo que se diponibilize um recibo que além do resumo do documento eletrônico possua informações de data e hora da transação, este poderá ser repudiado pelos interlocutores.

Outra limitação relevante diz respeito as necessidades técnicas dos módulos disponibilizados aos usuários, sobretudo o de aplicação do instrumento de avaliação, como a necessidade de acesso à conta, senha e dados biométricos. A solução “on-line” demanda uma rede com alta taxa de transferência de dados e alto grau de disponibilidade. Um módulo “off-line” é mais complexo em termos de desenvolvimento e implantação, pois exige a replicação de toda a base de dados dos usuários para cada computador cliente disponibilizado. Ou seja, ambas as soluções são de difícil implementação.

O estabelecimento de procedimentos manuais minoram algum dos problemas elencados. Dentre os procedimentos propostos destacam-se a impressão e a assinatura pelo candidato das respostas por ele apresentadas ao instrumento de avaliação e o respectivo recibo impresso e assinado pelo fiscal. Entretanto, este tipo de procedimento reduz amplamente os benefícios de um processo à distância mediado por computador, como tornar imprescindível a presença e atuação direta de um fiscal no local de avaliação.

Para contornar estes obstáculos é apresentada no capítulo 7 uma proposta de processo de avaliação somativa à distância mediado por computador com a utilização da tecnologia de infra-estrutura de chaves públicas.

Capítulo 7

Modelo da avaliação somativa à distância mediada por computador utilizando infra-estrutura de chaves públicas

No capítulo 6 foi apresentado um modelo de avaliação somativa à distância mediada por computador. No presente capítulo apresenta-se um modelo que engloba o anterior, alterando-o pela utilização de uma infra-estrutura de chaves públicas.

Como apresentado na revisão da literatura, especificamente na seção 2.4, e detalhado no capítulo 3, a utilização de uma infra-estrutura de chaves públicas pode garantir o sigilo, a integridade, a autoria, o não repúdio e a tempestividade de documentos eletrônicos, podendo solucionar as limitações do modelo anterior.

Para agregar tais características em um processo de avaliação mediado por computador pode-se tanto utilizar infra-estruturas já existentes como implementar uma infra-estrutura de chaves públicas específica para processos de avaliação, ou para um processo de avaliação em especial.

Em se valendo de infra-estruturas já disponíveis, e portanto genéricas, pode-se fazer uso de certificados já utilizados por parte dos atores para outros fins, dispensando a emissão de novos certificados. Neste caso deve-se, a partir do estabelecimento dos requisitos mínimos necessários para que os certificados sejam aceitos, definir a confiança nas autoridades certificadoras e nos classes de certificados emitidos.

Um exemplo hipotético para ilustrar esta aplicação é imaginar que a carteira de identidade venha a ser substituída por um cartão eletrônico com certificado digital. Neste caso, os certificados digitais tipo “identidade civil”, emitidos por cartórios “homologados” pelo “cartório brasil”, seriam aceitos como identidade de um candidato.

No caso em pauta, apesar de haver mudanças na forma de autenticação do usuário para entrar no sistema de avaliação, o princípio básico de se manter uma base de dados de usuários se mantém. Já no que tange a comunicação entre as partes, há de se estabelecer um protocolo específico para se garantir as características almejadas de segurança. Outro complicador é encontrar uma infra-estrutura de chaves públicas cuja política atenda aos requisitos de um processo de avaliação.

Por outro lado, a utilização de uma infra-estrutura de chaves públicas montada especificamente para processos de avaliação, ou para um processo de avaliação em especial, permite obter os direitos e dados do usuário do próprio certificado. Desta forma, é possível dispensar a base de dados de usuário de módulos do sistema, facilitando seu desenvolvimento e implementação. Este é o modelo de avaliação proposto neste capítulo, especificamente na seção 7.2.

Entretanto, como se trata de uma infra-estrutura de chaves públicas montada especificamente para processos de avaliação, ou para um processo de avaliação em especial, é preciso previamente definir as entidades que irão compor sua organização, suas responsabilidades e características. Todos estes elementos compõem uma política de certificação, a qual regulamentará esta infra-estrutura, denominada neste trabalho de política da ICP-Aval, cuja proposta é descrita na seção 7.1.

7.1 Política da infra-estrutura de chaves públicas aplicada ao processo de avaliação

A política proposta para a infra-estrutura de chaves públicas aplicada ao processo de avaliação somativa à distância se restringirá à atender as características essenciais ao processo de funcionamento da ICP-aval. As informações não constantes são referentes a especificações genéricas que não alteram o fluxo das transações existentes no modelo de funcionamento, como dados de contato, responsabilidades da AC e tarifas de serviço.

Assim, a organização dos componentes da ICP-Aval é abordada na seção 7.1.1, suas classes de certificados, na seção 7.1.2, os procedimentos para emissão e revogação dos mesmos, nas seções 7.1.3 e 7.1.4, e os procedimentos para auditoria desta infra-estrutura de chaves públicas, na seção 7.1.4.

7.1.1 Componentes da ICP-aval

A política da ICP-Aval requer a reunião de vários componentes para prover serviços de certificação digital, tempestividade e criptografia temporal. Com este objetivo a ICP-Aval define seis componentes da sua política. A seguir estes componentes são apresentados com seus direitos e responsabilidades:

1. Autoridades Certificadoras (AC):
    - proteger suas chaves privadas;
    - emitir e disponibilizar certificados e LCRs, atendendo às regras estabelecidas na política da ICP-aval
    - prover meios que tornem possível processos de auditoria nas suas operações.
2. Autoridades de Registro (AR):
    - receber requisições de emissão de certificados;
    - receber requisições de revogação de certificados;
    - analisar os dados contidos em requisições de emissão e revogação de certificados;
    - encaminhar requisições aprovadas para a AC responsável, de acordo com a classe e finalidade em que o certificado será enquadrado;
    - informar a rejeição da requisição ao solicitante;
    - prover meios que tornem possível processos de auditoria nas suas operações.
3. Autoridade de Datação (AD):
    - prover serviço de datação de documentos eletrônicos;
    - manter seus serviços disponíveis 24 horas por dia, 7 dias por semana;

- prover meios que tornem possível processos de auditoria nas suas operações.

4. Diretório Público (DP):

   - armazenar certificados e LCRs emitidos pelas ACs componentes da ICP-Aval;
   - disponibilizar mecanismos de busca apropriados que permitam aos usuários facilmente localizar e obter certificados e LCRs;
   - maximizar a disponibilidade e o desempenho no acesso aos documentos armazenados;
   - manter seus serviços disponíveis 24 horas por dia, 7 dias por semana.

5. Serviço de Criptografia Temporal (SCT):

   - prover mecanismos que possibilitem aos usuários determinar o tempo futuro em que uma informação cifrada poderá ser decifrada;
   - prover meios que tornem possível processos de auditoria nas suas operações;

6. Entidade Final (EF):

   - gerar requisições de emissão ou revogação de certificados obedecendo a regras previamente definidas;
   - fornecer documentação exigida perante a AR a fim de viabilizar a validação de uma determinada requisição;
   - responsabilizar-se pela segurança e uso da sua chave privada correspondente a um certificado emitido pela ICP-Aval;
   - validar as informações constantes no certificado emitido e só então utilizá-lo;
   - informar a AR competente eventual caso de discrepância dos dados contidos no certificado.

7.1.1.1 Autoridades Certificadoras

A política da ICP-Aval adota como modelo de confiança a estrutura hierárquica, sendo composta por três diferentes AC, classificada por seu nível hierárquico:

- ***AC Raiz:*** possui certificado auto-assinado e emite certificados para ACs Intermediárias. A responsabilidade pela criação da AC raiz compete ao coordenador do concurso, o qual possui a função de liderança dentro do processo de avaliação;

- ***ACs Intermediárias (ACIs):*** emitem e revogam certificados para ACs subordinadas. Cada AC intermediária é responsável por ACs subordinadas que emitem certificados enquadrados em uma determinada classe;

- ***ACs subordinadas (ACS):*** emitem apenas certificados para entidades finais. A sua atuação se restringe a apenas uma classe de certificado e ao atendimento de um processo específico dentro do concurso.

A organização destas ACs dentro da estrutura hierárquica é baseada na classes de certificados que a política da ICP-aval implementa.

O primeiro nível da hierarquia da política da ICP-aval é composta somente por uma AC, denominada AC-Raiz. Esta autoridade é criada pelo coordenador do concurso, que é o responsável pela chave privada desta AC.

O coordenador tem como obrigação a manutenção do sigilo da chave, através do uso de equipamentos criptográficos que incrementem a segurança e o gerenciamento de uso em operações de emissão de certificados LCRs.

Após a construção da AC do primeiro nível, o processo de criação das ACs Intermediárias para compor o segundo nível da hierarquia é iniciado. Este nível é composto por três autoridades: ACI-email, ACI-pessoal e ACI-servidor. Esta organização se baseia na classes a serem apresentadas na seção 7.1.2.

O administrador de cada AC intermediária é definida pelo coordenador. Este administrador é responsável por gerar o par de chaves da sua AC e encaminhar uma requisição auto-assinada para a AC-Raiz emitir o certificado.

Após a conferência e emissão do certificado das ACIs, estas podem emitir os certificados para as AC subordinadas, regidas pelas políticas definidas pelo coordenador do concurso.

A política de uma ACI não pode estar em desacordo com os critérios definidos na política da AC-Raiz, uma vez que esta última é quem emite o certificado da primeira. A política de cada ACI restringe a emissão de certificados à ACs subordinadas e a uma única classe. A restrição

da classe da ACS, é relacionada com a ACI, por exemplo a ACI-email gera apenas ACSs com a política restrita a emissão de certificados classe e-mail.

Toda ACI deve possuir ao menos uma ACS, pois a ICP deve disponibilizar pelo menos uma AC para cada classe. Entretanto a quantidade de ACS não está restrita, pois o número de ACs é definida pelo coordenador, conforme a necessidade para atendimento das regras do concurso.

O gerenciamento de uma ACS deve ser composto por administradores e operadores, uma vez que a demanda de requisições de certificados da ICP-aval é concentrada nestas ACs. Os administradores são os indivíduos definidos pelo coordenador do concurso que realizam as tarefas de maior responsabilidade na operação de uma AC, como a geração de chaves, gerenciamento dos operadores, instalação da AC, manutenção da chave privada; enquanto os operadores são responsáveis pela execução de tarefas rotineiras, como verificação das requisições.

Após a construção das ACSs a estrutura hierárquica da ICP-aval está completa. A figura 7.1 ilustra a organização das ACs para o processo de avaliação.

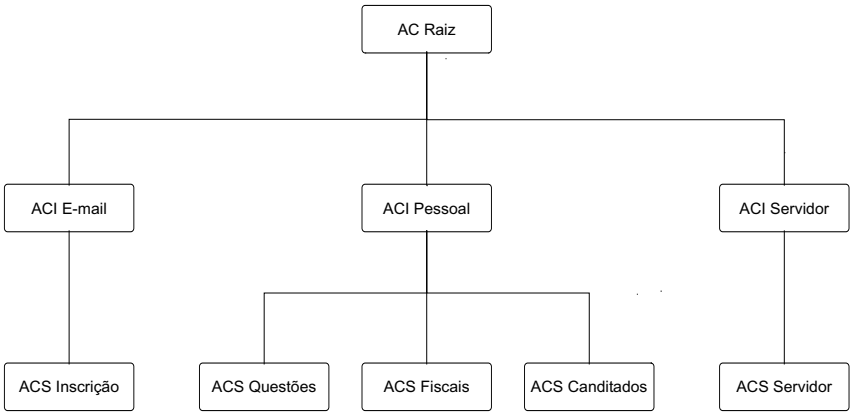

Figura 7.1: Estrutura hierárquica da ICP-aval

Quanto a operação das ACs regidas pela política da ICP-aval, a AC-raiz e as ACIs operam em off-line, com a finalidade de incrementar a segurança contra ataques de redes de comunicação de dados. A perfomance não é afetada devido ao fato destas ACs emitirem certificados somente para um número reduzido de ACs. Já a ACS devem ser mantidas on-line e disponíveis.

Esta descrição do processo de criação da estrutura hierárquica das ACs não mencionou a participação de um importante elemento, a Autoridade de Registro. Entretanto, processos que

envolvem emissão de certificados pelas ACs são feitos por meio desta entidade, conceituada a seguir.

7.1.1.2 Autoridades de Registro

A solicitação de certificados a uma AC é feita através de uma AR, ou seja, para solicitar um certificado a uma AC um usuário deverá requerê-lo a uma AR que a encaminhará. Estas requisições somente serão aceitas pelas ACs se procedentes de ARs com as quais mantenham relação de confiança.

O vínculo entre uma AR e a AC emissora do seu certificado é automático, pois, ao emitir o certificado de uma AR específica a AC tem certeza da veracidade dos dados constantes no certificado e portanto atribui crédito ao sujeito deste. A responsabilidade de criação destas entidades é do responsável pela AC para a qual prestará serviços.

No caso da vinculação não ser automática, é responsabilidade do administrador da AC criar a relação de confiança com uma ou mais ARs. Através destes relacionamentos, o administrador definirá quais ARs prestarão serviços para sua AC.

A AC-Raiz e todas as ACIs possuem apenas uma AR relacionada a elas, uma vez que são poucos os certificados que devem gerenciar. Já uma ACS pode definir várias ARs para trabalhar em conjunto. Um exemplo onde esta configuração é muito útil, é uma ACS, subordinada a uma ACI-pessoal, que emite certificados para os candidatos na fase de homologação de inscrições. Devido ao fato da demanda de emissão de certificados para homologação de candidatos ser muito grande em concursos de grande abrangência, a possibilidade da ACS possuir várias ARs é muito atrativa. Isto permite a AC prevenir possíveis sobrecargas em uma AR, adotar estratégica de alocação das ARs baseada na abrangência demográfica do concurso de modo a facilitar o acesso do usuário aos serviços prestados.

7.1.1.3 Autoridade de Datação

A política da ICP-aval contém pelo menos uma Autoridade de Datação (AD). A designação de uma ou mais Autoridades de Datação será feita pelo coordenador do concurso.

A AD tem como responsabilidade a datação confiável dos documentos eletrônicos utilizados no concurso, de forma prover uma âncora temporal. Devido a característica da AD trabalhar

através de recebimento de resumos criptográficos e devolução de recibos datados, esta autoridade pode ser uma entidade contratada ou implementada, desde que satisfaçam os requisitos definidos.

Se a AD for uma entidade externa, antes da contratação o coordenador deverá examinar e averiguar se as técnicas adotadas na implementação da entidade não fere a política e atende os requisitos de auditoria necessários ao concurso.

Entretanto, se a AD for uma entidade interna, além de atender os requisitos definidos, deve seguir os mesmos procedimentos adotados para criação de uma ACI, tornando-se uma entidade de nível 2.

7.1.1.4 Diretório Público

O diretório público (DP) é responsável pela manutenção de um repositório de certificados digitais emitidos pelas Autoridades Certificadoras. Além desta função a política da ICP-aval permite a inclusão do serviço OCSP *Online Certificate Status Protocol* (VIEGA; MESSIER; CHANDRA, 2002), que é um serviço de verificação do estado do certificado, por exemplo, revogado.

A política da ICP-aval exige a definição de pelo menos um diretório público, entretanto cada AC pode implementar seu próprio DP, compondo uma ICP de vários DPs.

Além da ICP poder ser constituída por vários diretórios públicos, uma AC também pode possuir vários DPs. Uma AC com vários DPs deve replicar o armazenamento dos seus certificados digitais em em cada um destes, cujos endereços constarão nas extensões do certificados.

Todos os DPs de ICP regida pela política da ICP-aval deve possuir autenticação realizada através da emissão do certificado pela ACI-servidor.

7.1.1.5 Serviço de Criptografia Temporal

Na política definida para a ICP-aval, a entidade que disponibiliza o Serviço de Criptografia Temporal (SCT), descrita na seção 3.3, deve atender os requisitos para ser utilizada na manutenção do sigilo do instrumento de avaliação até o momento de sua aplicação, evitando o acesso antecipado ao documento. Como no caso da AD, esta entidade pode ser externa à ICP.

7.1.2 Classes dos certificados

As classes dos certificados a serem utilizadas no concurso diferenciam os requisitos de confiança necessários para a emissão dos certificados enquadrados em cada classe e identificam as aplicações em que estes certificados poderão ser utilizados.

A política da ICP-Aval contempla três classes de certificado:

- ***Classe E-mail:*** utilizado na autenticação de contas de e-mail, de forma a garantir um processo eficaz para uma grande demanda de solicitação de inscrição;
- ***Classe Pessoal:*** utilizado na autenticação de indivíduos no sistema;
- ***Classe Servidor:*** utilizado na autenticação de equipamentos servidores.

A personalização dos certificados para adequação em cada uma das classes definidas é baseada nos procedimentos e informações adicionais que constarão no campo dos certificados. Estes procedimentos são de responsabilidades das autoridades certificadora e de registro. As seções a seguir detalham estas características.

7.1.2.1 Certificados Classe E-mail

Os certificados classe e-mail são os certificados que exigem menor grau de confiança no processo de autenticação. Este certificado apenas autentica a conta de e-mail, referindo-se a existência desta, e nunca em relação ao seu proprietário.

A emissão ocorre de forma automática, sem interferência manual do operador da AR ou da AC. Os processos de conferência de dados das requisições em ambas as entidades também é automatizado, incluindo a emissão do desafio e verificação de resposta da posse da conta de e-mail.

A identificação do usuário (DN - *distinguished name*) conterá, entre outros dados, o CPF do sujeito, a fim de impedir a emissão de certificados para um mesmo sujeito com endereços de e-mail diferentes.

Esta classe de certificado proporciona uma forma rápida de distribuição de certificados para os usuários, possibilitando seu uso no processo inicial de inscrição do concurso para posterior substituição por certificados da classe pessoal, quando da homologação da inscrição.

A validade dos certificados desta classe está compreendida entre a data de emissão do certificado e o prazo final para que o candidato busque sua homologação.

Como extensão necessária a esta classe de certificados, tem-se:

- *Dados do concurso:* Identificação do concurso que o usuário está se inscrevendo.

7.1.2.2 Certificados Classe Pessoal

Os certificados da classe pessoal autenticam o indivíduo, por isto exige um processo de identificação mais rigoroso. Este processo inclui apresentação de documentos a uma AR de confiança da AC que realizará a emissão do certificado.

Cada AR analisa os documentos que deverão ser apresentados de acordo com a política que a AC a qual irá submeter a requisição aprovada. Os documentos para identificação do sujeito na classe pessoal são:

- Cédula de Identidade ou Passaporte se estrangeiro;
- Cadastro de Pessoa de Física - CPF;
- Comprovante de residência;
- Autorização emitida por indivíduo responsável, participante do processo de avaliação, informando qual a papel do sujeito e dados do concurso.

Os certificados da classe pessoal são necessários para autenticarão dos usuários quando dos processos de avaliação. Todos os usuários deverão, obrigatoriamente, possuir um certificado da classe pessoal, inclusive os candidatos homologados.

O candidato do concurso deverá obter um certificado da classe pessoal quando ocorrer a homologação da sua inscrição, revogando desta maneira o certificado da classe e-mail que ele possuía. O certificado da classe pessoal lhe dará acesso ao sistema de avaliação, algo não atendido por um certificado da classe e-mail.

As extensões necessárias a esta classe de certificado são:

- *Dados do concurso:* Identificação do concurso que o usuário está se inscrevendo;
- *Dados sobre o papel:* Informações sobre a papel que o usuário terá dentro do concurso;

- *Dados biométricos:* Dados biométricos do candidato que deverão ser utilizados na aplicação;
- *Dados de escolha:* Dados das opções escolhidas pelo candidato quando da inscrição.

7.1.2.3 Certificados Classe Servidor

Os certificados desta classe permitem a autenticação de equipamentos servidores e a criação de canais de comunicação seguros, protegendo o sigilo e a integridade de informações envolvidas em uma comunicação entre usuários e servidores.

A autenticação de servidores permite que o usuário tenha certeza de que o sistema em que está conectado é de fato o sistema original e não uma fraude construída com objetivos ilícitos.

A criação de um canal seguro entre servidor e usuário ocorre através de recursos e protocolos criptográficos, tal como o protocolo *Secure Sockets Layer (SSL)*. As informações que trafegam dentro deste canal terão a sua confidencialidade e integridade asssegurada durante todo o seu trajeto.

As extensões que deverão estar presentes em um certificado enquadrado nesta classe são:

- *Dados do concurso:* Identificação do concurso que o usuário está se inscrevendo;
- *Dados sobre a revogação:* Papel do indivíduo que pode solicitar a revogação do certificado.

7.1.3 Procedimentos para emissão de certificados

O procedimento geral para solicitação de certificados para o concurso, comum a todas as classes, é constituído pelos seguintes passos:

1. geração de um par de chaves pública e privada;
2. geração de uma requisição de emissão de certificado;
3. envio desta requisição para a AR.

Após os procedimentos comuns a todas as classes de certificados, as etapas subseqüentes são específicas para cada uma das classes, de forma a prover a autenticação de acordo com o

nível de segurança exigido, assim os procedimentos para averiguação do sujeito são descritas individualmente para cada classe, como descrito a seguir.

7.1.3.1 Certificados Classe E-mail

A emissão dos certificados de e-mail é automática, ou seja, não existe a necessidade de intervenção de um operador da AR ou AC para sua aprovação. A autenticação consiste apenas na constatação da existência da conta de e-mail e da acessibilidade por parte do solicitante.

O solicitante envia sua requisição para AR, esta extrai os dados da requisição. A AR remete para o e-mail, constante na requisição, um desafio. Este desafio consiste em um dado, o qual o solicitante deverá informar na etapa seguinte para prosseguimento da solicitação, isto garante que o solicitante tem acesso a conta de e-mail para a qual se está requerendo certificado. Devido ao fato deste certificado autenticar apenas a conta de e-mail e não o sujeito, este procedimento é suficiente para autorizar ou não a emissão.

Se a resposta recebida pela AR for válida, esta assina a requisição como prova de sua aprovação e encaminha a requisição para a AC. A AC, por sua vez, valida a assinatura da AR, verifica se as extensões solicitadas na requisição são convergentes com sua política e emite o certificado, caso todos os requisitos sejam satisfeitos. Após emitido, o certificado é encaminhado ao DP e ao e-mail constante no certificado.

7.1.3.2 Certificados Classe Pessoal

A emissão de certificados classe pessoal exige uma maior interação do solicitante do certificado com a AR.

A AR, ao receber a requisição, encaminha um pedido ao solicitante, onde são listados os documentos que devem ser apresentados a AR para que esta possa dar prosseguimento no processo de emissão do certificado. A requisição somente será encaminhada para AC quando o solicitante apresentar a documentação exigida e somente no caso desta documentação satisfizer os requisitos estabelecidos, uma vez que cabe a AR validar estes documentos.

Se determinado na política, no momento em que o solicitante comparece perante a AR, será celebrado o firmamento das responsabilidades das partes envolvidas através de um contrato.

Em seqüência, cabe a AC apenas verificar a assinatura da AR, se o pedido está de acordo

com sua política e verificar as extensões da requisição. Se os dados da requisição forem convergentes com sua política, deverá emitir o certificado, que será encaminhado ao DP e a AR, que por sua vez grava o certificado no cartão do usuário.

No caso de candidatos homologados a o processo de emissão do certificado pela AC será automático, sendo validada apenas a assinatura da AR constante da requisição.

7.1.3.3 Certificados Classe Servidor

Os procedimentos necessários para emissão dos certificados da classe servidor são semelhantes ao da classe pessoal, a diferença consiste na necessidade de comprovação de documentos diferentes e nos direitos e deveres do contrato a ser firmado entre as partes.

Certificados servidores autenticam máquinas, porém a emissão daqueles devem associar pessoas responsáveis pela manutenção destas. Assim a documentação a ser apresentada na AR referem-se aos responsáveis pela administração da máquina.

7.1.4 Procedimentos para revogação de certificados

A regra geral para a permissão do pedido de revogação em uma ICP genérica está relacionada ao sujeito do certificado, porém ocorrem casos em que o sujeito do certificado não poderá controlar a revogação do próprio certificado, como definido na política da ICP-Aval.

O procedimento para pedido de revogação de certificado deve considerar as extensões dos certificados, onde estão especificados as pessoas autorizadas a realizar a solicitação. A política da ICP-Aval adota como procedimento padrão, a inclusão da informação do papel autorizado a solicitar a revogação do certificado em um campo de extensão. Como por exemplo, os certificados emitidos para os “elaboradores de questões” do concurso terão o pedido de revogação concedido somente ao “responsável pela elaboração da prova”, assim nem mesmo o próprio sujeito do certificado possui permissão para isto.

Porém existem algumas exceções a regra, por exemplo, a responsabilidade de pedido de revogação do certificado somente é imputada ao usuário descrito na extensão após a conferência das informações do certificado por parte do usuário, podendo este recusá-lo, devido a informações incorretas e solicitar a revogação deste. No caso de suspeita do comprometimento da chave privada, o usuário deverá solicitar a pessoa indicada em seu certificado com poder de revogação

a revogação do mesmo.

As especificações de cada classe de certificado são descritas nas próximas seções.

7.1.4.1 Certificados Classe E-mail

Pedidos de revogação de certificados de e-mail somente poderão ser feitos pelos responsáveis pela coordenação das inscrições do concurso. Desta forma, no campo de extensão constará o papel do sujeito na organização do concurso.

A requisição é feita e encaminhada para a AR, esta verifica se o autor do pedido é um usuário com o papel correspondente. Esta verificação é realizada através da conferência da assinatura do pedido, a qual deve ter sido utilizado o certificado digital emitido pela ICP-Aval.

Caso confira, a AR encaminha o pedido para AC emitir a lista de certificados revogados. A AC emite a lista de certificado de acordo com a periodicidade constante ou data pré-definidas.

Para casos de usuários constatarem erros nas informações do certificado, a forma para revogação do mesmo é através da solicitação de outro certificado. A emissão de outro certificado com as mesmas informações, implica na revogação automática do certificado anterior, com emissão de um aviso endereçado ao e-mail constante naquele certificado, e a emissão de um novo.

7.1.4.2 Certificados Classe Pessoal

Os certificados de classe pessoal poderão ser revogados pelo usuário que possuir o papel informado na extensão da revogação, quando o sujeito do certificado suspeitar do comprometimento da chave ou quando o sujeito constatar erro nas informações contidas no certificado.

Todos os pedidos devem ser encaminhados para AR. A AR verifica se o solicitante possui permissão para requerer aquela revogação de acordo com a justificativa do pedido e confirma a identificação do solicitante através da conferência da assinatura digital, ou mediante comparecimento deste ao seu estabelecimento.

Após a execução de todos os procedimentos necessários, a AR encaminha as requisições para a AC, que as analisa e revoga os certificados, com conseqüente emissão da LCR.

7.1.4.3 Certificados Classe Servidor

O pedido de solicitação de revogação para a classe servidor é uma informação mais crítica e exige a apresentação de solicitação de revogação mais formal, inclusive com assinatura de termo de responsabilidade por parte do requerente.

Após este procedimento a AR encaminha um pedido de revogação do certificado para AC.

7.1.5 Auditoria

O processo de auditoria nas entidades deve estar relacionado as diretrizes definidas no edital do concurso. Entretanto os procedimentos padrões devem abranger a:

- Política de Segurança;
- Segurança física;
- Administração dos serviços;
- Investigação de pessoal;
- PC e DPC utilizadas;
- Contratos;
- Considerações de sigilo.

7.2 O modelo de avaliação proposto

Com a definição da política da infra-estrutura de chaves públicas montada especificamente para processos de avaliação, seção 7.1, pode-se descrever um modelo de avaliação que a utilize. A proposta envolve a adição da infra-estrutura de chaves públicas descrita ao modelo de avaliação somativa à distância mediada por computador apresentado no capítulo 6, que por sua vez representa uma sofisticação do modelo do processo de avaliação apresentado no capítulo 5. Este modelo é descrito de forma textual e simplificada, porém é baseado no modelo formal apresentado no apêndice C, representado através da UML e desenvolvido obedecendo-se a metodologia RUP.

Nos modelos anteriores há a necessidade de comunicação e armazenamento manual para dar garantias de segurança ao processo. Já no modelo ora proposto o processo de comunicação e armazenagem dos documentos é totalmente computadorizado.

Assim, com a adição da infra-estrutura de chaves públicas como ator, foi acrescido ao diagrama de caso de uso geral apresentado na figura 6.1, página 106, o caso de uso comunicação e armazenamento seguro. O novo diagrama de caso de uso geral é apresentado na figura 7.2, onde os atores, como nos casos anteriores, foram suprimidos para facilitar a visualização.

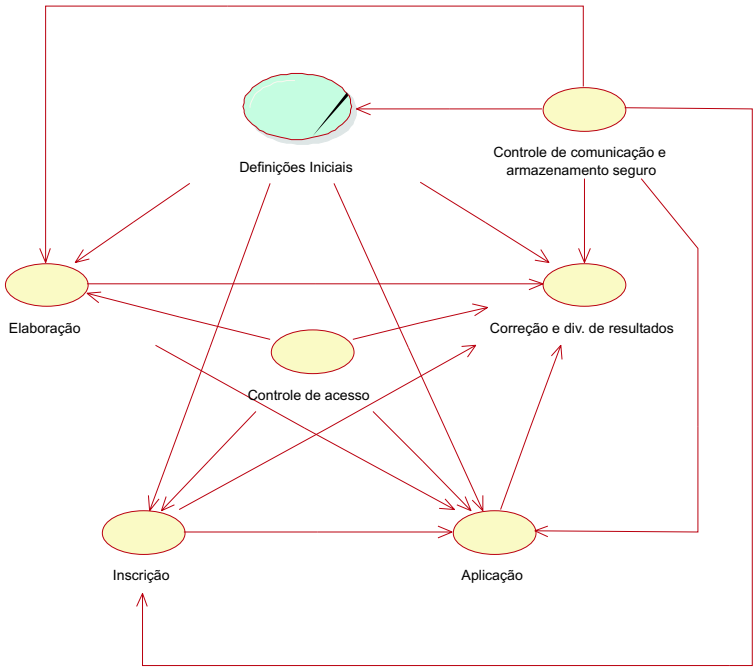

Figura 7.2: Diagrama do caso de uso da avaliação somativa à distância mediada por computador com utilização da ICP-Aval

O diagrama exposto na figura revela as fases do processo modelado e suas inter-relações. A comunicação e armazenamento de informações é apresentado como um processo à parte, o que minimiza as alterações nos casos de uso já modelados. Este caso de uso será abordado na próxima seção deste documento.

7.2.1 A comunicação e o armazenamento de informações

As transações realizadas entre usuários, destes com o sistema ou vice-versa, são representadas pelo caso de uso comunicação e armazenamento seguro, que tem por objetivo permitir comunicação e armazenamento seguro de informações. Através de seu uso é possível verificar a autenticidade, integridade, e tempestividade dos dados, garantir sigilo e não permitir repúdio por parte dos interlocutores. Para que este objetivo seja alcançado é necessário que a infra-estrutura de chaves públicas esteja operacional e que os atores e o sistema já possuam certificados emitidos e válidos.

Para um melhor entendimento de como o modelo implementa estas características de segurança apresenta-se na figura 7.3 seu diagrama de atividades.

Baseado neste diagrama pode-se visualizar como os requisitos de segurança podem ser atendido em várias situações de um processo de avaliação. Para exemplificar, descreve-se a seguir a situação em que um usuário necessite disponibilizar um documento para outro usuário, com todos os requisitos de segurança apresentados.

Do ponto de vista do sistema, a primeira atividade a ser executada é receber solicitação de um usuário que deseja disponibilizar um documento para outro. A partir desta informação deverá ser disponibilizado ao usuário remetente uma interface que o permita assinar o documento, que envolve cifrar o resumo deste com sua chave privada, correspondente à chave pública de seu certificado, emitido pela ICP-Aval.

Em seguida o sistema deverá disponibilizar uma lista de destinatários possíveis. A partir da escolha feita pelo remetente o sistema buscará as chaves públicas do destinatário e de seus superiores no diretório público da infra-estrutura de chaves públicas, caso não as encontre no próprio computador cliente ou no servidor. Com estas informações o sistema disponibilizará nova interface com recursos para cifrar o documento de forma que somente o destinatário e seus superiores possam ter acesso ao seu conteúdo, o que envolverá a utilização de chave de seção. Neste ponto o remetente deverá cifrar o documento.

A seguir deverá ser disponibilizado ao remetente a opção de enviar o documento com protocolação. Caso o usuário tenha solicitado tal recurso o sistema deverá, ao receber o documento, protocolar a transação. O ato de protocolar a transação implica em enviar o resumo do documento assinado e cifrado para protocolação na infra-estrutura de chaves públicas, que

Figura 7.3: Diagrama de atividade da comunicação e armazenamento seguro

consiste no recebimento de recibo com datação. Em posse deste recibo, o sistema o armazena, o disponibiliza ao remetente e armazena o documento recebido.

Neste ponto o sistema deverá enviar uma mensagem ao destinatário requerendo que ele busque o documento enviado e disponibilizar uma interface que possibilite esta operação. Através desta interface, para ter acesso ao documento, o destinatário deverá assinar um recibo, que constitui-se no resumo do documento original assinado e cifrado, obtendo sua liberação. Cabe

salientar que somente o destinatário e seus superiores possuem as chaves privadas capazes de garantir o acesso ao conteúdo do documento disponibilizado.

Finalizando o sistema deverá protocolar o recibo assinado pelo destinatário, armazená-lo e enviá-lo ao remetente, como prova de que o documento foi recebido pelo destinatário.

Cabe ressaltar que “documento” é uma denominação genérica que pode representar qualquer dado eletrônico a ser armazenado por entidade persistente, como questões, respostas enviadas e nota atribuída.

Este caso de uso é formalmente modelado na seção C.4, do apêndice C.

7.2.2 O acesso ao sistema

Como descrito na seção 6.1.1, do capítulo 6, o caso de uso controle de acesso tem por objetivo permitir o acesso de usuários ao sistema dentro de suas funções no processo de avaliação. Porém, diferentemente do modelo apresentado anteriormente a pré-condição para tal é o usuário possuir um certificado válido.

Neste caso de uso a utilização da infra-estrutura de chaves públicas possibilita o acesso sem a necessidade de consulta a banco de dados de usuários, como identificação, conta, senha e direitos de acesso.

Os dados e direitos de acesso nos usuários constam dos certificados digitais, emitidos pela infra-estrutura de chaves públicas, e apresentados pelo usuário quando do acesso, cabendo ao sistema verificar sua validade. Conforme definido na política ICP-Aval, especificamente na seção 7.1.2, certificados da “classe pessoal” devem ser utilizados para acessar o sistema.

A validade do certificado apresentado é verificada a partir: dos dados do próprio certificado, como sua classe, a autoridade que o emitiu e sua validade temporal; e de consulta à LCR, lista de certificados revogados.

As atividades descritas no diagrama apresentado na figura 7.4 representam o modelo proposto para o caso de uso controle de acesso com a utilização da ICP-Aval. Note-se que a atividade de solicitar conta e senha é substituída pela solicitação de certificado. Assim, através deste diagrama pode-se descrever as ações das partes envolvidas quando do acesso ao sistema, como feito a seguir.

O usuário apresenta seu certificado (que envolve a utilização de sua chave privada), e

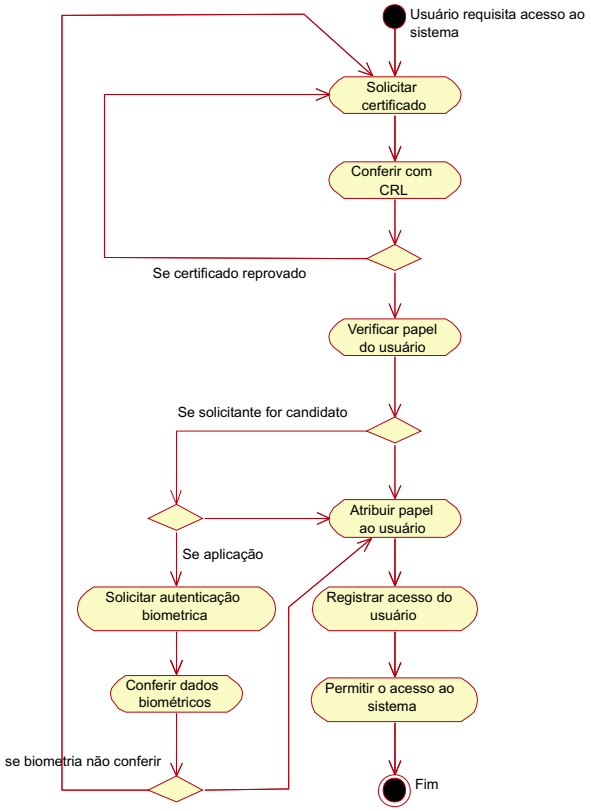

Figura 7.4: Diagrama de atividades do controle de acesso com utilização da ICP-Aval

aguarda a resposta do sistema. Caso seja necessário o usuário ainda se submeterá à um leitor de dados biométricos, para então receber resposta do sistema quanto ao acesso.

Por sua vez o sistema, ao receber o certificado do usuário, checará se a autoridade que o emitiu é confiável, sua validade temporal e se o certificado consta da LCR, sendo que estas verificações poderão exigir consulta a ICP. Caso a aplicação requeira, o sistema disponibilizará os meios e solicitará a leitura de dados biométricos ao usuário, que serão comparados com informações contidas no próprio certificado. No caso de todas as informações serem válidas, o sistema atribuirá os direitos previstos no certificado ao usuário, registrará e permitirá o acesso.

O acesso ao sistema utilizando infra-estrutura de chaves públicas, representado pelo caso de uso controle de acesso, é formalmente modelado na seção C.5.1, do apêndice C.

7.2.3 A fase de definições iniciais

O caso de uso definições iniciais, apesar de já ter sido descrito nos dois capítulos anteriores, merece uma nova abordagem, pois nele será disponibilizada a ICP-Aval, afetando todos os outros casos de uso.

As principais alterações em relação ao modelo apresentado na seção 6.1.2, do capítulo 6, é a supressão da atividade de cadastro de usuários, a disponibilização da ICP-Aval como ator e o envio de mensagens assinadas aos usuários para que estes possam solicitar seus certificados.

Assim, o caso de uso definições iniciais passa a ter as atividades descritas na figura 7.5.

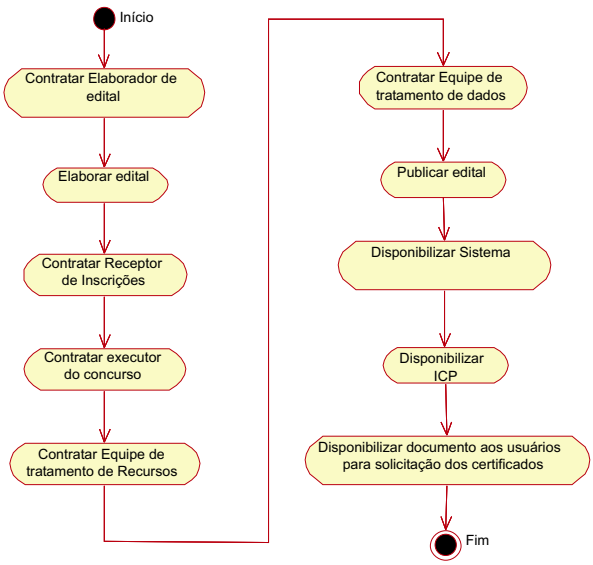

Figura 7.5: Diagrama de atividades da fase de definições iniciais do processo de avaliação à distância mediado por computador utilizando a ICP-Aval

Ao analisar este diagrama, percebe-se que antes da disponibilização do sistema deve ser feita a disponibilização da infra-estrutura de chaves públicas, sendo a atividade final deste caso de uso o envio de documento que permita aos usuários obterem seu certificado digital.

A disponibilização da ICP-Aval deve ser iniciada pelo coordenador do concurso, que deverá solicitá-la à equipe de tratamento de dados. Com o objetivo de atender esta solicitação a equipe de tratamento de dados deverá, com os dados do concurso em questão e seguindo a política da ICP-Aval especificada na seção 7.1, construir ou implementar a infra-estrutura de chaves públicas.

Em seguida e com um certificado para o servidor do sistema e para si a equipe de tratamento de dados deverá disponibilizar, parametrizar e inicializar o sistema. Para parametrizar o sistema deve-se consultar o edital e os contratos já firmados de forma a ter os elementos de escolha para parametrização. Tendo estes elementos a mão, a equipe de tratamento de dados poderá definir papéis a serem desempenhados pelos atores do sistema, suas atribuições e prazos envolvidos. Ao final da execução desta atividade, o coordenador do concurso deve ser informado que o sistema foi disponibilizado.

Com os papéis definidos, a equipe de tratamento de dados deverá atribuí-los aos usuários, assinar esta atribuição e enviar-lhes este documento. Para tal o sistema deverá disponibilizar uma interface que permita a equipe de tratamento de dados fazer esta escolha, buscar informações dos papéis e contratos, permitir assinatura do documento com dados que devem ser inseridos nos certificados dos usuários, como dados do concurso, seu papel e prazo de validade, e enviar esta mensagem assinada aos contratados. Em posse deste documento os contratados poderão solicitar seus certificados à ICP-Aval.

Cabe salientar que esta última atividade descrita, de disponibilizar documento para que os contratados possam obter seus certificados na infra-estrutura de chaves públicas, será assumida como implícita a atividade de armazenar contrato nos próximos casos de uso, diminui-se assim suas alterações.

O modelo formal deste caso de uso é apresentada na seção C.5.2, do apêndice C.

7.2.4 Atividades comuns aos demais casos de uso

As atividade dos demais casos de uso podem envolver situações já tratadas neste capítulo. Neste caso, estas ações específicas serão consideradas como utilizando os casos de uso modelados, minimizando assim modificações nas propostas anteriores.

Por exemplo, as atividades que envolvem comunicação utilizarão o caso de uso comunicação e armazenamento seguro. Isto implicará em alterações na interface disponibilizada ao usuário, onde serão apresentadas as opções possibilitadas pelo uso da ICP-Aval, e as correspondes atividades decorrentes destas escolhas, como o armazenamento de recibos e de informações assinadas e cifradas, quando for o caso. Cabe salientar que as informação assinadas e/ou cifradas são armazenadas nas entidades persistentes originais, e não em uma entidade persistente

específica, o que significa que a estrutura da base de informação permanecerá inalterada.

Outra atividade alterada é o ato de armazenar contratos. Conforme detalhado no final do caso de uso definições iniciais, seção 7.2.3, a atividade de armazenar contratos deverá acarretar no envio de documento assinado aos contratados com informações que devem constar em seus certificados. Em posse deste documento, assume-se que cada contratados solicite e receba o certificado da ICP-Aval. Desta forma os usuários do sistema terão meios de acessá-lo através do mecanismo de controle de acesso baseado em certificados.

Estas ações passam a ser assumidas como implícitas e transparentes aos modelos dos casos de uso elaboração, inscrição, aplicação e correção e divulgação dos resultados, apresentados nos capítulo 5 e 6. Entretanto, a forma como as atividades destes casos de uso são implementadas é substancialmente afetada, como apresentado a seguir.

7.2.5 A fase de elaboração

Os objetivos e as atividades do caso de uso elaboração permanecem os descritos na seção 5.3, do capítulo 5, apesar da adição da ICP-Aval. Entretanto, a forma e os resultados da execução destas atividades sofrem alteração, análogo ao apresentado na seção 6.1.4, do capítulo 6.

A escolha do coordenador de elaboração, dos elaboradores e dos revisores, culmina no armazenamento dos contratos, tal qual abordado no capítulo anterior. Porém, ao invés de cadastrar os usuários no sistema a equipe de tratamento de dados deverá enviar para cada contratado um documento específico assinado. Este documento deverá conter dados do contratado, dados do concurso e de seu papel no mesmo, afim de que possa ser utilizado para solicitar seu certificado, que possibilita, entre outras aplicações, o acesso ao sistema.

Já as atividades de solicitação e retorno de questões elaboradas e revisadas, bem como a escolha das mesmas, além de exigirem o acesso ao sistema pelo uso de certificado, como descrito na seção C.5.1, utiliza todos os recursos disponibilizados no caso de uso comunicação e armazenamento seguro, descrito na seção 7.2.1.

Por exemplo, conforme o diagrama de atividades apresentado na figura 7.3, página 133, para que um elaborador apresente uma questão em resposta a uma solicitação previa do coordenador de elaboração, ele deverá: assinar a questão; cifrá-la de forma que somente o coordenador

de elaboração e o coordenador do concurso tenham acesso; enviar a questão cifrada solicitando protocolação; receber recibo de envio; e receber confirmação de recebimento do destinatário.

Para tal, o sistema deverá: disponibilizar interface cliente com os meios pelo quais o elaborador possa assinar o resumo da questão, utilizando de sua chave privada; buscar no diretório público da infra-estrutura de chaves públicas os dados coordenador de elaboração e o coordenador do concurso, incluindo suas chaves públicas; disponibilizar interface cliente com os meios pelos quais o remetente possa cifrar o documento de forma que apenas o coordenador de elaboração e o coordenador do concurso possam ter acesso ao conteúdo, o que deverá incluir a utilização de chave de seção; enviar a questão recebida para protocolação na infra-estrutura de chaves públicas, que envolve a emissão de recibo de envio com datação; armazenar recibo de envio e a questão; disponibilizar o recibo de envio ao elaborador; avisar o destinatário da disponibilidade da questão; disponibilizar interface cliente que possibilite a assinatura da questão recebida por parte do coordenador de elaboração, liberando-a; enviar o recibo de recebimento para protocolação; e enviar recibo de recebimento protocolado para o remetente.

Por sua vez, o coordenador de elaboração, após receber o aviso, deverá: buscar a questão através da interface do sistema; e assinar recibo de recebimento do documento.

Desta forma obter-se-á um banco de questões armazenadas de forma segura, cuja forma de implementação dá garantias de sigilo, integridade, autoria, não negação e tempestividade.

Já a montagem do instrumento de avaliação, atividade atribuída ao coordenador de elaboração, além dos recursos já descritos, utiliza serviços de criptografia temporal. Sua utilização confere ao instrumento de avaliação a característica de que o acesso ao seu conteúdo seja viável apenas na data e hora acertada para início da avaliação.

A modelagem formal desta fase em um processo manual é apresentada no apêndice A, com sua especificação detalhada na seção A.7.2 e sua realização mostrada na seção A.8.2. As alterações advindas da adição do computador são modeladas na seção B.5.2, do apêndice B, e as resultantes da utilização da ICP-Aval, na seção C.5.3, do apêndice C.

7.2.6 Alterações na fase de inscrição

A adição da ICP-Aval não modifica os objetivos e as atividades deste caso de uso, descritos na seção 5.4, do capítulo 5. Porém, a execução destas atividades e seus resultados sofrem

alteração, análogo ao ocorrido com a introdução da mediação do computador no processo de avaliação à distância, apresentado na seção 6.1.5, do capítulo 6.

A contratação do homologador de inscrições e da equipe de publicidade, feita pelo coordenador do concurso, análogo ao realizado no caso de uso elaboração, seção 7.2.5, finaliza com o envio de documento para cada contratado, contendo seus dados, dados do concurso e de seu papel no mesmo. Este documento deverá ser utilizado para solicitar seu certificado, que possibilita, entre outras aplicações, o acesso ao sistema.

Em paralelo à campanha publicitária, o receptor de inscrição deverá estar recebendo inscrições baseado nas regras estabelecidas no edital. Neste modelo, o candidato, ao final do processo de inscrição deve receber documento assinado que lhe permita solicitar a ICP-Aval um certificado de e-mail, que contém, entre outras dados, sua inscrição no concurso.

Esta classe de certificado proporciona uma forma rápida de distribuição de certificados para os usuários, possibilitando seu uso no processo inicial de inscrição do concurso para posterior substituição por certificados da classe pessoal, no momento em que será homologada a inscrição.

Ao finalizar o prazo para que potenciais candidatos realizem a inscrição, o homologador de inscrições deverá solicitar ao receptor de inscrições que as disponibilize, neste caso uma requisição assinada e protocolada. Em resposta, o receptor de inscrição disponibilizará os documentos destas inscrições para análise, assinados e protocolados.

Com acesso às inscrições, o homologador de inscrição poderá homologá-las. Para tal deverá analisar se as inscrições atendem aos requisitos de inscrição. A sua conclusão deverá ser adequadamente armazenada, novamente em formato digital atendendo as regras de segurança estabelecidas.

Conhecendo os dados dos homologados, o homologador de inscrições deve buscar e analisar os locais específicos de aplicação do instrumento de avaliação, restrito às localidades previstas no edital, e submetê-las ao coordenador do concurso para contratação.

Com a decisão sobre os locais de aplicação do instrumento de avaliação tomada e com acesso aos dados dos homologados, o homologador deve relacionar os candidatos com o local de aplicação, armazenar esta informação e encaminhar a cada candidato homologado documento assinado contendo seus dados, seu papel de candidato homologado, bem como o local e data da realização da avaliação. O candidato deverá apresentar este documento (arquivo)

presencialmente a uma AR do concurso e solicitar um certificado pessoal com biometria, em cartão eletrônico, a ser ser utilizado, principalmente no momento da aplicação do instrumento de avaliação.

A modelagem formal desta fase em um processo manual é apresentada no apêndice A, com sua especificação detalhada na seção A.7.3, e sua realização mostrada na seção A.8.3. As alterações resultantes da adição do computador são modeladas na seção B.5.2, do apêndice B, e as resultantes da utilização da ICP-Aval, na seção C.5.3, do apêndice C.

7.2.7 A fase de aplicação

O caso de uso aplicação tem por objetivo propiciar a aplicação do instrumento de avaliação, em iguais condições e simultaneamente, aos candidatos homologados, com a conseqüente disponibilização de suas respostas ao coordenador de aplicação. A adição da ICP-Aval não modifica este objetivo ou as atividades envolvidas no processo, contudo altera a forma como estas atividades são implementadas, análogo ao ocorrido com a introdução da mediação do computador no processo de avaliação à distância, apresentado na seção 6.1.6, do capítulo 6.

Como destacado nos casos de uso anteriores, descritos neste capítulo, no final da atividade de contratação do coordenador de aplicação, coordenadores locais de aplicação e fiscais, a ação de armazenar o contrato implica no envio de documento para cada contratado contendo seus dados, o papel que desempenharão e dados do concurso, de forma que cada um deles possa requisitar seu certificado junto à ICP-Aval.

Da mesma forma que o processo baseado em sistema computacional convencional, a capacitação da equipe de campo poderá ser realizada a distância, bastando, quando necessário, uma reunião prévia à aplicação para consolidar as instruções.

A atividade de preparação do local de aplicação envolve principalmente a identificação dos locais, a disponibilização dos equipamentos e por em condições a execução de estratégias de contingência. A maior mudança desta atividade ocorre na preparação para receber os candidatos e na não necessidade de identificar a posição de aplicação do instrumento de avaliação para cada candidato. Outra diferença consiste na instalação do módulo de avaliação em cada máquina.

A atividade de receber os candidatos fica sensivelmente alterada, uma vez que o acesso ao local de aplicação pode ser conferido automaticamente pela apresentação de seu certificado

digital. Neste primeiro momento, o sistema poderá simplesmente checar se o certificado é válido, se corresponde ao concurso específico, se aquele é o local de aplicação para o candidato e seu horário de chegada, dando acesso no caso das condições terem sido atendidas. Destaca-se o fato de não ser necessário consulta a nenhuma lista de candidatos, sendo necessário apenas uma checagem nos dados do próprio cartão e da LCR.

Igualmente revolucionária é a forma de encaminhar o candidato a sua posição de avaliação. Como inexistem listas de candidatos, ele poderá ser encaminhado a uma posição aleatoriamente escolhida pelo sistema quando de sua recepção, que deverá contar com um registro de alocação das posições. Este grau de liberdade vai depender das informações disponíveis quando da geração do certificado de homologação dos candidatos. Naquele momento já pode ser definido a posição, ou pelo menos a sala de cada candidato, porém, através da metodologia proposta isto não é imprescindível.

A identificação do candidato em sua posição de avaliação é um processo mais rígido. Como explicado na seção 7.2.2, o usuário deverá apresentar seu certificado (que neste caso envolve a utilização de sua chave privada) e se submeter à um leitor de dados biométricos, para então obter acesso ao sistema.

Note que o acesso ao sistema não dá acesso ao instrumento de avaliação, uma vez que o mesmo foi cifrado utilizando-se de criptografia temporal. Assim a distribuição do instrumento de avaliação passa a ser uma atividade menos crítica, sendo que o acesso ao seu conteúdo só poderá ser obtido em data e hora determinada. Através do serviço de criptografia temporal, uma chave para abrir o documento será disponibilizada na data e hora agendada para início do processo de avaliação.

Já a fiscalização da aplicação em si permanece um processo de vigilância para evitar que um candidato seja ajudado ou perturbado por outrém, ou que tenha acesso a algum tratamento ou informação que lhe confira vantagem. Além das ações visíveis, o módulo de aplicação, ao ser acionado, deverá impedir que quaisquer outros processos venham a ser executados no equipamento utilizado.

Após o acesso ao sistema, o candidato estará no módulo aplicação. Este, como no modelo que utiliza sistema computacional convencional, prevê redundância das informações e possui características que facilitam sua auditoria.

Basicamente, este módulo deverá funcionar de forma a disponibilizar o instrumento de

avaliação, a partir da data e horário pré-determinados, e permitir sua resolução por parte do candidato. Como garantia do correto funcionamento do sistema e de qual instrumento de avaliação está sendo disponibilizado, seus resumos (o resultado da aplicação da função resumo criptográfico sobre um arquivo) deverão ser armazenados no cartão eletrônico do candidato. A medida que o candidato resolve o instrumento de avaliação, suas respostas deverão ser temporariamente armazenadas na máquina local, no servidor local e no servidor central, a depender das condições de rede, que deverão conter a identificação do autor e da máquina local utilizada para gerá-las. Desta forma é possível, a qualquer tempo, realocar um candidato como estratégia de contingência, sem prejuízo ao mesmo.

Ao final da aplicação o candidato deverá assinar eletronicamente suas respostas, que deverão ser gravadas na máquina local e enviadas ao servidor local, que por sua vez deverá assiná-las, enviá-las ao servidor central e devolver seu resumo assinado ao módulo de aplicação, que deverá armazená-lo no cartão do candidato. No caso de o servidor local ficar inacessível, esta operação deverá ser efetuada com o servidor central. Em caso de igual indisponibilidade, o fiscal deverá fazer o papel do servidor local, e utilizando uma mídia removível gravar as respostas do candidato e devolver seu resumo assinado.

Assim a atividade de receber as respostas dadas ao instrumento de avaliação por cada candidato deixa de ser executada pelo fiscal e passa a sê-lo pelo sistema, exceto quando do uso de estratégias de contingência.

Já o preenchimento da ata de ocorrência permanece sob responsabilidade do fiscal, que deverá ser assinada eletronicamente e disponibilizada ao coordenador local.

Ao coordenador local cabe dar atenção às ocorrências relatadas em ata, tratá-las com as medidas cabíveis e disponibilizá-las, já tratadas ao coordenador de aplicação, que coordena todo o processo e poderá atuar em casos não solucionados pelos coordenadores locais.

Cabe destacar que a não necessidade de busca dos dados dos candidatos em uma base de dados facilita o desenvolvimento e implantação do módulo de avaliação. Outra conseqüência é a facilidade de funcionamento sem acesso à rede, ou com uma rede de baixa performance, pois não há a necessidade de consulta nem à base de dados de usuário, nem ao instrumento de avaliação armazenado no servidor, que já estará na máquina, porém não acessível até o momento da aplicação.

Outra mudança importante diz respeito ao perfil dos fiscais. Eles terão de ter condições

de disponibilizar o sistema, de identificar rapidamente eventuais necessidades e operacionalizar o encaminhamento de um candidato a outro equipamento cliente. Este conhecimento poderá ser pré-requisito de contratação ou envolver estratégias de capacitação.

Os locais de aplicação, mais especificamente a posição de avaliação, que envolve a máquina, o sistema e o ambiente físico, são passíveis de novas abordagens com a utilização desta tecnologia. Estes locais podem ser divididos em posições isoladas, contar com dispositivos de monitoração como câmeras e microfones, e auditados, de forma a dispensar a presença física de um fiscal. No limite, no caso de um candidato não poder se deslocar até um ambiente auditado e não ser viável de se auditar um ambiente que lhe seja acessível, poder-se-ia pensar em uma roupa para avaliação, que consistiria em um traje auditado, que monitore interações com o meio e disponibilize visor e dispositivos de entrada. Apesar desta abordagem poder afetar o desempenho do candidato, inferindo as questões levantadas pela utilização do computador em processos de avaliação (MCDONALD, 2002), pode ser um solução prática no futuro.

A modelagem formal desta fase em um processo manual é apresentada no apêndice A, com sua especificação detalhada na seção A.7.4 e sua realização mostrada na seção A.8.4. As alterações derivadas da adição do computador são modeladas na seção B.5.2, do apêndice B, e as resultantes da utilização da ICP-Aval, detalhadas na seção C.5.3, do apêndice C.

7.2.8 A fase de correção e divulgação dos resultados

Para uma abordagem descritiva desta fase deve-se observar as atividades apresentadas no diagrama mostrado na figura 5.6, página 102, que do ponto de vista macro permanecem inalteradas.

A atividade de contratação do coordenador de correção, selecionado pelo próprio coordenador do concurso, e avaliadores de respostas, levantados pelo coordenador de correção, permanecem inalteradas, exceto pelo fato de que ao armazenar os contratos deve ser enviado documento para cada contratado contendo seus dados, o papel que desempenharão e dados do concurso, de forma que cada um deles possa requisitar seu certificado junto à ICP-Aval.

De forma semelhante aos modelos anteriores, o coordenador de correção deve iniciar o processo de atribuir nota às respostas dadas às questões objetivas, cujo gabarito já foi entregue junto com as questões, tarefa a ser realizada pela equipe de tratamento de dados.

As atividades que envolvem as questões dissertativas, necessitam de forma mais visível do caso de uso comunicação e armazenamento seguro, seção 7.2.1, pois o coordenador de correção deverá distribuir as respostas descritivas a pelo menos dois avaliadores, com supressão da identificação dos candidatos, para manter tratamento igual aos candidatos (HAYDT, 2002). Estes deverão atribuir sua nota as respostas das questões. Na seqüência é solicitado à equipe de tratamento de dados atribuir nota às questões subjetivas, tarefa feita pelo cálculo da média da nota dos avaliadores.

Com as notas de cada questão de cada candidato já atribuídas, a equipe de tratamento de dados deve atribuir nota aos candidatos, identificar os aprovados e classificá-los, dando destaque aos classificados dentro do número de vagas disponíveis. Ressalta-se o fato das informações necessárias para se determinar a aprovação e classificação dos candidatos estarem armazenadas com identificação de, no mínimo, autoria. Portanto, como a informação levantada é inferida, não necessita assinatura.

Neste ponto o coordenador desta fase pode enviar para publicação o resultado preliminar e, após decorrido o prazo de recursos, o resultado final, agora assinados digitalmente. Neste caso é importante a assinatura, pois representa uma situação em dado momento a qual se prestará contas.

Apesar de não ter sido modelado, os recursos referentes a fase de aplicação e correção devem ser feitos pelo candidato através do sistema, pois sua identidade, e a integridade de seu pleito, estará garantida pelo uso de seu certificado digital.

A modelagem formal desta fase em um processo manual é apresentada no apêndice A, com sua especificação detalhada na seção A.7.5 e sua realização mostrada na seção A.8.5. Já as alterações conseqüentes da adição do uso do computador são modeladas na seção B.5.2, do apêndice B, e as resultantes da utilização da ICP-Aval, apresentadas na seção C.5.3, do apêndice C.

7.3 Conclusão

O modelo proposto utiliza a infra-estrutura de chaves pública definida na seção 7.1, denominada ICP-Aval, de forma a conferir características de segurança da informação aos documentos eletrônicos utilizados em seus processos.

As propriedades adicionadas aos documentos eletrônicos utilizados resolvem os problemas averiguados quando do levantamento da avaliação somativa à distância mediada por computador, salientados na conclusão do capítulo 6, seção 6.2.

Ao garantir o sigilo das informações, atribui-se mais confiabilidade ao processo de elaboração e revisão de questões e de montagem e distribuição do instrumento de avaliação. Destaca-se que ao instrumento de avaliação adiciona-se características temporais de acesso, tornando o acesso ao seu conteúdo inviável antes do momento de aplicação, independente de ter-se conseguido acesso ao arquivo previamente. Assim, assegura-se que nenhum candidato tenha conhecimento prévio das informações contidas no instrumento de avaliação.

Por assegurar a integridade dos documentos eletrônicos, o uso da ICP-Aval afiancia aos autores que o conteúdo das informações por eles disponibilizadas não podem ser alteradas sem que esta alteração fique evidente, quer sejam eles elaboradores ou candidatos. Por outro lado, seu emprego confirma aos que estão tendo acesso a um documento que este não foi alterado, particularidade especialmente de interesse aos candidatos quando do acesso ao instrumento de avaliação.

A ICP-Aval endossa a autoria do documento eletrônico, o que além de dar a outros ciência da autoria, garante ao autor que o documento não poderá ser substituído por outro em seu nome. Por exemplo, desta forma é computacionalmente inviável trocar-se as respostas entregues por um candidato.

Por outro lado, ao inviabilizar o repúdio, o emprego da ICP-Aval assegura aos que estão tendo acesso a um documento que o autor não poderá negar sua autoria. Os candidatos não poderão alegar que as respostas apresentadas ao instrumento de avaliação não são suas, tampouco os responsáveis pela avaliação poderão negar qual instrumento foi disponibilizado ao candidato e que suas respostas foram entregues. De forma semelhante, caso haja recursos contra o edital, questão ou correção, não se poderá negar sua autoria.

Ao conferir tempestividade, além de se garantir que os prazos foram respeitados, diminui-se a probabilidade de fraude, pois o recibo com datação é fornecido por entidade externa ou auditável, inviabilizando, por exemplo, a troca de respostas entregues pelo candidato com conivência de pessoal interno.

Além dos benefícios apontados, o emprego da ICP-Aval possibilita o acesso dos usuários ao sistema sem a necessidade de acesso à base de dados do usuário, facilitando assim o

desenvolvimento e implantação de módulos específicos.

Possibilita ainda, no que tange ao quesito “à distância”, novas abordagens com respeito aos locais de aplicação, podendo esta ser feita em ambientes auditados e monitorados, sem a presença física do fiscal.

Percebe-se entretanto, que a implementação de uma infra-estrutura de chaves públicas para um processo de avaliação pode ser economicamente inviável, conforme abordado na seção 3.1.7, do capítulo 3.

Por fim, cabe destacar que o modelo proposto é funcional porém não é único, ou seja, existem outras formas de se implementar uma avaliação somativa à distância com a utilização de infra-estrutura de chaves públicas. Contudo ele atende todos os requisitos levantados para processo de avaliação somativa à distância.

Capítulo 8

Modelo de Infra-estrutura de Chaves Públicas como Organização Virtual no processo de avaliação à distância mediado por computador

O capítulo 7 apresentou a utilização de uma ICP aplicada ao processo de avaliação somativa a distância, onde o atendimento de vários requisitos de segurança pôde ser constatado. Porém uma restrição crítica, o alto custo necessário para disponibilizar uma ICP, pode tornar inviável a criação da infra-estrutura proposta, conforme apresentado na seção 3.1.7, do capítulo 3.

Apesar do investimento necessário para disponibilizar esta tecnologia, os benefícios proporcionados pela certificação digital, relacionados no capítulo anterior, justificam a busca de soluções alternativas que tornem a construção da ICP-Aval viável economicamente.

Este capítulo apresenta um modelo de ICP que visa minimizar ou reduzir a restrição existente nas ICPs atuais através da utilização do conceito de organização virtual. A seção 8.1 apresenta um modelo para viabilizar a ICP como organização virtual e a seção 8.2 apresenta uma política que atenda as necessidades do processo de avaliação através deste novo modelo.

8.1 Infra-estrutura de Chaves Públicas como Organização Virtual

Nesta seção propõe-se a implementação da ICP-Aval como organização virtual, à qual será denominada de ICPV.

O conceito aqui utilizado de organização virtual consiste em uma entidade, criada a partir do estabelecimento de parcerias entre várias entidades, com propósito específico e período de vida curto.

Este conceito permite duas abordagens que podem ter efeitos econômicos. A primeira, oriunda da formação de parcerias, implica na utilização de recursos já disponíveis nos parceiros que compõe a organização virtual para a implementação da ICP-Aval, ao invés da utilização de instalações, equipamentos e mão de obra exclusivos para este propósito. A segunda, possibilitada devido a estas organizações terem um tempo de vida curto, permite a diminuição de alguns requisitos de segurança da ICP-Aval que não comprometam a segurança da aplicação, podendo novamente acarretar em redução de custos.

De forma mais específica, a redução de custos pode ser alcançada através da distribuição do controle do coordenador para vários parceiros que já possuam ICPs consolidadas. Este fato permite que estes parceiros cooperem na criação e gerenciamento de uma ICPV, alcançando as vantagens proporcionadas por uma organização virtual, tal como a dispensa de uma nova estrutura física adequada, equipamentos específicos e contratação de profissionais capacitados.

Ademais, a possibilidade de distribuição do controle do coordenador quebra o paradigma do controle único do concurso e abre novas perspectivas em relação ao processo de avaliação modelado. Por exemplo, o caso de várias instituições desejarem partilhar, no todo ou em parte, processos de avaliação, sem abdicar do controle, pode ser atendido pela perspectiva da organização virtual. Outra situação é a de várias entidades não terem capacidade isolada para se responsabilizar por um concurso, porém através da formação de uma organização virtual poderem se comprometer com o processo e compartilhar sua coordenação.

Assim, é importante destacar que neste ponto do trabalho a formação de parceria deixa de ser apenas uma abordagem para diminuir custos e passa a ser um requisito da proposta.

Outra forma de buscar a redução dos custos envolvidos em uma ICP é atacar especificamente os elementos que demandam maior investimento, como os destinados a garantir a

segurança das chaves privadas de autoridades certificadoras que prestam serviços para aplicações críticas, onde um alto grau de confiança é exigido. Dado que processos de avaliação em geral possuem um curto período de execução, podem ser adotadas alternativas para reduzir o custo necessário para tornar seguras as chaves privadas das autoridades certificadoras utilizadas no processo. Uma destas alternativas utiliza protocolos criptográficos de compartilhamento de segredos, seção 3.2, para dividir estas chaves em várias partes, sendo cada uma destas mantida secretamente por participantes do processo.

Este enfoque, permite que organizações que não tenham infra-estrutura física adequada, que corresponde a uma parcela significativa do custo da ICP, conforme abordado na seção 3.1.7, possam participar da parceria, considerando que sua parcela da chave seja criada e armazenada em cartão eletrônico. Se o número de parceiros sem esta infra-estrutura for abaixo do número mínimo necessário para se realizar uma assinatura, a segurança não é comprometida. Entretanto, no limite, mesmo que todos estejam nesta situação o nível de segurança pode ser aceitável para o processo de curta duração com a adoção de critérios adequados para fatores como: seleção de parceiros; número mínimo de parceiros; e um limiar alto para assinatura.

Em detrimento da ICPV, uma aparente solução para aplicações que possuam as características citadas anteriormente é a utilização de serviços de ICPs já consolidadas. Entretanto, a utilização de ICPs já constituídas no processo de avaliação modelado é inviável devido a rigidez das suas políticas. As ICPs convencionais trabalham com políticas rígidas que tornam o processo de construção destas dispendioso, conforme detalhado na seção 3.1.7, e demorado. Estas características são resultantes do atendimento de requisitos de segurança e funcionamento, estabelecidos por órgãos competentes, tal como o Comitê Gestor da ICP-Brasil, ou para atender a padrões específicos, como o ITU-T X.509 ou FIPS-140-2. Esta observância, torna uma ICP mais consolidada, uma vez que os requisitos estabelecidos por estes órgãos ou recomendações são resultados de estudos que buscam regulamentar instruções para que uma ICP seja o mais robusta possível.

Além disso, a tentativa de adequar estas políticas às necessidades da aplicação poderá incorrer em violação destas e conseqüentemente resultar na necessidade de revogação de todos certificados já emitidos e posterior re-emissão destes, para adequá-los a nova política, o que torna inviável a adoção deste procedimento.

A proposta da Infra-estrutura de Chaves Públicas como Organização Virtual tem como

propósito prover um modelo de ICP que elimine ou atenue as restrições do modelo convencional para o processo de avaliação à distância mediado por computador identificadas através do modelo apresentado no capítulo 7.

A primeira etapa para a elaboração da proposta consiste em levantar os critérios mínimos que a ICPV deve atender. Estes requisitos são:

1. Prover os serviços equivalentes aos prestados por uma ICP convencional;
2. Prover serviços que sejam compatíveis com as aplicações que utilizam os serviços de uma ICP convencional;
3. Permitir que vários parceiros realizem o gerenciamento de uma entidade através da responsabilidade compartilhada;
4. Prover formas com baixo custo operacional para gerenciamento compartilhado das entidades;
5. Manter os mesmos requisitos de segurança exigidos por uma ICP convencional, porém em um nível compatível com o tempo de existência;
6. Permitir um processo ágil de criação da ICPV; e
7. Fornecer mecanismos de auditoria.

A partir destes requisitos, pode-se detalhar o ciclo de vida do ICPV, que possui cinco fases, a saber:

1. ***Fase inicial:*** Definição da estratégia a ser adotada para a formação da ICPV. Nesta fase são definidos os serviços a serem prestados, a forma de auditoria das operações realizadas, a seleção dos parceiros que integrarão a ICPV e suas competências;
2. ***Configuração:*** Elaboração de políticas que irão reger as entidades e parceiros integrantes da ICPV. Estas políticas consistem de um maior detalhamento e formalização da estratégia definida na fase anterior e é alcançada através de discussões e negociações entre parceiros;

3. ***Constituição:*** Implantação da ICPV. A constituição ocorre através da criação, de forma cooperativa, das entidades componentes que proporcionarão o funcionamento da ICPV;

4. ***Operação:*** Disponibilização dos serviços a serem prestados pela ICPV, além da manutenção dos processos de auditoria em funcionamento. Estes envolvem atividades administrativas e operacionais que incluem: emissão e revogação de certificados e emissão de listas de certificados revogados; e

5. ***Dissolução:*** Encerramento da relação entre os parceiros. Nesta etapa também se concentram as atividades relacionadas a preparação da ICPV para dissolução, como armazenamento de documentos para conferência futura.

Estas fases da ICPV são ilustradas através da figura 8.1.

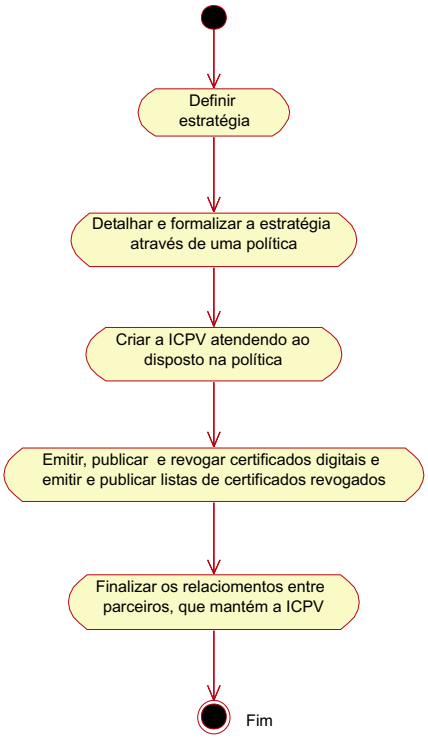

Figura 8.1: Ciclo de vida da ICPV

Já a estrutura da ICP proposta é ilustrada através da figura 8.2. Nota-se que ela é semelhante a estrutura hierárquica de uma ICP convencional, apresentada na figura 3.5, página 65.

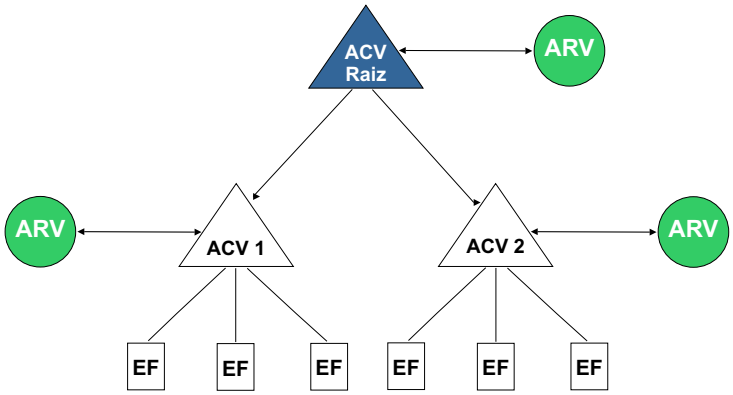

Figura 8.2: Estrutura da ICPV

A figura 8.3 ilustra o ambiente de funcionamento da ICPV proposta construída através da cooperação de parceiros ICP1 e ICP2. A circunferência apresentada na figura representa a delimitação do ambiente de cada ICP convencional, as linhas contínuas que ligam duas entidades representam relações de confiança entre ACs, as linhas pontilhadas simbolizam parcerias que compõem uma entidade e o triângulo representa a autoridade certificadora virtual.

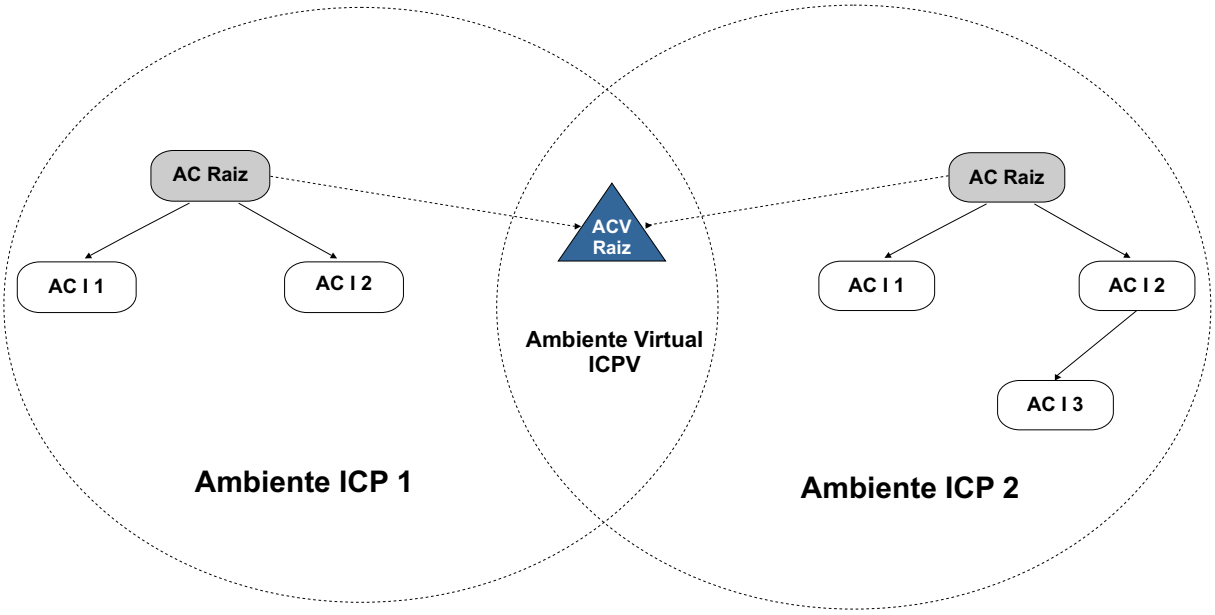

Figura 8.3: Ambiente da ICPV

Cada parceiro ao realizar os procedimentos necessários para construção da entidade, passa a ter posse da estrutura da ICPV. Assim a infra-estrutura da ICPV, tanto física quanto lógica, é mantida nas ICPs dos parceiros, criando um ambiente denominado *ambiente virtual*.

A representação da sua existência ocorre somente quando os parceiros que a compõem cooperam e emitem operações em nome deste ambiente. Este ambiente virtual encontra-se replicado em cada parceiro, porém a operacionalização só é possível através da reunião destes, por isto este ambiente é representado como a intersecção do ambiente das ICP dos parceiros.

Entretanto a construção dos componentes da ICPV nem sempre requer todos os passos do ciclo de vida apresentado. Estes componentes podem ser agrupados e tratados também como organizações virtuais, pois possuem as mesmas características de representação de um grupo de usuários e tempo de vida curto. Como cada componente possui particularidades, implica em procedimentos diferenciados para sua criação.

As seções seguintes descrevem os componentes dentro do contexto de organizações virtuais.

8.1.1 Autoridade Certificadora como Organização Virtual

A *Autoridade Certificadora como Organização Virtual* (ACV) é o principal elemento caracterizador da virtualidade da ICPV, pois concentra o principal serviço da ICP: a emissão de certificados digitais. Assim o ponto crítico da implementação de uma ICPV são as ACVs.

O grande obstáculo para viabilizar um controle distribuído está relacionada a rigidez da política. A ACV permite um novo conceito de implementação desta entidade pois é criada e operada através da cooperação entre parceiros de um grupo.

Independente das características inerentes a uma ACV, os documentos que ela emite, certificados digitais e listas de certificados revogados, devem poder ser vistos pelos usuários da mesma maneira como seriam vistos se eles tivessem sido emitidos por uma AC convencional. Assim, em uma ACV:

1. o processo de geração de chaves não deve necessitar de uma terceira entidade confiável;

2. a segurança da chave privada da ACV deve ser distribuída de forma que todos os parceiros estejam envolvidos;

3. os parceiros não podem atuar de forma individual na emissão e revogação de certificados e na emissão de listas de certificados revogados;

4. o funcionamento da ACV deve ser transparente ao usuário em todas as fases da certificação, inclusive após a emissão do certificado;

5. deve-se disponibilizar métodos de auditoria que permitam verificar quais parceiros participaram em prol de determinada operação para casos de auditoria;

6. deve-se prover um mecanismo de assinatura através da cooperação de parceiros no processo de emissão de certificados com baixo custo operacional;

7. a política da ACV deve apresentar o nível de responsabilidade de cada parceiro e suas funções; e

8. as ACs que constituem o caminho de certificação até uma ACV-raiz devem ser ACVs.

Antes do ínicio do processo de operacionalização da ACV é necessário definir o grupo de parceiros que irá compor uma ACV, sendo que todas as ACVs devem possuir mais de uma parceiro para compor o seu gerenciamento. Os principais critérios de escolha da quantidade de parceiros pode ser baseada na demanda de requisições estimadas que a ACV irá receber, incremento do grau de segurança e descentralização do gerenciamento.

Uma vez definida as políticas e os critérios de escolha dos parceiros deve-se definir os processos de geração e utilização das chaves, detalhado na próxima seção, de gerenciamento da assinatura em grupo utilizando compartilhamento de segredo, apresentado na seção 8.1.1.2, página 158, de certificado digital do grupo, seção 8.1.1.3, página 162, e de auditoria, seção 8.1.1.4, página 163.

8.1.1.1 Geração e utilização das chaves da ACV

Os processos de criação e operação de uma ACV consistem basicamente na geração e utilização de um par de chaves assimétricas. Estes processos devem ser executados de maneira cooperativa pelos parceiros que controlarão a ACV, o que tornará esta dependente da colaboração destes parceiros para realizar ações equivalentes às de uma AC convencional, tal como

emitir certificados digitais, impedindo, desta forma, que um parceiro possa realizar uma ação isoladamente em nome desta.

A geração do par de chaves é realizada na etapa de construção e operacionalição da ACV. Nesta etapa os parceiros devem criar, de forma distribuída, o par de chaves assimétricas que será utilizado para os propósitos da ACV. Ao término deste processo, somente a chave pública da ACV poderá ser conhecida por todos. A chave privada correspondente deve ser controlada de maneira distribuída pelos parceiros. Para tanto, é necessário a utilização esquemas de compartilhamento de segredos específicos.

A operação da ACV ocorre quando esta emite certificados digitais e listas de certificados revogados, o que exige a utilização da sua chave privada em processos de assinaturas digitais. O esquema de assinatura digital que a ACV utilizará, deve considerar o fato da chave privada encontrar-se distribuída em partes entre os parceiros que a controlam. Este esquema deve, inclusive, assegurar o não comprometimento destas partes da chave privada.

Tendo como princípio o atendimento dos requisitos de segurança estabelecidos para uma ACV, buscou-se na literatura científica esquemas de compartilhamento de segredos que melhor atendessem tais requisitos.

Dentre os trabalhos analisados, o esquema de Kazuo Takaragi, Kunihiko Miyazaki e Masashi Takahashi (TAKARAGI; MIYAZAKI; TAKAHASHI, 2000) atende alguns requisitos da ACV, como a dispensa do uso de uma entidade central que controle tanto o processo de distribuição das partes da chave quanto o processo de assinatura. Este trabalho é baseado no protocolo de compartilhamento de segredos de Pedersen (PEDERSEN, 1991), no esquema de assinatura de Nyberg-Ruepple (TAKARAGI; MIYAZAKI; TAKAHASHI, 2000) e em uma variação do esquema de assinatura ElGamal (PARK; KUROSAWA, 1996). Estes dois últimos protocolos tornam a compatibilidade com aplicações que trabalham com certificação digital uma tarefa árdua, visto que a maior parte das aplicações suportam apenas algoritmos difundidos, tais como o RSA e ElGamal.

A partir desta proposta foi apresentado o trabalho de Li, Dai e Zhang (2001) para implementações de Autoridades Certificadoras para empresa virtuais. Entretanto a restrição da compatibilidade com as aplicações é mantida, devido a permanência da utilização da variação do esquema ElGamal e do Nyberg-Ruepple.

Já o esquema de Ivan Damgård e Maciej Koprowski (DAMGÅRD; KOPROWSKI, 2001), além de atender os mesmos requisitos de uma ACV, não possui a restrição da utilização de pro-

tocolos não padronizados, pois o par de chaves que gera e utiliza são compatíveis ao algoritmo RSA. Este esquema é composto por dois protocolos. O primeiro torna possível a criação distribuída de um par de chaves assimétricas, aplicáveis ao algoritmo RSA. O segundo permite que as entidades do grupo que cooperaram na construção do par de chaves possam utilizar estas em processos de assinaturas digitais, sem que para isso seja necessária uma entidade central que controle este processo.

O protocolo de geração distribuída de chaves RSA utilizado pelos autores, foi proposto em (FRANKEL; MACKENZIE; YUNG, 1998). Este protocolo permite que ao término da sua execução, todos os parceiros que compõem um grupo conheçam uma chave pública e que cada um deles conheça apenas uma parte da chave privada correspondente. Nenhuma entidade, interna ou externa ao grupo, conhecerá esta chave privada, ou mesmo será capaz de construí-la individualmente. Esta somente poderá ser utilizada ou construída através da união de t das suas partes, o que conseqüentemente exigirá a cooperação de t dos n parceiros do grupo, sendo $t \leq n$.

Já o protocolo de geração de assinatura permite que os parceiros do grupo gerem de maneira distribuída e segura assinaturas digitais, sendo preservada a confidencialidade da chave privada como um todo e das partes secretas, mantidas por estes.

Desta forma, este esquema pode ser adotado para viabilizar a proposta da ICPV. Assim o procedimento de geração distribuída da chave é possível através da implementação do protocolo e da reunião dos parceiros para cooperarem na realização deste.

Já o protocolo de assinatura permite que um limiar de parceiros atue no processo a fim de gerar uma assinatura digital válida. Entretanto, para isto, os parceiros devem se organizar a fim de decidir quantos deles constituirão este limiar, escolher um responsável por reunir as informações geradas por estes e retornar o documento assinado ao destinatário em cada processo de assinatura.

Assim, a seguir, é proposto um mecanismo que coopere no gerenciamento da realização da assinatura através do protocolo de assinatura apresentado por Damgård e Koprowski (2001).

8.1.1.2 Gerenciamento de assinatura em grupo utilizando compartilhamento de segredo

A primeira etapa da proposta de um mecanismo para gerenciamento de assinatura em grupo utilizando compartilhamento de segredo foi o levantamento dos requisitos necessários a este.

Este mecanismo deve atender a requisitos mínimos de segurança, os quais são:

- o processo de escolha de parceiros que atuarão em um processo de assinatura deve ser imparcial;
- o tempo para execução de uma etapa por um usuário deve ser limitado e controlado;
- a atuação de um parceiro deve ser substituída pela de outro, quando aquele não retornar sua resposta durante o período de tempo definido;
- deve ser possível determinar qual parceiro executou determinada operação; e
- devem ser registradas todas as operações de modo a permitir processos de auditoria sobre estas.

A proposta de viabilização da ICPV consiste em um esquema que engloba todos estes requisitos de gerenciamento das assinaturas em grupo que pode ser implementado tanto como um equipamento específico, quanto como um programa a ser executado em um servidor. O programa de computador é uma estrutura de dados que realiza as etapas necessários fornecendo o serviço através da sua instalação em um equipamento da estrutura da ICPV, enquanto como equipamento as rotinas são implementadas dentro de um dispositivo específico para esta aplicação. O uso de equipamento específico incrementa segurança ao processo, uma vez que suas rotinas aceitam somente requisições para esta aplicação específica, dificultando possíveis ataques.

Este esquema de gerenciamento de assinaturas foi denominado *módulo gerenciador de assinatura em grupo - MGAG*. Este módulo tem como responsabilidade realizar o controle de assinatura de uma requisição recebida de uma AR, realizando um papel intermediador entre as entidades participantes através do controle das atividades executadas pelos parceiros.

Para realizar o controle da assinatura em todos os processos, o MGAG dispõem de cinco mecanismos e dois repositórios. Os mecanismos são: verificador de assinatura, gerador de

seqüência aleatória de parceiros - *GSAP*, gerenciador do cabeçalho de controle de assinatura, datador e gerador de assinatura. Os dois repositórios são o de certificados e o de requisições.

Todos estes componentes realizam o controle de um cabeçalho que acompanha a requisição do momento da submissão do documento pela ARV até o término da assinatura. Através deste documento, denominado *cabeçalho de controle de assinatura* - CCA, o MGAG consegue atender todos os requisitos de um gerenciador de assinatura em grupo. A figura 8.4 ilustra a requisição à ACV e o interação do MGAG com os parceiros.

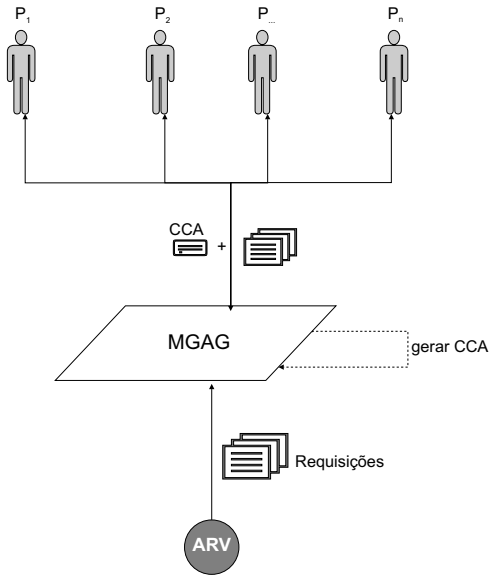

Figura 8.4: Geração do CCA pela MGAG

O CCA contém informações do estado atual da requisição, as quais permitem ao módulo constatar falhas e atrasos no processo, do parceiro que encontra-se responsável pela execução de uma tarefa em dado momento e da integridade dos seus dados. Este cabeçalho é composto por quatro campos:

identificador da requisição: assinatura do CCA com a chave privada do MGAG;

contador: campo que possui a informação de quantos parceiros já concluíram uma etapa da assinatura;

vetor ordenado de parceiros: mantém todos os parceiros em um vetor, definindo a ordem dos parceiros para aplicação da parte do segredo de liberação da chave privada; e

vetor de participantes da assinatura: lista somente os usuários que realizaram o procedimento de assinatura.

O CCA é gerado pelo MGAG ao receber a requisição pela ARV, conforme ilustra a figura 8.5. O processo inicial é a conferência da assinatura da ARV pelo *verificador de assinatura* (passo 2). O verificador busca no repositório de certificados o certificado da ARV correspondente para realizar a conferência da assinatura (passo 3). Se este certificado não estiver contido neste repositório, automaticamente a requisição é descartada, pois os certificados contidos neste repositório são cadastrados pelo administrador do sistema, definindo as ARVs em que a ACV confia.

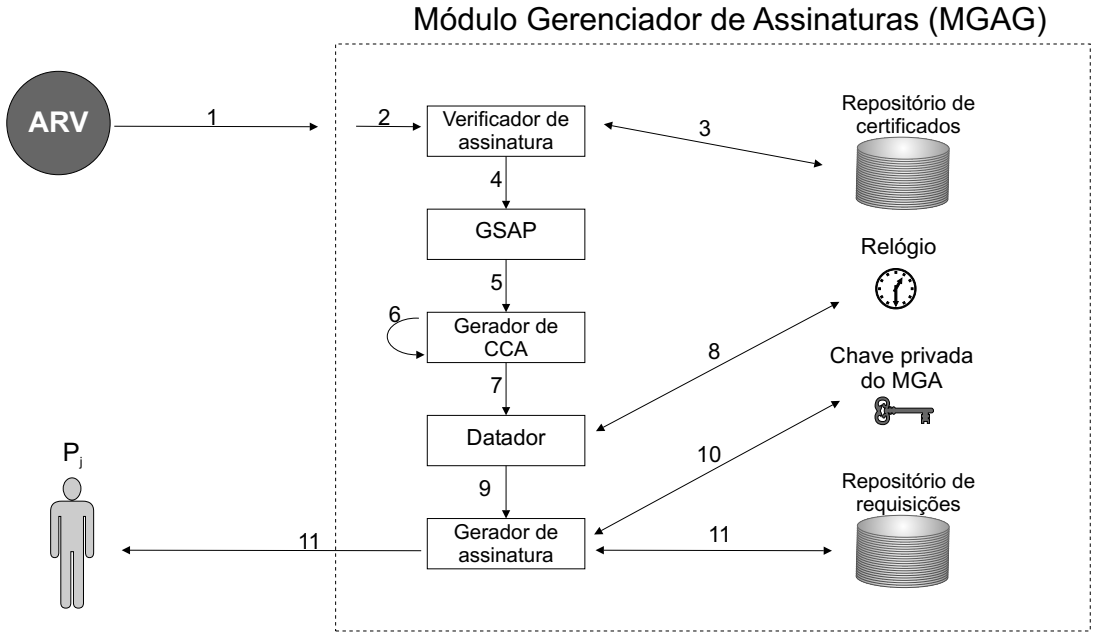

Figura 8.5: Construção da CCA

Se o certificado estiver contido no repositório, é devolvido ao módulo *verificador de assinatura*, que procede a conferência. Se a assinatura não for inválida, a requisição também é descartada. Caso contrário, o módulo *GSAP*, executa um algoritmo de escolha de parceiros (passo 4), que atenda a aleatoriedade do processo de escolha dentre os parceiros definidos pelo administrador.

O *gerenciador de CCA* monta uma mensagem com a seqüência de parceiros realizada pelo GSAP (passos 5 e 6), inicia o campo do contador com zero e passa para o módulo *datador*

incluir âncora temporal ao CCA (passo 7).

O *datador* busca a informação da hora no seu relógio interno que é sincronizado com uma fonte confiável de tempo configurado pelo administrador (passo 8). Todas estas informações são então assinadas pelo *gerenciador de assinatura*.

Em seguida, o *gerenciador de CCA* busca a sua chave privada MGAG para assinar e prover o requisito de autenticidade e integridade ao CCA (passos 9 e 10). Este certificado deve ser emitido pela ACV ao qual este módulo pertencerá. Este procedimento deve ser realizado através do controle da cooperação dos parceiros no processo de assinatura por um administrador do sistema definido. Esta é a único certificado que deve ser gerenciado manualmente para emissão, todos os certificados subseqüentes emitidos são gerenciados pelo MGAG.

Na última etapa da primeira fase, o MGAG envia o CCA e a requisição para o parceiro selecionado e armazena no *repositório de requisições* a requisição, o tempo atual do relógio adicionado do período de tempo permitido para o usuário executar uma ação e identificação do parceiro para qual esta requisição está sendo enviada (passo 11).

Ao receber a requisição o parceiro deve conferir a autenticidade do CCA, se autêntica, assinar a requisição com sua parte da chave e devolvê-la ao MGAG. Caso a devolução não tenha sido realizada em tempo hábil o MGAG envia a requisição para outro parceiro e atualiza a informação de qual parceiro encontra-se com a requisição e o próximo limite de tempo.

Caso o parceiro realize a assinatura, o MGAG inicia o processo de atualização do CCA, o qual é apresentado na figura 8.6.

Esta atualização pode seguir dois fluxos dependendo do estado do CCA:

- se o CCA estiver com o contador igual ao limiar de parceiros necessários para compor a assinatura o MGAG verifica se a assinatura foi realizada corretamente, disponibiliza o certificado ao diretório público e o devolve para a ARV. O MGAG também exclui a requisição do *repositório de requisições* e envia o CCA com todas as etapas de assinaturas realizadas para que todos parceiros insiram a informação em seus arquivos de registro; e

- se o contador da CCA não tiver alcançado o limiar dos parceiros, o MGAG deve atualizar o CCA e as informações do *repositório de requisições* e encaminhar para o próximo parceiro.

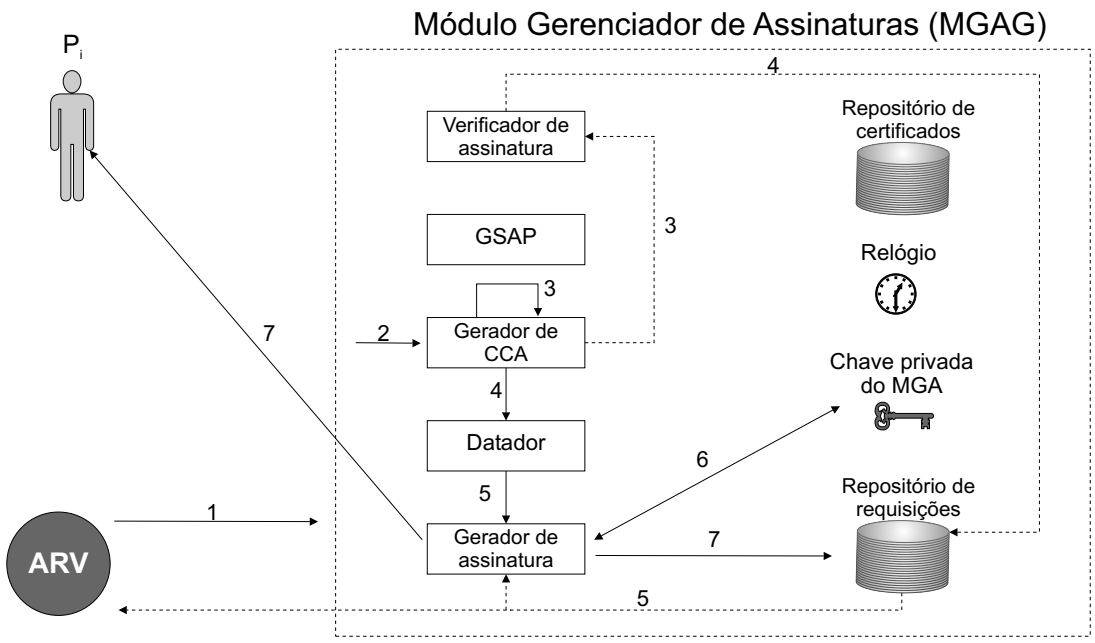

Figura 8.6: Atualização do CCA pelo MGAG

Este módulo de gerenciamento deve estar disponível em um número de parceiros definidos e manter a sincronização dos serviços para que em casos de falhas no equipamento, outro parceiro passe a assumir este serviço.

A ARV conseguirá saber qual módulo está ativo através da configuração da ACV que indicará e atualizará este parâmetro, mantendo-o sempre disponível. O algoritmo de atendimento da aleatoriedade deve garantir que a demanda de requisição entre os parceiros seja homogênea afim de evitar não sobrecarregar algum deles.

8.1.1.3 Certificado Digital do Grupo

Os certificados digitais emitidos pela ACV devem apresentar as informações que identifique a natureza de organização virtual da ICPV e os parceiros que possuem o controle desta. Estes campos são:

- Emissor: dados da Organização Virtual que representa o grupo de parceiros;
- Extensão de restrição(BasicConstraint): Autoridade Certificadora;
- Extensão de integrantes do grupo: informações dos parceiros que gerenciam a ACV; e

- Extensão de Política (CertificatePolicies): dados de OID com informação de ACV e adicionar o endereço da PC.

Mantendo a extensão BasicConstraint com informações padrões do campo, a verificação do caminho de certificação de uma ICPV permance igual a de uma ICP convencional.

Porém a informação da característica de OV é adicionada na extensão da política, apontando para o PC e DPC. Estes documentos devem descrever a organização virtual, como detalhes sobre os parceiros que compõem o grupo, o objetivo de construção, a linha de tempo da operacionalização; e também apresentar os protocolos referentes a geração de chave e de operacionalização utilizados pela ACV.

Todos certificados da ICPV são semelhantes e compatíveis com aplicações e algoritmos que trabalham com certificados convencionais, inclusive os de construção de caminho de certificação.

8.1.1.4 Auditoria

Cada componente da ICPV deve possuir um sistema de conferência das ações executadas. Se este componente for composto por vários parceiros, como a ACV-raiz, este deve manter o registro das ações executadas em cada um dos parceiros.

O registro da ações dos parceiros que gerenciam um componente da ACV resultará em arquivos replicados, pois quando estas ações são realizadas através da cooperação entre eles, são inseridas no arquivo de registro de cada um. A manutenção do registro em cada parceiro incrementa o grau de dificuldade destes forjarem alterações dos registros.

As ações individuais que não implicam em ações globais como por exemplo consultas a requisições de emissão de certificados pendentes, devem ser mantidas no arquivo local da entidade que realizou a ação.

Outro fator que auxilia o processo de auditoria é o armazenamento dos registro do MGAG em um arquivo externo ao módulo, ao término da execução dos passos do esquema de assinatura. Assim os registros permitem a identificação dos parceiros que realizaram determinada ação. Através das informações controladas pelo CCA durante o processo de assinatura, é possível identificar não somente os parceiros que participaram, mas também os que não cumpriram a sua etapa, pois estes possuem o registro da ordem definida de interação do parceiros e quais a

efetivaram.

8.1.2 Autoridades de Registro como Organização Virtual

Uma *Autoridade de Registro como Organização Virtual* (ARV) é qualquer autoridade de registro que preste serviços dentro de uma ICPV.

Uma ARV passa a existir dentro de uma determinada ICPV quando uma ACV, integrante desta, emite um certificado digital para uma entidade, para que esta atue como autoridade de registro nos processos de emissão e revogação de certificados realizados pelas ACVs desta ICPV.

Outra maneira de uma ARV existir é através do estabelecimento de confiança entre uma ou mais ACVs, integrantes de uma determinada ICPV, e uma AR externa a esta organização.

Portanto, uma ARV pode ser constituída de duas maneiras:

1. Através da emissão do seu certificado por uma ACV;
2. Através da celebração de um contrato de prestação de serviços entre a ICPV e uma AR externa.

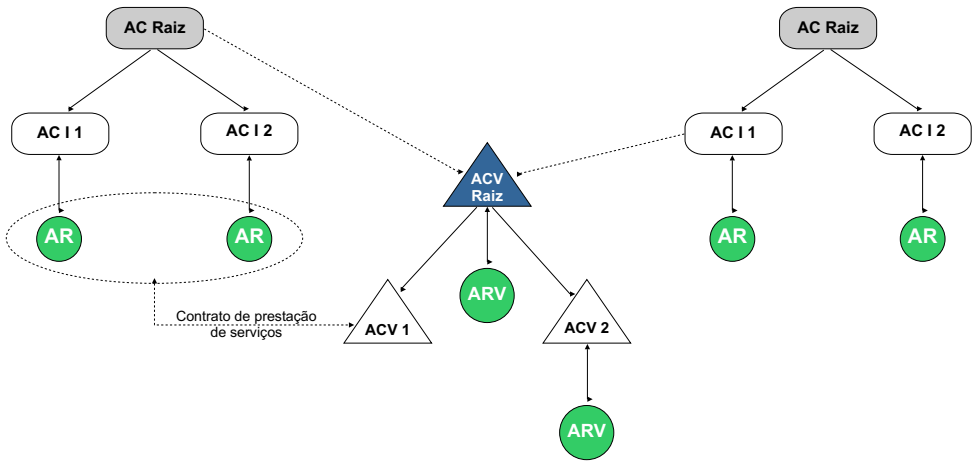

Figura 8.7: ARV

Independente do modo como foi constituída uma ARV, ela é considerada como parte integrante da ICPV até que esta seja destruída, ou ocorra revogação do certificado da ARV.

Assim como ACs tradicionais, as ACVs recebem e tratam requisições de emissão e revogação de certificados somente das ARs que confiam. Normalmente esta relação de confiança é estabelecida através da emissão de um certificado da AC para a AR, assim como aquela realizou a autenticação desta para emissão do certificado ela confia nesta entidade. Entretanto, o modo de comunicação com a ACV difere-se pelo fato de ser controlado e executado pelo MGAG.

8.1.3 Dissolução da ICPV

A dissolução da ICPV representa a última fase do ciclo de vida de uma ICPV. Esta fase tem grande relevância, devido a formalização da extinção da parceria formada. Através da dissolução da ICPV ocorre a interrupção dos seus serviços, dissolução de autoridades certificadoras virtuais, autoridades de registro virtuais e relacionamentos criados entre os parceiros.

Esta fase pode ocorrer somente no tempo definido na fase de configuração, ou nas condições nela estabelecidas, não estando os parceiros habilitados a realizarem este processo por livre arbítrio.

Não obstante, é necessários documentar todo o processo de dissolução da ICPV. Os documentos que registram este fato devem ser assinados pelos parceiros e devidamente protocolados em uma Autoridade de Datação, afim de garantir que a data e o tempo em que foram encerrados os serviços da ICPV possam ser determinados precisamente. Entretanto, para sua conferência, os certificados digitais da entidades devem estar acessíveis mesmo após o encerramento da atividade para averiguação.

Após concluída a dissolução da ICPV, o fato deve ser levado ao conhecimento público através de publicações nos meios de comunicação devidos.

Para a dissolução das ARVs, basta revogar seus certificados, semelhante ao processo de ARs convencionais.

Já o componente ACV de uma ICPV deve realizar procedimentos específicos para realizar sua dissolução, descritos na seção a seguir.

8.1.3.1 Dissolução da ACV

A dissolução da ACV deve abranger a destruição de sua chave privada, ou de suas partes, revogação do certificado e documentação do processo de dissolução.

O processo de dissolução de uma ACV difere quanto ao tipo da autoridade, podendo esta ser uma ACV para usuários finais ou uma ACV raiz.

A dissolução de uma ACV para usuários finais ocorre através da revogação do seu certificado, procedimento este executado pela ACV emissora. Tendo o seu certificado revogado, uma ACV se torna incapaz de emitir certificados válidos e portanto seus serviços não são mais utilizados.

Já a dissolução de uma ACV raiz não pode ser realizada da mesma maneira, pois o seu certificado é auto-assinado, ou seja, o seu certificado digital não foi emitido por outra a autoridade certificadora e sim por ela mesma.

8.2 Política da ICPV no processo de avaliação mediado por computador

A disponibilização de uma ICP para o processo de avaliação mediado por computador utilizando os conceitos da proposta da ICPV necessita de uma política equivalente a apresentada no capítulo 7.

A proposta de uma nova política para o processo de avaliação pode utilizar várias definições da política da ICP-Aval, visto que a maior parte das alterações concentram-se nos processos de construção das entidades, sendo mantidos os serviços prestados. Por esta razão, as informações da política que não sofrem alterações serão omitidas nas seções seguintes nas quais estarão descritas a política da ICPV-Aval.

8.2.1 Organização ACV

A política da ICPV-Aval restringe a sua hierarquia somente à ACVs, não sendo permitido a integração de uma AC convencional à infra-estrutura. Esta restrição está relacionada a necessidade de adequação das políticas das ACs convencionais à política da ICPV.

O primeiro passo para a criação de uma ACV é definir os parceiros que participarão nas ações de operacionalização desta. Em seguida, o grupo utiliza o protocolo de geração de chaves de Damgård e Koprowski (2001), para que o grupo tenha posse da chave pública e cada parceiro mantenha seu pedaço do segredo para reconstruir a chave privada.

Com estas informações disponíveis, juntamente com o protocolo de assinaturas abordado na seção 8.1.1.1, é possível realizar a geração da requisição do certificado, ou a emissão do certificado auto-assinado.

Para a emissão de certificados para ACV-raiz, inicialmente deve ser criada uma requisição a qual contém a informação da chave pública e em seguida executar todos os passos do protocolo de assinatura, descrito em (DAMGÅRD; KOPROWSKI, 2001), para gerar a assinatura do certificado. Assim o certificado auto-assinado da ACV-raiz é emitido. Para que esta se torne operacional, o certificado do MGAG é emitido neste momento, seguindo os mesmos procedimentos anteriores. Após a disponibilização do módulo, a ACV-raiz se torna operacional, estando apta a receber requisições das ARVs, para emitir o certificado para as ACVs intermediárias.

O primeiro passo para a construção de uma ACV intermediária é encaminhar a requisição de emissão de certificado assinado pelos parceiros do grupo para ACV-raiz, a qual emite o certificado.

A criação das ACVSs são semelhante as ACVIs.

O processo de emissão certificados apresentados nesta seção no qual foi omitida a informação da colaboração dos parceiros deve considerar a assinatura em grupo, uma vez que todas as ACVs são compostas por parceiros. Outra informação omitida foi a inserção de ARV no processo de avaliação prévia das requisições, porém este fato deve-se apenas para facilitar o entendimento da organização da AC, sendo apresentado estas entidades na seção seguinte.

8.2.2 Organização da ARV

Autoridades de Registro como Organização Virtual, ARVs, podem ser Autoridade de Registro já existentes, ou entidades criadas por uma ACV, para que em conjunto ofereçam serviços para uma ACV.

A implementação de uma ARV é muito mais simples que a ACV. A ARV necessita tratar apenas a relação de confiança com as ACVs.

Porém antes do estabelecimento do relacionamento de confiança virtual a ACV deve emitir um certificado para AR classificando-a como ARV.

Entre as ACVs e ARVs a relação de confiança pode ser estabelecida de duas formas:

através da utilização de listas de confiança ou através da construção de AR para prestar serviços somente a ACV. A figura 8.7 apresenta a organização de uma ICPV composta por ACV trabalhando com ARVs os relacionamentos virtuais mantidos entre estas.

A implementação de listas de confiança consiste no cadastro de ARVs que terão as requisições encaminhadas aceitas por uma ou mais ACVs. As entidades responsáveis pelo cadastro são as ACVs, as quais definem quais ARVs devem ser incluídas nesta lista, criando um relacionamento referenciado com *relacionamento de confiança virtual*.

8.2.3 Procedimentos para emissão e revogação de certificados

Os procedimentos de solicitação de emissão e revogação de certificados da ICPV mantém-se iguais a política da ICP-aval. Assim a emissão e revogação de certificados para usuários finais é semelhante ao processo de requisição a uma AC convencional, pois as interações entre o usuário e a ICPV mantém-se transparente aos usuários, alterando somente os processos internos da ICP.

Os certificados emitidos por ACVs são compatíveis com as aplicações que um certificado convencional mantém, entretanto algumas característica destes certificado são diferentes, conforme apresentado na seção 8.1.1.3.

8.2.4 Dissolução da ICPV

A dissolução de uma ICPV-Aval deve obedecer os métodos descritos na seção 8.1.3, entretanto a política da ICPV-Aval deve adicionar etapas a este processo de forma a garantir a validade de alguns documentos após a dissolução da ICPV.

Esta situação ocorre devido a características dos processos de avaliação estarem suscetíveis ao recebimento de possíveis impetrações de processos judiciais, como por exemplo para revisão de provas e anulação de questões.

Porém a manutenção do funcionamento da ICPV até o término destes processos se depara com o princípio de temporalidade da ICPV, que é planejada para atender aplicações com curto período de existência, pois estes podem prolongar-se por um período de tempo muito grande.

Entretanto esta necessidade não invalida a utilização da ICPV, pois o armazenamento de documentos podem ser mantidos em uma outra estrutura após a dissolução da ICPV.

Desta forma os documentos gerados durante o ciclo de vida da ICPV que necessitem de posterior conferência deve ser mantido de forma segura. Neste sentido, Notoya (2002) apresentou uma proposta que permite que documentos eletrônicos possam ser armazenados por longo período de tempo mantendo a integridade de seus atributos, denominada Infra-estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos (IARSDE). Em síntese, a IARSDE assegura aos documentos eletrônicos que armazena a manutenção da validade das assinaturas neles constantes, utilizando para isso mecanismos que controlam a validade da tecnologia utilizada para gerar a assinatura e datação destes documentos.

Através de uso de uma estrutura que proporcione o armazenamento seguro dos documentos necessários da ICPV, a dissolução desta pode ser realizada. Para tal, deve-se submeter os documentos assinados pela ICPV que exijam armazenamento, certificados digitais da ACV, documentação de constituição dos componentes da ICPV e os registros de ações do período de construção até o processo de dissolução da ICPV, para a IARSDE.

8.3 Conclusão

A infra-estrutura de chaves públicas como organização virtual (ICPV) proposta neste capítulo implementa as políticas da infra-estrutura de chave públicas para processos de avaliação (ICP-Aval), possibilita a gerência compartilhada do processo e, a depender da forma de implementação, pode reduzir seus custos, valendo-se da infra-estrutura dos parceiros e da diminuição dos requisitos de segurança, sem comprometer o processo de avaliação.

Para viabilizá-la, propôs-se um processo de criação e operação do par de chaves da autoridade certificadora virtual (ACV) que atende os requisitos do processo de geração de chaves não necessitar de uma terceira entidade confiável, da segurança da chave privada da ACV ser distribuída de forma que todos os parceiros estejam envolvidos e de os parceiros não poderem atuar de forma individual na emissão e revogação de certificados e na emissão de listas de certificados revogados. Porém, como o requisito de que a segurança da chave privada da ACV deve ser distribuída de forma que todos os parceiros estejam envolvidos não depende somente da criação das chaves, foi exposto um método que permite implementar assinaturas através da cooperação dos parceiros.

O esquema de assinatura digital proposto atende os requisitos de o funcionamento da

ACV ser transparente ao usuário em todas as fases da certificação, inclusive após a emissão do certificado, de disponibilizar métodos de auditoria que permitam verificar quais parceiros participaram em prol de determinada operação e de prover um mecanismo de assinatura através da cooperação de parceiros no processo de emissão de certificados com baixo custo operacional.

A política da ICPV incrementa a política da ICP-Aval, atendendo aos requisitos de apresentar o nível de responsabilidade de cada parceiro e suas funções e de que as ACs, que constituem o caminho de certificação até uma ACV-raiz, serem ACVs.

Assim atendeu-se os requisitos para a criação da ICPV viabilizando sua implementação para processos de avaliação somativa a distância mediado por computador.

Capítulo 9

Conclusão

Esta pesquisa objetivou a apresentação de um modelo de infra-estrutura de chaves públicas como organização virtual para processos de avaliação somativa à distância mediada por computador que satisfizesse os requisitos mínimos de segurança e diminuísse os custo de utilização desta tecnologia em relação ao processo apresentado com a utilização da infra-estrutura de chaves públicas convencional.

Como estratégia para atingir este objetivo buscou-se, inicialmente, obter um modelo de avaliação somativa à distancia convencional. Neste sentido representou-se o processo por meio da "Linguagem de Modelagem Unificada" (*Unified Modeling Language* - UML) adotando a metodologia de "Processo Unificado da Rational" (*Rational Unified Process* - RUP). A aplicação desta metodologia iterativa incremental resultou em uma visão múltipla dos processos envolvidos e permitiu que a perspectiva sobre eles fosse aprimorada durante o levantamento.

Um dos mais evidentes legados desta etapa foi o levantamento das principais fases do processo e seus atores. As fases foram definidas como: definições iniciais; elaboração das questões; inscrição dos candidatos; aplicação do instrumento de avaliação; correção das respostas e divulgação dos resultados. Por outro lado, os principais atores aventados foram os: avaliados; elaboradores de questão; revisores de questões; coordenadores; fiscais; e avaliadores.

Após a modelagem do processo de avaliação somativa à distancia convencional utilizou-se a mesma metodologia RUP e representação UML, considerando a agregação de sistemas computadorizados ao processo, para se obter um modelo de avaliação somativa à distancia mediada por computador.

Os benefícios mais patentes do modelo mediado por computador são a possibilidade de: utilizar elaboradores e revisores independentemente de seu local de atuação, facilitando o uso de especialistas; distribuição on-line do instrumento de avaliação, minimizando a logística de transporte e distribuição de material impresso; montagem do instrumento de avaliação durante a aplicação, através da seleção aleatória em um banco de questões ou mesmo simulação; atendimento dos inscritos via sistema; correção automática das respostas dadas às questões objetivas; e, classificação imediata dos candidatos. Porém, apesar de ter adicionado uma série de potencialidades ao processo, este modelo apresenta dificuldades técnicas quanto aos dados transacionados e armazenados digitalmente, como as dificuldades para manter o sigilo e a integridade, comprovar a autoria, inviabilizar o repúdio, comprovar a tempestividade, bem como a demanda por conectividade e limitações quanto aos locais de aplicação da avaliação.

Para contornar estes obstáculos foi acrescido ao modelo mediado por computador uma infra-estrutura de chaves públicas (ICP). Isto demandou a proposição de uma política para uma infra-estrutura de chaves públicas aplicada a avaliação (ICP-Aval). Neste ponto, pôde-se obter um modelo resultante, novamente por meio da aplicação da metodologia iterativo incremental RUP e representação UML.

Este novo modelo garante o sigilo das informações, atribuindo mais confiabilidade ao processo de elaboração e revisão de questões, bem como de montagem e distribuição do instrumento de avaliação. Por assegurar a integridade dos documentos eletrônicos, o uso da ICP-Aval afiancia aos autores que o conteúdo das informações por eles disponibilizadas não podem ser alteradas sem que esta alteração fique evidente, quer sejam eles elaboradores ou candidatos. Por endossar a autoria do documento eletrônico, o que além de dar a outros ciência da autoria, a ICP-Aval garante ao autor que o documento não poderá ser substituído por outro em seu nome, o que, por exemplo, torna computacionalmente inviável se substituir as respostas entregues por um candidato. Por outro lado, ao inviabilizar o repúdio, o emprego da ICP-Aval assegura aos que estão tendo acesso a um documento que o autor não poderá negar sua autoria, o que implica que os candidatos não poderão alegar que as respostas apresentadas ao instrumento de avaliação não são suas, nem tampouco os responsáveis pela avaliação poderão negar qual instrumento foi disponibilizado ao candidato e que suas respostas foram entregues. Ao conferir tempestividade, diminui-se a probabilidade de fraude, tanto por tornar inviável o acesso ao instrumento de avaliação antes do momento de aplicação, como por garantir que os prazos sejam respeitados, pois

a datação é realizada por entidade externa ou auditável, inviabilizando, por exemplo, a troca de respostas entregues pelo candidato com conivência de pessoal interno.

Além dos benefícios apontados, o emprego da ICP-Aval possibilita o acesso dos usuários ao sistema sem a necessidade de acesso à base de dados do usuário, facilitando assim o desenvolvimento e implantação de módulos específicos. Possibilita ainda, no que tange ao quesito "à distância", novas abordagens com respeito aos locais de aplicação, podendo esta ser feita em ambientes auditados e monitorados, sem a presença física do fiscal.

Percebe-se entretanto, que a implementação de uma infra-estrutura de chaves públicas para um processo de avaliação somativa à distância pode ser economicamente inviável, como também centralizada.

Por fim, para superar estas limitações foi apresentado uma infra-estrutura de chaves públicas como organização virtual (ICPV) que, além de implementar sua própria política, implementa as políticas da ICP-Aval, possibilitando gerência compartilhada do processo e redução de custos.

Segundo a VeriSign, empresa referência no segmento de segurança da informação, são necessários mais de 300 mil dólares por ano para manter um ICP operacional. Este valor pode ser significativamente minorado pela adoção da ICPV, por meio do compartilhamento das infra-estruturas já existentes ou atenuação dos requisitos de segurança, sem comprometer o processo de avaliação.

Assim, além de satisfazer o objetivo inicial de possibilitar a redução de custo de implementação, o modelo proposto possibilitou a quebra o paradigma do controle único do concurso e abre novas perspectivas em relação ao processo de avaliação modelado, como o atendimento de situações onde várias instituições desejam partilhar, no todo ou em parte, processos de avaliação, sem abdicar do controle. Isto se dá por meio do partilhamento de chave privada entre parceiros do processo.

A eventual disseminação de utilização do modelo ICPV tenderia a diminuir a discrepância entre a evolução verificada nos processos de capacitação à distância e o processo de avaliação somativa, destinado a selecionar e certificar indivíduos. Esta fato poderia levar a maior aceitação de capacitações à distância, por focar mais o resultado do que o método utilizado na formação.

Em relação a proposta, resguarda-se a aplicabilidade nas condições atuais de difusão de infra-estruturas de chaves públicas nas organizações, que acredita-se estar em expansão.

A partir deste trabalho vislumbra-se desdobramentos futuros, como o de implementação o modelo proposto, pesquisas dos efeitos organizacionais e sociais de sua aplicação, a aplicação deste modelo à outros processos de avaliação, como a avaliação formativa e de desempenho, e a proposta de modelos variantes.

Referências Bibliográficas

ADAMS, C.; LLOYD, S. *Understanding PKI: Concepts, Standards, and Deployment Considerations*. 2ª. ed. [S.l.]: Addison Wesley, 2002.

ALTERMAN, P. The us federal pki and the federal bridge certification authority. *Computer Networks*, 2001.

ALVES-MAZZOTTI, A. J.; GEWANDSZNAJDER, F. *O Método Nas Ciências Naturais e Sociais - Pesquisa Quantitativa e Qualitativa*. 2. ed. São Paulo, SP: Pioneira, 2001.

ARDIGO, J. D. *Poligrafo Computadorizado Para Sinais Biomédicos*. Dissertação (Mestrado) — UFSC, 1994.

BAKER, E.; MAYER, R. Computer-based assessment of problem solving. *Computers in Human Behavior*, v. 15, p. 269–282, 1999.

BAYER, D.; HABER, S.; STORNETTA, W. S. Improving the efficiency and reliability of digital time-stamping. *Sequences91: Methods in Communication, Security, and Computer Science*, p. 329–334, 1991.

BENNETT, R. E. *Reinventing Asessment: Speculations on the Future of Large-Scale Educational Testing.* NJ: Educational Testing Service, Policy Information Center., 1998.

BEZERRA, E. *Princípios de Análise e Projeto de Sistemas Com UML*. Rio de Janeiro: Campus, 2002.

BLOOM, B. S.; HASTINGS, T.; MADAUS, G. *Manual de Avaliação Formativa e Somativa Do Aprendizado Escolar*. São Paulo, SP: Pioneira, 1983.

BONELLI, M. *ORGANIZAÇÕES VIRTUAIS: DEFINIÇÃO DE UM MODELO*. Dissertação (Mestrado) — UDESC, 2001.

BONNIOL, J.-J.; VIAL, M. *Modelos de Avaliação*. Porto Alegre, RS: Artmed Editora Ltda, 1997.

BOOCH, J. R. G.; JACOBSON, I. *Uml - Guia Do Usuário*. Rio de Janeiro: Campus, 2000.

BOWDITCH, J. L.; BUONO, A. F. *Elementos de Comportamento Organizacional*. São Paulo: Pioneira, 1997.

BRASIL. *Secretaria de Educação a Distância*. 2003. Http://www.mec.gov.br/seed/.

BULL, J. Computer-assisted assessment: Impact on higher education institutions. *Educational Technology & Society*, v. 2, n. 3, 1999.

BURR, W. *Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations*. [S.l.], setembro 1998.

BUSINESS Modeling with the UML and Rational Suite Analyst Studio. [S.l.], 2003.

BYRNE, J. A. The virtual corporation. *Business Week*, p. 98–103., February 1993.

CARSWELL, L. The 'virtual university': Toward an internet paradigm? In: *Innovation and Technology in Computer Science Education 1998*. [S.l.: s.n.], 1998. p. 46–50.

CHOKHANI, S.; FORD, W. *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. [S.l.], March 1999.

CHOU, S.-W. Computer systems to facilitating organizational learning: IT and organizational context. *Expert Systems with Applications*, 2002.

COYLE, J.; SCHNARR, N. *Os Desafios Da Organização Virtual*. New York: John Wiley & Sons,, 1997.

CULLEN, P.-A. Contracting, co-operative relations and extended enterprises. *Technovation*, Elsevier Science Ltd., v. 20, p. 363–372, 2000. Base JDA - pdf.

DAMGÅRD, I.; KOPROWSKI, M. Practical threshold rsa signatures without a trusted dealer. In: (ED.), B. P. (Ed.). *Advances in Cryptology - EUROCRYPT 2001: Second Symposium, PADO 2001, Aarhus, Denmark, May 21-23, 2001, Proceedings*. [S.l.]: Springer-Verlag Heidelberg, 2001. (Lecture Notes in Computer Science, v. 2045/2001), p. 152.

DAVIDOW, W. H.; MALONE, M. S. *A Corporação Virtual*. São Paulo: Pioneira, 1993.

DEWETT, T.; JONES, G. R. The role of information technology in the organization: A review, model, and assessment. *Journal of Management*, Elsevier Science Inc., p. 313–346, 2001. Base JDA - pdf.

DIFFIE, W.; HELLMAN, M. New direction in criptography. *IEEE Transactions on Information Theory*, November 1976.

EBOLI, M. *UNIVERSIDADES CORPORATIVAS*. São Paulo, SP: Editora Schmukler, 2000. Http://www.fia.com.br/livros/99/liv99_unicorp.htm.

ENSHER, E. A.; NIELSON, T. R.; GRANT-VALLONE, E. Tales from the hiring line: Effects of the internet and techonology on HR process. *Organizational Dynamics*, Elsevier Science, v. 00, n. 100, p. 1–22, 2002.

EXTREME CHAOS. [S.l.], 2000.

FALCONER, D. J.; MACKAY, D. R. The key to the mixed method dilemma. In: *10th Australasian Conference on Information Systems*. [S.l.: s.n.], 1999. p. 286–197.

FERNANDES, A. D. Risking trust in a public key infrastructure: Old techniques of managing risk applied to new technology. *Decision Support Systems*, Elsevier Science, p. 303–322, 2001.

FERREIRA, A. B. de H. *Dicionário Aurélio Eletrônico: Século XXI*. 3ª. ed. Rio de Janeiro, RJ: Editora Nova Fronteira S.A, 1999.

FIORESE, M. *Uma Proposta de Autenticação de Usuários Para Ensino a Distância*. Dissertação (Mestrado) — Universidade Federal do Rio Grande do Sul, março 2000.

FORD, W.; BAUM, M. S. *Secure Electronic Commerce - Building the Infrastructure for Digital Signatures and Encryption*. [S.l.]: Prentice-Hall, Inc, 1997.

FOWELL, S. L.; SOUTHGATE, L. J.; BLIGH, J. G. Evaluating assessment: The missing link? *Medical Education*, v. 33, p. 276–281, 1999.

FRANKEL, Y.; MACKENZIE, P. D.; YUNG, M. Robust efficient distributed RSA-key generation. In: . [S.l.: s.n.], 1998. p. 663–672.

GIL, A. C. *Como Elaborar Projetos de Pesquisa*. 4. ed. São Paulo: Editora Atlas S.A., 2002.

GOLDMAN, S.; AL at. *Competidores Ágeis e Organizações Virtuais*. Eindhoven: Van Nostrand Reinhold, 1995.

GRANDE Dicionário Universal Da Lingua Portuguesa. [S.l.]: Texto Editora, 2003. Http://www.universal.pt/.

GUERRA, T. G. *La Investigación Social Cuantitativa*. Nuevo León, México: Publicaciones Universidad de Montemorelos, 1996.

GUNASEKARANA, A. et al. E-commerce and its impact on operations management. *Int. J. Production Economics*, Elsevier Science B.V., p. 185–197, 2002.

HABER, S.; STORNETTA, W. S. How to time-stamp a digital document. *Journal of Cryptology*, v. 3, n. 2, p. 99–111, 1991.

HACK, L. E. *Mecanismos Complementares Para a Avaliação Do Aluno Na Educação a Distância*. Dissertação (Mestrado) — Universidade Federal do Rio Grande do Sul, junho 2000.

HALL, R. H. *Organizações: Estrutura e Processos*. 3. ed. Rio de Janeiro: Prentice Hall do Brasil., 1982.

HARDWICK, M. et al. Lessons learned developing protocols for the industrial virtual enterprise. *Computer-Aided Design*, Elsevier Science Ltd., v. 32, p. 159–166, 2000. Base JDA - pdf.

HAYDT, R. C. *Avaliação Do Processo Ensino-Aprendizagem*. 6. ed. São Paulo, SP: Editora Ática, 2002.

HELLENS, L. V. *Research Design for the PhD Thesis: Enterprise Reference Architectures and Modelling Frameworks*. [S.l.]: Griffith University - School of Computing and Information Technology, 2001.

HONG, I. B. A new framework for interorganizational systems based on the linkage of participants' roles. *Information & Management*, v. 39, p. 261–270, 2002. Base JDA - pdf.

HOUSLEY, R.; POLK, T. *Planning for PKI - Best Practices Guide for Deploying Puclic Key Infrastucture*. 1. ed. [S.l.]: Wiley, 2001.

HUNT, R. Technological infrastructure for PKI and digital certification. Elsevier Science B V, p. 1460–1471, 2001.

INGEMARSSON, I.; SIMMONS, G. J. A protocol to set up shared secret schemes without the assistance of a mutually trusted party. *Advances in Cryptology - EUROCRYPT'90*, p. 266–282, 1991.

IP, W. et al. Genetic algorithm solution for a risk-based partner selection problem in a virtual enterprise. *Computers & Operations Research*, Elsevier Science Ltd., 2001. BASE JDA - pdf - in press.

ITU. *Information Technology – Open Systems Interconnection – the Directory: Overview of Concepts, Models and Services*. 1997. Recomendation X.500.

ITU-T. *The Directory - Authentication Framework*. [S.l.], 2000.

JACKSON, W.-A.; MARTIN, K. M.; O'KEEFE, C. M. Efficient secret sharing without a mutually trusted authority. *Advances in Cryptology - EUROCRYPT'95*, p. 183–193, 1995.

KANUKA, H. Assessing higher levels of learning in post-secondary education. *Academic Exchange*, p. 106–111, 2001. Winter.

KASPER-FUEHRERA, N. M. A. E. C. Communicating trustworthiness and building trust in interorganizational virtual organizations. *Journal of Management*, v. 27, p. 235–254, 2001.

KATZ, D.; KAHN, R. L. *Psicologia Social Das Organizações*. 3. ed. São Paulo: Atlas, 1987.

KEIL, T. et al. Information and communication technology driven business transformation - a call for research. *Computers in Industry*, Elsevier Science, p. 263–282, 2000.

KHALIL, O.; WANG, S. Information technology enabled meta-management for virtual organizations. *Int. J. Production Economics*, v. 75, p. 127–134, 2002. Base JDA - pdf.

KRUCHTEN, P. *The Rational Unified Process*. 2 ed.. ed. [S.l.]: Addison Wesley, 2000.

KUMAR, A. N. On changing from written to on-line tests in computer science i: An assessment. In: *Innovation and Technology in Computer Science Education 1999*. [S.l.: s.n.], 1999. p. 25–28.

LAKATOS, E. M.; MARCONI, M. A. *Metodologia Científica*. 3. ed. São Paulo: Editora Atlas S.A., 2000.

LAKATOS, E. M.; MARCONI, M. A. *METODOLOGIA DO TRABALHO CIENTIFICO*. 6. ed. São Paulo: Editora Atlas S.A., 2001.

LANG, E. *AVALIAÇÃO DE DESEMPENHO HUMANO: HISTÓRIA, EVOLUÇÃO, METODOLOGIA E REALIDADE*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2001.

LARMAN, C. *Utilizando UML e Padrões - Uma Introdução À Análise e Ao Projeto Orientados À Objetos*. Porto Alegre: Bookman, 2000.

LEEM, C. S.; KIM, S. Introduction to an integrated methodology for development and implementation of enterprise information systems. *The Journal of Systems and Software*, Elsevier Science Inc, v. 60, p. 249–261, 2002.

LI, B.; DAI, K.; ZHANG, S. Virtual certificate authority for virtual enterprises. *IEEE*, p. 222–224, 2001.

LIMA, A. de O. *Avaliação Escolar - Julgamento X Construção*. Petrópolis, RJ: Vozes, 1994.

LLOYD, S. Understanding certification path construction. *PKI Forum*, setembro 2002.

LLOYD, S. et al. Ca-ca interoperability. *PKI Forum*, março 2001.

LOPES, J.; BARBOZA, J. O. AVALIAÇÃO - AUTORITARISMO x MEDO x APRENDIZAGEM: AVALIANDO AS COMPETÊNCIAS. 2003.

LUCAS, S. R. Assessment of learning outcomes in an online environment. *Academic Exchange*, p. 63–69, 2001. Winter.

MARTIN, J. *Cybercorp: A Nova Revolução Empresarial*. Nova Iorque: Amacom, 1996.

MAY, T. C. *Timed-Release Crypto*. 1993. Http://cypherpunks.venona.com/date/1993/02/msg00129.html.

MCDONALD, A. S. The impact of individual differences on the equivalence of computer-based and paper-and-pencil educational assessments. *Computers & Education*, v. 39, p. 299–312, 2002.

MENEZES, A. J.; OORSCHOT, P. C. van; VANSTONE, S. A. *Handbook of Applied Cryptography*. [S.l.]: CRC Press, 1996.

MONT, M. C.; HARRISON, K.; SADLER, M. The hp time vault service: exploiting ibe for timed release of confidential information. In: *Proceedings of the twelfth international conference on World Wide Web*. Budapest, Hungary: ACM Press, 2003. p. 160–169.

MOSES, T. *PKI Trust Models*. [S.l.], 2002.

NIST. Security requirements for cryptographic modules - fips pub 140-2. *Federal Information Processing Standards Publication - National Institute of Standards and Technology*, Maio 2001.

NOTOYA, A. E. *IARSDE- Infra-Estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos: Validade de documento eletrônico por tempo indeterminado*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2002.

OFFODILE, O. F.; ABDEL-MALEK, L. L. The virtual manufacturing paradigm: The impact of IT/IS outsourcing on manufacturing strategy. *International Journal Production Economics*, v. 75, p. 147–159, 2002.

PANTELI, N.; DIBBEN, M. R. Revisiting the nature of virtual organizations: Reflections on mobile communication systems. *Futures*, Elsevier Science Ltd., v. 33, p. 379–391, 2001. Base JDA - pdf.

PARIKH, M.; VERMA, S. Utilizing internet technologies to support learning: An empirical analysis. *International Journal of Information Management*, v. 22, p. 27–46, 2002.

PARK; KUROSAWA. New elgamal type threshold digital signature scheme. *TIEICE: IEICE Transactions on Communications/Electronics/Information and Systems*, 1996.

PASQUAL, E. S. *IDDE - Uma Infra-estrutura para a Datação de Documentos Eletrônicos*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2002.

PEDERSEN, T. P. A threshold cryptosystem without a trusted party. *Advances in Cryptology - EUROCRYPT'91*, v. 547, p. 522–526, 1991.

PERLMAN, R. An overview of pki trust models. *IEEE Network*, dezembro 1999.

PHILIP, G.; BOOTH, M. E. A new six 's' framework on the relationship between the role of information systems (IS) and competencies in 'IS' management. *Journal of Business Research*, Elsevier Science Inc., v. 51, p. 233–247, dezembro 2001.

PODESTÁ, M.; MEINEL, C. The necessity of a public key infrastructure for a virtual university. *Institut für Telematik e.V.,Trier*, 2000.

POLK, W. T.; HASTINGS, N. E. Bridge certification authorities: Connecting B2B public key infrastructures. *National Institute of Standards and Technology*, 2000.

PORTO, E. (Ed.). *Dicionário Da Lingua Portuguesa*. fevereiro 2003. Http://www.portoeditora.pt. Avaliação, avaliar, valia, valer, merecimento, merecer, mérito.

PRESSMAN, R. S. *Engenharia de Software*. São Paulo: Makron Books, 1995.

PRESTON, J. A.; SHACKELFORD, R. Improving on-line assessment: An investigation of existing marking methodologies. In: *Innovation and Technology in Computer Science Education 1999*. [S.l.: s.n.], 1999. p. 29–32.

QUATRANY, T. *Modelagem Visual Com Rational Rose 2000 e UML*. Rio de Janeiro: Editora Ciência Moderna Ltda, 2001.

RAJAGOPAL, P. An innovation - diffusion view of implementation of enterprise resource planning (ERP) systems and development of a research model. *Information & Management*, Elsevier Science B.V., p. 87–114, 2002.

RAMOS, F.; JUNCO, M. de L. A.; ESPINOSA, E. Soccer strategies that live in the B2B world of negotiation and decision-making. *Decision Support Systems*, Elsevier Science B.V., 2002.

RATIONAL Unified Process. [S.l.], 2003.

RIVEST, R.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, February 1978.

RIVEST, R. L.; SHAMIR, A.; WAGNER, D. A. *Time-lock puzzles and timed-release Crypto*. http://theory.lcs.mit.edu/ rivest/RivestShamirWagner-timelock.pdf, Fevereiro 1996.

ROBEY, D.; BOUDREAU, M.-C.; ROSE, G. M. Information technology and organizational learning: A review and assessment of research. *Accounting Management and Information Technologies*, Elsevier Science Ltd., p. 125–155, 2000.

ROOS, M. *Integrating Time-Stamping and Notarization*. Dissertação (Mestrado) — University of Tartu - Estonia, Maio 1999.

ROVAI, A. P. Online and traditional assessments: What is the difference? *Internet and Higher Education*, v. 3, p. 141–151, 2000.

SABO, J. T.; DZAMBASOW, Y. A. Pki policy white paper. *PKI Forum*, março 2001.

SALM, J. F. *EXTENSÕES DA UML PARA DESCREVER PROCESSOS DE NEGÓCIO*. Dissertação (Mestrado) — UFSC, 2003.

SANTOS, A. R. D. *Metodologia Científica: A Construção Do Conhecimento*. 3. ed. Rio de Janeiro: DP&A editora, 2000.

SANTOS, R. B. D. *Gerenciador Virtual de Documentos*. Palhoça, Santa Catarina: [s.n.], 2002.

SANTOS, W. D. *AVALIAÇÃO NA EDUCAÇÃO FÍSICA ESCOLAR - ANÁLISE DE PERIÓDICOS DO SÉCULO XX*. 2002. Http://www.proteoria.net/relatorios. TCC.

SCHEFFEL, G. V. *Segurança Na Avaliação Não Presencial*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, maio 2002.

SCHNEIER, B. *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*. [S.l.]: New York, 1996.

SCRIVEN, M.; STUFFLEBEAM, D. *Avaliação Educacional II: Perspectivas, Procedimentos e Alternativas*. Petrópolis, RJ: Vozes, 1978.

SHAMIR, A. How to share a secret. *Communications of the ACM*, v. 22, n. 11, p. 612–613, Novembro 1979.

SILVA, E. L. D.; MENEZES, E. M. *Metodologia Da Pesquisa e Elaboração de Dissertação*. 3. ed. rev. atual.. ed. Florianópolis: Laboratório de Ensino a Distância da UFSC, 2001.

SMITH, P. L.; RAGAN, T. J. *Instructional Design*. 2. ed. New York, NY: John Wiley & Sons Inc., 1999.

SOUTO, M. A. M.; ZANELLA, R. Ferramentas de suporte a monitoração do aluno em um ambiente inteligente de ensino na web. *XII Simpósio Brasileiro de Informática na Educação - SBIE*, 2001.

STALLINGS, W. *Cryptography and Network Security*. 2. ed. [S.l.]: Prentice Hall, 1998.

STALLINGS, W. *Cryptography and Network Security. Principles and Practice*. [S.l.]: Prentice Hall, New York, 1999.

STANDARDS, N. I. of; TECHNOLOGY. *Secure Hash Standard*. [S.l.], May 1993.

STEWART, R. A.; MOHAMED, S.; DAET, R. Strategic implementation of IT/IS projects in construction: A case study. *Automation in Construction*, Elsevier Science B.V., v. 11, p. 681–694, 2002.

STINSON, D. R. *Cryptography : Theory and Practice*. [S.l.]: CRC Press, 1995.

STINSON, D. R.; WEI, R. Unconditionally secure proactive secret sharing scheme with combinatorial structures. *Selected Areas in Cryptography*, p. 200–214, 1999.

TAKARAGI, K.; MIYAZAKI, K.; TAKAHASHI, M. A threshold digital signature issuing scheme without secret communication. *Submission to the IEEE P1363 Study Group for Future Public-Key Cryptography Standards*, November 2000.

TAO, Y.-H.; HOB, I.-F.; YEH, R. C. Building a user-based model for web executive learning systems - a study of taiwans medium manufacturing companies. *Computers & Education*, v. 36, p. 317–332, 2001.

VERA, A. A. *Metodologia Da Pesquisa Científica*. Porto Alegre, RS: Editora Globo, 1976.

VERBO, E. (Ed.). *Dicionário Enciclopédico Verbo*. fevereiro 2003. Http://enciclopediaverbo.clix.pt/.

VERISIGN. *Total Cost of Ownership for Public Key Infrastructure*. [S.l.], Fevereiro 2002.

VIEGA, J.; MESSIER, M.; CHANDRA, P. *Network Security with OpenSSL*. [S.l.]: O'Reilly, 2002.

WAHL, M.; HOWES, T.; KILLE, S. *Lightweight Directory Access Protocol (v3)*. [S.l.], Dezembro 1997.

WANG, S. Meta-management of virtual organizations: Toward information technology support. *Internet Research: Electronic Networking Applications and Policy*, v. 10, n. 5, p. 451–458, 2000.

WATSON-MANHEIM, M. B.; CROWSTON, K.; CHUDOBA, K. M. Discontinuities and continuities: A new way to understand virtual work. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 2002.

WILCOX, P. A.; GURAU, C. Business modelling withUML: The implementation of CRM systems for online retailing. *Jornal of Retailing and Consumer Service*, v. 10, p. 181–191, 2003.

WOS, E. R. *UMA ABORDAGEM DOCIMOLÓGICA: NUMA VISÃO DE QUALIDADE NO ENSINO*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2002.

YEONG, W.; HOWES, T.; KILLE, S. *Lightweight Directory Access Protocol*. [S.l.], Março 1995.

ZHUGEA, H. et al. A federation-agent-workflow simulation framework for virtual organisation development. *Information & Management*, Elsevier Science B.V., p. 325–336, 2002. Base JDA - pdf.

Apêndice A

Modelagem da avaliação somativa à distância

Este apêndice apresenta a modelagem de uma avaliação somativa à distância adotando a metodologia RUP e a representação UML.

O concurso para contratação de mão de obra, aplicado em vários lugares simultaneamente, é um dos exemplos mais completos de avaliação somativa à distância, sendo que outros modelos de avaliação somativa podem ser obtidos pela sua simplificação.

Assim, o modelo de avaliação somativa à distância modelado neste trabalho tem como base um concurso com o objetivo de certificar e classificar candidatos.

Seguindo a metodologia e a representação propostas são apresentados na seqüência deste documento: título; objetivo; modelo de negócio; regras de negócio; atores do sistema; especificação dos use case do sistema; e realização dos use cases do sistema.

A.1 Título do modelo

Avaliação somativa à distância.

A.2 Objetivo do modelo

Certificar e classificar candidatos.

A.3 Modelo de negócio

O modelo de negócio deve exprimir o que é necessário ao processo para que seja implementado de forma a certificar e classificar um candidato.

Neste caso específico, identificou-se a necessidade de se implementar cinco etapas distintas, porém interdependentes, que para a realização do processo de avaliação. Estas são: negociação e definições iniciais; elaboração; inscrição; aplicação; e correção e divulgação de resultados, cujos escopos são descritos a seguir.

A.3.1 Negociação e definições iniciais

A partir do interesse do contratante, na etapa de definições iniciais são definidas as regras para a implementação do processo de avaliação.

A.3.2 Elaboração

Observada as definições iniciais, inicia-se a fase de elaboração, verificação e escolha das questões a serem utilizadas no instrumento de avaliação.

A.3.3 Inscrição

Em paralelo a elaboração da avaliação a ser aplicada pode-se iniciar a inscrição e homologação dos candidatos.

A.3.4 Aplicação

Em posse da avaliação elaborada e com os candidatos inscritos, pode-se proceder a aplicação dos instrumentos de avaliação.

A.3.5 Correção e divulgação dos resultados

Esta etapa envolve a correção das respostas aos instrumentos de avaliação aplicados, sua interpretação, divulgação das notas, da aprovação (certificação) e da classificação.

A.4 Regras de negócio (requisitos do sistema)

As atividades a serem realizadas para se implementar o modelo de negócio proposto são:

- escolher colaboradores do processo de elaboração de edital
- definir os objetivos da avaliação (somativa, diagnóstica ou formativa)
- definir conteúdo programático (o que avaliar)
- definir um instrumento de avaliação de aplicação viável (praticidade)
- garantir que os procedimentos adotados no processo sejam legais (legalidade)
- definir processo de recepção de inscrição
- elaborar e publicar as regras do processo (edital)
- acolher e responder recursos referentes às regras do processo
- escolher colaboradores do processo de elaboração do instrumento de avaliação
- elaborar questões
- validar questões elaboradas (outro corrige para ver se é apropriada e não será anulada)
- garantir que os que acertem as questões escolhidas sejam aptos a executar as tarefas exigidas para o cargo (escolher questões dentre as elaboradas)
- garantir equalização das questões em relação ao programa
- garantir que as questões discriminem
- montar instrumento de avaliação (impressão ou documento eletrônico, etc...)
- garantir resultado semelhante caso seja aplicada outra avaliação, com outro instrumento, ao mesmo público, sem intervenção formativa (validade)
- garantir que, se fosse possível aplicar outra avaliação, com o mesmo instrumento, ao mesmo público, sem intervenção formativa (confiabilidade), o resultado seja semelhante

- garantir sigilo do processo
- escolher colaboradores do processo de inscrição dos candidatos
- definir campanhas publicitárias
- dar condições de inscrições de candidatos
- homologar e divulgar inscrições
- escolher e divulgar local de aplicação da avaliação
- acolher e responder recursos referentes às homologações
- escolher colaboradores do processo de aplicação do instrumento de avaliação (coordenadores e fiscais)
- aplicar prova (transporte e distribuição)
- fiscalizar aplicação (candidato [identidade e postura] e aplicação [tempo, igualdade de cond.de infra, ...])
- garantir simultaneidade da aplicação
- garantir iguais condições de aplicação
- recolher e encaminhar provas aplicadas
- acolher e responder recursos referentes às questões e aplicação
- escolher colaboradores do processo de correção e divulgação dos resultados
- corrigir as respostas dos candidatos ao instrumento
- garantir igualdade de tratamento na correção (garantindo o sigilo do candidato, tendo vários corretores)
- interpretar o resultado da correção
- verificar aprovação dos candidatos

- classificar candidatos aprovados
- divulgação do resultado preliminar - encaminhar relatório p/ imprensa ou WEB
- acolher e responder recursos referentes às correções e classificação
- divulgação do resultado Final - encaminhar relatório p/ imprensa ou WEB
- tratamento de situações não previstas devem ser encaminhadas, de acordo com a hierarquia, até o coordenador do concurso, se necessário

A.5 Atores do sistema

Os atores que participam deste modelo são:

1.Contratante

- aquele que contrata o processo de seleção

2.Coordenador do Concurso

- aquele que coordena todo o processo

3.Candidato

- aquele que se submete ao processo de avaliação

4.Elaborador de edital

- aquele que elabora as regras do processo

5.Imprensa

- órgão que dá publicidade aos dados (impressa, web, etc...)

6.Equipe de tratamento de recursos

- aquele que recebe e responde os recursos interpostos no âmbito administrativo
- este ator também é responsável por assessorar aspectos jurídicos do edital e de decisões administrativas

7.Coordenador da Elaboração

- aquele que coordena a elaboração do instrumento de avaliação

8.Elaborador de questões

- aquele que elabora as questões do instrumento de avaliação
- preferencialmente composto por uma dupla ou trio

9.Revisor de questões

- aquele que revisa as questões elaboradas

10.Equipe de tratamento de dados

- aquele que dá tratamento computacional aos dados do concurso (candidatos, questões, respostas, listas de classificação, etc..)

11.Equipe de publicidade e propaganda

- aquele que elabora e implementa as campanhas publicitárias para maximizar inscrições

12.Receptor de Inscrição

- aquele que recebe as inscrições (pode ser o caixa da agência bancária)

13.Homologador de inscrição

- aquele que homologa as inscrições
- responsável pela elaboração da logística de aplicação do concurso, envolvendo a definição de espaço físico, distribuição de candidatos, divulgação, etc...

14.Coordenador de aplicação

- aquele que coordena a aplicação
- responsável pelos coordenadores locais

15.Coordenador local de aplicação

- aquele que coordena a aplicação do instrumento em um determinado local
- responsável pelos fiscais

16.Fiscal

- aquele que aplica o instrumento

17.Coordenador de correção

- aquele que coordena a etapa de correção

18.Avaliador de respostas

- aquele que avalia as respostas as questões do instrumento

A.6 Use cases do sistema

O use case geral, envolvendo todos os use cases do sistema, é apresentado através da figura A.1. Note-se que os atores foram suprimidos do diagrama para facilitar a visualização.

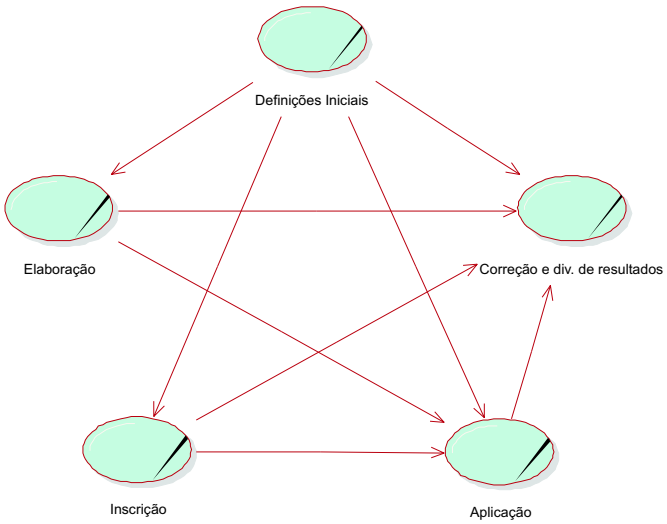

Figura A.1: Diagrama de use case da avaliação

A.7 Especificação dos use cases

Seguindo a metodologia RUP, a especificação dos use cases faz parte da fase de concepção e envolve a descrição de seu objetivo, pré-condições, iniciador, fluxo de atividades principais, alternativas e de exceção. Esta fase envolve ainda a construção dos diagramas de caso de uso, que descreve o contexto do negócio, e o de atividades, que descreve seu comportamento ou os seus fluxos.

Na seqüência deste documento são apresentadas as especificações dos use cases definições iniciais, elaboração das questões e do instrumento de avaliação, inscrição dos candidatos, aplicação do instrumento de avaliação, correção e divulgação dos resultados.

A.7.1 Especificação do use case definições iniciais

A.7.1.1 Objetivo

O objetivo principal desta fase é definir as regras para o processo de avaliação, que culmina com a publicação das mesmas.

A.7.1.2 Pré-condições

- necessidade de mão de obra
- disponibilidade de vaga
- possibilidade legal de contratação

A.7.1.3 Iniciado por

- Contratante

A.7.1.4 Fluxo principal

- contratar elaborador do edital
- elaborar edital
- contratar o receptor de inscrição

- contratar execução
- contratar equipe de tratamento de dados
- contratar equipe de tratamento de recursos
- publicar o edital

A.7.1.5 Fluxo alternativo

- se surgir necessidade de alteração de edital após publicação
  - fazer alteração
  - republicar edital
  - aguardar prazos legais
- se houver recurso administrativo contra o edital
  - receber recursos
  - analisar recurso
    - se procedente
      - atender recurso
      - responder recurso ao impetrante
      - republicar edital
      - aguardar prazos legais
    - se não procedente
      - responder recurso ao impetrante

A.7.1.6 Fluxo de exceção

- caso haja recurso judicial contra o edital
  - defender edital contra o recurso, após citação
    - caso haja liminar

·atender liminar

–se não

∗aguardar decisão

∗acatar decisão

●se detectada ilegalidade não passível de correção

–cancela o concurso

●se fato novo inviabilizar futura contratação de pessoal

–cancela o concurso

A.7.1.7 Pós-condições

●parcerias contratadas

●edital publicado e válido

A.7.1.8 Especificações adicionais

●Atores participantes

–Contratante

–Elaborador de edital

–Receptor de inscrição

–Coordenador do concurso

–Equipe de tratamento de recursos

–Equipe de tratamento de dados

–Imprensa

A.7.1.9 Diagrama de use case

A figura A.2 apresenta o diagrama de use case da fase de negociação e definições iniciais. Nesta diagrama pode-se visualizar os atores envolvidos no processo.

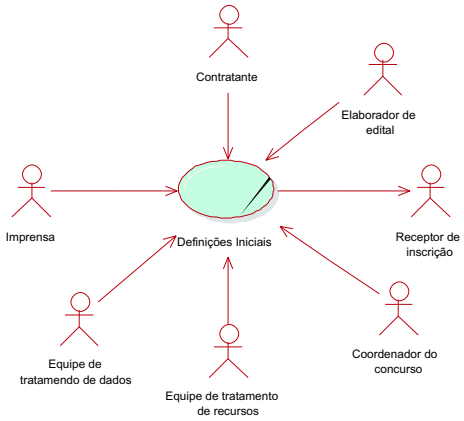

Figura A.2: Diagrama de use case da fase de negociação e definições iniciais

A.7.1.10 Diagrama de atividades

A figura A.3 mostra o diagrama de atividades, do fluxo principal, do use case de negociação e definições iniciais. Através deste pode-se perceber as atividades que devem ser desempenhadas para a execução desta fase do processo.

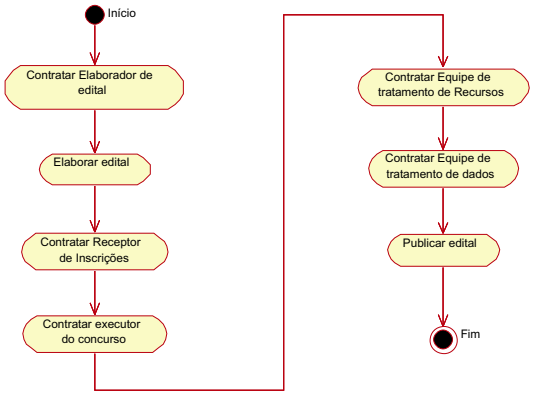

Figura A.3: Diagrama de atividades de negociação e definições iniciais

A.7.2 Especificação do use case elaboração

A.7.2.1 Objetivo

Elaborar, verificar e escolher questões a serem utilizadas no instrumento da avaliação.

A.7.2.2 Pré-condições

●edital publicado na fase de negociação e definições iniciais

A.7.2.3 Iniciado por

●Coordenador do Concurso

A.7.2.4 Fluxo principal

●escolher o coordenador da elaboração

●escolher elaboradores e revisores

●elaborar questões

●revisar as questões elaboradas

●escolher as questões a serem utilizadas

●montar instrumento de avaliação

A.7.2.5 Fluxo alternativo

●se não for encontrado elaborador com o perfil apropriado

–exigir que questões sejam elaboradas por uma comissão

●se questões solicitadas não retornarem

–encaminha para outro elaborador

●se revisor encontrar problema nas questões elaboradas

–se problemas detectados forem pequenos ou de forma

∗corrigir e submeter à aprovação do elaborador

–se não

∗se o problema da questão for exceção, no que tange a abrangência do programa ou na qualidade da questão

·solicitar nova questão ao elaborador

∗se não

·solicita questão a outro elaborador

·retira elaborador original do quadro de elaboradores

–se questões retornadas de um elaborador não obedecerem o nível de dificuldade (ou proporção) solicitado

∗se exceção

·solicita outra(s) questão(ões) ao elaborador

∗se não

·encaminha solicitação a outro elaborador

A.7.2.6 Fluxo de exceção

●se ocorrer fatores que inviabilizam o concurso

–reunião com o coordenador do concurso

–parar o trabalho em andamento

–receber e armazenar o trabalho já concluído

–pagar trabalho executado

–desmobilizar equipe

A.7.2.7 Pós-condições

●banco de questões disponível

●instrumento de avaliação disponível

A.7.2.8 Especificações adicionais

- Atores participantes
  - Coordenador do concurso
  - Coordenador de elaboração
  - Elaborador de questões
  - Revisor de questões
  - Equipe de tratamento de dados

A.7.2.9 Diagrama de use case

A figura A.4 apresenta o diagrama de use case da fase de elaboração. Nesta diagrama pode-se visualizar os atores envolvidos no processo.

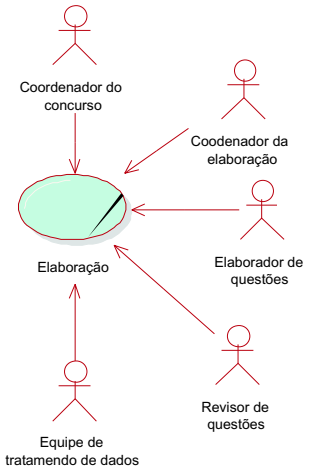

Figura A.4: Diagrama de use case da fase de elaboração

A.7.2.10 Diagrama de atividades

A figura A.5 mostra o diagrama de atividades, do fluxo principal, envolvidas na elaboração das questões.

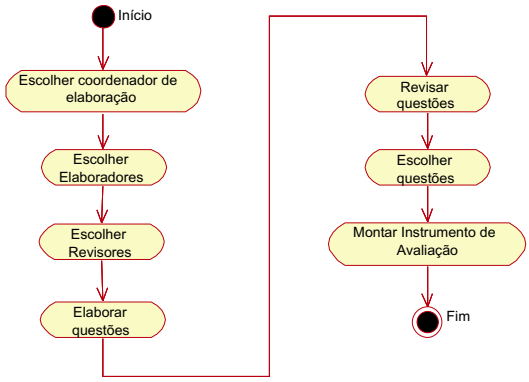

Figura A.5: Diagrama de atividades da fase de elaboração

A.7.3 Especificação do use case inscrição

A.7.3.1 Objetivo

Promover e permitir inscrição por parte dos candidatos

A.7.3.2 Pré-condições

- edital publicado na fase de negociação e definições iniciais

A.7.3.3 Iniciado por

- Coordenador do Concurso

A.7.3.4 Fluxo principal

- contratar homologador de inscrições
- contratar campanhas publicitárias
- receber inscrições do receptor de inscrição
- homologar inscrições
- contratar locais de aplicação do instrumento de avaliação
- divulgar homologação e local de aplicação

A.7.3.5 Fluxo alternativo

- ●se o número de inscrições for insuficiente para viabilizar o concurso
  - –prorrogação dos prazos do concurso
  - –contratar campanhas publicitárias
- ●se ocorrer mudanças quanto ao local de aplicação
  - –comunicação aos candidatos
  - –se tempo exíguo
    - ∗prorrogação dos prazos do concurso
- ●se houver recurso administrativo contra o edital
  - –receber recursos
  - –analisar recurso
    - ∗se procedente
      - ·atender recurso
      - ·responder recurso ao impetrante
      - ·republicar homologados
      - ·aguardar prazos legais
    - ∗se não procedente
      - ·responder recurso ao impetrante

A.7.3.6 Fluxo de exceção

- ●caso haja recurso judicial contra o edital
  - –defender edital contra o recurso, após citação
    - ∗caso haja liminar
      - ·atender liminar
  - –se não

∗aguardar decisão

∗acatar decisão

●se concurso anulado (inclusive por decisão judicial)

–atender previsões pertinentes do edital

–se não houver previsões pertinentes

∗tomar decisões administrativas

A.7.3.7 Pós-condições

●banco de dados de candidatos homologados com seus respectivos locais de avaliação

A.7.3.8 Especificações adicionais

●Atores Participantes

–Coordenador do concurso

–Equipe de publicidade e propaganda

–Receptor de Inscrição

–Candidato

–Equipe de tratamento de dados

–Homologador de inscrição

–Imprensa

–Equipe de tratamento de recursos

A.7.3.9 Diagrama de use case

A figura A.6 apresenta o diagrama de use case da fase de inscrição. Nesta diagrama pode-se visualizar os atores envolvidos neste processo.

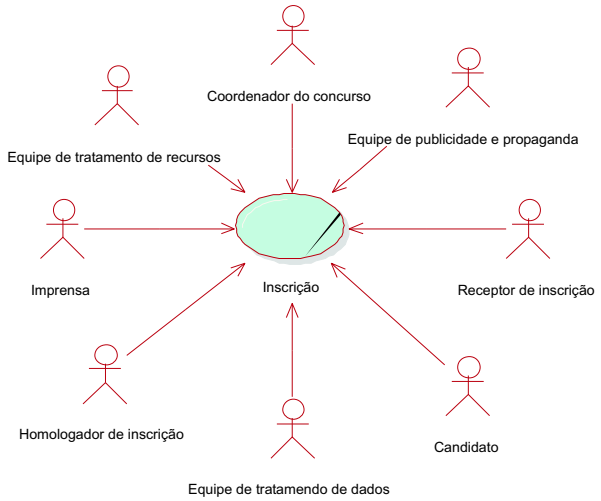

Figura A.6: Diagrama de use case da fase de inscrição

A.7.3.10 Diagrama de atividades

A figura A.7 mostra o diagrama de atividades que devem ser desempenhadas para a execução desta fase do processo.

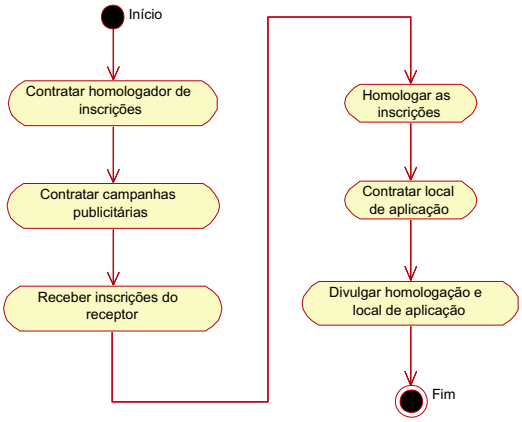

Figura A.7: Diagrama de atividades da fase de inscrição

A.7.4 Especificação do use case aplicação

A.7.4.1 Objetivo

Aplicação dos instrumentos de avaliação aos candidatos homologados

A.7.4.2 Pré condições

●etapas de elaboração e inscrição concluídas

A.7.4.3 Iniciado por

●Coordenador do Concurso

A.7.4.4 Fluxo principal

●escolher o coordenador da aplicação

●escolher coordenadores locais e fiscais

●capacitar da equipe de campo

●transportar e distribuir os instrumentos de aplicação aos coordenadores de aplicação local

●preparar locais (identicação)

●transportar e distribuir os instrumentos de aplicação aos fiscais

●controlar acesso dos candidatos

●controlar aplicação do instrumento de avaliação

●receber respostas ao instrumento de avaliação

●conferir material de respostas entregues pelo candidato

●preencher ata de aplicação

●transportar respostas e atas ao coordenador local

●conferir material entregue pelos fiscais

- transportar respostas e atas ao coordenador de aplicação
- conferir material entregue pelos coordenadores locais

A.7.4.5 Fluxo alternativo

- se candidato falta
  - registro em ata
- se candidato chega atrasado
  - é impedido de participar do processo, considerado faltante
- se candidato transgride alguma regra ao fazer o concurso
  - se não atrapalhar outros
    - é registrado em ata
  - se perturbar
    - é retirado do processo de aplicação
    - faz-se registro em ata
- se o local de aplicação se torna inviável
  - escolher novo local e divulgá-lo
  - manter equipe para receber candidatos no local original
- se faltar algum membro da equipe de aplicação
  - se coordenador
    - executar plano de contingência
  - se fiscal
    - acionar fiscais suplentes
- se os instrumentos de avaliação não chegam a tempo
  - retardar início

–buscar formas alternativas de obter e duplicar instrumento de avaliação

●se faltar instrumentos de avaliação para algum candidato

–retardar início

–duplicar instrumento de avaliação

●se houver conflito de documentos em um candidato que se apresenta para se submeter a avaliação

–permitir que o candidato participe do processo

–detalhar o conflito em ata

●se conferência candidato presente / respostas entregues não conferir

–registrar em ata

A.7.4.6 Fluxo de exceção

●se o sigilo da prova ficar comprometido como um todo

–anula-se a etapa de elaboração e aplicação

●se o sigilo da prova ficar comprometido parcialmente

–caso esta situação não esteja prevista em edital

∗anula-se a etapa de elaboração e aplicação

–se não

∗atende o previsto

●se um local de aplicação se torna inviável, no momento de aplicação

–caso esta situação não esteja prevista em edital

∗anula-se a etapa de elaboração e aplicação

–se não

∗atende o previsto

- se as respostas de uma sala não forem entregues
  - caso esta situação não esteja prevista em edital
    - anula-se a etapa de elaboração e aplicação
  - se não
    - atende o previsto
- se as respostas de um local de aplicação não forem entregues
  - caso esta situação não esteja prevista em edital
    - anula-se a etapa de elaboração e aplicação
  - se não
    - atende o previsto
- caso haja recurso judicial
  - defender contra o recurso, após citação
    - caso haja liminar
      - atender liminar
  - se não
    - aguardar decisão
    - acatar decisão

A.7.4.7 Pós-condições

- respostas dos candidatos ao instrumento de avaliação entregues ao coordenador de aplicação

A.7.4.8 Especificações adicionais

- Atores participantes
  - Coordenador do concurso

–Coordenador de aplicação

–Coordenador local de aplicação

–Fiscal

–Candidato

A.7.4.9 Diagrama de use case

A figura A.8 apresenta o diagrama de use case da fase de aplicação do instrumento de avaliaçào. Nesta diagrama pode-se visualizar os atores envolvidos neste processo.

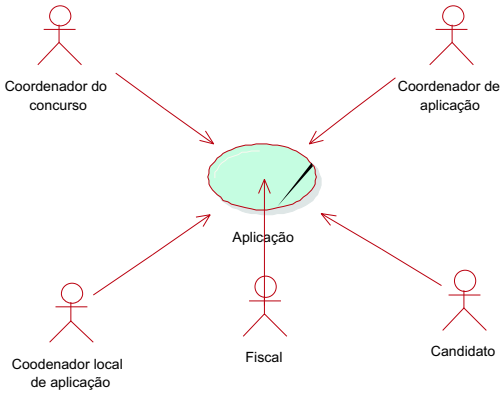

Figura A.8: Diagrama de use case da fase de aplicação

A.7.4.10 Diagrama de atividades

A figura A.9 mostra o diagrama de atividades, do fluxo principal, que devem ser desempenhadas para a execução desta fase do processo.

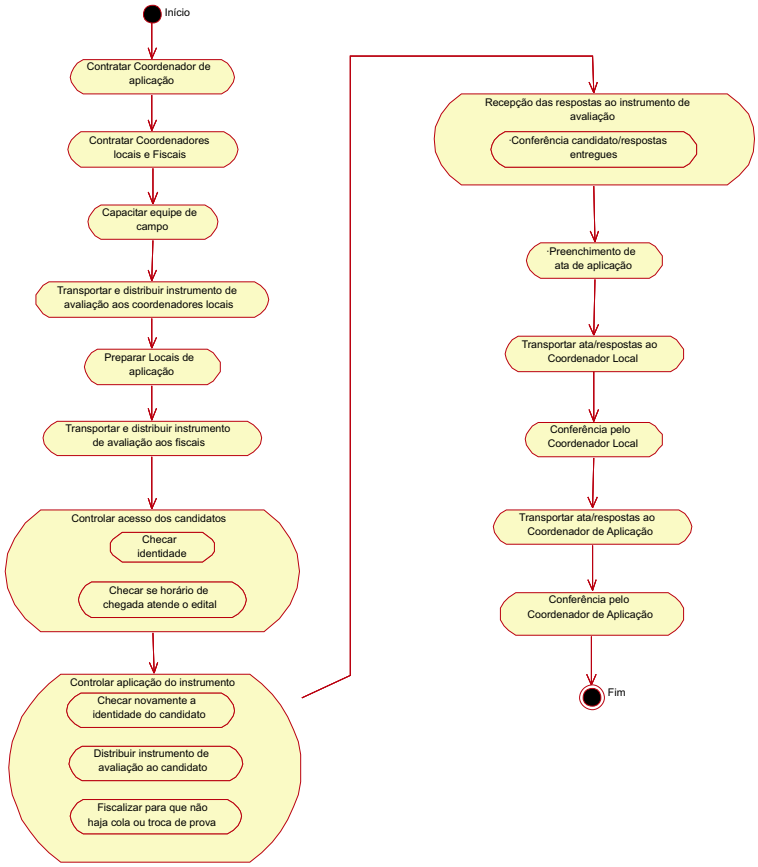

Figura A.9: Diagrama de atividades da fase de aplicação

A.7.5 Especificação do use case correção e divulgação dos resultados

A.7.5.1 Objetivo

Certificar e classificar os candidatos segundo suas respostas ao instrumento de avaliação

A.7.5.2 Pré condições

- Etapa de aplicação concluída

A.7.5.3 Iniciado por

- Coordenador do Concurso

A.7.5.4 Fluxo principal

- contratar coordenação de correção
- contratar avaliadores de respostas
- atribuir nota às respostas das questões objetivas
- distribuir cópias das respostas às questões discursivas para dois avaliadores, com supressão dos dados do candidato
- receber avaliações dadas para cada resposta das questões discursivas
- atribuir nota às respostas das questões discursivas
- atribuir nota para cada candidato
- identificar e classificar candidatos aprovados
- identificar candidatos classificados em relação às vagas disponíveis
- divulgar resultado preliminar
- divulgar resultado final

A.7.5.5 Fluxo alternativo

- se houver divergência flagrante na avaliação de resposta a mesma questão dissertativa de um candidato
  - enviar resposta a um terceiro avaliador
  - calcular a média desta terceira avaliação com a mais próxima das outra duas
- se houver recursos administrativos contra às questões
  - receber recursos
  - analisar recurso
  - envia recurso aos elaboradores devidos
    - se procedente

·anula a questão, pontuando-a para todos os candidatos

·responder recurso ao impetrante

·divulga a todos

∗se não procedente

·armazenar resposta fundamentada do elaborador

·indeferir recurso

·informar o recorrente que seu recurso foi indeferido

●se houver recursos administrativos contra a correção

–receber recursos

–analisar recurso

–conferir resposta do candidato com os dados armazenados na avaliação

–envia recurso aos avaliadores devidos

∗se procedente

·pontua a questão

·reclassificação dos candidatos aprovados

·divulga a todos

∗se não procedente

·armazenar resposta fundamentada do avaliador

·indeferir recurso

·informar o recorrente que seu recurso foi indeferido

A.7.5.6 Fluxo de exceção

●caso haja recurso judicial contra a correção

–defender contra o recurso, após citação

∗caso haja liminar

·atender liminar

–se não

∗aguardar decisão

∗acatar decisão

A.7.5.7 Pós-condições

●resultado final (classificação dos candidatos aprovados) homologado

A.7.5.8 Especificações adicionais

●Atores participantes

–Coordenador do concurso

–Coordenador de correção

–Equipe de tratamento de recursos

–Equipe de tratamento de dados

–Avaliador de respostas

–Elaborador de questões

–Imprensa

A.7.5.9 Diagrama de use case

A figura A.10 apresenta o diagrama de use case da fase de correção e divulgação dos resultados. Nesta diagrama pode-se visualizar os atores envolvidos neste processo.

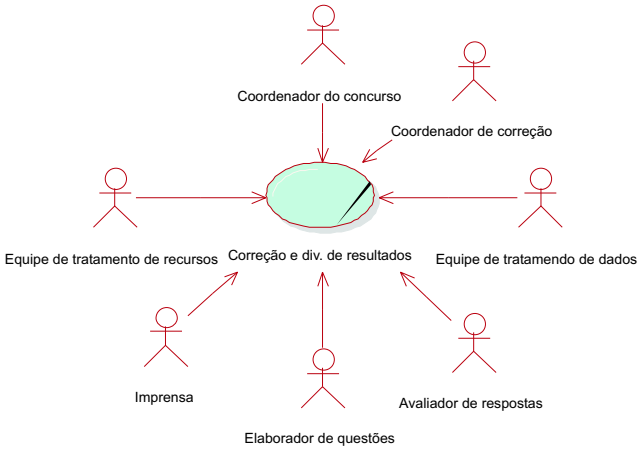

Figura A.10: Diagrama de use case da fase de correção e divulgação dos resultados

A.7.5.10 Diagrama de atividades

A figura A.11 mostra o diagrama de atividades, do fluxo principal, que devem ser desempenhadas para a execução desta fase do processo.

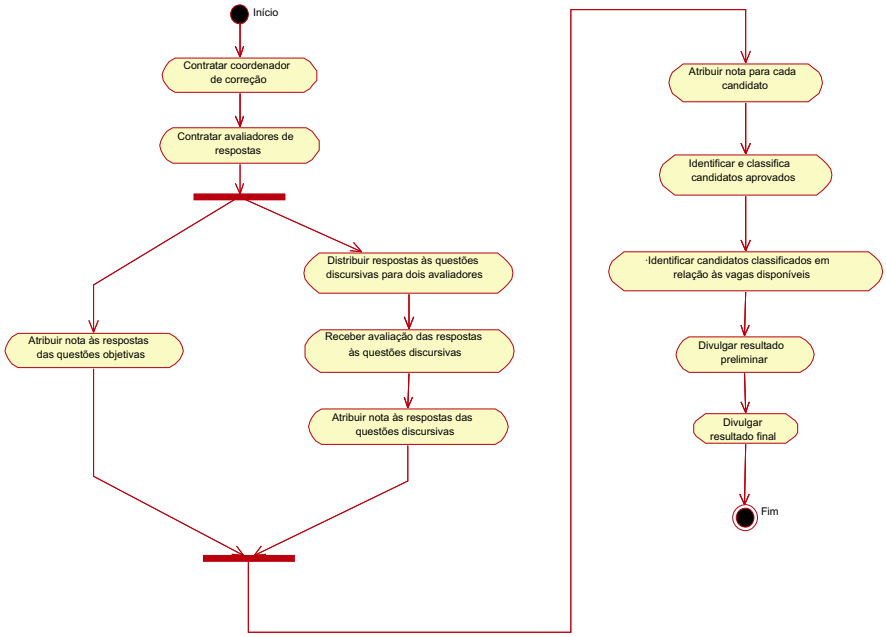

Figura A.11: Diagrama de atividades da fase de correção e divulgação dos resultados

A.8 Realização dos use cases

A realização de use cases envolve a construção dos diagramas de: classes participantes, que descreve uma estrutura estática do negócio; seqüência, que descreve as interações dinâmicas entre os atores e o que eles estão manipulando; e de estado, que permite uma análise dos estados de espera do sistema.

Os esteriótipos de classe utilizados nesses diagramas são o de interface, de controle e persistente, que são explicados na seção 4.4.3.1. Como esta modelagem se refere aos processos sendo executados de forma genérica e manual, neste modelo as classes podem representar, respectivamente:

- de interface
  - opções e formulários
- de controle
  - ações em função das opções escolhidas
- persistente
  - documentos em papel

A figura A.12 apresenta o diagrama de realização dos use cases.

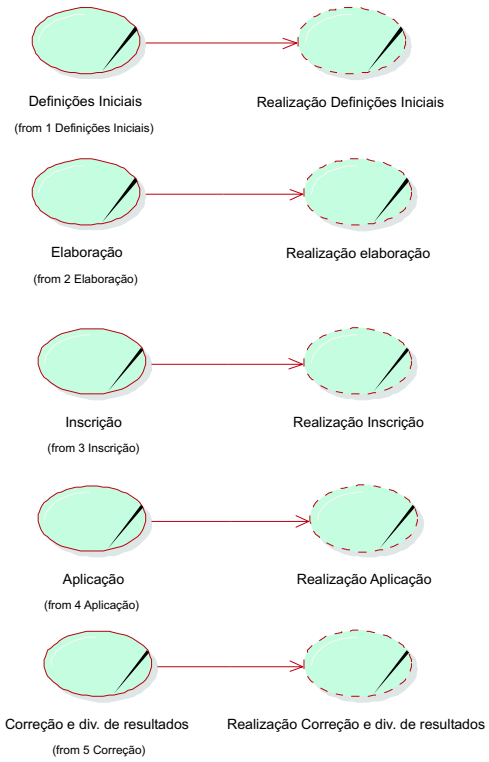

Figura A.12: Diagrama de realização da avaliação

Na seqüência deste documento são apresentadas as realizações dos use cases definições iniciais, elaboração das questões e do instrumento de avaliação, inscrição dos candidatos, aplicação do instrumento de avaliação, correção e divulgação dos resultados.

A.8.1 Realização do use case definições iniciais

A.8.1.1 Diagrama de classes participantes

Através do diagrama de classes participantes apresentado na figura A.13, percebe-se as classes interface, controle e persistente que estão envolvidos neste processo.

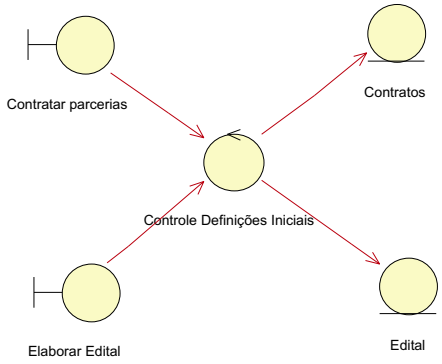

Figura A.13: Diagrama de classes participantes da fase de negociação e definições iniciais

A.8.1.2 Diagrama de seqüência

Os diagramas de seqüência apresentado nas figuras A.14, A.15 e A.16 representam as interações entre os atores a as classes participantes deste use case relativas ao seu fluxo principal de atividades.

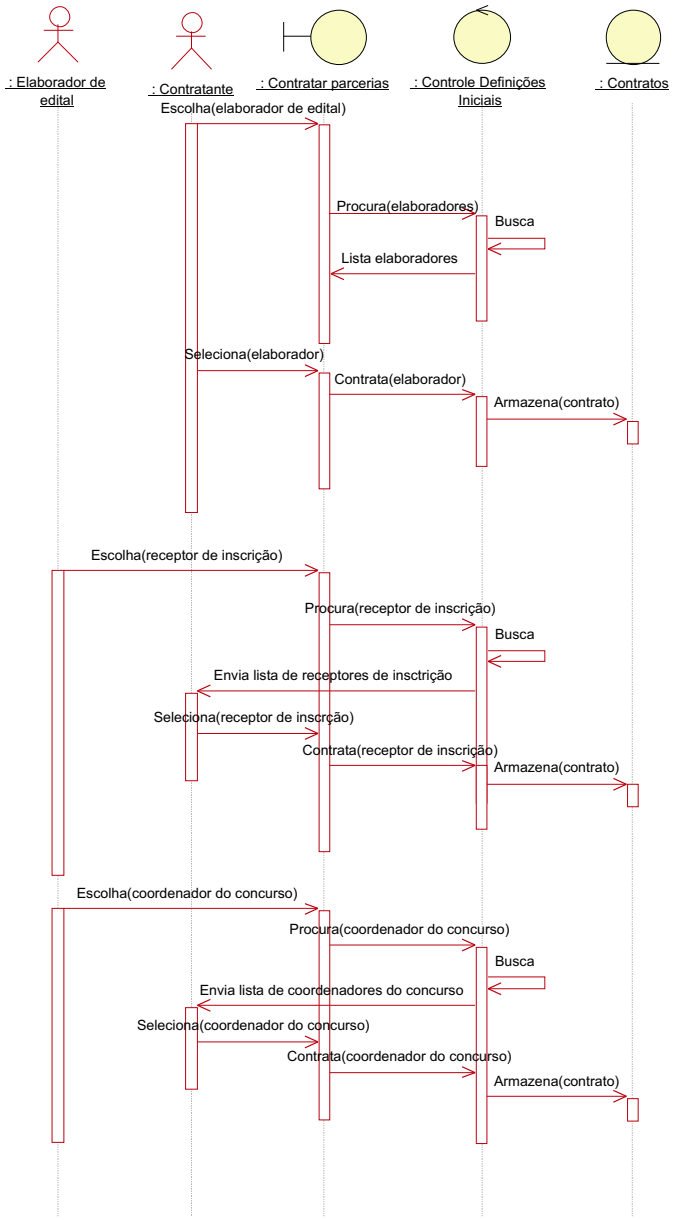

Figura A.14: Diagrama de seqüência 1 da fase de negociação e definições iniciais

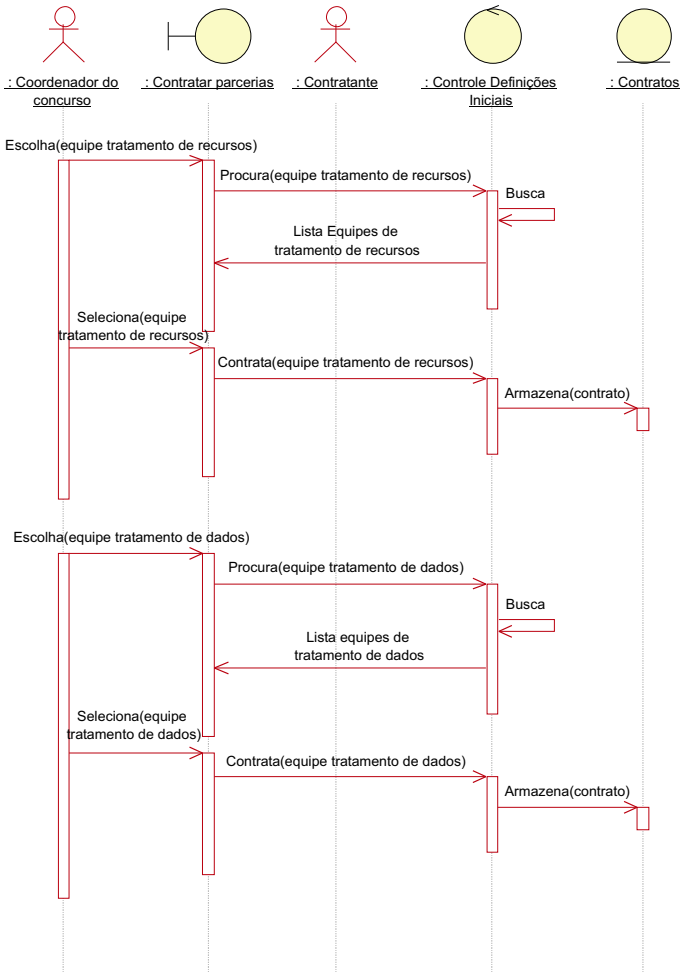

Figura A.15: Diagrama de seqüência 2 da fase de negociação e definições iniciais

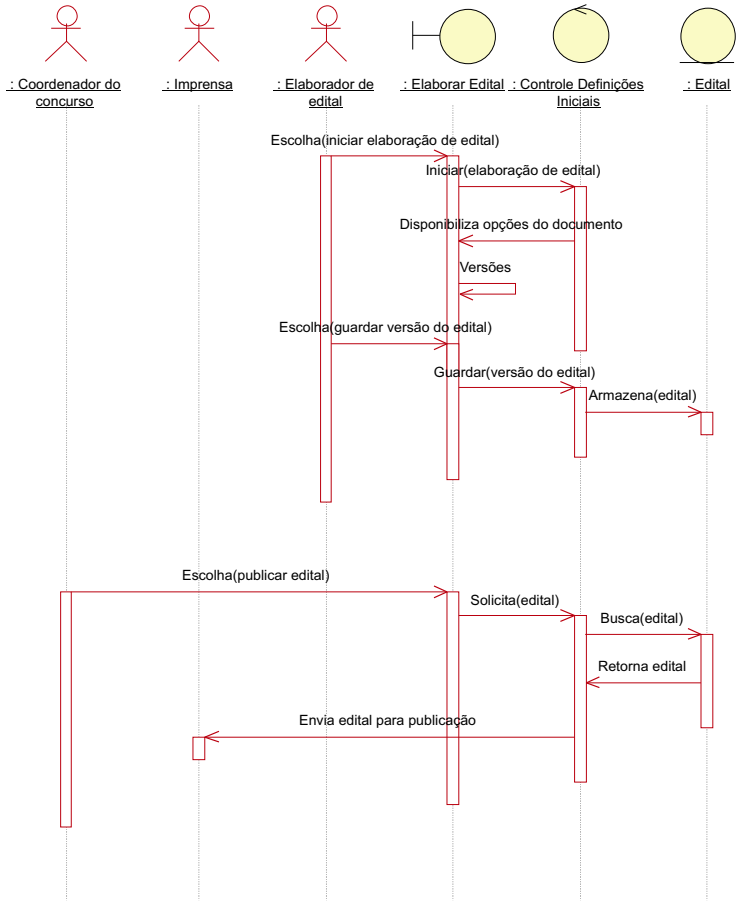

Figura A.16: Diagrama de seqüência 3 da fase de negociação e definições iniciais

A.8.1.3 Diagrama de estados

A figura A.17 apresenta o diagrama de estado deste use case.

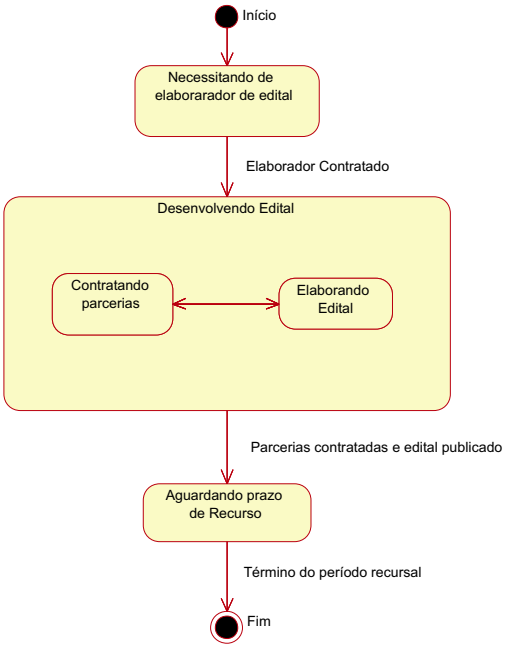

Figura A.17: Diagrama de estados da fase de negociação e definições iniciais

A.8.2 Realização do use case elaboração

A.8.2.1 Diagrama de classes participantes

Através do diagrama de classes participantes apresentado na figura A.18, percebe-se as classes interface, controle e persistente que estão envolvidos neste processo.

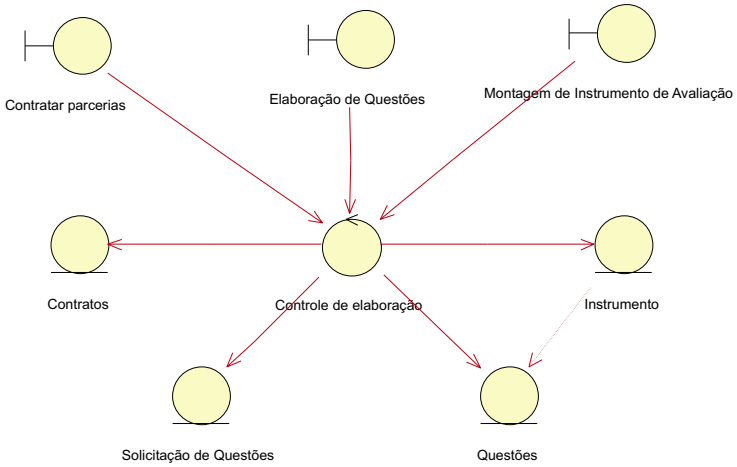

Figura A.18: Diagrama de classes participantes da fase de elaboração

A.8.2.2 Diagrama de seqüência

Os diagramas de seqüência apresentado nas figuras A.19, A.20 e A.21 representam as interações entre os atores a as classes participantes deste use case relativas ao seu fluxo principal de atividades.

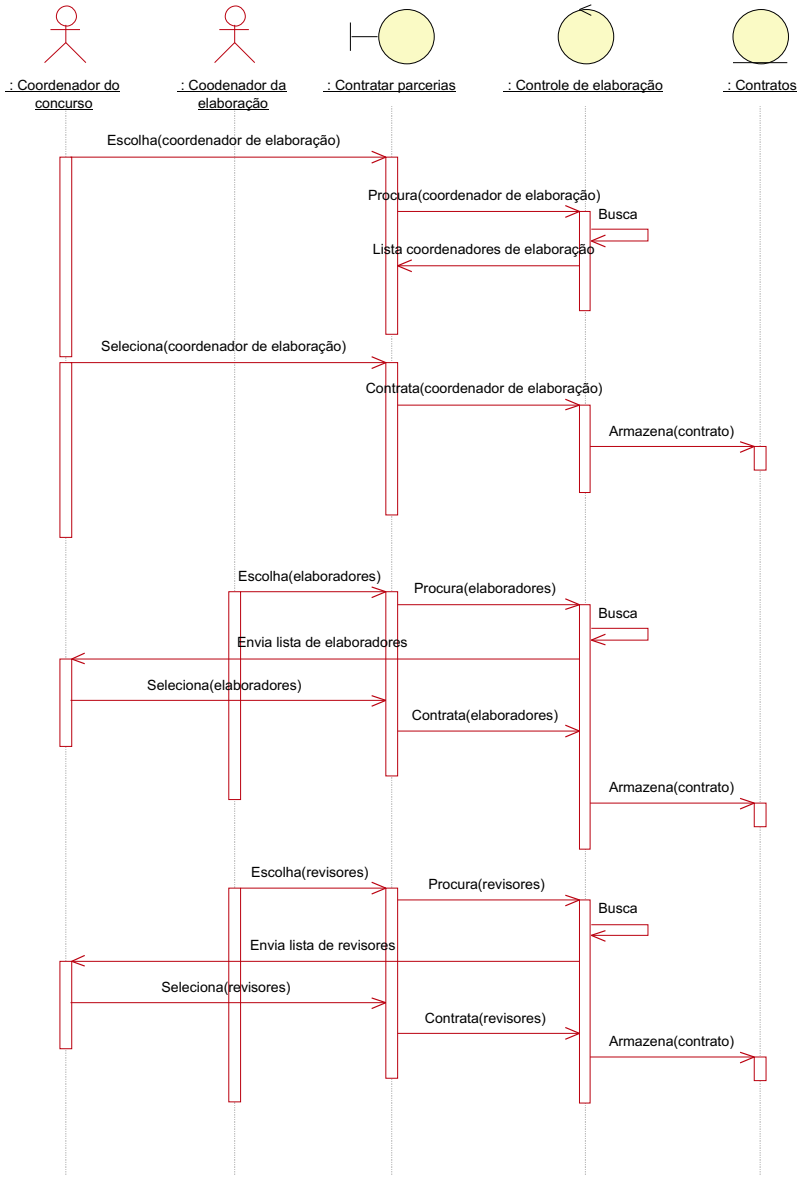

Figura A.19: Diagrama de seqüência 1 da fase de elaboração

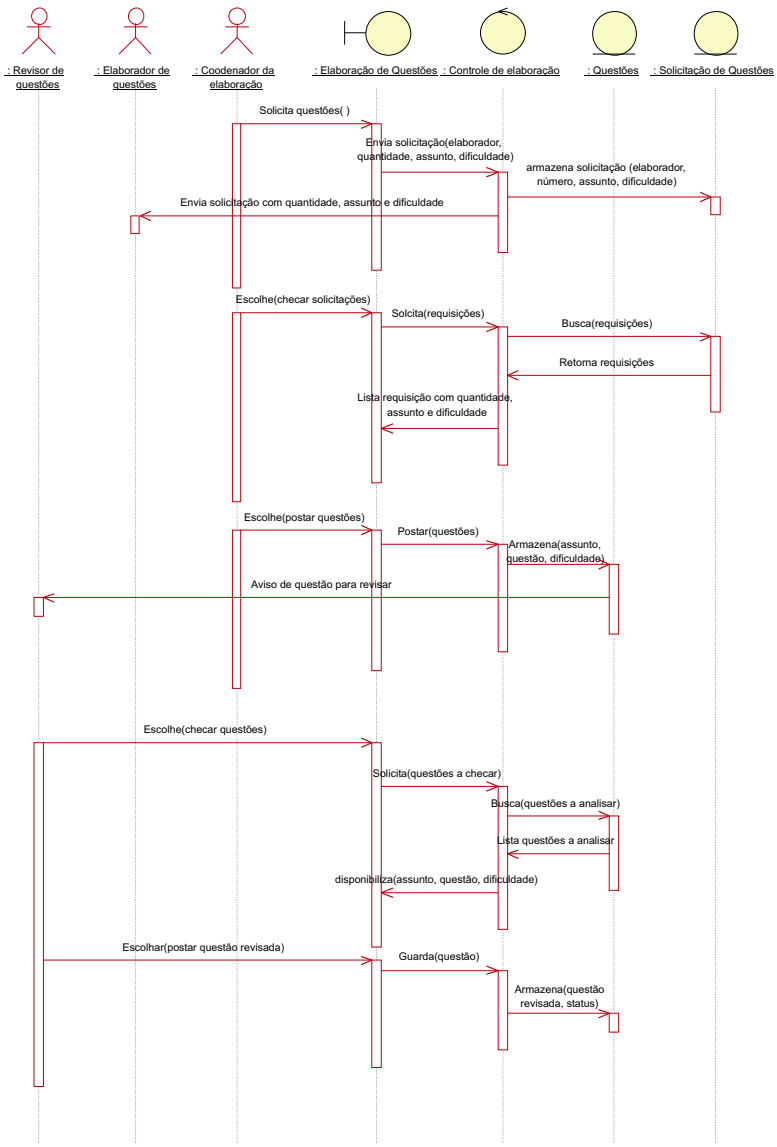

Figura A.20: Diagrama de seqüência 2 da fase de elaboração

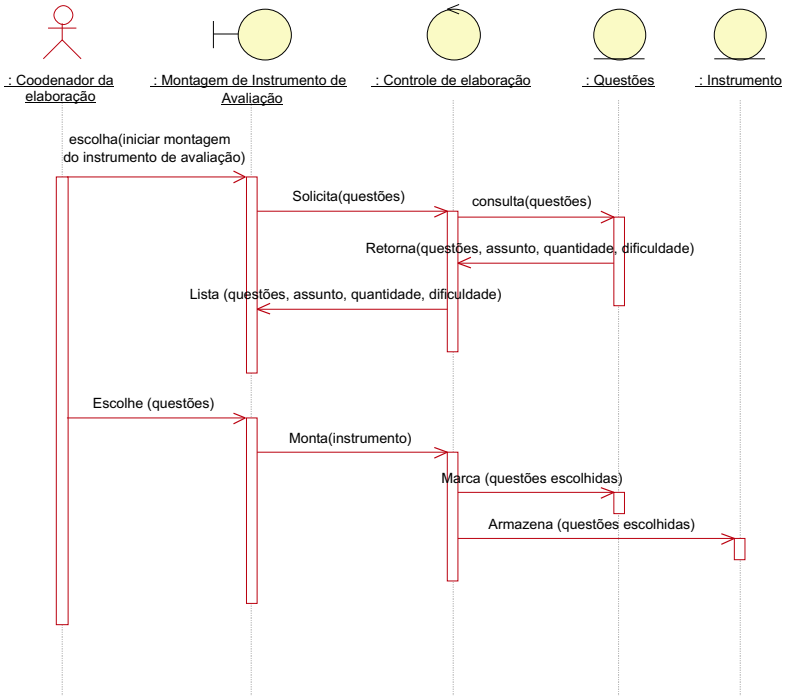

Figura A.21: Diagrama de seqüência 3 da fase de elaboração

A.8.2.3 Diagrama de estados

A figura A.22 apresenta o diagrama de estado deste use case.

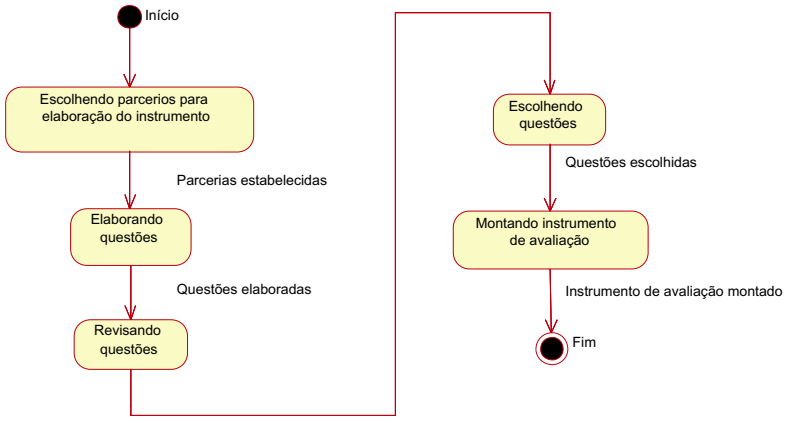

Figura A.22: Diagrama de estados da fase de elaboração

A.8.3 Realização do use case inscrição

A.8.3.1 Diagrama de classes participantes

Através do diagrama de classes participantes apresentado na figura A.23, percebe-se as classes interface, controle e persistente que estão envolvidos neste processo.

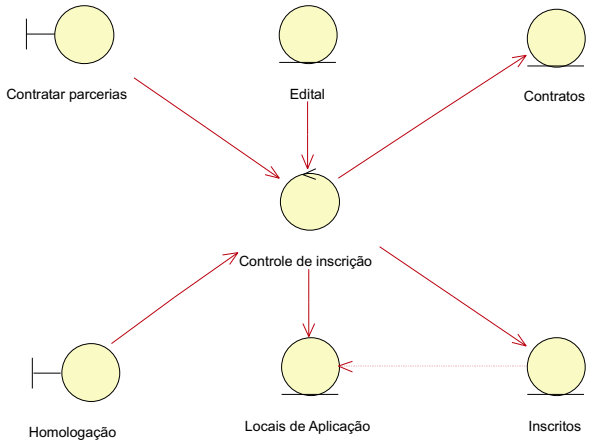

Figura A.23: Diagrama de classes participantes da fase de inscrição

A.8.3.2 Diagrama de seqüência

Os diagramas de seqüência apresentado nas figuras A.24, A.25, A.26 e A.27 representam as interações entre os atores a as classes participantes deste use case relativas ao seu fluxo principal de atividades.

Figura A.24: Diagrama de seqüência 1 da fase de inscrição

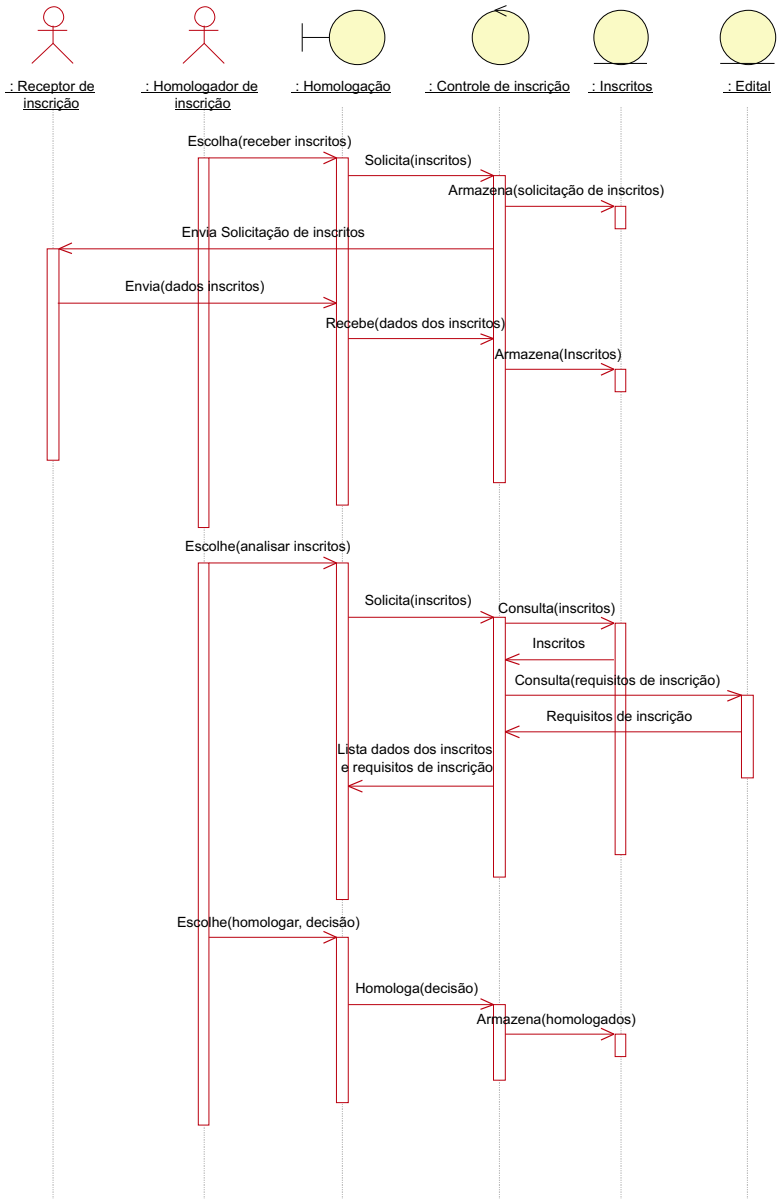

Figura A.25: Diagrama de seqüência 2 da fase de inscrição

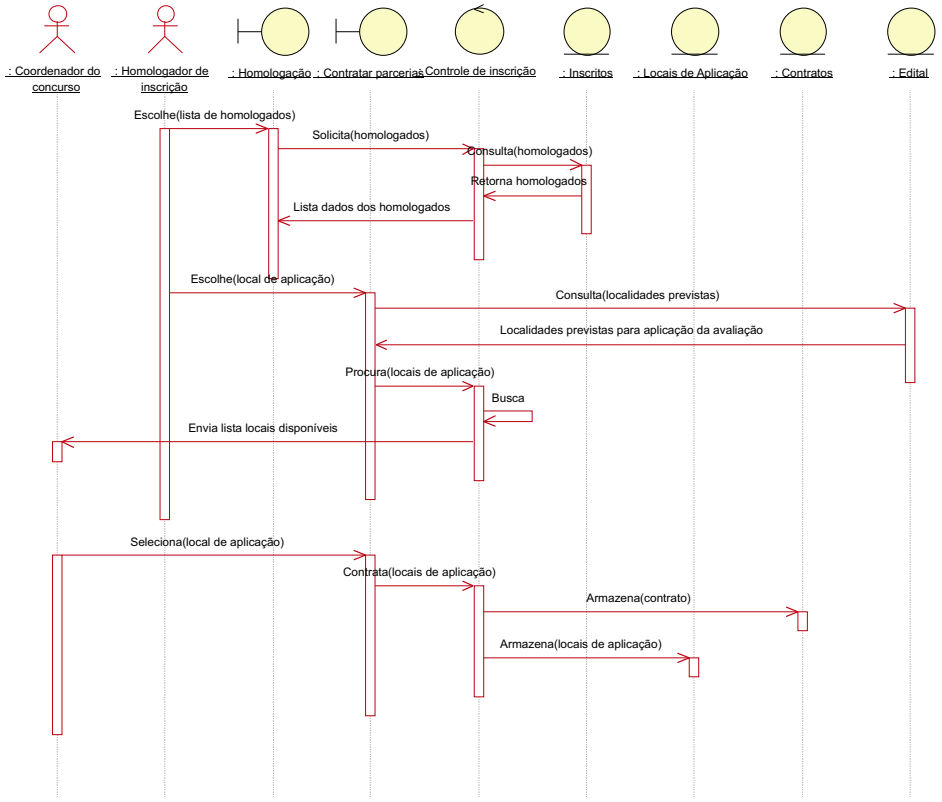

Figura A.26: Diagrama de seqüência 3 da fase de inscrição

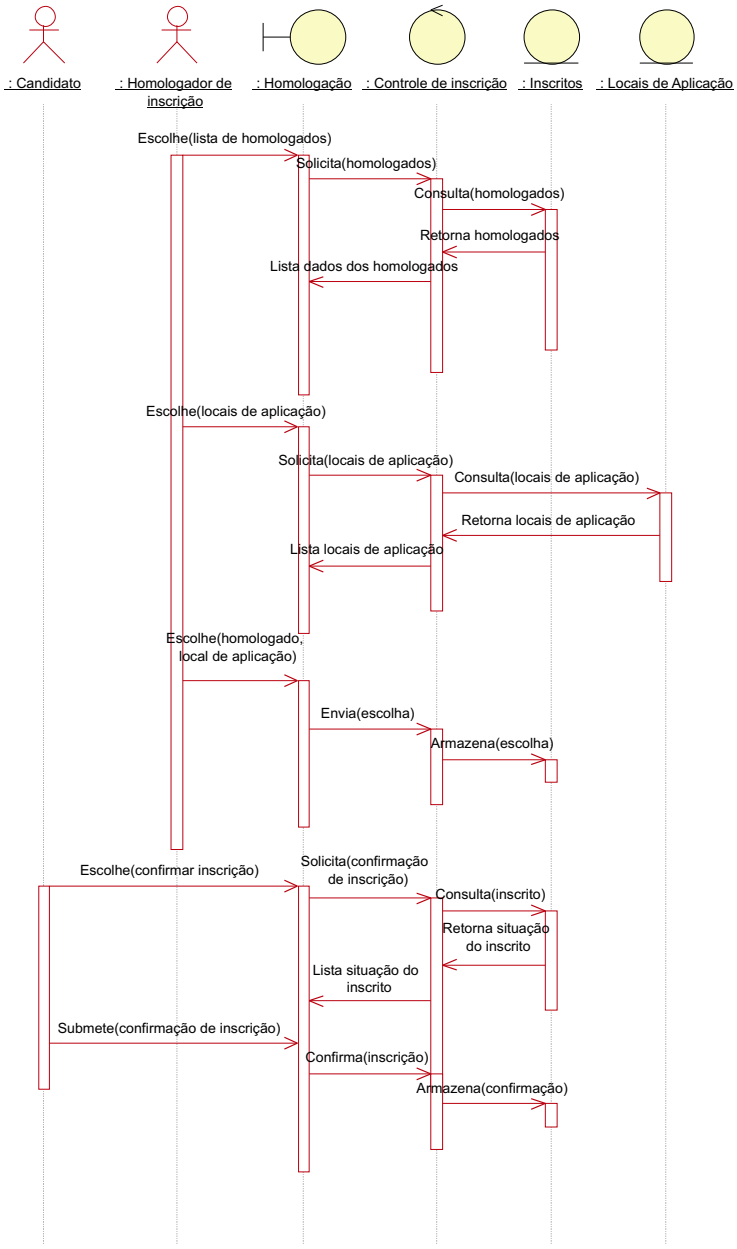

Figura A.27: Diagrama de seqüência 3 da fase de inscrição

A.8.3.3 Diagrama de estados

A figura A.28 apresenta o diagrama de estado deste use case.

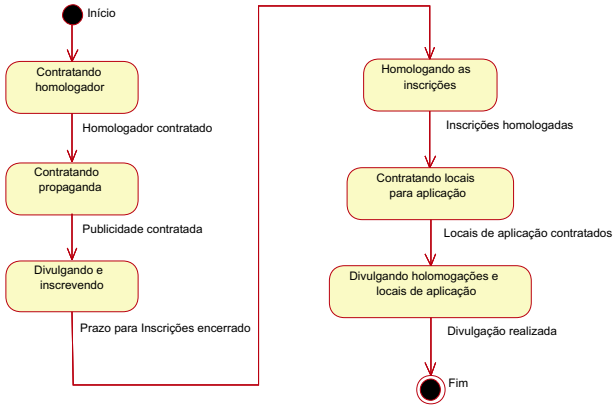

Figura A.28: Diagrama de estados da fase de inscrição

A.8.4 Realização do use case aplicação

A.8.4.1 Diagrama de classes participantes

Através do diagrama de classes participantes apresentado na figura A.29, percebe-se as classes interface, controle e persistente que estão envolvidos neste processo.

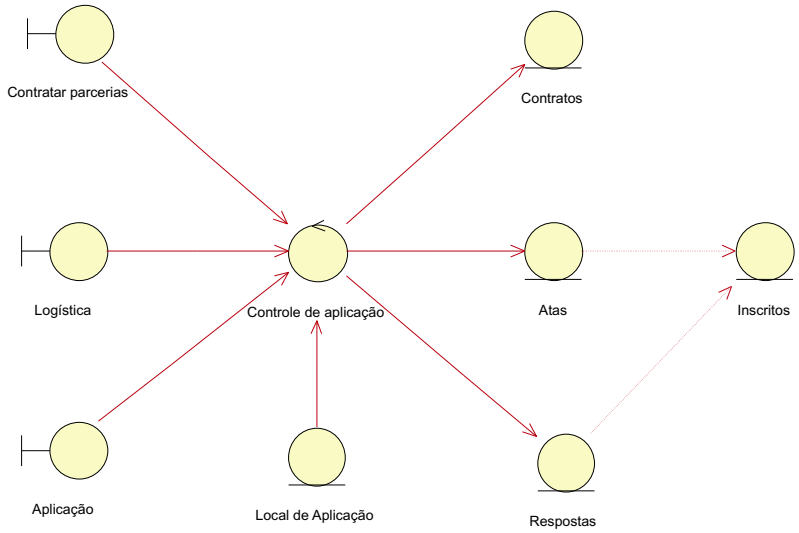

Figura A.29: Diagrama de classes participantes da fase de aplicação

A.8.4.2 Diagrama de seqüência

Os diagramas de seqüência apresentado nas figuras A.30, A.31, A.32 e A.33 representam as interações entre os atores a as classes participantes deste use case relativas ao seu fluxo principal de atividades.

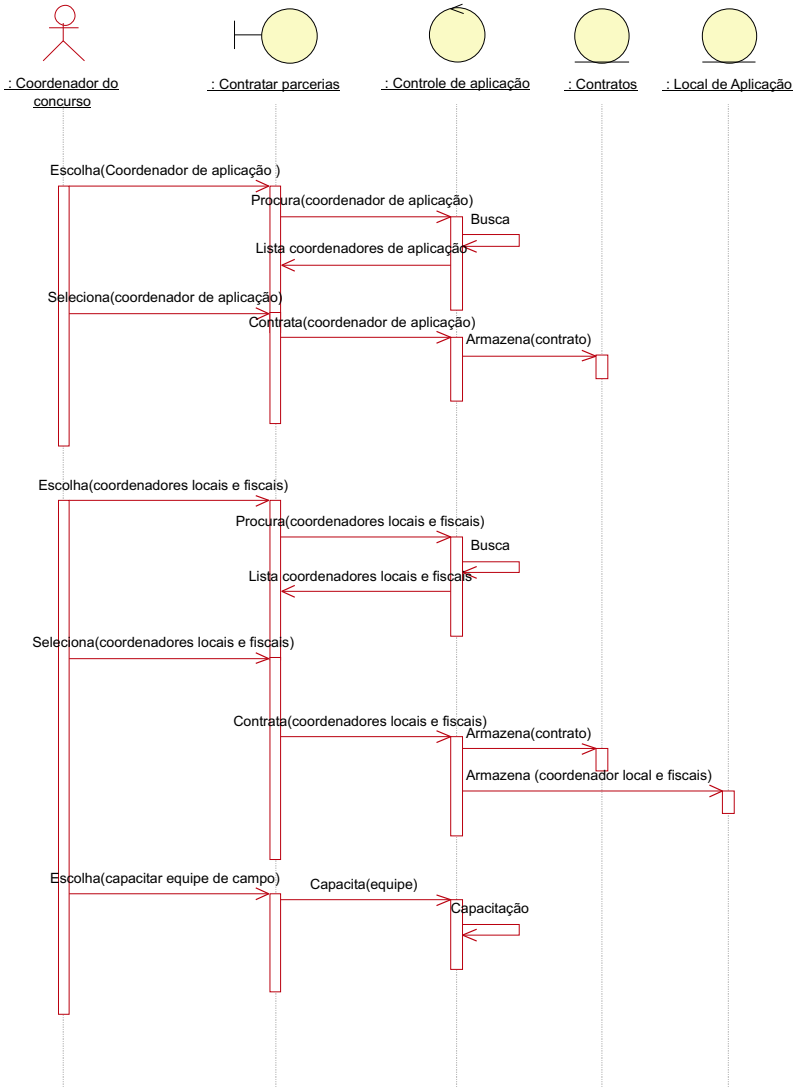

Figura A.30: Diagrama de seqüência 1 da fase de aplicação

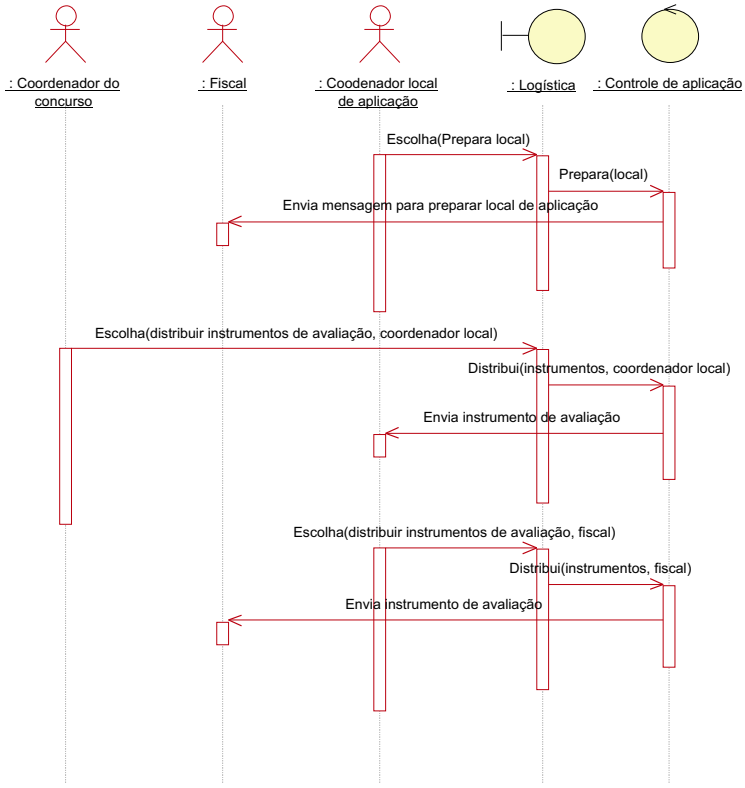

Figura A.31: Diagrama de seqüência 2 da fase de aplicação

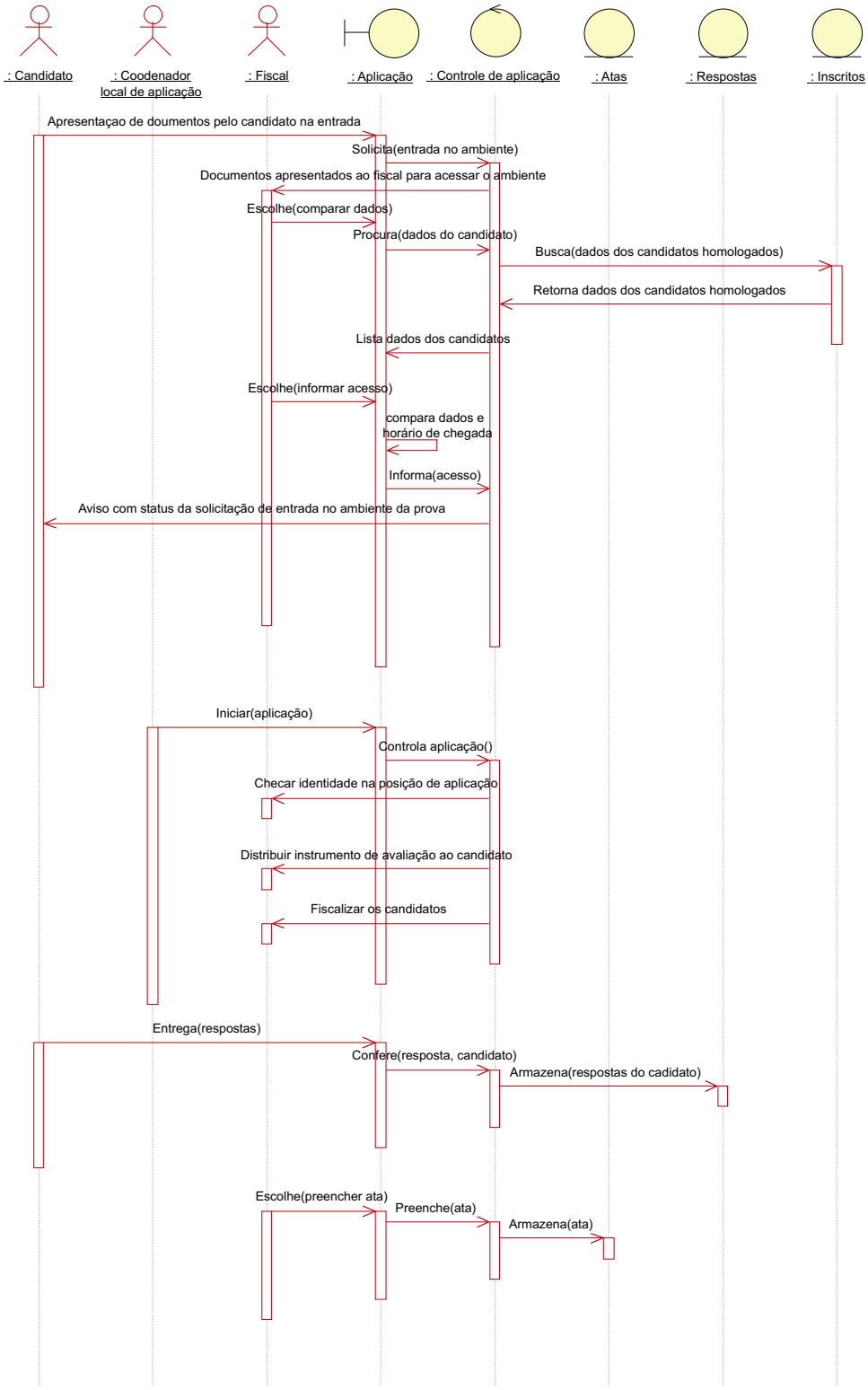

Figura A.32: Diagrama de seqüência 3 da fase de aplicação

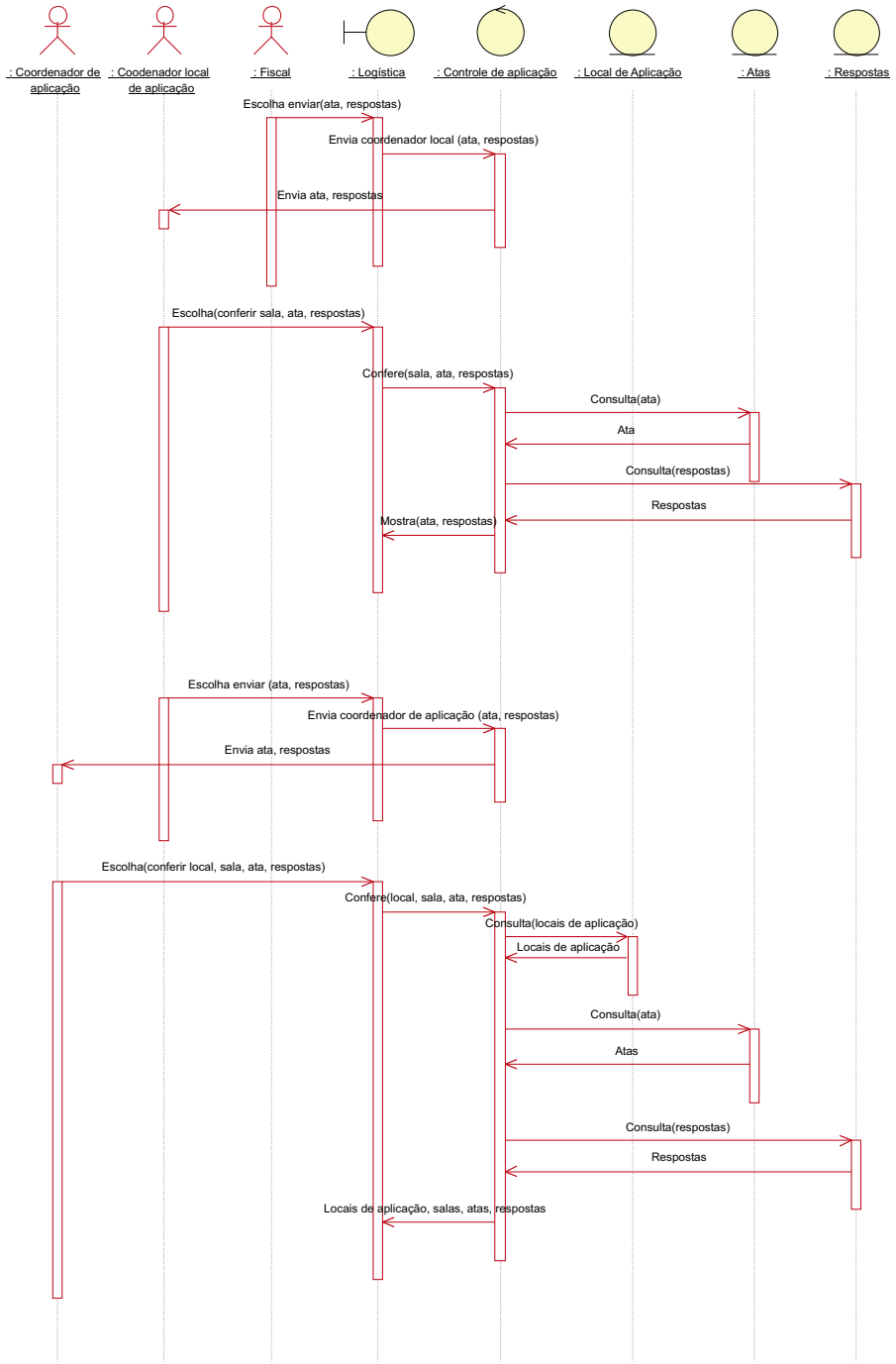

Figura A.33: Diagrama de seqüência 4 da fase de aplicação

A.8.4.3 Diagrama de estados

A figura A.34 apresenta o diagrama de estado deste use case.

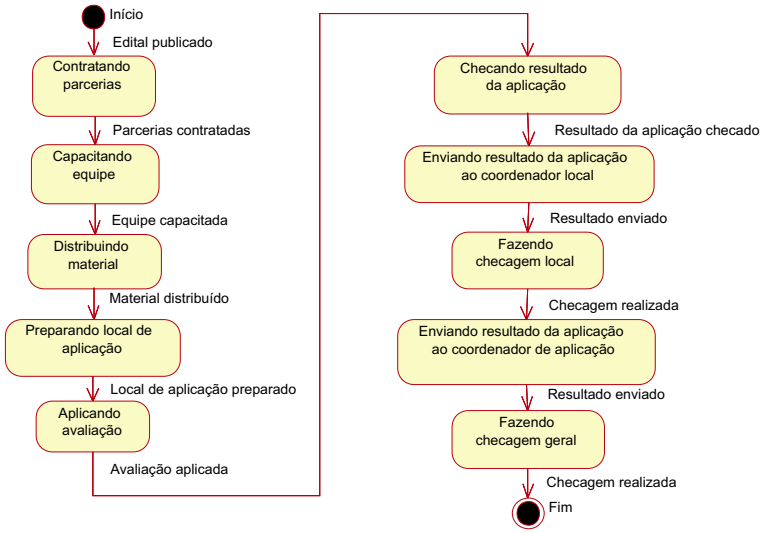

Figura A.34: Diagrama de estados da fase de aplicação

A.8.5 Realização do use case correção e divulgação dos resultados

A.8.5.1 Diagrama de classes participantes

Através do diagrama de classes participantes apresentado na figura A.35, percebe-se as classes interface, controle e persistente que estão envolvidos neste processo.

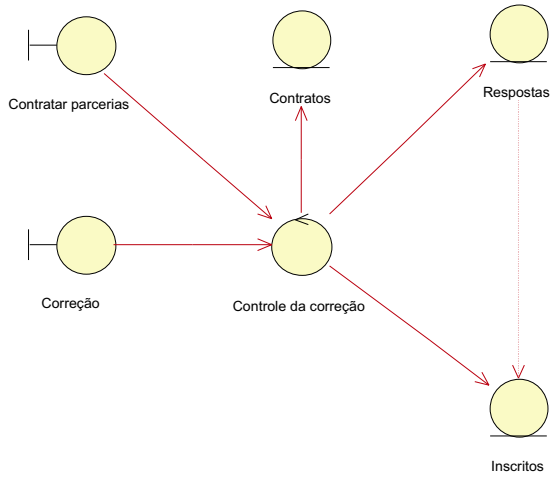

Figura A.35: Diagrama de classes participantes da fase de correção e divulgação dos resultados

A.8.5.2 Diagrama de seqüência

Os diagramas de seqüência apresentado nas figuras A.36, A.37 e A.38 representam as interações entre os atores a as classes participantes deste use case relativas ao seu fluxo principal de atividades.

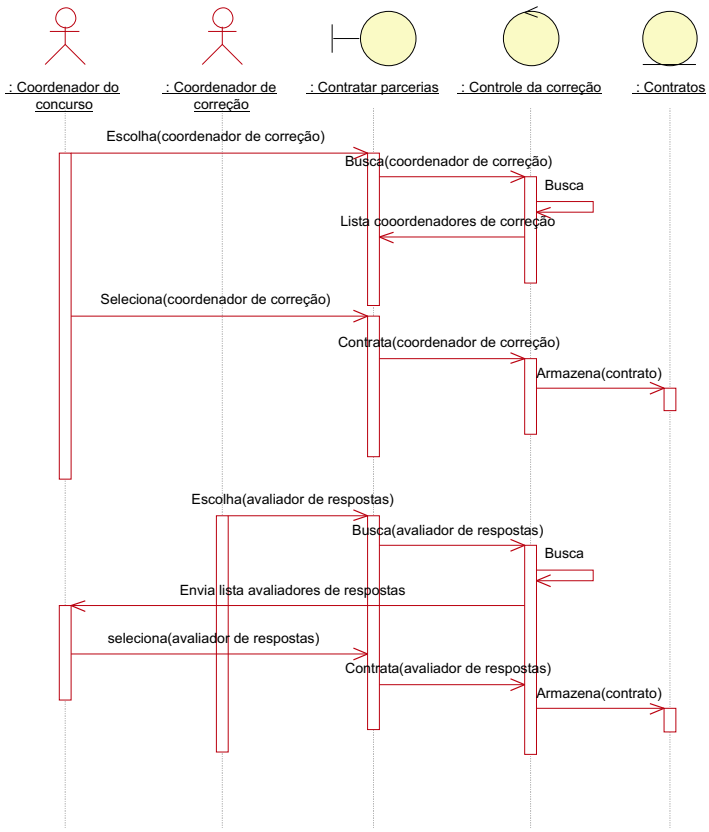

Figura A.36: Diagrama de seqüência 1 da fase de correção e divulgação dos resultados

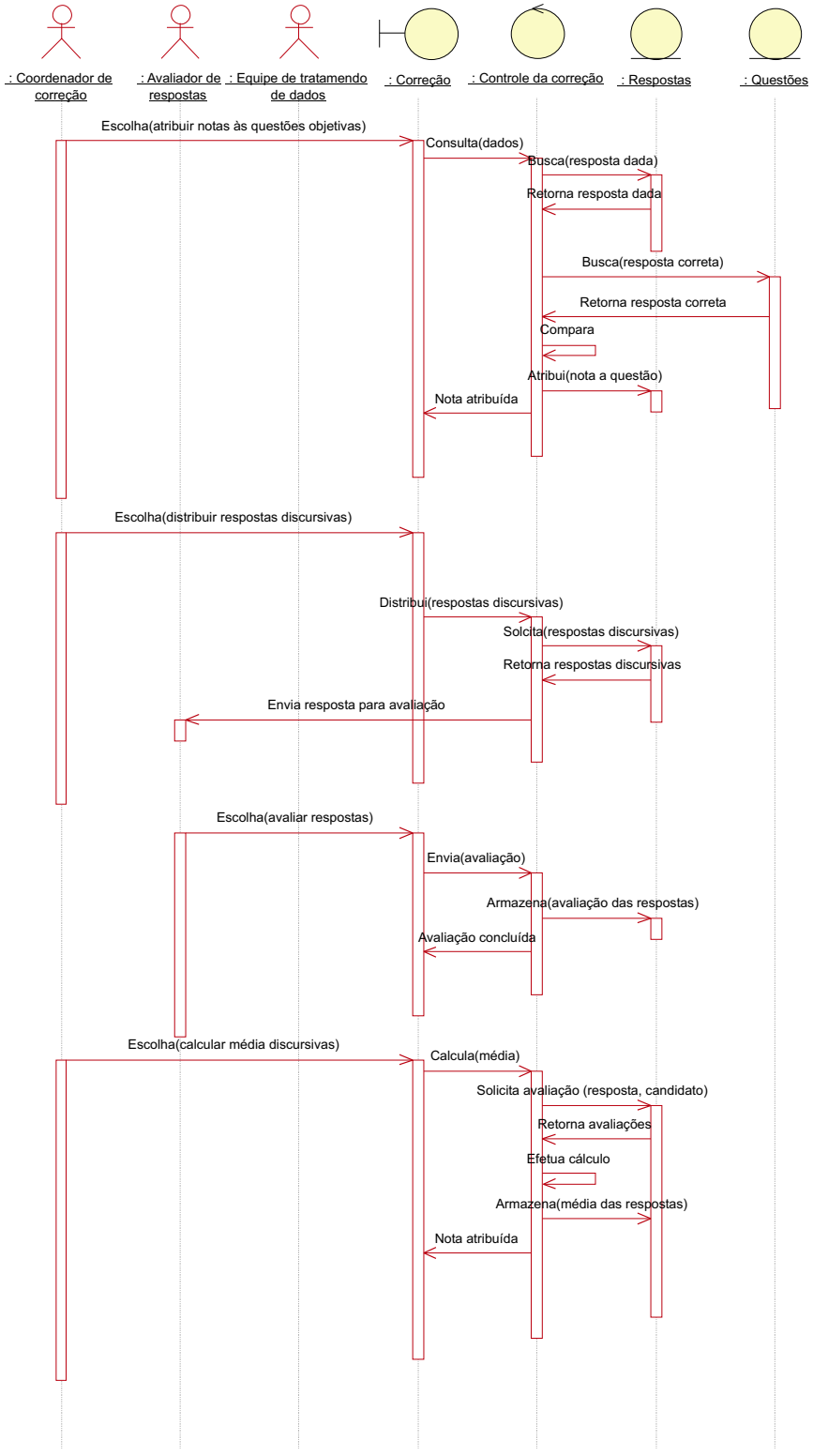

Figura A.37: Diagrama de seqüência 2 da fase de correção e divulgação dos resultados

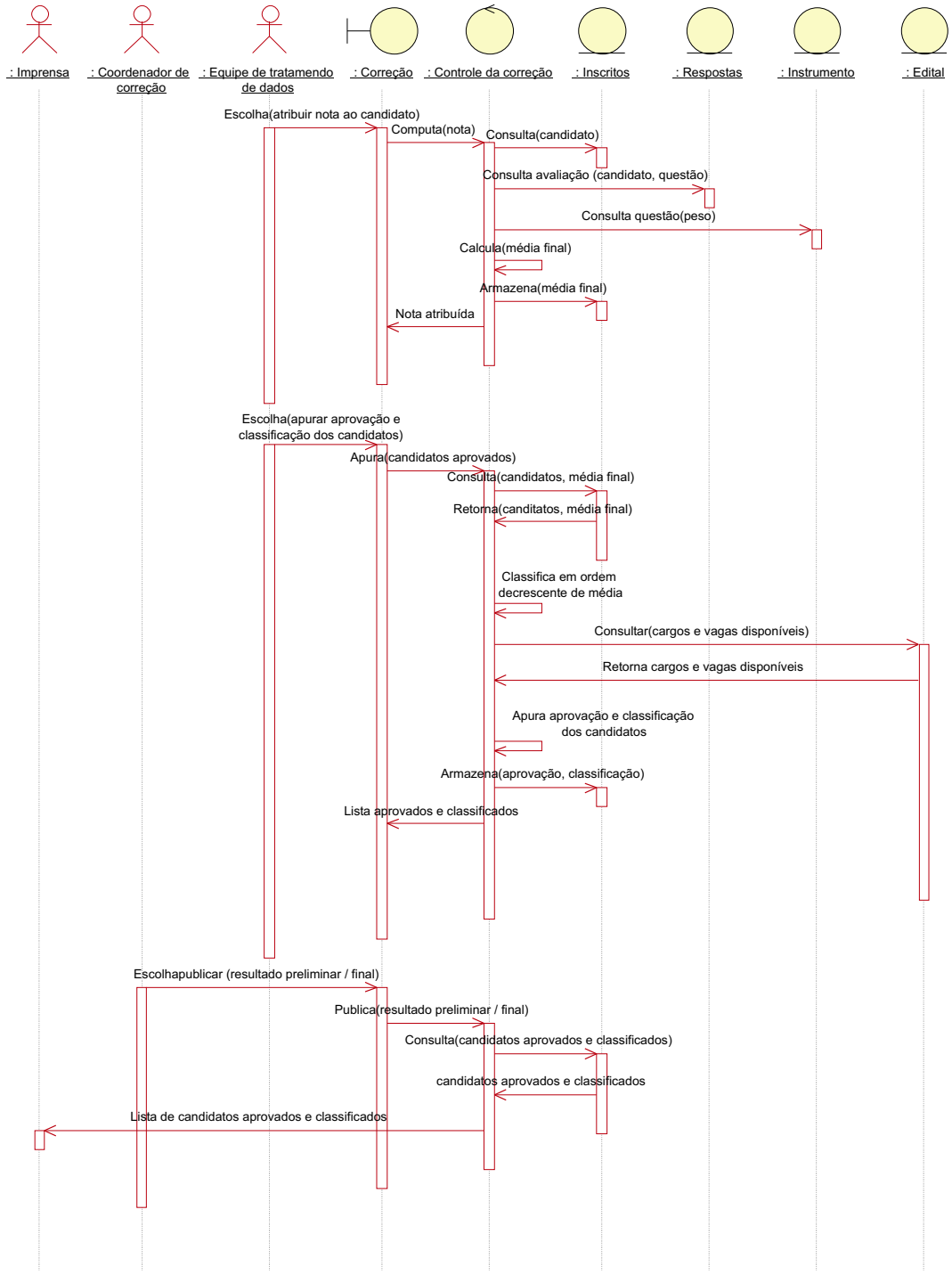

Figura A.38: Diagrama de seqüência 3 da fase de correção e divulgação dos resultados

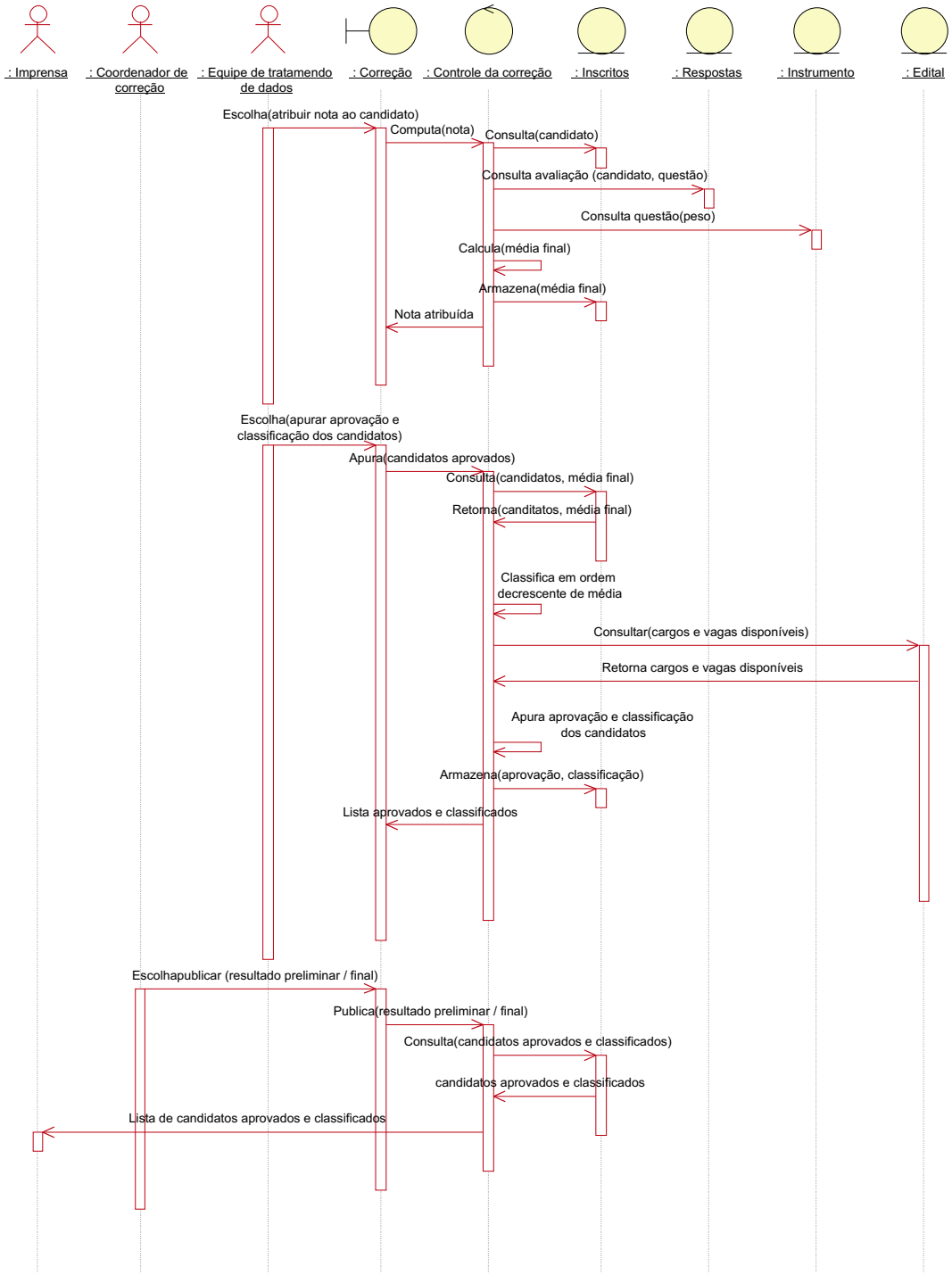

Figura A.39: Diagrama de seqüência 4 da fase de correção e divulgação dos resultados

A.8.5.3 Diagrama de estados

A figura A.40 apresenta o diagrama de estado deste use case.

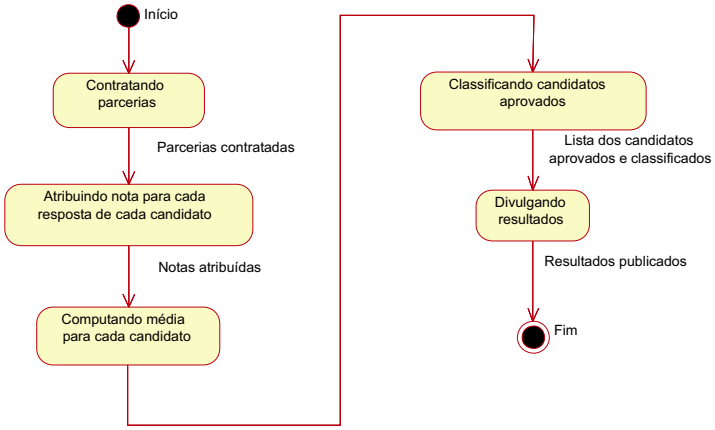

Figura A.40: Diagrama de estados da fase de correção e divulgação dos resultados

Apêndice B

Modelagem da avaliação somativa à distância mediada por computador

Neste apêndice é apresentada a modelagem do processo proposto de avaliação somativa à distância mediado por computador, utilizando a metodologia RUP e a representação UML.

A modelagem é feita sobre o modelo de avaliação somativa à distância modelado no apêndice A mediado por computador. Assim, na seqüência, são apresentadas apenas as diferenças em relação ao modelo anterior.

B.1 Alteração das regras de negócio

Além das diferenças no que tange a infra-estrutura (servidor, rede e computadores clientes) o modelo mediado por computador necessita da adição das seguintes regras de negócio:

- contratado deverá dispor de um sistema e servidor que atenda os requisitos especificados
- permitir acesso somente à usuários cadastrados
- a autenticação deve ser baseada em papéis, ou seja, um ator só poderá acessar áreas do sistema que lhe competem
- armazenar dados em banco de dados acessível somente ao administrador da base de dados (membro do ator equipe de tratamento de dados)

- permitir controle de solicitação e elaboração das questões
- permitir importação dos dados das inscrições feitas pelo receptor de inscrição
- permitir controle de homologação de inscrições
- locais de aplicação deverão dispor de computadores e rede com os requisitos mínimos para implementação da avaliação
- o sistema deve permitir a execução do instrumento de avaliação pelo candidato em uma interface computacional (on-line e off-line)
- a autenticação dos candidatos na hora da aplicação deve ser feita com a solicitação de conta, senha e biometria
- na aplicação o sistema deverá permitir que as ações efetuadas no computador do candidato sejam somente as previstas para a execução do instrumento de avaliação
- permitir controle do processo de correção e divulgação dos resultados

B.2 Alteração nos atores

Em relação aos atores, foi adicionado o ator:

- usuário
  - que representa qualquer usuário cadastrado no sistema

B.3 Alteração no use case geral

Na modelagem realizada no apêndice A o processo de comunicação e armazenagem dos documentos é feito diretamente pelos interlocutores e de forma manual. A utilização do computador permite agilizar os processos e melhorar o potencial do instrumento de avaliação.

A modelagem já realizada das fases do processo se aplica igualmente ao modelo computadorizado. As principais diferenças são justamente considerar que o sistema é computadorizado

e, portanto, necessita de um módulo adicional de controle de acesso, que permeia os use cases já modelados.

Assim, foi acrescido ao diagrama de use case geral o use case controle de acesso, conforme figura B.1. Note-se que os atores foram suprimidos do diagrama para facilitar a visualização.

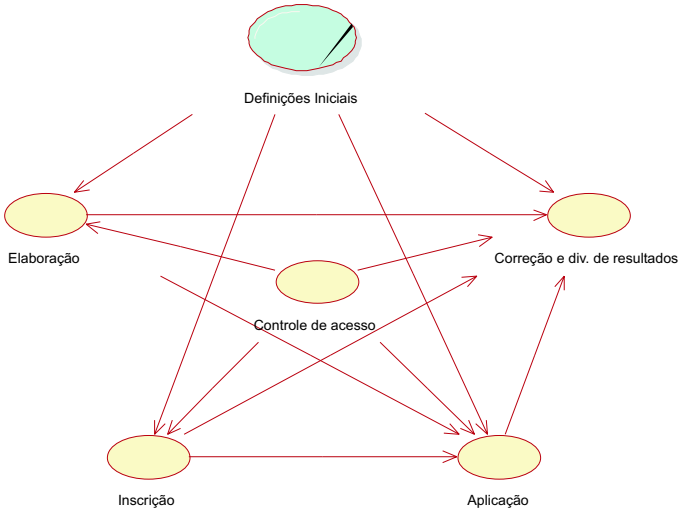

Figura B.1: Diagrama de use case da avaliação somativa à distância mediada por computador

B.4 Modelagem do use case controle de acesso

O modelo deste use case é apresentado na seqüência através de sua especificação e realização.

B.4.1 Especificação do use case controle de acesso

Seguindo a metodologia RUP, a especificação deste use case envolve a descrição de seu objetivo, pré-condições, inicializador, fluxo principal, fluxo alternativo, fluxo de exceção, do diagrama de use case e do diagrama de atividades.

B.4.1.1 Objetivo

Controlar o acesso de usuários ao sistema dentro de suas funções no processo de avaliação.

B.4.1.2 Pré-condições

- usuários devem estar cadastrados e identificados no sistema
- papéis devem ter sido definidos
- papéis devem ter sido atribuídos aos usuários

B.4.1.3 Iniciado por

- qualquer usuário que deseje acessar o sistema

B.4.1.4 Fluxo principal

- mostrar tela de entrada do sistema
- solicitar conta/senha
- conferir dados informados
- verificar níveis de acesso
- registrar acesso do usuário
- permitir o acesso ao sistema

B.4.1.5 Fluxo alternativo

- se conta/senha não conferirem com dados armazenados
  - reencaminhar para tela de solicitação de conta/senha com mensagem de erro
- se usuário tentar acessar informação que não lhe compete
  - não dar acesso à informação solicitada e mostrar mensagem de erro

- se usuário autenticado for candidato e acessar o sistema durante a aplicação
  - solicita identificação biométrica
  - confere identificação biométrica
    - se identificação biométrica conferir
      - dar acesso ao instrumento de avaliação
    - se não
      - reencaminhar para tela de solicitação de conta/senha com mensagem de erro

B.4.1.6 Fluxo de exceção

- sistema não está acessível
  - contatar administrador do sistema
- sistema cai no meio de uma transação
  - tentar novamente
  - caso o erro persista
    - contatar administrador do sistema
- papel atribuído erroneamente
  - contatar administrador do sistema

B.4.1.7 Pós-condições

- concedido acesso do usuário ao sistema em conformidade com seu papél
- armazenado registro de acesso

B.4.1.8 Especificações adicionais

- Atores participantes
  - Candidato

–Usuário (representando os atores abaixo)

∗Coordenador do Concurso

∗Equipe de tratamento de recursos

∗Coordenador da Elaboração

∗Elaborador de questões

∗Revisor de questões

∗Equipe de tratamento de dados

∗Receptor de Inscrição

∗Homologador de inscrição

∗Coordenador de aplicação

∗Coordenador local de aplicação

∗Fiscal

∗Coordenador de correção

∗Avaliador de respostas

B.4.1.9 Diagrama de use case

Na figura B.2 é apresentado o diagrama de use case controle de acesso representando seu relacionamento com os atores envolvidos.

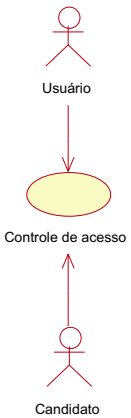

Figura B.2: Diagrama de use case do controle de acesso

O ator usuário representa todos os atores que tem acesso ao sistema computadorizado, a exceção do candidato.

B.4.1.10 Diagrama de atividades

A figura B.3 mostra as atividades necessárias para acesso ao sistema, que inclui a solicitação de conta, senha e, em alguns casos, dados biométricas.

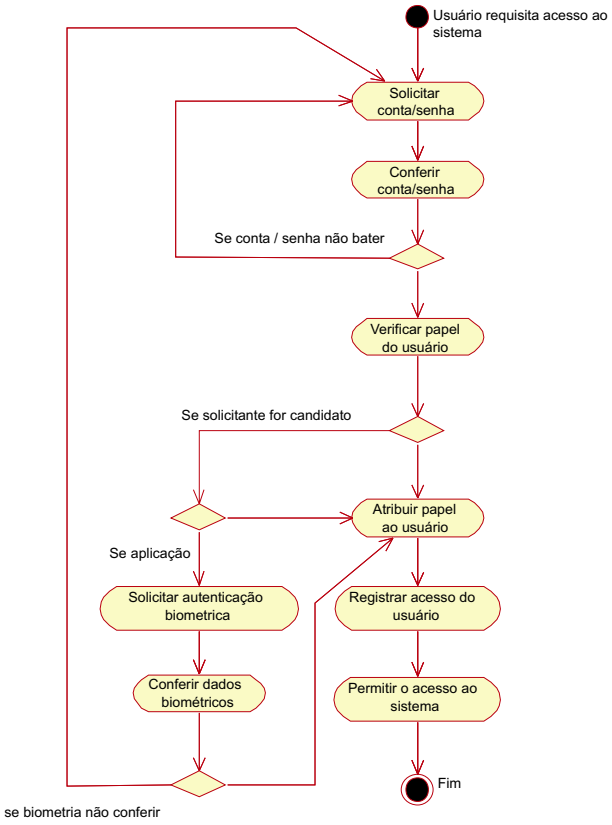

Figura B.3: Diagrama de atividades do controle de acesso

B.4.2 Realização do use case controle de acesso

A realização deste use case envolve a migração da visão de negócio para uma visão de implementação. Esta migração é consolidada pelos diagramas de classes participantes, seqüência e estado.

Como esta modelagem se refere aos processos sendo executados por sistema computacional, neste modelo as classes podem representar, respectivamente:

- de interface
  - telas disponibilizadas ao usuário com opções e formulários
- de controle
  - ações a serem implementadas pelo programa em função das opções escolhidas pelo usuário
- persistente
  - tabelas em banco de dados ou arquivo digital

B.4.2.1 Diagrama de classes participantes

Através do diagrama de classes participantes apresentado na figura B.4, percebe-se que a classe persistente usuário, relacionado com a entidade papéis, onde o sistema busca dados de conta e senha, e a classe persistente inscritos, relacionada com local de aplicação, onde o sistema busca os dados biométricos.

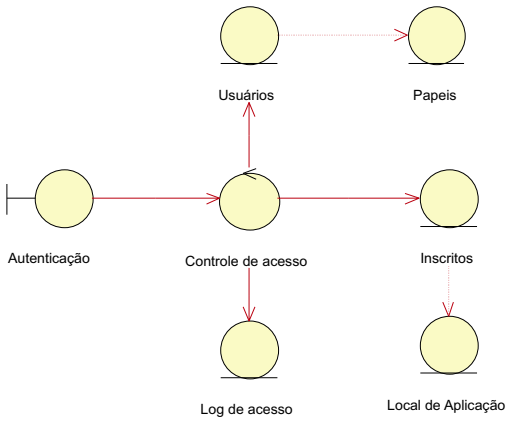

Figura B.4: Diagrama de classes participantes do controle de acesso

B.4.2.2 Diagrama de seqüência

O diagrama de seqüência apresentado na figura B.5 representa as interações entre os atores a as classes participantes deste use case relativas ao seu fluxo principal, sem e com a requisição de biometria.

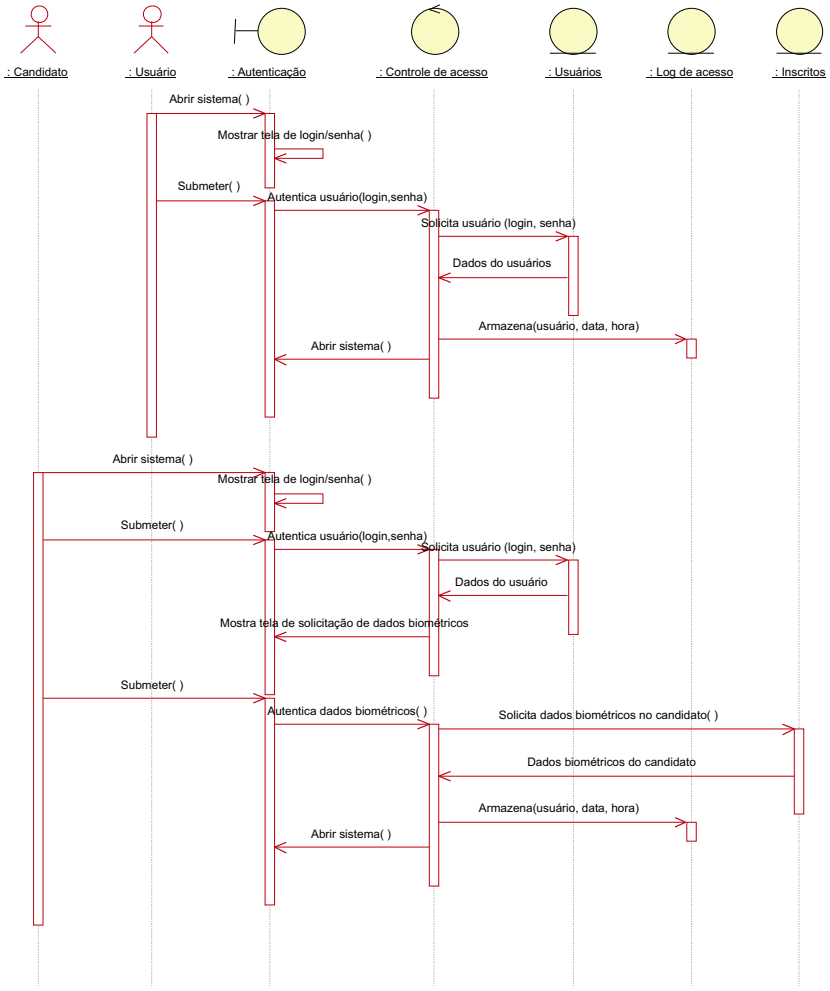

Figura B.5: Diagrama de seqüência do controle de acesso

B.4.2.3 Diagrama de estados

A figura B.6 apresenta o diagrama de estado deste use case.

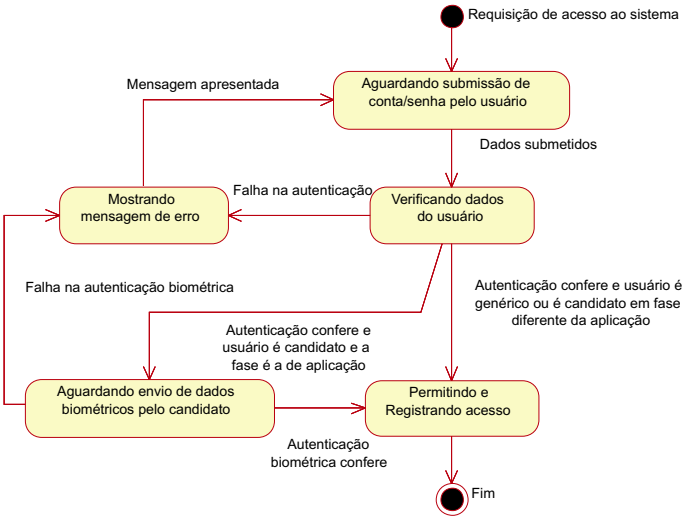

Figura B.6: Diagrama de estados do controle de acesso

B.5 Alterações nos use case do modelo de avaliação

No início de cada use case será considerado que os atores já estejam cadastrados no sistema, ou que o serão a partir do armazenamento de contratos de cada processo. Assim, a adição do sistema computadorizado implicará em pequenas alterações nos use cases, excetuando-se o acesso ao sistema, modelado na seção B.4, e a fase de definições iniciais.

Cabe salientar que o sistema ora proposto não garante a validade legal e o sigilo das informações transacionadas e armazenadas. Assim há a necessidade de se manter cópia física dos documentos com assinaturas manuais para enfrentar disputas legais.

A seguir são apresentadas as alteração em relação aos use case do modelo de avaliação com computador, onde os itens sem alteração são omitidos.

B.5.1 use case definições iniciais

Na seqüência deste documento são apresentadas as mudanças em relação ao modelo manual.

B.5.1.1 Fluxo principal

Ao fluxo principal são adicionadas as seguintes atividades:

- disponibilizar sistema
- cadastrar usuários certificados

B.5.1.2 Pós-condições

A pós-condição usuário cadastrado deve ser substituída por:

- sistema operacional
- usuários cadastrados

B.5.1.3 Especificações adicionais

- Ator participante acrescentado:
  - usuário

B.5.1.4 Diagrama de use case

Com a adição do ator usuário o diagrama deste use case passa a ser o apresentado na figura B.7.

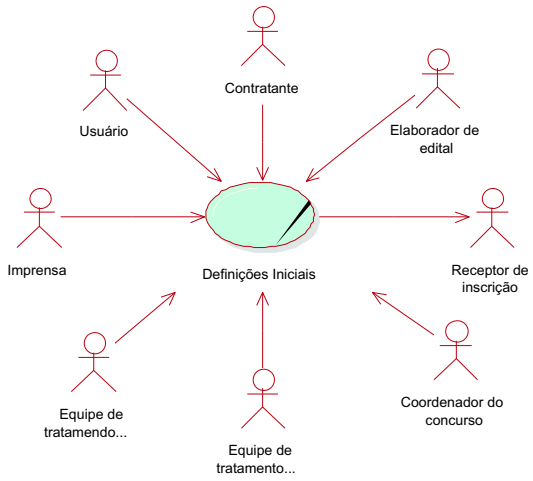

Figura B.7: Diagrama de use case da fase de definições iniciais com computador

B.5.1.5 Diagrama de atividades

No diagrama de atividades é adicionada a disponibilização do sistema e o cadastramento dos usuários, conforme a figura B.8.

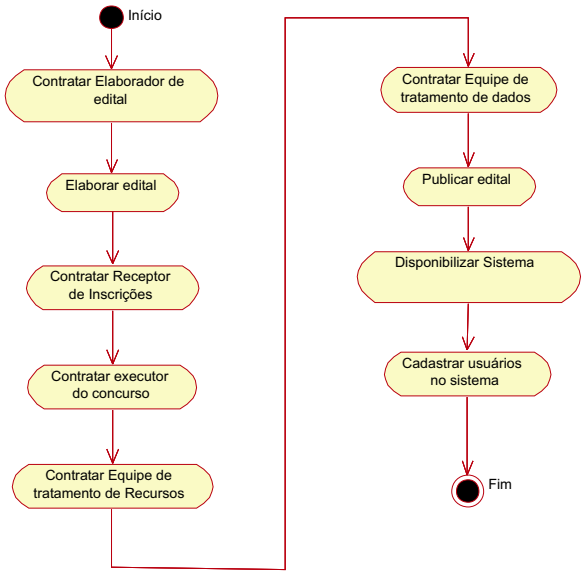

Figura B.8: Diagrama de atividades do use case definições iniciais com computador

B.5.1.6 Diagrama de classes participantes

Através do diagrama de classes participantes apresentado na figura B.9, percebe-se que a adição da interface sistema e das entidades persistentes contrato, papéis e usuários.

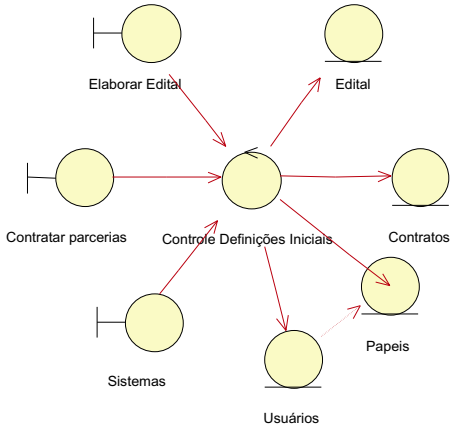

Figura B.9: Diagrama de classes participantes do use case definições iniciais com computador

B.5.1.7 Diagrama de seqüência

Acrescenta-se à seqüências já modeladas a seqüência de disponibilização do sistema e a de cadastramento do usuário, que são apresentados nas figuras B.10 e B.11, repectivamente. Assim o diagrama de seqüência final é composto pelas figuras A.14, A.15, A.16,B.10 e B.11.

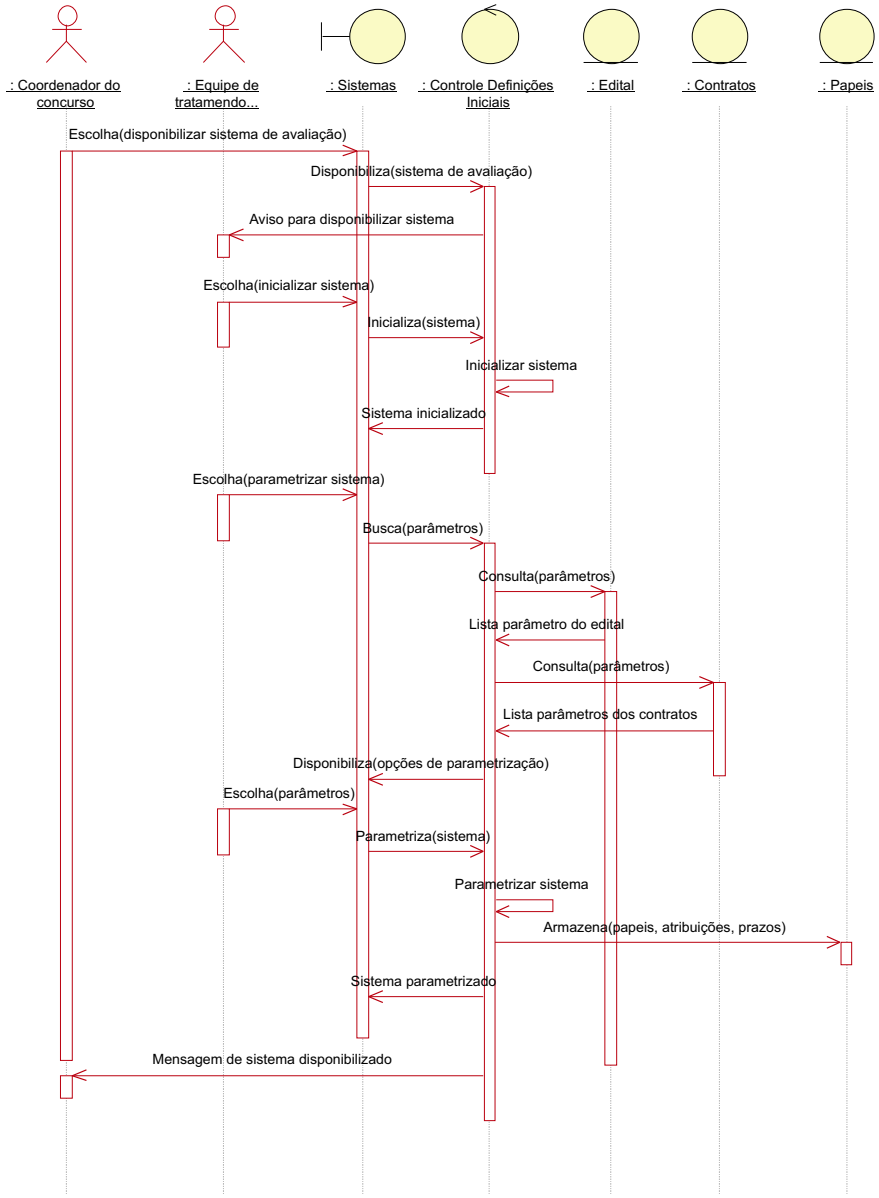

Figura B.10: Diagrama 3 de seqüência do use case definições iniciais com computador

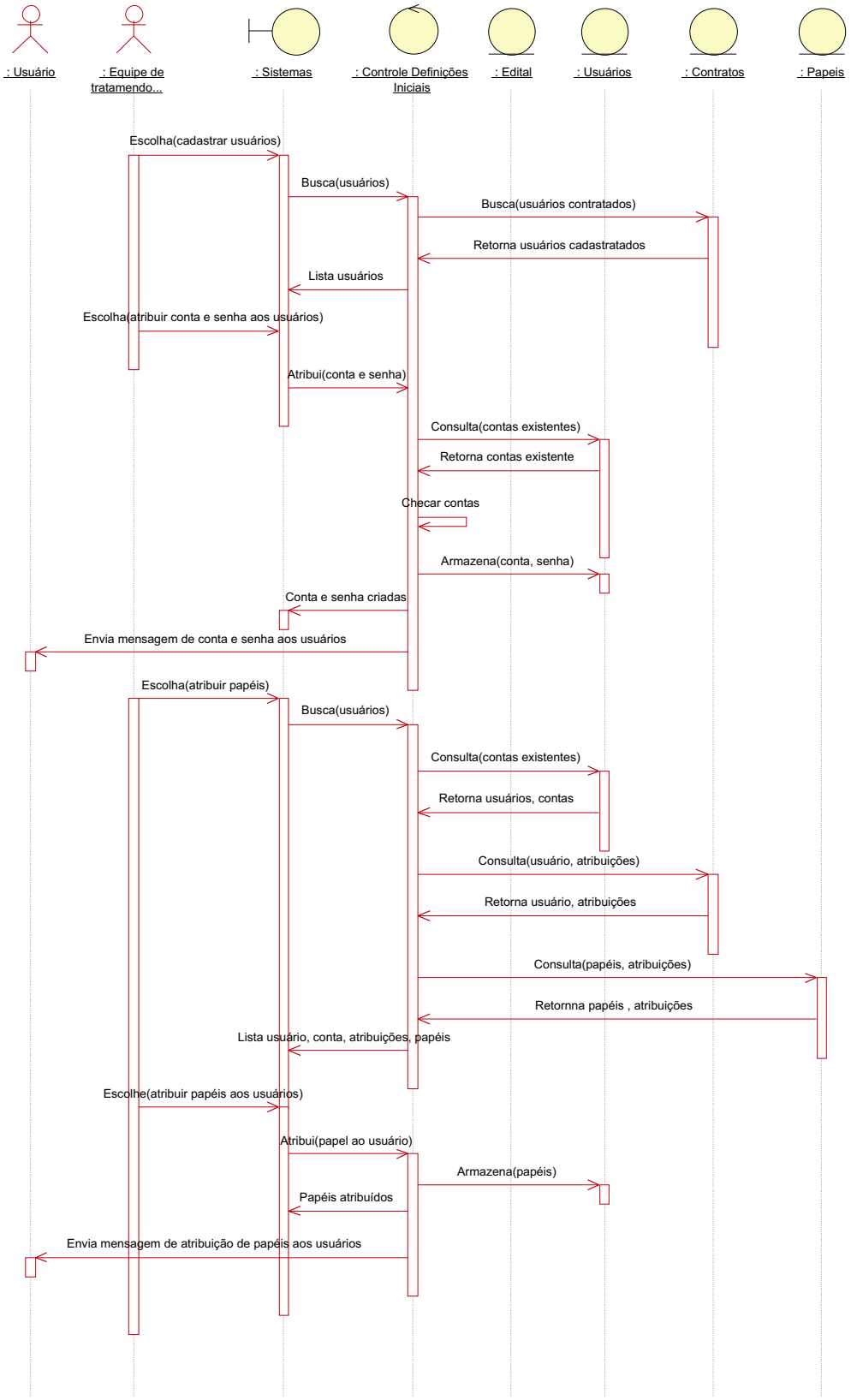

Figura B.11: Diagrama 4 de seqüência do use case definições iniciais com computador

B.5.1.8 Diagrama de estados

O diagrama de estado deste use case passa a ser o apresentado na figura B.12.

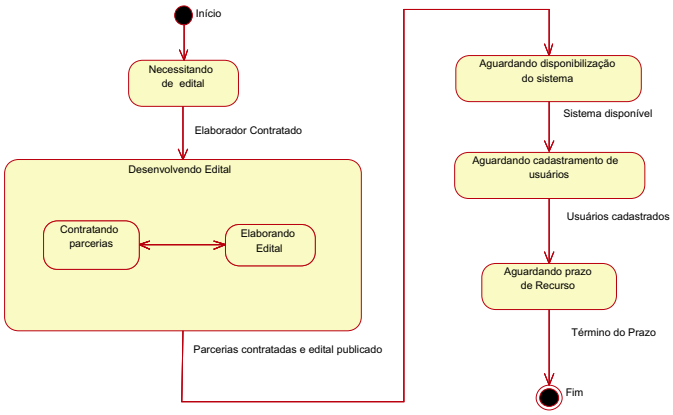

Figura B.12: Diagrama de estados do use case definições iniciais com computador

B.5.2 Demais use cases

A alteração mais evidente em relação a modelagem realizada no apêndice A é a introdução de um sistema computacional a partir do final da fase de definições iniciais.

Por se tratar da adição de um sistema, pode-se assumir que as entidades persistentes passem a ser tabelas em banco de dados. Entretanto, devido a tecnologia computacional convencional poder ser questionada no caso de disputa legal, será considerado que nos casos críticos seja mantida cópia em documento impresso assinada pelos interlocutores, ou, no mínimo, um recibo com resumo criptográfico assinado convencionalmente.

Outro fator relevante é assumir que a atividade de armazenar contratos implicará no cadastramento dos contratados como usuários do sistema. Assim, no início de cada fase se deverá considerar que os atores envolvidos estão cadastrados no sistema, ou o serão durante o processo, de forma transparente para o use case em questão.

Resguardadas esta exceções, as alterações nos use cases elaboração, inscrição, aplicação e correção e divulgação dos resultados restringem-se as alterações nas pré e pós-condições, como descrito a seguir.

B.5.2.1 Pré-condições

Adiciona-se a seguinte pré-condição a estes use cases:

- sistema disponível

B.5.2.2 Pós-condições

Como neste modelo o dados estão em formato digital pode-se considerar as seguintes pós-condições para cada use case:

- use case elaboração
  - banco de questões em formato digital
  - instrumento de avaliação, em formato digital
- use case inscrição
  - banco de dados de candidatos homologados com seus respectivos locais de avaliação
- use case aplicação
  - banco de dados de respostas dos candidatos ao instrumento de avaliação entregue ao coordenador de aplicação
- use case correção e divulgação dos resultados
  - banco de dados do resultado final (classificação dos candidatos aprovados) homologado

Apêndice C

Modelagem da avaliação somativa à distância mediada por computador com infra-estrutura de chaves públicas

Neste apêndice é feito a modelagem do processo proposto de avaliação somativa à distância mediada por computador com infra-estrutura de chaves públicas adotando a metodologia RUP e a representação UML.

A modelagem é feita sobre o modelo de avaliação somativa à distância mediada por computador apresentado no apêndice B adicionado de uma infra-estrutura de chaves públicas montada especificamente para processos de avaliação, ou para um processo de avaliação em especial, como ator.

Assim, na seqüência, são apresentadas apenas as diferenças em relação ao modelo anterior.

C.1 Alteração das regras de negócio

O negócio da avaliação em si não muda com a utilização de uma infra-estrutura de chaves públicas no processo. Entretanto, as regras de negócio sofrem alteração em função das novas possibilidades viabilizadas por esta tecnologia. Assim, deve-se acrescentar as regras de negócio os seguintes itens:

- viabilizar acesso ao sistema sem consulta a base de dados dos usuários, mediante utilização de certificado digital

- viabilizar comunicação e armazenamento seguro, o que implica em se poder verificar a autenticidade, integridade e tempestividade dos documentos eletrônicos, bem como garantir seu sigilo e não permitir repúdio por parte dos interlocutores, sem consulta a base de dados do sistema

C.2 Alteração nos atores

Nesta modelagem a infraestrutura de chaves pública não será modelada e sim tratada como ator no processo. Desta forma o seguinte ator é acrescido:

- ICP
  - este ator é responsável pela emissão e revogação de certificados digitais, além da protocolação de documentos eletrônicos

C.3 Alteração no use case do sistema

Na modelagem realizada no apêndice A o processo de comunicação e armazenagem dos documentos é feito diretamente pelos interlocutores e de forma manual. Igualmente, na modelagem apresentada no apêndice B o processo manual de registro se mantém necessário, pois, apesar da tecnologia computacional ter sido agregada, a mesma não confere as garantias necessárias. Já no modelo ora proposto o processo de comunicação e armazenagem dos documentos é totalmente computadorizado.

Ao invés de alterar todos os use cases dos modelos anteriores, detalhando o processo de comunicação e armazenamento em cada diagrama, optou-se por modelar este processo à parte, representando todo o processo de comunicação e armazenamento requeridos.

Assim, foi acrescido ao diagrama de use case geral o use case comunicação e armazenamento seguro, conforme figura C.1. Note-se que os atores foram suprimidos do diagrama para facilitar a visualização.

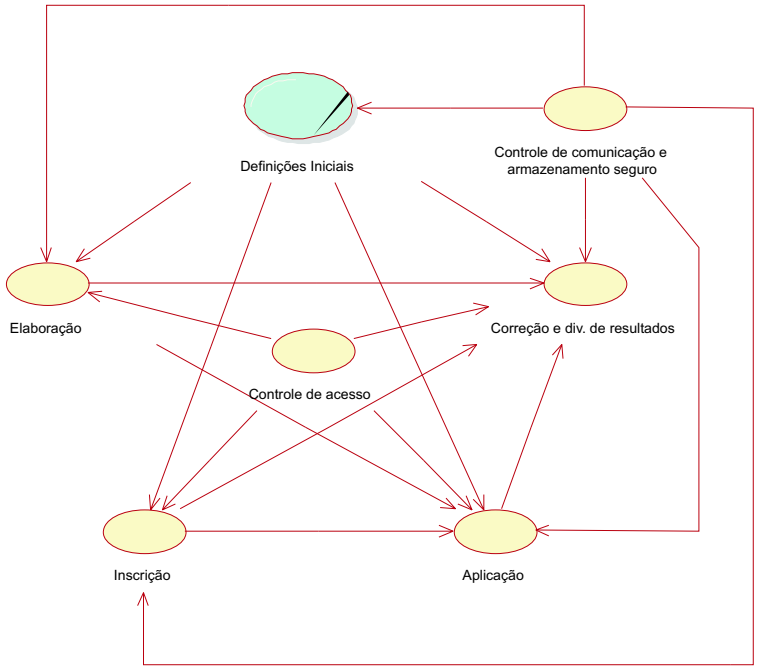

Figura C.1: Diagrama de use case da avaliação somativa à distância mediada por computador com infra-estrutura de chaves públicas

C.4 Modelagem do use case comunicação e armazenamento seguro

Com o objetivo de facilitar a visualização deste use case é apresentado na seqüência sua especificação e realização.

C.4.1 Especificação do use case comunicação e armazenamento seguro

Seguindo a metodologia RUP, a especificação deste use case envolve a descrição de seu objetivo, pré-condições, inicializador, fluxo principal, fluxo alternativo, fluxo de exceção, do diagrama de use case e do diagrama de atividades.

C.4.1.1 Objetivo

O objetivo deste use case é permitir comunicação e armazenamento seguro de informações.

C.4.1.2 Pré-condições

- infra-estrutura de chaves públicas operacional
- atores e sistema já possuírem certificados emitidos e válidos

C.4.1.3 Iniciado por

- usuário
- sistema

C.4.1.4 Fluxo principal

- disponibilizar tela para submissão de documento eletrônico
- disponibilizar opção de assinatura
- viabilizar assinatura do documento
- disponibilizar opção de destinatário
- buscar dados dos destinatários e seus superiores
- disponibilizar opção de cifragem
- cifrar documento de forma a permitir acesso somente ao destinatário e seus superiores
- disponibilizar opção de protocolação
- receber documento
- protocolar transação
- armazenar recibo

- disponibilizar recibo ao originador da transação
- armazenar documento
- enviar aviso ao destinatário
- mostrar interface para recepção do documento por parte do destinatário
- disponibilizar documento eletrônico ao destinatário
- protocolar transação
- armazenar recibo assinado pelo destinatário
- enviar recibo assinado pelo destinatário ao originador

C.4.1.5 Fluxo alternativo

- se dados do destinatário e seus superiores não disponíveis na máquina cliente
  - buscar dados no diretório público da ICP
    - se ICP indisponível
      - disponibilizar tela para submissão de documento eletrônico com mensagem de erro
- se o originador do envio do documento for o próprio sistema
  - disponibilizar tela para submissão de documento eletrônico
  - disponibilizar opção de assinatura
  - viabilizar assinatura do documento
  - disponibilizar opção de destinatário
  - buscar dados dos destinatários e seus superiores
  - disponibilizar opção de cifragem
  - cifrar documento de forma a permitir acesso somente ao destinatário e seus superiores

–disponibilizar opção de protocolação

–protocolar transação

–armazenar recibo

–armazenar documento

–enviar aviso ao destinatário

–mostrar interface para recepção do documento por parte do destinatário

–disponibilizar documento eletrônico ao destinatário

–protocolar transação

–armazenar recibo assinado pelo destinatário

–enviar recibo assinado pelo destinatário ao originador

●se o destinatário do documento for o próprio sistema

–disponibilizar tela para submissão de documento eletrônico

–disponibilizar opção de assinatura

–viabilizar assinatura do documento

–disponibilizar opção de destinatário

–disponibilizar opção de cifragem

–cifrar documento de forma a permitir acesso somente ao destinatário e seus superiores

–disponibilizar opção de protocolação

–receber documento

–protocolar transação

–armazenar recibo

–disponibilizar recibo ao originador da transação

–armazenar documento

●se assinatura não for requerida

–disponibilizar tela para submissão de documento eletrônico

–disponibilizar opção de assinatura

–disponibilizar opção de destinatário

–buscar dados dos destinatários e seus superiores

–disponibilizar opção de cifragem

–cifrar documento de forma a permitir acesso somente ao destinatário e seus superiores

–disponibilizar opção de protocolação

–receber documento

–protocolar transação

–armazenar recibo

–disponibilizar recibo ao originador da transação

–armazenar documento

–enviar aviso ao destinatário

–mostrar interface para recepção do documento por parte do destinatário

–disponibilizar documento eletrônico ao destinatário

–protocolar transação

–armazenar recibo assinado pelo destinatário

–enviar recibo assinado pelo destinatário ao originador

●se sigilo não for requerido

–disponibilizar tela para submissão de documento eletrônico

–disponibilizar opção de assinatura

–viabilizar assinatura do documento

–disponibilizar opção de destinatário

–buscar dados dos destinatários e seus superiores

–disponibilizar opção de cifragem

–disponibilizar opção de protocolação

–receber documento

–protocolar transação

–armazenar recibo

–disponibilizar recibo ao originador da transação

–armazenar documento

–enviar aviso ao destinatário

–mostrar interface para recepção do documento por parte do destinatário

–disponibilizar documento eletrônico ao destinatário

–protocolar transação

–armazenar recibo assinado pelo destinatário

–enviar recibo assinado pelo destinatário ao originador

●se protocolação não for requerida

–disponibilizar tela para submissão de documento eletrônico

–disponibilizar opção de assinatura

–viabilizar assinatura do documento

–disponibilizar opção de destinatário

–buscar dados dos destinatários e seus superiores

–disponibilizar opção de cifragem

–cifrar documento de forma a permitir acesso somente ao destinatário e seus superiores

–disponibilizar opção de protocolação

–receber documento

–armazenar documento

–enviar aviso ao destinatário

–mostrar interface para recepção do documento por parte do destinatário

–disponibilizar documento eletrônico ao destinatário

●se sistema for off-line

–protocoloção local

–base de usuários destino fixa

C.4.1.6 Fluxo de exceção

●sistema não responde

–reiniciar o sistema

●não retorno do recibo ao usuário

–reenvia solicitação

●acesso a ICP indisponível, com dados do usuário destino na máquina cliente

–entrega de recibo temporário pelo próprio sistema

–envio de recibo protocolado quando o acesso a ICP for restabelecido

C.4.1.7 Pós-condições

●documento armazenado e entregue ao destinatário, com requisitos de entrega atendidos

C.4.1.8 Especificações adicionais

●Atores participantes

–usuário

–ICP

C.4.1.9 Diagrama de use case

Na figura C.2 é apresentado o diagrama de use case comunicação e armazenamento seguro representando seu relacionamento com os atores envolvidos.

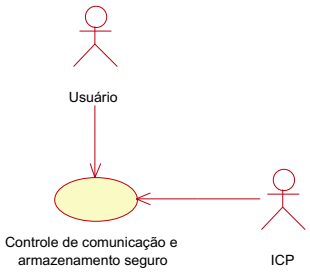

Figura C.2: Diagrama de use case da comunicação e armazenamento seguro

O ator usuário representa todos os atores que tem acesso ao sistema computadorizado, a exceção da ICP. Qualquer troca de documentos eletrônicos, entre usuários ou destes com o sistema, que necessitem das características de segurança, serão realizadas através deste use case.

C.4.1.10 Diagrama de atividades

A figura C.3 representa o diagrama de atividades do use case comunicação e armazenamento seguro.

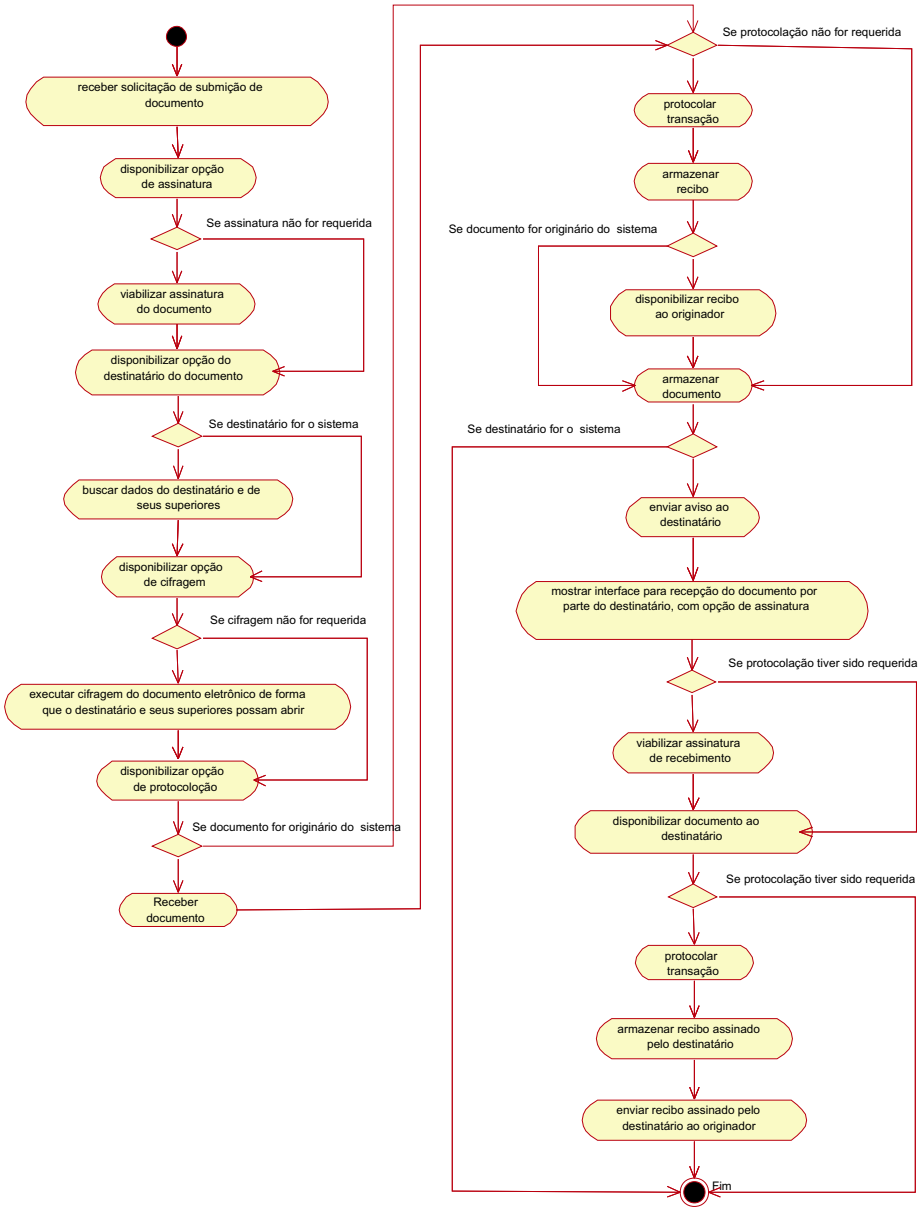

Figura C.3: Diagrama de atividade da comunicação e armazenamento seguro

C.4.2 Realização do use case comunicação e armazenamento seguro

A realização deste use case envolve a migração da visão de negócio para uma visão de implementação. Esta migração é consolidada pelos diagramas de classes participantes, seqüência e estado.

C.4.2.1 Diagrama de classes participantes

O diagrama de classes participantes deste use case é apresentado na figura C.4. Neste, a entidade “recibo” representa o local de armazenamento dos recibos de comunicação. Já a entidade “dados” representa o local de armazenamento de todos os dados dos sistema que utilizem o use case “comunicação e armazenamento seguro”, à exceção dos recibos. Em uma implementação por programa é necessário modelar cada fluxo de armazenamento de forma independente, o que não foi feito no presente modelo.

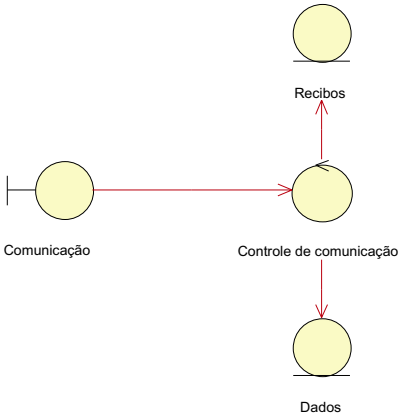

Figura C.4: Diagrama de classes participantes da comunicação e armazenamento seguro

C.4.2.2 Diagrama de seqüência

O diagrama de seqüência apresentado nas figuras C.5 e C.6 representa as interações entre os atores a as classes participantes deste use case relativas ao seu fluxo principal.

Destaca-se que a interação com o ator ICP, neste use case, se dá de duas formas: consulta ao diretório público (DP); e protocolação.

O diretório público (DP) é uma entidade persistente do ator ICP que contém os certificados dos usuários do sistema. Estes contém informações como: dados pessoais; chave pública; papel; hierarquia do papel; validade; e dados biométricos do usuário.

Na protocolação a ICP confere as propriedades de tempestividade e não repúdio ao sistema.

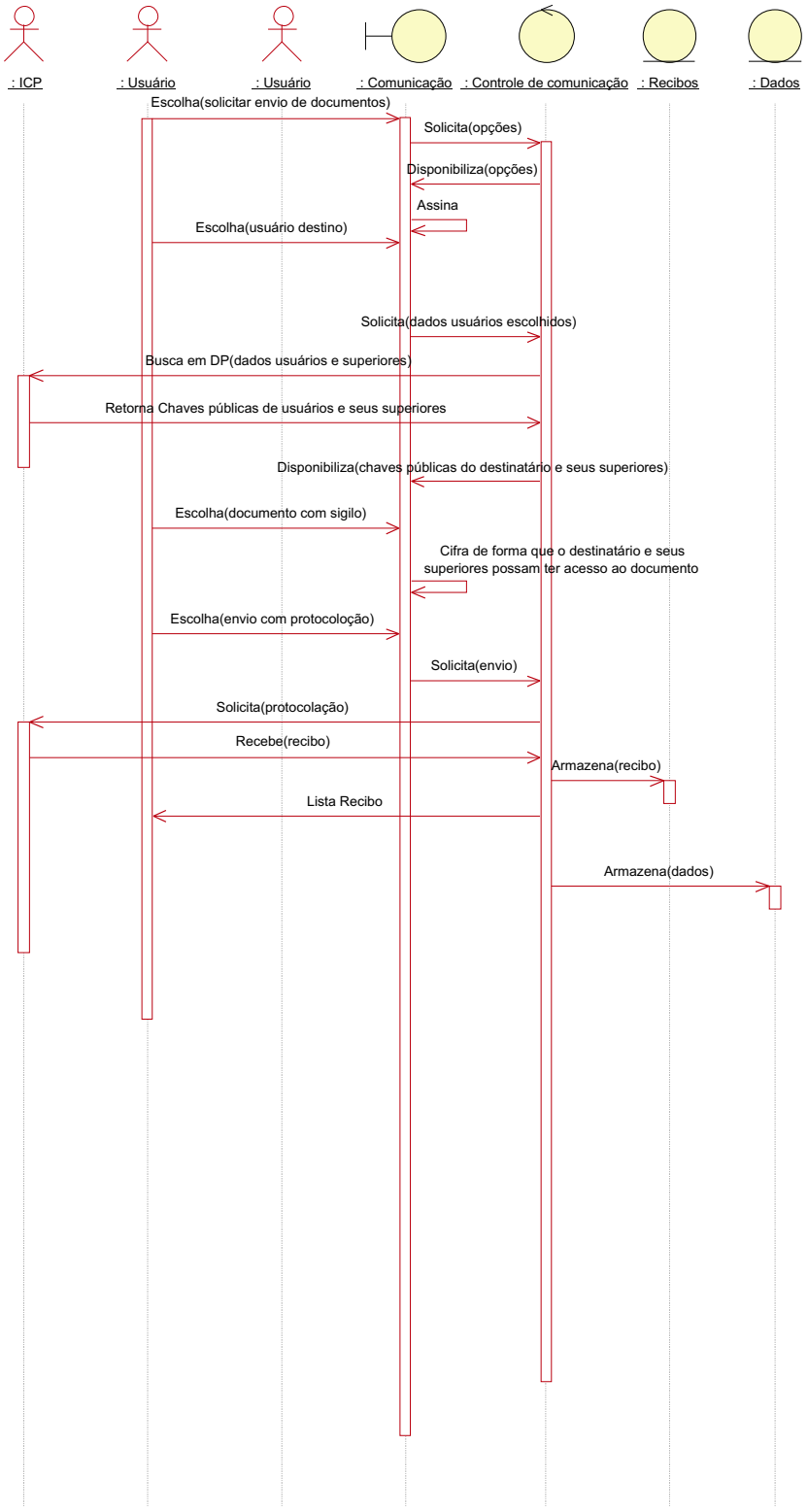

Figura C.5: Diagrama 1 de seqüência da comunicação e armazenamento seguro

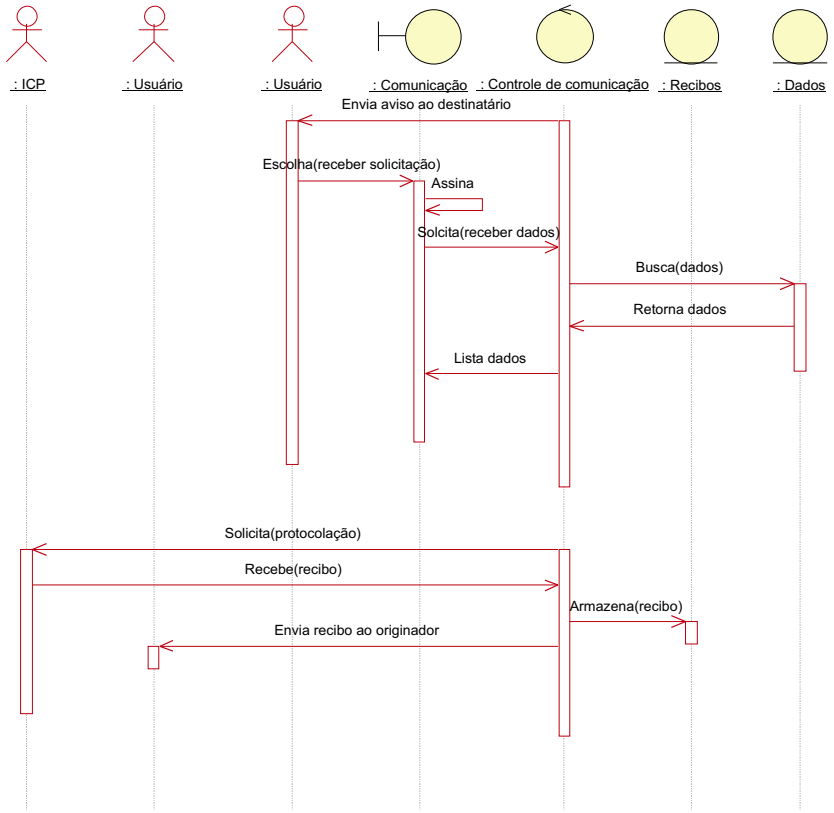

Figura C.6: Diagrama 2 de seqüência da comunicação e armazenamento seguro

C.4.2.3 Diagrama de estados

A figura C.7 apresenta o diagrama de estado deste use case.

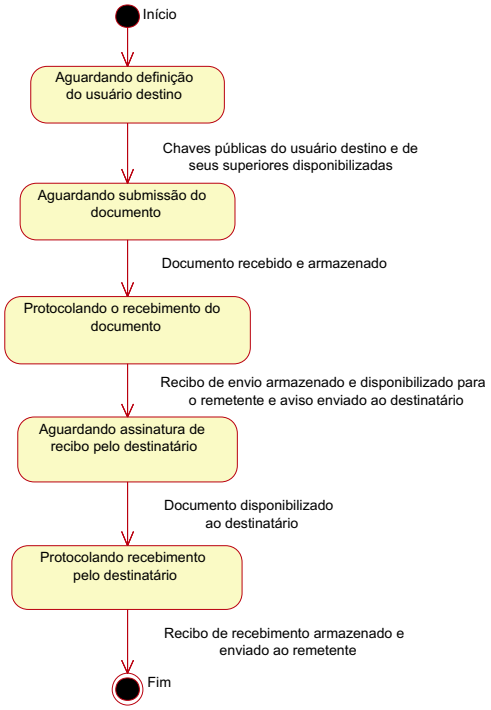

Figura C.7: Diagrama de estado da comunicação e armazenamento seguro

C.5 Alterações nos use case do modelo de avaliação com computador

A adição da infra-estrutura de chaves públicas afeta sobretudo a comunicação digital, conforme modelado na seção C.4, o acesso ao sistema e as definições iniciais.

Além disso, no modelo ora proposto, a ação de armazenar o contrato de atores, apresentada nos use case já modelados nos capítulos anteriores, implicará no envio de documento eletrônico assinado com dados dos atores para que estes possam requisitar seus certificados à infra-estrutura de chaves públicas. Desta forma, no início de cada use case será considerado que os atores possuam certificados válidos emitidos pela ICP, ou que serão emitidos a partir do armazenamento de contratos de cada processo. Portanto, as alterações nos use case restantes será pequena.

A seguir são apresentadas as alteração em relação aos use case do modelo de avaliação com computador, onde os itens sem alteração são omitidos.

C.5.1 use case controle de acesso

C.5.1.1 Pré-condições

A pré-condição para este use case passa a ser a seguinte:

- usuários devem possuir certificado válidos

C.5.1.2 Fluxo principal

No fluxo principal a atividade de solicitar conta/senha é substituída por:

- solicitar certificado

C.5.1.3 Fluxo alternativo

De forma coerente com a alteração do fluxo principal o fluxo alternativo é modificado da seguinte forma:

- se certificado não for válido ou estiver na CRL
  - reencaminhar para tela de solicitação de certificado com mensagem de erro
- se CRL não disponível na máquina local
  - busca na ICP
    - se ICP indisponível
      - reencaminhar para tela de solicitação de solicitação de certificado com mensagem de erro

C.5.1.4 Diagrama de use case

Com a adição do ator ICP o diagrama deste use case passa a ser o apresentado na figura C.8.

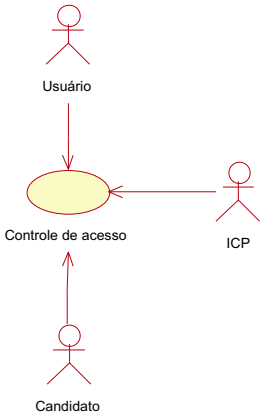

Figura C.8: Diagrama de use case do controle de acesso com ICP

C.5.1.5 Diagrama de atividades

A solicitação para acesso ao sistema passa a ter as atividades apresentadas na figura C.9, onde a solicitação de conta e senha passa a ser a de submissão de certificado.

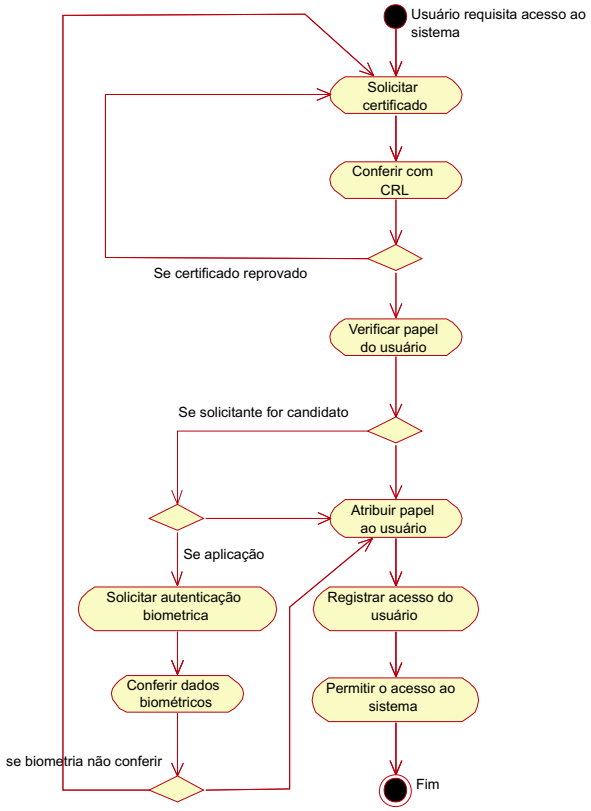

Figura C.9: Diagrama de atividades do controle de acesso com ICP

C.5.1.6 Diagrama de classes participantes

Através do diagrama de classes participantes apresentado na figura C.10, percebe-se que a classe persistente usuário foi suprimida, pois os dados do usuário passam a ser obtidos através de seus certificados.

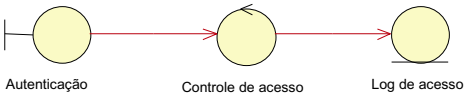

Figura C.10: Diagrama de classes participantes do controle de acesso com ICP

C.5.1.7 Diagrama de seqüência

Como apresentado na figura C.11, um certificado válido submetido para acesso ao sistema será confrontado com a lista de certificados revogados disponibilizada pela ICP.

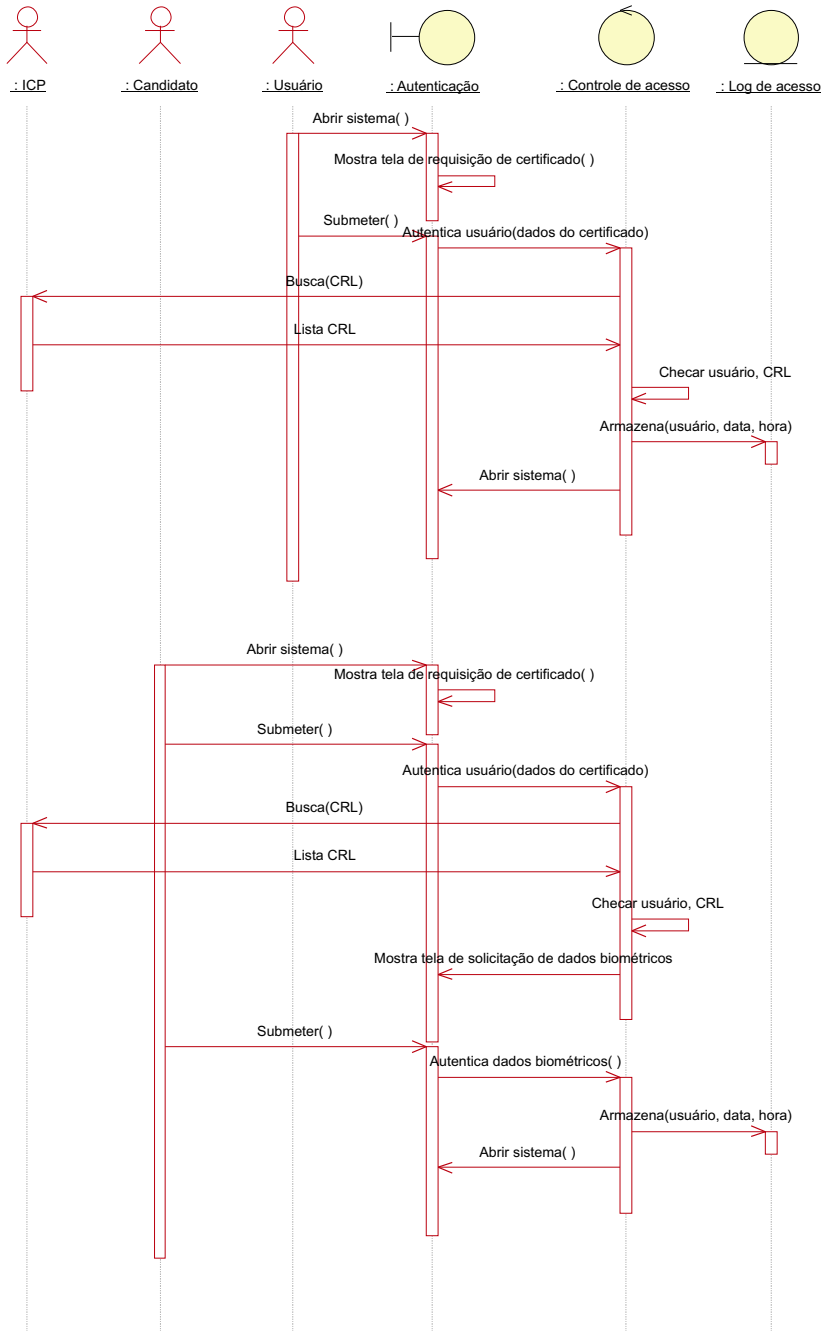

Figura C.11: Diagrama de seqüência do controle de acesso com ICP

C.5.1.8 Diagrama de estados

O diagrama de estado deste use case passa a ser o apresentado na figura C.12.

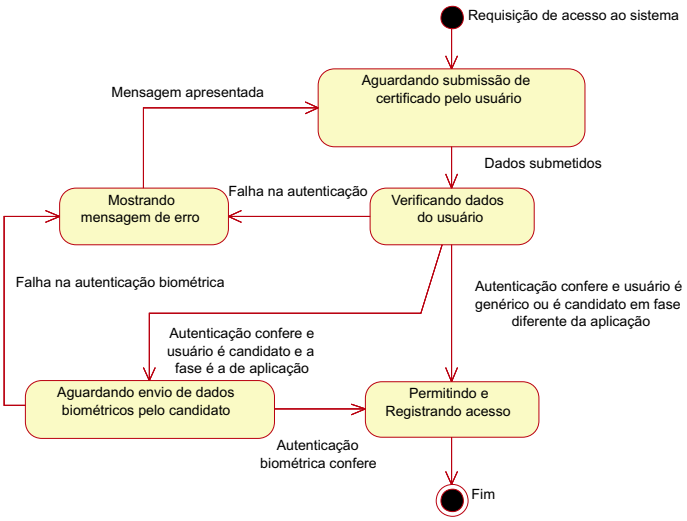

Figura C.12: Diagrama de estados do controle de acesso com ICP

C.5.2 use case definições iniciais

A grande diferença deste use case em relação ao implementado no modelo apenas com computador é a disponibilização de uma infra-estrutura de chaves públicas e a subtração do cadastramento do usuário visto que uma mensagem assinada com seu papel lhe é enviada para que possa solicitar o certificado.

Na seqüência deste documento são apresentadas as mudanças em relação ao modelo anterior.

C.5.2.1 Fluxo principal

Ao fluxo principal são adicionadas as seguintes atividades, substituindo a atividade de cadastrar usuários:

- Disponibilizar ICP
- Disponibilizar documento para usuários solicitarem certificados

C.5.2.2 Pós-condições

A póscondição usuário cadastrado deve ser substituída por:

- ICP operacional
- Documento que permita ao usuário solicitar seu certificado disponibilizado

C.5.2.3 Especificações adicionais

- Ator participante acrescentado:
  - ICP

C.5.2.4 Diagrama de use case

Com a adição do ator ICP o diagrama deste use case passa a ser o apresentado na figura C.13.

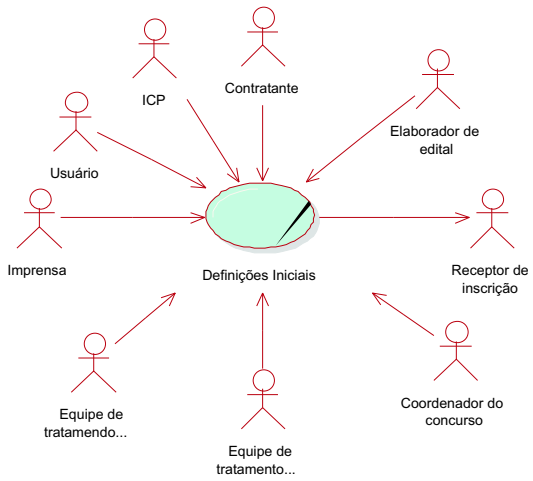

Figura C.13: Diagrama de use case da fase de definições iniciais com ICP

C.5.2.5 Diagrama de atividades

No diagrama de atividades é suprimida o cadastramento do usuáio e acrescido a disponibilização da ICP e o envio de documento que permita aos usuários solicitar seus certificados, como apresentado na figura C.14.

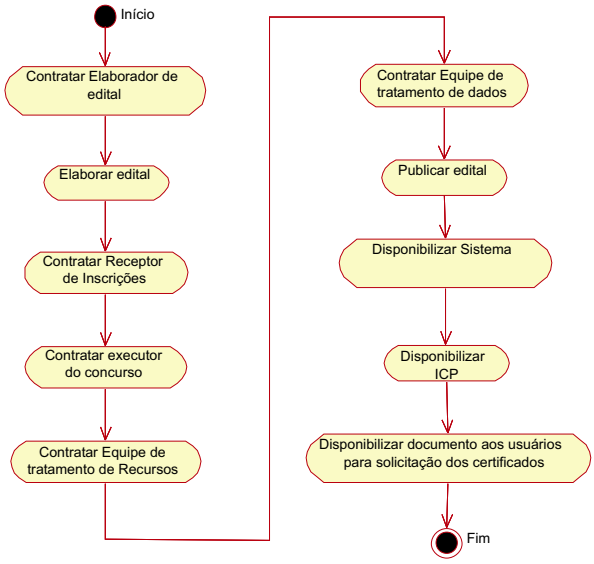

Figura C.14: Diagrama de atividades do use case definições iniciais com ICP

C.5.2.6 Diagrama de classes participantes

Através do diagrama de classes participantes apresentado na figura C.15, percebe-se que a classe persistente usuário foi suprimida, pois os dados do usuário são armazenados em seus certificados.

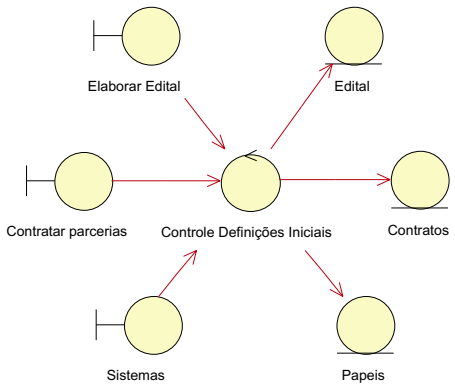

Figura C.15: Diagrama de classes participantes do use case definições iniciais com ICP

C.5.2.7 Diagrama de seqüência

Além de suprimir o diagrama de seqüência que ilustra o cadastramento do usuário, acrescenta-se a seqüência de disponibilização da ICP e de envio de documento aos usuários, que são apresentados nas figuras C.16 e C.17, repectivamente. Assim o diagrama de seqüência é composto pelas figuras A.14, A.15, A.16, B.10, C.16 e C.17.

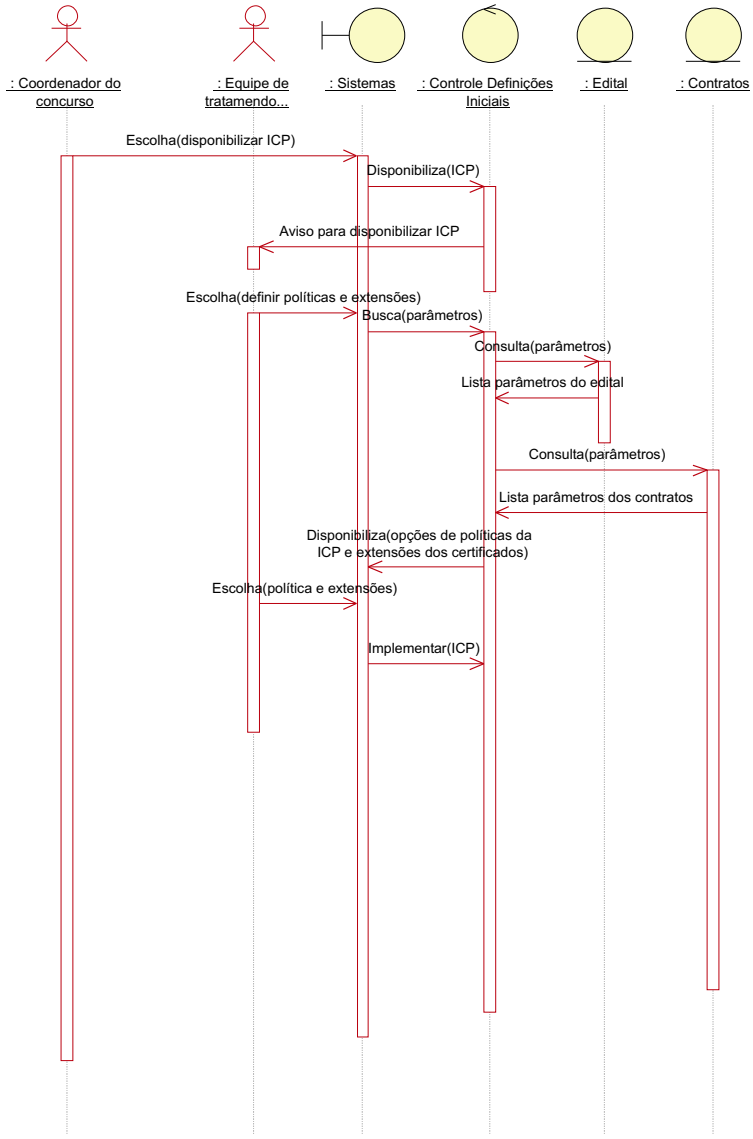

Figura C.16: Diagrama 4 de seqüência do use case definições iniciais com ICP

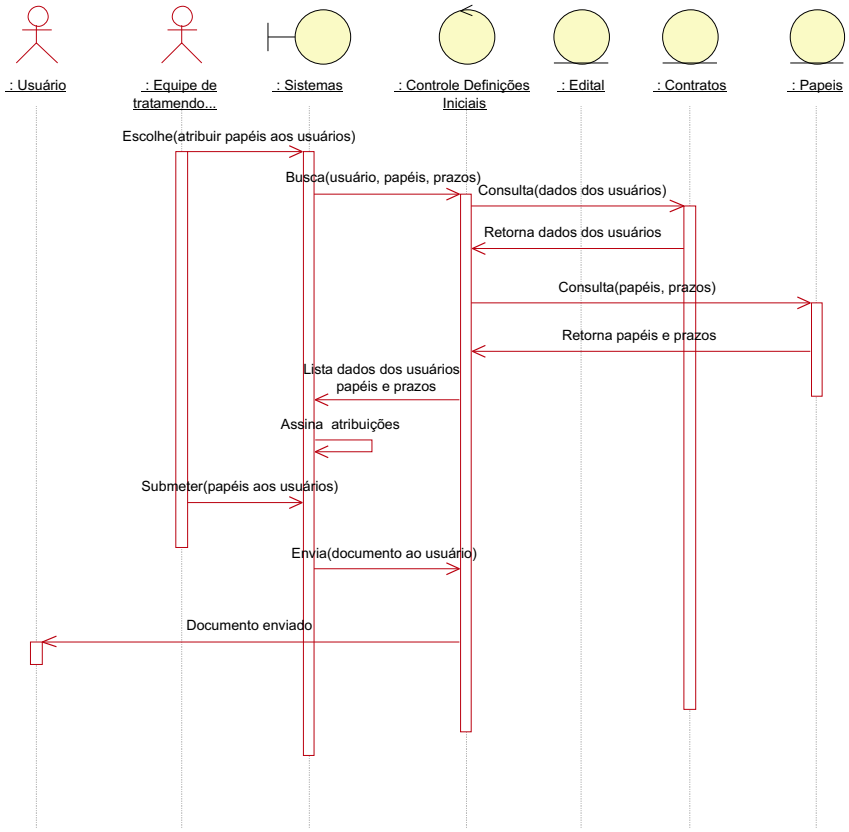

Figura C.17: Diagrama 5 de seqüência do use case definições iniciais com ICP

C.5.2.8 Diagrama de estados

O diagrama de estado deste use case passa a ser o apresentado na figura C.18.

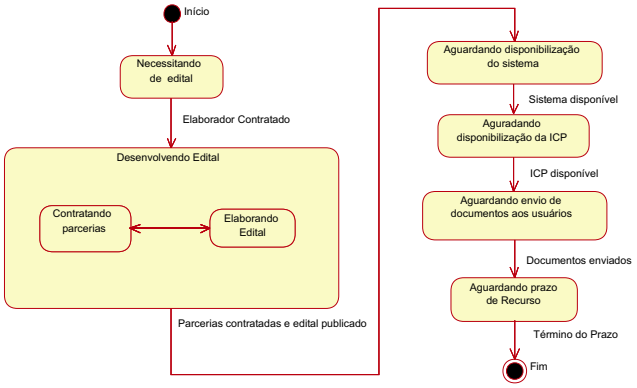

Figura C.18: Diagrama de estados do use case definições iniciais com ICP

C.5.3 Demais use cases

Como a comunicação, o acesso ao sistema e o envio de documento para solicitação de certificado são tratados à parte, as alterações nos use cases elaboração, inscrição, aplicação e correção e divulgação dos resultados restringem-se as alterações nas pré e pós-condições, como descrito a seguir.

C.5.3.1 Pré-condições

Adiciona-se a seguinte pré-condição a estes use cases:

- ICP disponível

C.5.3.2 Pós-condições

Como neste modelo tanto a comunicação como o armazenamento se dá de forma segura, pode-se considerar as seguintes pós-condições para cada use case:

- use case elaboração
  - banco de questões seguro, em formato digital
  - instrumento de avaliação seguro, em formato digital
- use case inscrição
  - banco de dados seguro de candidatos homologados com seus respectivos locais de avaliação
- use case aplicação
  - banco de dados seguro de respostas dos candidatos ao instrumento de avaliação entregue ao coordenador de aplicação
- use case correção e divulgação dos resultados
  - banco de dados seguro do resultado final (classificação dos candidatos aprovados) homologado