FABRÍCIO ABRÃO COSTA

MODERNIZAÇÃO DOS PROCESSOS DE AUDITORIA E FISCALIZAÇÃO DA ICP BRASIL

FLORIANÓPOLIS – SC

2010

UNIVERSIDADE DO ESTADO DE SANTA CATARINA – UDESC
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO

FABRÍCIO ABRÃO COSTA

MODERNIZAÇÃO DOS PROCESSOS DE AUDITORIA E FISCALIZAÇÃO DA ICP BRASIL

Dissertação apresentada à Universidade do Estado de Santa Catarina como requisito para a obtenção do título de Mestre em Administração.

Orientador: Carlos Roberto De Rolt

FLORIANÓPOLIS – SC

2010

FABRÍCIO ABRÃO COSTA

MODERNIZAÇÃO DOS PROCESSOS DE AUDITORIA E FISCALIZAÇÃO DA ICP BRASIL

Dissertação aprovada como requisito parcial para a obtenção do grau de Mestre em Administração, no curso de Mestrado Profissional em Administração, do Programa de Pós-Graduação em Administração da Universidade do Estado de Santa Catarina.

Banca Examinadora:

Orientador:

_____
Prof. Dr. Carlos Roberto De Rolt
Universidade do Estado de Santa Catarina

Membro:

_____
Prof. Dr. Julio da Silva Dias
Universidade do Estado de Santa Catarina

Membro Externo:

_____
Prof. Dr. Ricardo Felipe Custódio
Universidade Federal de Santa Catarina

Florianópolis - SC, __/__/___

À minha namorada, família, amigos e colegas de trabalho, pelo incentivo, paciência e compreensão que tornaram possível este trabalho.

AGRADECIMENTOS

A Deus, pela vida.

Em especial a meus pais, Regina e Luiz (*in memorian*), por todos os esforços realizados pela minha educação e formação como pessoa e como profissional.

A toda minha família, pilar de minha vida, meus avós, pais, irmãs, tios, tias, primos e primas, pelo apoio dado sempre que necessário.

A minha namorada Francine, por todo o seu apoio, compreensão, paciência, estímulo e amor.

Ao meu orientador Carlos Roberto De Rolt, pela confiança depositada em minha capacidade em realizar este trabalho.

Aos professores Julio da Silva Dias, Nério Amboni e Mário César Barreto Morais, pelas valiosas sugestões dadas no desenvolvimento da pesquisa.

A meus colegas de trabalho, pela compreensão e apoio sem as quais a execução deste trabalho seria mais difícil.

Aos meus colegas de mestrado, pela troca de experiências e amizade.

A ESAG e seus professores, pela oportunidade dada, pelo conhecimento compartilhado e pelo tempo despendido pela minha formação.

E finalmente a todos meus amigos, pelas risadas que tornaram o mestrado uma experiência mais leve de ser realizada.

Estamos nos anos inicias de um tempo que chamo de "década digital" - uma era em que computadores deixarão de ser meramente úteis para se tornar uma parte significativa e indispensável de nossa vida diária.

BILL GATES

RESUMO

A Infraestrutura de Chaves Públicas Brasileira é um conjunto de técnicas, arquiteturas, organização, práticas e procedimentos, definidos pelas organizações governamentais e privadas brasileiras que suportam, em conjunto, a implementação e a operação de um sistema de certificação. O produto das organizações que formam essa estrutura é o certificado digital, um documento eletrônico particular de uma pessoa física ou jurídica que garante a autenticidade, integridade e validade jurídica de documentos em forma eletrônica e possibilita as transações eletrônicas seguras. As entidades que fazem parte da Infraestrutura de Chaves Públicas Brasileira recebem auditorias constantes a fim de verificar e controlar o perfeito seguimento de todas as normas a que estão submetidas, de modo a garantir a qualidade e confiabilidade dos serviços oferecidos. Apesar das entidades da estrutura existirem em função da certificação digital e da confiança nos documentos e nas transações eletrônicas, seus processos de auditoria e fiscalização não utilizam plenamente todas as vantagens e facilidades que o certificado digital, o documento eletrônico e a tecnologia da informação e comunicação proporcionam. O presente trabalho foca na modernização e automação destes processos. Na pesquisa foi utilizada uma abordagem teórico-empírica, utilizando a revisão da literatura sobre o assunto e a pesquisa nos documentos de normatização da Infraestrutura de Chaves Públicas Brasileira para entender a atual situação dos seus processos de auditoria e poder desenvolver e propor uma nova metodologia para a realização automatizada da auditoria e fiscalização das entidades da estrutura, utilizando a certificação digital e o documento eletrônico nas transações entre o sistema e seus usuários. A pesquisa mostra que a nova metodologia proposta é viável e possível de ser implementada, porém necessita de mais estudos para ser possível implantá-la.

PALAVRAS-CHAVE: Infraestrutura de Chaves Públicas. Auditoria. Gestão de processos.

ABSTRACT

The Brazilian Public Key Infrastructure is a set of techniques, architectures, organization, practices and procedures defined by brazilian government and private organizations that support, in overall, the implementation and operation of a certification system. The product of the organizations that form this structure is the digital certificate, a particular electronic document of a person or organization which guarantees the authenticity, integrity and legal validity of documents in electronic form and enables safes electronic transactions. The entities that are part of Brazilian Public Key Infrastructure receive constant audits to verify and control the perfect follow all the rules that are submitted in order to ensure quality and reliability of services offered. Although the structure of entities exist on the basis of digital certification and trust in the electronic documents and digital transactions, their process of auditing and supervision are not using and enjoying fully all the advantages and facilities that the digital certificate, electronic document and information technology and communication provides. This work focuses on the modernization and automation of these processes. In the survey was used a theoretical-empirical approach using the literature review on the subject and research in normative documents of Brazilian Public Key Infrastructure to understand the current status of their audit procedures and be able to develop and propose a new methodology to achieve automated auditing and supervision of entities of the structure, using digital certification and electronic document transactions between the system and its users. Research shows that the new methodology proposal is feasible and can be implemented, but needs more studies to be able to deploy it.

KEYWORDS: Brazilian Public Key Infrastructure. Auditing. Process Management.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

AC – Autoridade Certificadora

AC Raiz – Autoridade Certificadora Raiz

ACT – Autoridade de Carimbo de Tempo

AR – Autoridade Registradora

BPM - *Business Process Modeling*

BPMN - *Business Process Modeling Notation*

CG – Comitê Gestor

CNPJ - Cadastro Nacional de Pessoas Jurídicas

DAFN - Diretoria de Auditoria, Fiscalização de Normalização

DES - *Data Encryption Standard*

DPC - Declarações de Práticas de Certificação

FGTS - Fundo de Garantia por Tempo de Serviço

HSM - *Hardware Security Model*

ICP - Infraestrutura de Chaves Públicas

ICP Brasil - Infraestrutura de Chaves Públicas Brasileira

ITI – Instituto de Tecnologia da Informação

ITU - *International Telecommunication Union*

ITU-T - *International Telecommunication Union Standardization Sector*

PC - Políticas de Certificado

PLAAO – Plano Anual de Auditoria Operacional

PS - Políticas de Segurança

PSC – Prestador de Serviço de Certificação

PSS – Prestador de Serviços de Suporte

SCT - Sistema de Carimbo do Tempo

SIGE – Sistema Integrado de Gestão Empresarial

SUMARIO

1 INTRODUÇÃO

1.1 TEMA E PROBLEMA DE PESQUISA

A segunda metade do século passado foi marcada por uma revolução que mudou a forma como as pessoas e as organizações se relacionam. A popularização dos computadores e a sua adoção cada vez mais frequente no trabalho e no lazer resultaram em uma revolução socioeconômica tão intensa que não era vista desde a revolução industrial no século XIX. A revolução informacional, possibilitada pelos computadores e as redes que eles formam, deu origem a uma sociedade onde o acesso à informação tornou-se fácil e abrangente. O mundo ficou menor, as distâncias diminuíram, a comunicação ficou mais rápida e dinâmica e o conhecimento tornou-se abundante e largamente disseminado (CASTELLS, 1999).

A revolução das redes de computadores foi relevante não apenas no aspecto social, com a facilitação da interação e acesso ao conhecimento pelas pessoas comuns. As empresas, os negócios e a economia em geral sofreram grandes abalos com a nova maneira de se comunicar que emergiu a partir da utilização cada vez mais frequente das redes computacionais. Neste novo cenário, os mercados tornaram-se mais dinâmicos e as organizações precisaram se adaptar a um ambiente cada vez mais mutável, fruto da nova realidade de se fazer negócios, fazendo surgir uma economia baseada na tecnologia da informação denominada de economia digital (TAPSCOTT, 2006).

Na economia digital reuniões são feitas em frente a telas de computadores com pessoas que podem estar em lados opostos do mundo, mas estão se vendo e se comunicando em tempo real. Negócios são fechados e contratos são assinados através de documentos eletrônicos que transitam com rapidez pelas redes mundiais de comunicação digital. O ambiente de intensas mudanças imposto pela economia digital forçou as empresas a se adaptarem, correndo o risco de perda de vantagem competitiva caso ignorassem o cenário econômico nascente.

Mas mesmo com as vantagens que o uso do documento eletrônico oferece, há um problema ao decidir utilizá-los ao invés de utilizar documentos em papel: a falta de segurança. Os documentos eletrônicos por si só não são confiáveis como os

documentos em papel a ponto de apresentarem os atributos necessários para terem servirem de prova jurídica, tais como a autenticidade, a integridade, a tempestividade e o não repúdio. Além dessas, é desejável que um documento possa ter o atributo do sigilo, quando a informação contida nele deva ser acessada apenas pelas partes desejadas.

Dessas necessidades, a partir de 1976 foram criadas técnicas de segurança dos dados digitais que possibilitam ao documento eletrônico apresentar os atributos necessários para se tornar confiável (DIFFIE; HELLMAN,1976), e a primeira delas foi o sigilo através da criptografia.

A criptografia é um processo que permite que um documento eletrônico, que possui um conteúdo legível, seja cifrado através de algoritmos ativados por uma senha, uma chave criptográfica. Depois de cifrado, apenas quem possui a chave para decifrar o conteúdo do documento consegue ler a informação nele contida como era originalmente.

Dois métodos principais de cifrar documentos eletrônicos foram criados: a criptografia simétrica e a criptografia assimétrica. Pela criptografia simétrica a mesma chave que cifra a mensagem é usada para decifrá-la. Pela criptografia assimétrica uma chave é usada para cifrar a mensagem e outra é usada para decifrá-la, e a partir de uma chave não é possível descobrir a outra. O segundo método é mais seguro que o primeiro pelo fato de a chave usada para atribuir o segredo à informação não precisar ser compartilhada para que a informação possa ser acessada.

Através do conceito da criptografia assimétrica, River, Samir e Adleman (1978) criaram um algoritmo de criptografia de dados, o RSA, que utiliza um par de chaves para cifrar e decifrar dados. Esta técnica foi utilizada na concepção dos certificados digitais, que possibilitaram ao documento eletrônico obter as características necessárias para ser confiável como substituto dos documentos em papel. Certificados digitais são um tipo de documento eletrônico gerado a partir de técnicas criptográficas assimétricas. Possuem a função de documentos de identificação digitais e são gerados por partes confiáveis que possuem responsabilidades sobre eles.

Um certificado digital possui informações da pessoa física ou jurídica a quem

identifica, além de informações da entidade confiável que o gerou e é responsável pela sua validade. O certificado digital pode ser distribuído a quem interessar, devido a isso ele é a chave pública de um par de chaves do qual faz parte, e a chave privada à qual é relacionado apenas o dono do certificado digital possui acesso através de uma senha. O que a chave pública cifra só é possível decifrar com a chave privada respectiva, e o que a chave privada cifra só é possível decifrar com a chave pública respectiva.

Com a chave privada de um certificado digital, é possível inserir uma assinatura digital, através de algoritmos criptográficos, em um documento eletrônico que o relacione à chave e assim garantir sua autenticidade e não repúdio do mesmo modo como um documento em papel assinado por uma pessoa (MCCULLAGH, 1998). A integridade do documento é garantida quando é feita a verificação da informação original com a informação assinada. Caso o texto original tenha sido alterado após o documento ter sido assinado, ao ser comparado com a informação assinada, a mudança é constatada.

Para garantir o atributo da tempestividade em documentos eletrônicos, é necessário existir outra parte confiável que, com o uso de certificados digitais e protocolos definidos em padrões e normas de formatos e de comunicações mundialmente seguidos, emite um carimbo do tempo eletrônico e o relaciona a um documento eletrônico (HARBER, 1991; BULDAS, 2000; RFC 3161, 2001). Esse processo é denominado de protocolo eletrônico e o tempo é fornecido por um relógio de precisão por uma entidade denominada de Autoridade de Carimbo do Tempo (ACT). Com o carimbo do tempo é possível saber quando a assinatura de um documento eletrônico era válida.

A entidade confiável responsável por emitir um certificado digital e garantir a sua validade é denominada de Autoridade Certificadora (AC). Ela desempenha o papel de uma organização que possui confiabilidade e poderes jurídicos legais para gerar esses documentos de identidade digital. Para que uma pessoa física ou jurídica possa solicitar um certificado digital, ela deve apresentar-se a uma Autoridade Registradora (AR), que desempenha o papel de um balcão de atendimento de uma Autoridade Certificadora, para comprovar a sua legalidade existencial. A Autoridade Registradora encaminha o pedido de geração de

certificado digital à Autoridade Certificadora a qual representa para que esta inicie o processo de geração da identidade digital do solicitante. Para gerar o certificado digital a Autoridade Certificadora utiliza os sistemas de *software* e de *hardware* para este fim que estão hospedados em um ambiente fisicamente seguro e controlado, que forma outra entidade denominada de Prestador de Serviços de Suporte (PSS). Quando pronto, o certificado digital gerado pode ser recebido diretamente na Autoridade Registradora onde foi solicitado ou ser recebido através da internet.

O Prestador de Serviços de Suporte é contratado por uma Autoridade Certificadora, uma Autoridade Registradora ou uma Autoridade de Carimbo do Tempo para disponibilizar a infraestrutura física e lógica para os serviços de emissão de certificados digitais e de carimbos do tempo e/ou os recursos humanos especializados para executar os serviços. Possui uma sala-cofre, um tipo de ambiente seguro, vigiado e controlado por sensores de movimento, calor, luminosidade e câmeras de vídeo, além de guardas armados e níveis de autorização de entrada acessíveis apenas por métodos criptográficos de segurança como: biometria, senha e identificação por certificados digitais. É neste ambiente seguro que o Prestador de Serviços de Suporte armazena os sistemas necessários para gerar os certificados e carimbos de tempo digitais.

No Brasil existe uma regulamentação para o funcionamento das entidades descritas. Essa regulamentação é denominada de Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), um conjunto de técnicas, práticas e procedimentos que foram traçadas pelo seu Comitê Gestor (CG) com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chaves públicas. A ICP-Brasil é composta por uma cadeia de Autoridades Certificadoras. Essa cadeia é formada por uma Autoridade Certificadora Raiz – AC Raiz, Autoridades Certificadoras e Autoridades de Registro, e por uma autoridade gestora de políticas, o Comitê Gestor da ICP-Brasil.

As Autoridades Certificadoras credenciadas na ICP-Brasil são auditadas pela AC Raiz antes de iniciarem seus serviços. A AC Raiz, por sua vez, é mantida e controlada pelo Instituto Nacional de Tecnologia da Informação (ITI), uma autarquia vinculada à Presidência da República. A auditoria verifica se as exigências das normas da ICP-Brasil são integralmente cumpridas para só depois credenciar uma

Autoridade Certificadora. Após o credenciamento persiste o dever de a Autoridade Certificadora cumprir todas as obrigações assumidas. Essa verificação é feita através de uma auditoria anual onde a equipe de auditoria do ITI verifica se todas as normas e exigências impostas pela legislação da ICP-Brasil estão sendo cumpridas.

O objetivo das auditorias é verificar o cumprimento das resoluções, normas, procedimentos e atividades dos Prestadores de Serviço de Certificação (PSC), Autoridades Certificadoras e Autoridades de Registro, com a finalidade de examinar se as operações de cada um deles, isolada ou conjuntamente, estão em conformidade com as suas respectivas Declarações de Práticas de Certificação (DPC), Políticas de Certificado (PC), Políticas de Segurança (PS), e as demais resoluções e normas estabelecidas para as entidades integrantes da ICP-Brasil.

A fiscalização tem o mesmo objetivo das auditorias, com a diferença que uma auditoria é realizada de forma pontual e planejada conjuntamente entre o auditor e o PSC, através de um cronograma bem definido. A fiscalização é realizada sempre que haja suspeita de desrespeito às normas e regras da ICP-Brasil por um PSC.

Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do Comitê Gestor da ICP-Brasil, as atividades de auditoria e fiscalização em todas as entidades da ICP-Brasil são de responsabilidade da AC Raiz. Porém, as auditorias podem ser realizadas por terceiros por ela autorizados, mas as fiscalizações não. Há uma regulamentação, no âmbito da Infraestrutura de Chaves Públicas Brasileira, para as atividades de auditoria e de fiscalização a serem realizadas pela AC Raiz ou pelos terceiros por ela autorizados.

Existe uma normatização a ser seguida para a auditoria e para a fiscalização das entidades pertencentes à estrutura da ICP-Brasil. Os processos dessa normatização são na sua maioria realizados de forma manual e com suporte do papel como substrato para armazenar as informações de todas as atividades de execução e conclusão de auditoria, o que os tornam lentos e custosos. Essa característica é observada em processos justamente em uma instituição que tem como objetivo facilitar e garantir a segurança do uso de documentos eletrônicos e sistemas automatizados através da utilização da certificação digital.

O uso do documento eletrônico, utilizado em conjunto com as técnicas de

certificação e protocolação digital disponibilizadas por uma Infraestrutura de Chaves Públicas, torna possível a automação dos processos de organizações pelas redes de computadores, tornando-os mais ágeis, dinâmicos, baratos, eficientes e dotando-os de segurança e validade jurídica.

No Brasil a estrutura que possibilita a confiança no uso do documento eletrônico é representada pela ICP-Brasil e controlada pelo ITI através da AC Raiz. No entanto, para a mais relevante de suas atividades, a auditoria, o documento eletrônico não é utilizado para a automação de seus processos e, consequentemente, para diminuir os custos e aumentar a eficiência dessas atividades. A ICP-Brasil realiza seus processos de auditoria de modo contrário à finalidade a que se propõe: possibilitar o uso do documento eletrônico em qualquer processo de forma segura, confiável e eficiente.

Com a utilização das técnicas de certificação e protocolação digital é possível automatizar os processos de auditoria da ICP-Brasil em um sistema eficiente, ágil e seguro. Esse sistema seria acessível através das redes de computadores somente a pessoas e organizações devidamente credenciadas. Ele proporcionaria um maior e mais eficiente controle da fiscalização das entidades da estrutura pela AC Raiz e pelo ITI.

Com as características possibilitadas pela automação dos processos de auditoria da ICP-Brasil, ela seria dotada de uma grande vantagem competitiva frente ao modelo tradicional de auditoria manual e com a utilização do papel. Isto resultaria em um maior controle destes processos e maior agilidade e simplicidade no seu gerenciamento. Algo que poderia acontecer também seria o barateamento do certificado digital, possibilitado pela redução de custos com estes processos, o que poderia ocasionar em uma maior popularização de seu uso.

Este é o tema que orientará esta pesquisa, a modernização dos processos de auditoria e fiscalização da ICP-Brasil através da automação e utilização do documento eletrônico seguro. Dessa forma a pergunta que orientará esta pesquisa é: como os processos de auditoria e de fiscalização da ICP-Brasil podem ser modernizados através da automação e do uso de documentos eletrônicos seguros?

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Propor um modelo para modernizar os processos de auditoria e fiscalização da ICP-Brasil, através da automação e do uso do documento eletrônico seguro.

1.2.2 Objetivos Específicos

- Mapear os processos de realização de auditoria e de fiscalização da ICP-Brasil;
- Modelar o estado atual da arte dos processos de realização de auditoria e de fiscalização da ICP-Brasil utilizando BPMN - *Business Process Modeling Notation*;
- Identificar os processos de realização de auditoria e de fiscalização da ICP-Brasil que podem ser automatizados;
- Identificar onde é possível utilizar o documento eletrônico seguro nos processos automatizados de realização de auditoria e de fiscalização da ICP-Brasil;
- Propor um modelo para a automação e uso do documento eletrônico seguro nos processos de realização de auditoria e de fiscalização da ICP-Brasil;
- Modelar a proposta utilizando BPMN - *Business Process Modeling Notation*;
- Analisar o impacto do modelo proposto sobre o modelo praticado atualmente.

1.3 JUSTIFICATIVA DA PESQUISA

A tecnologia da informação, com o suporte das redes de computadores e do

uso dos documentos eletrônicos, possibilita a automação dos processos, tornando-os mais dinâmicos, ágeis e com menores custos de execução. Entretanto, é necessário haver confiança nos documentos e transações eletrônicas para que possam ser utilizados como substitutos eficientes aos documentos e transações utilizando o papel como substrato.

A confiabilidade é garantida com o uso dos certificados digitais, que por sua vez têm sua confiabilidade garantida por estruturas compostas por normas para as entidades que a compõe, cada uma com tarefas distintas nos processos do ciclo de vida dos certificados digitais. Essas estruturas são denominadas de Infraestruturas de Chaves Públicas (ICP). No Brasil existe uma estrutura deste tipo com abrangência nacional e mantida pelo Instituto de Tecnologia da Informação, uma autarquia ligada ao governo Federal. Essa estrutura recebe o nome de Infraestrutura de Chaves Públicas Brasileira, a ICP-Brasil.

Existem processos importantes na ICP-Brasil que, apesar de serem executados em uma estrutura que existe para tornar seguro o uso do documento eletrônico e das transações eletrônicas, ainda não utilizam com eficiência os benefícios da segurança da informação possibilitados pelo uso dos certificados digitais. Muitos desses processos importantes não são automatizados, ainda são executados de forma manual e com o uso do papel como subtrato para a troca e guarda de informações.

Toda organização que deseja fazer parte da estrutura da ICP-Brasil deve provar que esta apta a seguir as normas para as atividades da entidade que ela pretende desempenhar. Os processos para realizar essa prova exigem muito trâmite de documentos e produzem grande quantidade de relatórios e documentação em papel. Esta é a auditoria pré-operacional da organização candidata.

Após ser aprovada, a organização recebe auditorias programadas e constantes enquanto ela fizer parte da estrutura, pela AC Raiz ou por entidades que a representam e são capacitadas a realizar auditorias nas entidades da estrutura. Vários dos processos destas auditorias constantes que poderiam ser automatizados também ainda são manuais e geram grandes quantidades de relatórios e outros documentos em papel.

Estes processos de auditoria e fiscalização representam um paradoxo ao objetivo de uma Infraestrutura de Chaves Públicas, que é garantir a confiabilidade nos documentos e transações eletrônicas, tornando possível utilizá-los com a mesma confiabilidade dos documentos em papel e das transações manuais. A automação dos processos poderia torná-los mais eficientes e dinâmicos. A eficiência e a dinamicidade reduziriam os seus custos de execução, aumentariam o controle dos processos e tornaria mais simples seu gerenciamento.

Além do maior controle dos processos, o que seria o principal benefício ocasionado pela auomação, o custo da estrutura também poderia sofrer um impacto benéfico. O custo da ICP-Brasil é justamente um fator que atualmente traz riscos à viabilidade da estrutura e pode torná-la inviável em longo prazo, devido ao produto ter um alto preço final, o que dificulta a disseminação de seu uso.

Para manter uma Infraestrutura de Chaves Públicas dispendiosa funcionando é necessário que os seus produtos finais, os certificados digitais e também os carimbos do tempo, tenham preços que consigam viabilizá-la financeiramente. O certificado digital tem um período de validade curto, de um a três anos, e precisa ser renovado quando seu período de validade expira. Projetos de ampla inclusão digital que necessitem do uso do certificado digital, por exemplo, são inviáveis com os preços que os mesmo possuem atualmente.

Analisando a situação atual da estrutura, podemos visualizar os seguintes pontos críticos em relação aos processos de auditoria e fiscalização:

- A necessidade de auditorias com processos manuais para cadastramento e gerenciamento de todas as entidades que compõe a estrutura;
- Produção excessiva de documentos e relatórios em papel nas auditorias que poderiam não ser necessários se os processos fossem automatizados e utilizasse o documento eletrônico seguro.

Pelas normas, as auditorias e fiscalizações podem ser realizadas pela AC Raiz ou, no caso das auditorias, por entidades capacitadas a realizar auditorias nas entidades da ICP-Brasil. No caso de entidades capacitadas, a AC Raiz precisa ser informada dos resultados das auditorias realizadas por elas. O resultado de todas as auditorias em cada entidade da estrutura também deve ser de conhecimento de toda

entidade superior à entidade que a recebeu.

Utilizando a tecnologia da informação e as redes de computadores para tornar possível a automação dos processos de auditoria da ICP-Brasil, e utilizando a tecnologia dos certificados digitais e carimbos do tempo para possibilitar a segurança das transações realizadas no sistema automatizado e do armazenamento das informações em documentos eletrônicos seguros, é possível minimizar os custos e a complexidade destes processos e, consequentemente, do funcionamento da estrutura como um todo, tornando os processos mais simplifacos e possibilitando melhorar seu gerenciamento, e também pode impctar nos produtos finais, tornando-os mais baratos e acessíveis.

Um Sistema Integrado de Gestão Empresarial (SIGE) para integrar os dados e os processos de negócio de auditoria e fiscalização da estrutura da ICP-Brasil em um único sistema possibilitaria, além de maior eficiência e agilidade dos processos, também o compartilhamento destes serviços de auditoria entre as entidades da estrutura que o realizam, assim como também as que são afetadas por eles.

Todas as entidades que realizam auditoria e fiscalização poderiam acessar um único sistema integrado de auditoria utilizando a segurança proporcionada pelos certificados digitais, navegando apenas por áreas em que é permitido o seu acesso e registrando todos os seus passos através de assinaturas e protocolações digitais, dotando de validade jurídica os processos e documentos eletrônicos e utilizando a própria competência da ICP-Brasil em suas atividades.

O compartilhamento de serviços, quando adotado como estratégia de vantagem competitiva nas organizações, resulta em benefícios aos usuários do produto final, pois diminui os custos das operações e consequentemente diminui o custo do produto final (PORTER, 1999).

A automação dos processos de auditoria e fiscalização da ICP-Brasil proporcionada pelo sistema de serviços compartilhados seria visível nos benefícios proporcionados ao ITI pelo maior controle sobre as auditorias que ele teria, devido ao acesso mais ágil e facilitado às informações de todas as auditorias realizadas.

1.4 ESTRUTURA DA DISSERTAÇÃO

Quanto à sua estrutura, este trabalho está divido em seis capítulos da seguinte forma:

O primeiro capítulo apresenta a contextualização, o tema e o problema que orientaram o desenvolvimento da pesquisa, o objetivo geral e os objetivos específicos, e a relevância do tema estudado.

O segundo capítulo apresenta a revisão da literatura para a fundamentação da pesquisa. Este capítulo inicia com uma narrativa sobre a tecnologia da informação, sua história e como ela foi incorporada pela sociedade moderna para evidenciar sua importância nos dias atuais. Após é apresentado o conceito de documento eletrônico, o tipo de substrato para guardar informações que se tornou comum com a disseminação e uso da tecnologia da informação, e suas características e problemas. Em seguida é apresentado o conceito de Infraestrutura de Chaves Públicas, que soluciona os problemas do documento eletrônico, para depois então discorrer sobre uma Infraestrutura de Chaves Públicas em particular, a ICP-Brasil. É nesse ponto onde é tratado o tema central dessa pesquisa. Na continuação são apresentados os conceitos e ferramentas que serão utilizadas para a proposta a que esse trabalho se justifica, o conceito de Organizações Virtuais e Serviços Compartilhados e a ferramenta BPMN para o Mapeamento de Processos estudados na pesquisa.

No terceiro capítulo estão apresentados os procedimentos metodológicos da pesquisa, incluindo a caracterização, a coleta e análise dos dados e as limitações encontradas durante a pesquisa.

No quarto capítulo está o resultado dos dados coletados, através de uma descrição narrativa e gráfica dos processos estudados, para mostrar o estado atua da forma como são executados.

O quinto capítulo apresenta a discussão dos dados, onde são apresentados os problemas encontrados no estado atual da arte dos processos foco da pesquisa, e é apresentado o desenvolvimento do modelo da proposta para resolver os problemas através de uma nova forma de executar os processos de realização de

auditoria e de fiscalização da ICP-Brasil.

No sexto capítulo estão as considerações finais do estudo e as conclusões, relacionamento os objetivos propostos com os resultados alcançados. Também são feitas recomendações para futuras pesquisas.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 TECNOLOGIA DA INFORMAÇÃO

Definir o que é a Tecnologia da Informação é algo complicado. O seu conceito é mais abrangente do que os conceitos de processamento de dados, sistemas de informação, engenharia de *software*, informática ou o conjunto de *hardware* e *software*. Envolve também aspectos humanos, administrativos e organizacionais (KEEN, 1993).

Alter (1992) faz distinção entre a Tecnologia da Informação, que segundo o autor abrange apenas aspectos técnicos, com os Sistemas de Informação, que segundo o autor abrange as questões de fluxo de trabalho, pessoas e informação envolvida. Henderson e Venkatraman (1993) já definem a Tecnologia da Informação como envolvendo todos os aspectos.

Luftman *et al* (1993) e Weil (1992) definem um conceito mais amplo à Tecnologia da Informação. Segundo os autores o termo inclui os sistemas de informação, o uso de *hardware* e *software*, telecomunicações, automação e recursos multimídia utilizados pelas organizações para fornecer dados, informações e conhecimento. A Tecnologia da Informação é a aplicação de recursos tecnológicos para processar informações. É este conceito que será adotado para este trabalho.

Atualmente o mundo vive em uma era informacional onde praticamente toda a sociedade encontra-se interligada com todas as suas tarefas sendo realizadas por intermédio de computadores. A Tecnologia da Informação está presente em todos os setores profissionais e de lazer. As informações correm ao redor do mundo em altas velocidades através da grande rede de computadores da internet. Através dos computadores e das novas tecnologias tudo se encontra conectado e a informação nunca esteve tão à disposição como agora. Essa revolução informacional, assim como a revolução industrial, é um marco que mudou e ainda continua mudando as relações humanas de uma forma que elas nunca mais serão como eram antes (CASTELLS, 1999).

O termo tecnologia pode ser entendido como sendo uma ferramenta que utiliza o conhecimento técnico e científico para criar serviços, produtos ou processos

que melhorem a condição humana. Por esta definição de tecnologia pode-se afirmar que a história da Tecnologia da Informação é tão antiga quanto a história da humanidade, e que a linguagem foi a primeira Tecnologia da Informação criada pelo homem. Com o desenvolvimento das sociedades desenvolveram-se também as tecnologias utilizadas para processar a informação e o conhecimento que fora sendo criado. Ao longo da história, para armazenar informações, várias tecnologias foram desenvolvidas, como os tabletes de argila da Mesopotâmia, o papiro do Egito, o papel da China e a máquina de imprensa de Gutenberg. Com a necessidade de contar quantidades, tecnologias foram sendo criadas ao longo da história, como o ábaco, que evoluiu até as primeiras calculadoras analógicas de Pascal e Leibniz.

2.1.1 A Sociedade da Informação

O desenvolvimento dos computadores e das redes de computadores possibilitou que, no último quartel do século XX, uma nova forma de interação global entre pessoas e organizações surgisse e se difundisse. Essa sociedade moderna e sua forma de se relacionar socialmente, baseada nas novas tecnologias da informação e da comunicação, é chamada de Sociedade da Informação, ou ainda Sociedade do Conhecimento.

A Sociedade da Informação é uma forma evoluída de sociedade moderna e se caracteriza por um deslocamento de paradigma nas estruturas industriais e nas relações sociais. Tal qual a revolução industrial supôs uma profunda modificação das sociedades agrárias, A Sociedade da Informação designa uma forma nova de organização da economia e da sociedade (PEREIRA *et al*, 1997).

As características fundamentais da Sociedade da Informação são:

- Possuir a informação como matéria-prima;
- Alta penetrabilidade das novas tecnologias;
- Predomínio da lógica de redes;
- Flexibilidade e crescente convergência de tecnologias.

Nesse paradigma de sociedade a tecnologia se desenvolve para permitir ao homem atuar sobre a informação adaptando-as ou criando tecnologias novas para

novos usos, e não utilizar informação para agir sobre tecnologias como era feito no passado. Na nova tecnologia, todas as atividades humanas tendem a ser afetadas por ela, materialmente implementada em qualquer processo. Essa tecnologia possui alta capacidade de reconfiguração, reversão, modificação e reorganização e converge todas as tecnologias em processos comuns, como a microeletrônica, as telecomunicações, a optoeletrônica, os computadores em geral e até mesmo a biologia (CASTELLS, 1999).

2.2 DOCUMENTO ELETRÔNICO

Neste novo tipo de sociedade, a informação não depende mais de substratos físicos para ser armazenada. Agora a informação é armazenada em meios magnéticos e óticos através de bits, o chamado documento eletrônico. Ao se comparar o custo antes existente para armazenar a informação em papéis, dispositivos de áudio e de vídeo não digitais, fotografias em filmes fotossensíveis, entre outras formas de armazenamento não digitais, percebe-se que agora ele é ínfimo. A velocidade e facilidade de disseminação do documento eletrônico é enormemente maior do que o documento armazenado de forma física, o que aumenta em muito a velocidade e a agilidade nos processos.

O documento eletrônico permite desvincular a informação que ele armazena do substrato físico dos documentos em papel, permitindo que o conteúdo possa ser transmitido a longas distâncias através de redes de comunicação e ser armazenado em qualquer tipo de dispositivo computacional de armazenamento (DIAS, 2003). Ele se apresenta como um conjunto de bits que é visualizado com suporte computacional (SCHEIBELHOFER, 2001), através de ferramentas adequadas para interpretar o documento e tornar legível a informação contida nele.

Porém, o documento eletrônico apresenta algumas desvantagens em relação aos seus equivalentes em meio físico, particularmente ao papel, no que diz respeito à confiança em relação a ele. Alguns dos requisitos que o documento em papel apresenta e o documento eletrônico deve apresentar também para se tornar confiável são:

- Autenticidade - ser possível identificar quem criou o documento eletrônico. Como o documento eletrônico agora pode transitar livremente pela rede mundial de computadores, deve ser possível haver alguma maneira de ligar a pessoa que o criou a ele;
- Integridade - garantir que o documento eletrônico é original, não foi alterado depois que foi criado. Como a informação fica livre na rede de computadores, ela pode ser alterada facilmente por qualquer pessoa que tiver acesso a ela. Deve haver uma maneira de garantir que o documento eletrônico que armazena uma informação não sofreu modificações depois que foi criado;
- Não repúdio - garantir que quem criou o documento eletrônico não possa afirmar que não foi ele. Deve ser possível não apenas garantir a autenticidade do documento eletrônico, mas garantir que quem está ligado ao documento eletrônico realmente foi a pessoa que o criou ou que o autenticou;
- Tempestividade - ser possível identificar a data e hora universais exatas da criação do documento. Para saber exatamente quando um documento digital foi criado no tempo, deve-se atribuir a ele uma marcação de tempo universal por uma entidade confiável que garanta que ele foi criado naquela data e hora exata que a entidade definiu a ele.

Com a resolução destes problemas, o documento eletrônico se torna confiável para operações comerciais e processos jurídicos. Se a sociedade está em rede e a informação está armazenada em meio digital, que apresenta inúmeras vantagens em relação à informação armazenada em meio físico, nada mais lógico que o documento digital seja também utilizado em transações comerciais que reduziriam muito os custos com materiais e agilizariam enormemente os processos, apresentando uma vantagem competitiva muito grande à organização que adotasse o comércio eletrônico frente à organização que o ignorasse.

Além do comércio eletrônico, a confiança no documento eletrônico interessa às organizações também para protegerem as informações que elas armazenam. Com a informação digitalizada, fica mais simples para que a informação dos documentos sigilosos armazenados em meio digital sejam roubados, fragilizando e colocando em risco as organizações. Além dos requisitos já listados acima, o documento eletrônico deve apresentar mais uma característica que torne possível que informações sigilosas sejam armazenadas em meio digital sem que a

organização corra o risco de ser prejudicada com o vazamento das informações: a privacidade. O documento eletrônico precisa ter a possibilidade de ser cifrado e decifrado, para que a informação contida nele fique em segredo.

Com todos estes requisitos sendo atendidos, as organizações podem usar o documento digital sem preocupação em suas transações comerciais ou de contratos, no armazenamento de suas informações em mídias magnéticas e óticas e para garantir a transação segura de informações sigilosas através de computadores interligados em redes.

2.2.1 Criptografia

O termo criptografia vem do grego *kryptos*, cujo significado é oculto, e do grego *graphos*, cujo significado é escrita. O significado de criptografia é escrita oculta, ou seja, escrever de forma codificada. A criptografia surgiu da necessidade de registrar e transmitir informações de forma que apenas as partes envolvidas conseguissem ler a informação codificada. O processo de codificar uma informação é denominado de cifragem e o processo inverso, decodificar a informação, é chamada de decifragem.

A cifragem de um documento utiliza algoritmos matemáticos para modificar a informação. O algoritmo é ativado com uma chave, um segredo conhecido apenas pelas partes envolvidas, e a informação é então modificada utilizando a chave como o valor inicial para a execução do algoritmo. Para decifrar a mensagem modificada é necessário informar novamente uma chave para o algoritmo executar e transformá-la na mensagem original.

Quando essa chave é a mesma tanto para cifrar como para decifrar, o algoritmo é chamado de algoritmo de chave simétrica. Quando a chave para cifrar é diferente da usada para decifrar, o algoritmo é chamado de algoritmo de chaves assimétricas.

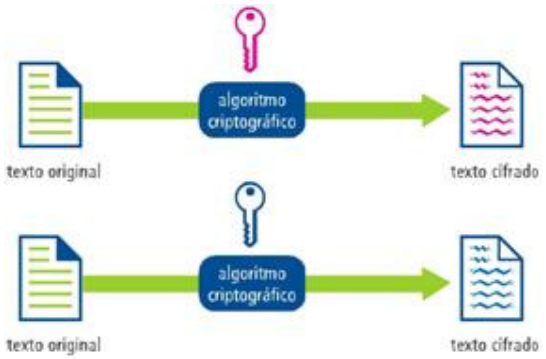

Ilustração 1 – Esquema de criptografia simétrica.

Fonte: O QUE É CERTIFICAÇÃO DIGITAL, p. 2

A história da criptografia é antiga e já era usada desde os hieróglifos do antigo Egito de 4000 atrás, mas onde ela começou a se mostrar mais relevante foi nas guerras mundiais do século XX. Nessa época, militares, diplomáticos e o governo em geral foram os maiores usuários das técnicas criptográficas, onde a criptografia foi usada como uma ferramenta para proteger os segredos e estratégias nacionais.

A proliferação de computadores e sistemas de comunicações na década de 1960 trouxe consigo a demanda do setor privado dos meios para proteger as suas informações em forma digital e também as empresas que começaram a prestar de serviços de segurança.

Ilustração 2 – Esquema de criptografia assimétrica com sigilo de informação.

Fonte: O QUE É CERTIFICAÇÃO DIGITAL, p. 4

Ilustração 3 - Esquema de criptografia assimétrica com autenticidade de informação.

Fonte: O QUE É CERTIFICAÇÃO DIGITAL, p. 5

O DES (*Data Encryption Standard*) é o mais conhecido dos mecanismos de criptografia. Começou a ser desenvolvido com o trabalho de Feistel (1974) na IBM no início da década de 1970 e culminou em 1977 com a adoção pela *U.S. Federal Information Processing Standard* para criptografar informações. Esse mecanismo de criptografia funciona de forma simétrica, ou seja, a mesma chave que é utilizada para cifrar o documento é utilizada para decifrá-lo. É um método criptográfico simples que restringe a confiabilidade no documento eletrônico.

O desenvolvimento mais marcante na história da criptografia veio em 1976 quando Diffie e Hellman (1976) publicaram *New Directions on Cryptography Techniques*. Este trabalho apresenta o revolucionário conceito de criptografia de chaves assimétricas e também fornece um método novo e engenhoso para troca de chaves. O novo método trazia o conceito de criptografia assimétrica, onde são utilizadas chaves distintas para cifrar e decifrar a informação, e a partir do conhecimento de uma chave não permite que se chegue a ter conhecimento da outra. Nesse método, uma chave é privada e deve ser mantida em segredo e a outra é pública e deve ser distribuída aos interessados.

Embora os autores não tivessem concretização prática de uma criptografia de chaves assimétricas na época, a ideia era clara e gerou um interesse amplo na comunidade de criptografia.

Em 1978, Rivest, Shamir e Adleman (1978) descobriram o primeiro e prático sistema de assinatura de criptografia de chaves assimétricas, conhecida como RSA. O ponto falho do algoritmo foi que ele não apresentava uma solução para relacionar

a chave pública a seu proprietário, o que abre brecha para fraudes no processo de proteger a informação.

Loren Kohnfelder (1978) propôs uma solução com a adoção de uma terceira entidade confiável, denominada de Autoridade Certificadora, que garante o relacionamento entre a chave pública e seu proprietário assinando a chave pública em um arquivo que contém também as informações do seu dono, o que controla a respectiva chave privada.

A partir do trabalho de Kohnfelder foi possível o desenvolvimento de uma infraestrutura de chaves públicas, formada por *softwares*, *hardwares*, técnicas criptográficas e serviços para o gerenciamento das chaves públicas dos usuários da estrutura, permitindo o uso de métodos criptográficos de chaves públicas de forma prática e confiável (DIAS, 2003).

2.3 INFRAESTRUTURA DE CHAVES PÚBLICAS

Uma Infraestrutura de Chaves Públicas é um órgão que tem como objetivo normatizar, fiscalizar e manter uma estrutura de emissão de chaves públicas. Utiliza o conceito de terceira parte confiável para as partes que utilizam os certificados digitais emitidos pelas entidades que fazem parte de sua estrutura. A Infraestrutura de Chaves Públicas é a responsável por definir as técnicas, práticas e procedimentos que devem ser seguidos pelas entidades que fazem parte dela, e compõe um sistema de certificação digital baseado em certificados digitais, o elemento mais básico da estrutura.

2.3.1 Certificado Digital

Os certificados digitais resolvem o problema de identificar quem controla a chave privada da respectiva chave pública e, segundo Housley (2001) *apud* Carlos (2007), deve possuir diversas características:

- Deve ser estritamente digital, para poder ser distribuído pelas redes de

computadores e processado automaticamente;

- Deve conter as informações do detentor da chave privada como o nome, organização e contato;
- Deve ser possível identificar a sua data de emissão;
- Deve ser criado por uma terceira parte confiável distinta de quem detém a chave privada;
- Deve ser diferençável de outros certificados digitais;
- Deve ser possível verificar se é genuíno ou falso;
- Deve ser inviolável e inalterável;
- Deve ser possível verificar imediatamente quando alguma informação no certificado se torna inválida;
- Deve ser possível determinar quais funções o certificado está habilitado a executar.

O ITU-T (1988), setor de padronização da *International Telecommunication Union*, determina que o certificado digital deva possuir as informações do nome, organização e dados para contato do detentor de sua chave privada, os campos de data com a sua validade inicial e final, as informações da terceira parte confiável que assinou o certificado e a assinatura do mesmo. O ITU-T também determinou (1993, 1997) que dentre as informações do certificado digital ele também teria extensões, sendo algumas pré-definidas que reforçam a identificação da terceira parte que assinou o certificado, como os atributos da sua chave e as restrições do seu caminho de certificação. O caminho de certificação é formado pelo certificado raiz e os certificados intermediários da terceira parte confiável, utilizados para assinar o certificado digital.

2.3.2 Lista de Certificados Revogados

Para poder ser possível verificar imediatamente quando um certificado digital se torna inválido, é preciso ter um meio de revogar o certificado em questão. Como o certificado é público e pode ser distribuído livremente, a maneira de fazer com que todos os seus detentores no momento saibam que ele está revogado é a terceira parte confiável publicar, em endereço fixo na internet, uma lista de certificados

revogados com a relação dos certificados que não são mais válidos.

Vários fatores podem tornar essa operação necessária, como a necessidade de alteração de dados do certificado digital antes do término de sua validade, o comprometimento de sua chave privada, o cancelamento de seu uso, o comprometimento da chave privada da terceira parte confiável que o assinou, entre outros.

A lista de certificados revogados é um arquivo digital para a validação eletrônica dos certificados digitais. É assinado pela terceira parte confiável que emitiu os certificados digitais, o que permite verificar sua integridade. Possui os campos com as datas de início e de expiração, a lista dos números seriais dos certificados revogados e a data de revogação e extensões opcionais.

2.3.3 Políticas de Certificação

Para ser possível determinar quais funções o certificado está habilitado a executar são utilizadas as Políticas de Certificação, definidas em documentos escritos pelos responsáveis por uma Autoridade Certificadora e que são seguidas para os seus processos de emissão de certificados. Os documentos onde elas são definidas geralmente são dois: as Políticas de Certificação – PC, e as Declarações de Práticas de Certificação – DPC.

As políticas de certificação são definidas como um conjunto de regras que indicam a aplicabilidade de aplicações com requisitos de segurança em comum de um certificado a uma comunidade ou classe de aplicação em particular (ITU-T, 1997).

As declarações de práticas de certificação são um conjunto de práticas seguidas pela Autoridade Certificadora e que definem as práticas relevantes ao ciclo de vida do certificado. São mais detalhadas que as Políticas de Certificação pois definem, além dos requisitos e restrições ao uso do certificado digital, também os procedimentos internos de gerenciamento dos procedimentos relativos ao certificado digital pela Autoridade Certificadora.

Uma infraestrutura de chaves privadas é formada de várias entidades, cada uma com tarefas e características distintas no gerenciamento do ciclo de vida dos certificados digitais. Essas entidades se dividem em Autoridades Certificadoras, Autoridades Registradoras, Repositórios de Certificados Digitais, Arquivos de Certificados Digitais, Módulos Públicos e Entidades Finais. A seguir serão explicados o que são e a função que desempenham na estrutura cada uma destas entidades.

2.3.4 Autoridade Certificadora

A Autoridade Certificadora é a entidade da infraestrutura responsável pela emissão dos certificados digitais e pela emissão e publicação das listas de certificados revogados, através de seu *hardware*, *softwares* e mão de obra especializada que a opera.

Ao assinar um certificado digital, a Autoridade Certificadora garante a autenticidade do certificado, por relacionar a chave pública com as informações do detentor da chave privada correspondente, e também sua validade, por incluir informações de data de início e de término de validade do certificado. Além das informações citadas, a Autoridade Certificadora também inclui no certificado digital outras informações que considerar relevantes. Esses certificados emitidos pela Autoridade Certificadora podem ser para entidades finais ou para outras Autoridades Certificadoras.

A emissão de listas de certificados revogados também é feita pela Autoridade Certificadora de modo a atestar a sua confiabilidade através de sua assinatura, de modo análogo à emissão dos certificados digitais. Essa lista é composta pelos certificados emitidos pela Autoridade Certificadora que já não são mais válidos, a data que o certificado perdeu sua validade e o motivo.

Uma infraestrutura de chaves públicas pode ter apenas uma Autoridade Certificadora, mas o mais comum é que existam outras Autoridades Certificadoras Intermediárias na estrutura que estejam abaixo de uma Autoridade Certificadora principal, a qual delega funções a essas outras entidades, como a emissão de certificados e de listas de certificados revogados.

É comum também uma Autoridade Certificadora delegar os processos de identificação de usuários que solicitam emissão de certificados digitais para uma entidade chamada de Entidade de Registro, que está relacionada à Autoridade Certificadora responsável por ela.

2.3.5 Autoridade Registradora

A Autoridade Certificadora pode ter mais de uma Autoridade Registradora sob sua responsabilidade. O número depende da abrangência dos serviços da Autoridade Certificadora, do número de clientes que ela possua ou da quantidade de tipos de certificados que ela tenha que emitir, o que torna necessário dividir a tarefa de verificar as requisições de certificados por quantas Autoridades de Registro seja necessário. No caso de haver emissão de diferentes tipos de certificados digitais, a divisão de tarefas para diferentes Autoridades Registradoras se justifica pelo fato de haver diferentes maneiras de verificação dos dados das requisições.

A Autoridade de Registro também é composta de *softwares*, *hardware* e mão de obra especializada. A requisição gerada é assinada por essa entidade, para que a Autoridade Certificadora a que está relacionada tenha certeza que os dados foram verificados por uma entidade de sua confiança e subordinação.

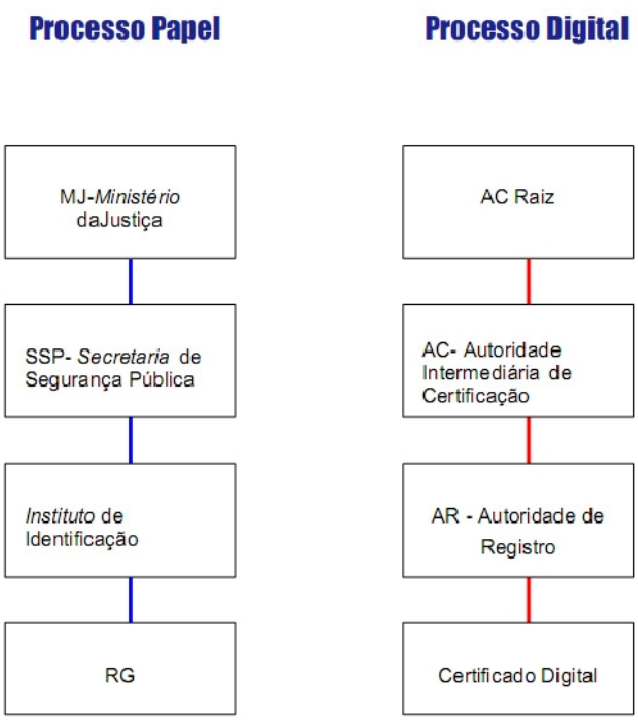

Ilustração 4 – Analogia entre o documento de identificação digital e o de papel.

Fonte: BROCARDO; DE ROLT; FERNANDES, 2006, p. 35

2.3.6 Repositório de Certificados Digitais

O Repositório de Certificados Digitais é uma entidade composta por *software* com a função de publicar os certificados digitais e as listas de certificados revogados emitidos por uma ou mais Autoridades Certificadoras a que está relacionado.

Os certificados digitais e listas de certificado revogados armazenados nessa entidade são assinados pela Autoridade Certificadora responsável por eles, o que garante a integridade e a autenticidade dos dados, tornando-os imunes a ataques de substituição e de fabricação [14].

Essa entidade faz a interação entre a Autoridade Certificadora e seus usuários, de onde é possível que estes obtenham os certificados digitais solicitados e as listas de certificados revogados para a validação dos mesmos. Dessa forma, a Autoridade Certificadora garante maior segurança a seus sistemas, por não torná-los disponíveis para acesso através de qualquer rede de comunicação. Essa tarefa fica a cargo do Repositório de Certificados, o qual deve estar sempre disponível e

seguro.

2.3.7 Arquivo de Certificados Digitais

Também relacionado a uma Autoridade Certificadora, os Arquivos de Certificados Digitais armazena os certificados digitais e as listas de certificados revogados emitidos por ela após o vencimento do período de validade dos mesmos.

Composta por *hardware* e *softwares*, esta entidade armazena os dados por prazo indeterminado, geralmente definido por normas jurídicas, para que possam ser utilizados na validação e verificação de documentos antigos assinados digitalmente sempre que for necessário.

2.3.8 Módulo Público

O módulo público também é relacionado e subordinado a uma Autoridade Certificadora, que pode ter um ou mais destas entidades, cuja função é fornecer uma interface ao usuário requisitar um certificado digital ou obter certificados digitais e listas de certificados revogados sem haver a necessidade de ter acesso direto a uma Autoridade de Registro, o que aumenta a segurança de uma Autoridade Certificadora.

2.3.9 Entidades Finais

Toda a estrutura da infraestrutura de certificados digitais e seus processos de gerenciamento do ciclo de vida dos certificados são voltados para a emissão de certificados para as Entidades Finais, que são qualquer detentor de um certificado digital sem permissão para assinar novos certificados digitais.

As Entidades Finais dividem-se em duas classes, e podem atuar alternadamente entre elas (HOUSLEY, 2001):

- Detentores de certificados – são usuários que possuem certificados

emitidos pela infraestrutura de certificados digitais e os utilizam, através das chaves privadas dos seus certificados particulares, para assinaturas e cifragens de dados;

- Entidades que confiam nos certificados – utilizam as chaves públicas dos certificados de outras entidades verificação de assinaturas, cifragem de dados, entre outros serviços de segurança.

2.4 ICP BRASIL

Para a elaboração deste capítulo foi utilizado o trabalho de Ribeiro *et al* (2004).

A Infraestrutura de Chaves Públicas Brasileira foi instituída pela Medida Provisória 2.200-2, de 24 de agosto de 2001, que criou o seu Comitê Gestor, a Autoridade Certificadora Raiz Brasileira e definiu as entidades que compõem a sua estrutura. Foi criada pelo Governo Federal com o objetivo de regulamentar as atividades de certificação digital no país, para incentivar a internet como meio para realização de negócios e inserir maior segurança às transações eletrônicas.

A ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira - é um conjunto de entidades, padrões técnicos e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais (RIBEIRO *et al*, 2004). É mantida pelo ITI, o Instituto Nacional de Tecnologia da Informação, que é uma autarquia federal vinculada à Casa Civil da Presidência da República.

O ITI integra o Comitê Executivo do Governo Eletrônico, no qual coordena o Comitê Técnico de Implementação do *Software* Livre no Governo Federal, e a ele compete a responsabilidade de estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital. Sua principal linha de ação é a popularização da certificação digital e a inclusão digital, atuando sobre variadas questões como:

- Sistemas criptográficos;
- *Software* livre;
- *Hardware* compatível com padrões abertos e universais;
- Convergência digital.

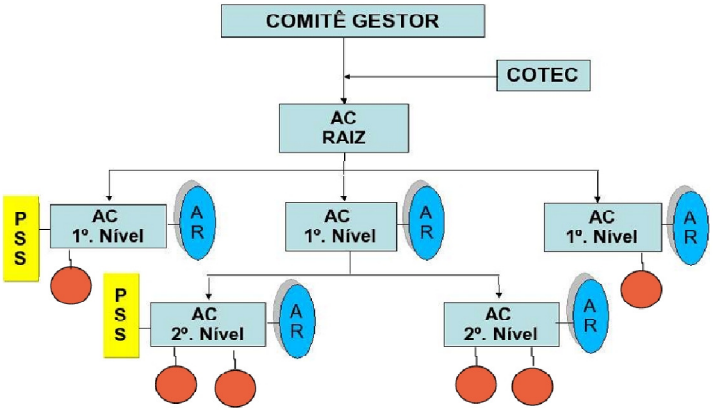

Ilustração 5 – Visão geral da ICP-Brasil.

Fonte: RIBEIRO *et al*, 2004, p. 6

Após a Medida Provisória 2.200-2, foram elaboradas as Resoluções do Comitê Gestor da ICP-Brasil, que são os regulamentos que regem as atividades das entidades integrantes da estrutura. Para assegurar que as entidades seguem todas as normas da estrutura, são realizadas auditorias no momento do credenciamento da entidade e anualmente. No credenciamento é verificado se a candidata a fazer parte da estrutura está apta a desenvolver as atividades a que se candidata conforme a regulamentação da estrutura, e anualmente é verificado se todos os procedimentos estão sendo executados seguindo conforme a mesma regulamentação.

A primeira entidade a receber auditoria na ICP-Brasil foi a sua Autoridade Certificadora Raiz, por uma comissão de membros de diversos órgãos do Governo Federal, para que o funcionamento dela fosse autorizado pelo seu Comitê Gestor.

Uma Infraestrutura de Chaves Públicas Brasileira é formada de várias entidades, cada uma com tarefas e características distintas, sendo elas: o Comitê Gestor, o Comitê Técnico, a Autoridade Certificadora Raiz, as Autoridades Certificadoras, as Autoridades Registradoras, os Prestadores de Serviços de Suporte, os Auditores Independentes e as Entidades Finais. A seguir serão explicados o que são e a função que desempenham cada uma destas entidades.

2.4.1 Comitê Gestor

O Comitê Gestor da ICP-Brasil possui as seguintes funções:

- Coordena a implantação e o funcionamento da ICP-Brasil;
- Estabelece a política, os critérios e as normas para credenciamento das AC, AR e demais PSS em todos os níveis da cadeia de certificação;
- Estabelece diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR;
- Define níveis da cadeia de certificação;
- Atualiza, ajusta e revisa os procedimentos e as práticas estabelecidas para a ICP-Brasil;
- Garante a compatibilidade da ICP-Brasil e promove a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança;
- Estabelece a política de certificação e as regras operacionais da AC Raiz;
- Homologa, audita e fiscaliza a AC Raiz e os seus prestadores de serviço;
- Aprova políticas de certificados, práticas de certificação e regras operacionais;
- Credencia e autoriza o funcionamento das AC e das AR;
- Autoriza a AC Raiz a emitir o correspondente certificado;
- Identifica e avalia as políticas de ICP externas;
- Negocia e aprova acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional;
- Certifica, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais;
- Pode delegar atribuições à AC Raiz.

2.4.2 Comitê Técnico

O Comitê Técnico – COTEC - é responsável por manifestar-se sobre as decisões e análises do Comitê Gestor, pois presta suporte técnico e assistência a ele.

2.4.3 Autoridade Certificadora Raiz

A AC Raiz é a autoridade principal da cadeia de certificação da ICP-Brasil. Possui as seguintes funções:

- Executa as políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor;
- Emite, expede, distribui, revoga e gerencia os certificados das AC de nível imediatamente subsequente ao seu;
- Gerencia a lista de certificados revogados;
- Executa atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil;
- Participa de tratativas para celebração de convênios e políticas de certificação internacionais.

2.4.4 Autoridade Certificadora

As Autoridades Certificadoras são entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular. Tem como funções:

- Emitir, expedir, distribuir, revogar e gerenciar os certificados;
- Colocá-los à disposição dos usuários as listas de certificados revogados e outras informações pertinentes;
- Manter o registro de suas operações.

2.4.5 Autoridade de Carimbo de Tempo

É a entidade na qual os usuários de serviços de carimbo do tempo, subscritores e terceiras partes, confiam para emitir carimbos do tempo. A ACT tem a responsabilidade geral pelo fornecimento do carimbo do tempo. É responsável pela operação de um ou mais Sistemas de Carimbo do Tempo, conectados à Rede de Carimbo do Tempo da ICP-Brasil.

Um Sistema de Carimbo do Tempo (SCT) é um dispositivo único constituído por *hardware* e *software* que gera os carimbos do tempo, sob o gerenciamento da ACT. Deve possuir um HSM (*Hardware Security Model*) contendo um relógio a partir do qual são emitidos os carimbos do tempo. Nesse HSM devem ser também realizadas as funções criptográficas de geração de chaves e assinaturas digitais.

2.4.6 Autoridade Registradora

As Autoridades de Registro são entidades operacionalmente vinculadas a uma Autoridade Certificadora. Tem como funções:

- Identificar e cadastrar usuários de forma presencial;
- Encaminhar solicitações de certificados à AC;
- Manter registros de suas operações.

2.4.7 Prestador de Serviços de Suporte

Os Prestadores de Serviços de Suporte são empresas contratadas por uma Autoridade Certificadora ou uma Autoridade Registradora para:

- Disponibilização de infraestrutura física e lógica;
- Disponibilização de recursos humanos especializados;
- Disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

2.4.8 Auditor Independente

Os Auditores Independentes são empresas de Auditoria Independentes

autorizadas pela AC Raiz para realizar auditorias nas entidades da ICP-Brasil. São contratadas pelas Autoridades Certificadoras para realizar auditorias operacionais ou pré-operacionais em entidades a elas subordinadas.

2.4.9 Entidade Final

As entidades finais se dividem em dois tipos:

Titulares de Certificados - São as pessoas físicas ou jurídicas que são titulares dos certificados digitais emitidos por uma das Autoridades Certificadoras integrantes da ICP-Brasil.

Terceiras Partes - É a parte que confia no teor, validade e aplicabilidade do certificado digital emitido por uma das Autoridades Certificadoras integrantes da ICP-Brasil.

2.4.10 Cadeia de Certificação

Uma cadeia de certificação pode ser criada por qualquer pessoa física ou jurídica, através de sistemas existentes, tanto pagos como gratuitos. Desde que ambas as partes, a parte que utiliza o certificado digital para assinar ou cifrar um documento e a parte que o recebe, aceitem que o certificado utilizado é válido.

Entretanto, para ser amplamente aceita, uma cadeia de certificação precisa oferecer garantias aos titulares e aos usuários dos seus certificados. A ICP-Brasil ofecere várias garantias, como (RIBEIRO *et al*, 2004):

- O par de chaves criptográficas deve ser gerado sempre pelo próprio titular e sua chave privada de assinatura é de seu exclusivo controle, uso e conhecimento.
- Os documentos assinados com processo de certificação da ICP-Brasil possuem validade jurídica;
- São utilizados padrões internacionais para os certificados bem como

algoritmos criptográficos e tamanhos de chaves que oferecem nível de segurança aceitável internacionalmente;

- As instalações e procedimentos das entidades credenciadas possuem nível de segurança física, lógica, de pessoal e procedimental em padrões internacionais;
- As entidades componentes da ICP-Brasil são obrigadas a declarar em repositório público as práticas de segurança utilizadas em todos os seus processos;
- As entidades estão sujeitas a auditoria prévia ao credenciamento e anualmente, para manter-se credenciadas;
- Os dados relativos aos certificados são mantidos por no mínimo 30 anos, para permitir comprovação e resolver dúvidas sobre a assinatura de documentos, atendendo legislações específicas de guarda de documentos;
- Todas as AC são obrigadas a contratar seguro para cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco;
- É obrigatória a validação presencial dos titulares para obtenção de certificados.

2.4.11 Normativo

Para garantir a compatibilidade da Infraestrutura de Chaves Públicas com outras cadeias de certificação, inclusive de outros países, o Comitê Gestor da ICP-Brasil elaborou suas regras e normas seguindo padrões internacionais, principalmente nas resoluções que dizem respeito a formatos de certificados, algoritmos criptográficos e padrões de segurança.

Utilizando com referência apenas normas nacionais, foram elaboradas as resoluções como as que dizem respeito aos critérios de segurança física para o armazenamento dos dados nas entidades da estrutura e as que dizem respeito aos aspectos legais de suas operações.

Para normatizar os processos de realização das auditorias e das fiscalizações

das entidades da estrutura, foram utilizadas como base tanto normas e recomendações nacionais quanto internacionais.

2.4.12 Auditorias

São realizadas dois tipos de auditorias nas entidades da ICP-Brasil:

- Pré-operacional – é a auditoria realizada em uma entidade candidata a ingressar na ICP-Brasil e pode apresentar os seguintes resultados:
  - Autorização do credenciamento da entidade;
  - Não autorização do credenciamento da entidade.
- Operacional - realizada anualmente de forma planejada, ou a qualquer momento através de fiscalizações caso exista suspeita de irregularidades. Pode apresentar os seguintes resultados:
  - Manutenção do credenciamento da entidade;
  - Suspensão da emissão de certificados pela entidade até a correção das irregularidades verificadas;
  - Descredenciamento da entidade;
  - Substituição / treinamento de mão de obra.

As auditorias são sempre realizadas por técnicos que devem possui experiência comprovada nas áreas de segurança da informação, tanto de ambientes físicos como lógicos, criptografia, infraestrutura de chaves pública e sistemas críticos. Também devem ser totalmente independentes da entidade auditada.

Nas resoluções também são definidas quem realiza as auditorias em cada uma das entidades, demonstradas na tabela abaixo:

Entidade	**EXECUTOR DA AUDITORIA**	
	Pré-operacional	**Operacional**
AC Raiz	Comitê Gestor da ICP-Brasil ou seus prepostos, formalmente designados	Comitê Gestor da ICP-Brasil ou seus prepostos, formalmente designados
AC subordinada	ITI/DAFN/CGAF	ITI/DAFN/CGAF

à AC Raiz, e seus PSS		
AC subordinada a outra AC, e seus PSS	ITI/DAFN/CGAF	Empresa de Auditoria Independente credenciada junto ao ITI
ACT	ITI/DAFN/CGAF	Empresa de Auditoria Independente credenciada junto ao ITI
AR	Empresa de Auditoria Independente credenciada junto ao ITI	Auditoria Interna da respectiva AR credenciada junto ao ITI Empresa de Auditoria Independente credenciada junto ao ITI
AR no Exterior	ITI/DAFN/CGAF ou, a seu critério, Empresa de Auditoria Independente credenciada junto ao ITI	Auditoria Interna da respectiva AR credenciada junto ao ITI Empresa de Auditoria Independente credenciada junto ao ITI
PSS de AR	Empresa de Auditoria Independente credenciada junto ao ITI	Auditoria Interna da respectiva AR credenciada junto ao ITI Empresa de Auditoria Independente credenciada junto ao ITI

Ilustração 6 – Entidades que podem realizar auditoria.

Fonte: ANEXO B

2.4.12.1 Etapas da Auditoria

As auditorias, tanto pré-operacionais como operacionais, seguem uma etapa para sua realização. Primeira é feita a análise dos documentos obrigatórios, depois a análise dos documentos complementares, em seguida é feito o planejamento dos testes da auditoria para em seguida ser realizada a auditoria de campo e, por fim, o encerramento da auditoria. Cada um destes processos será mais bem detalhado a seguir.

2.4.12.1.1 Análise de Documentos Obrigatórios

Na primeira etapa da auditoria, a análise dos documentos obrigatórios, é observada se as normas da ICP-Brasil que definem os padrões mínimos que devem ser seguidos pelas entidades estão sendo seguidos. As entidades baseiam-se nessas normas para escreverem seus documentos técnicos obrigatórios, nos quais estão definidos os procedimentos adotados por elas na sua própria cadeia de certificação. Estes documentos são:

- Política de Segurança – PS;
- Política de Certificados – PC;
- Declaração de Práticas de Certificação – DPC.

Os seguintes documentos são verificados nessa etapa da auditoria:

- Documentos relativos à habilitação jurídico-fiscal;
- Balanço Patrimonial da empresa;
- Documentos Técnicos Obrigatórios: PS, PC e DPC.

2.4.12.1.2 Análise de Documentos Complementares

Na Análise de documentos complementares, são solicitados e examinados outros documentos técnicos para checar o atendimento de outros itens obrigatórios pelas normas da ICP Brasil e para programar e dimensionar o trabalho de auditoria a ser executado. Como exemplo de alguns documentos que podem ser verificados nessa etapa, tem-se (RIBEIRO *et al*, 2004):

- Lista dos funcionários, com os respectivos cargos desempenhados e permissões de acesso lógico e físico;
- Planta baixa do prédio onde está instalada a entidade, com delimitação dos níveis de acesso físico;
- Topologia da rede de comunicação;
- Descrição dos sistemas e procedimentos utilizados para a manutenção da segurança física, lógica e da rede;
- Descrição dos procedimentos e sistemas usados para geração e

revogação de certificados e para geração e publicação de LCR;

- Descrição dos procedimentos e ferramentas que serão usados para apoiar as atividades de AR;
- Documentos obrigatórios que seguem as normas do Comitê Gestor, como:
    - Classificação da Informação;
    - Gerenciamento de Risco;
    - Plano de Continuidade de Negócios;
    - Plano de Extinção;
    - Entre outros.

2.4.12.1.3 Planejamento dos Testes

Na etapa de planejamento dos testes, é utilizada toda a documentação que foi analisada para conhecer as principais características do ambiente a ser auditado para preparar os testes, entrevistas e outras análises que serão realizadas durante a auditoria de campo e os instrumentos a serem utilizados.

2.4.12.1.4 Auditoria de Campo

No ambiente da entidade serão realizados os testes, entrevistas, verificação documental e outras análises programadas. O preenchimento instrumental é preparado e, se for necessário, é feita a solicitação e verificação de outros documentos adicionais.

2.4.12.1.5 Encerramento

No encerramento da auditoria é elaborado o relatório e os pareceres, utilizando como base os documentos verificados e o resultado das análises feitas no ambiente da entidade, e a organização do material nas pastas de auditoria. Caso alguma recomendação de auditora não pode ser cumprida antes do seu encerramento, é feito o seu acompanhamento também nessa etapa.

2.4.12.2 Auditoria Pré-Operacional de Autoridade Certificadora

Na auditoria pré-operacional de Autoridade Certificadora são verificados os cumprimentos de todos os itens de segurança e procedimentos constantes das normas da ICP-Brasil, da sua Política de Certificação, da sua Declaração de Práticas de Certificação e da sua Política de Segurança. Esses itens são agrupados nas seguintes áreas:

- Segurança de Pessoal;
- Segurança Física;
- Segurança Lógica;
- Segurança de Rede;
- Segurança da Informação;
- Gerenciamento de chaves criptográficas e do certificado da própria AC;
- Gerenciamento do ciclo de vida dos certificados emitidos;
- Procedimentos finais.

2.4.12.2.1 Segurança de Pessoal

A Segurança de Pessoal divide-se em três subáreas:

- Cargos, atribuições e autorizações de acesso;
- Contratação, desligamento e acompanhamento de desempenho;
- Treinamento técnico-operacional.

As análises dessas áreas são feitas através de análise documental e observação direta. Os procedimentos relativos à segurança de pessoas são a verificação de antecedentes e de idoneidade, o treinamento e reciclagem profissional, a rotatividade de cargos, as sanções por ações não autorizadas e os controles para contratação.

- Com relação a cargos, atribuições e autorizações de acesso, cada funcionário deve assinar contratos ou termos de responsabilidade contendo:

  - Condições do perfil que ocupará;
  - Compromisso de observar normas, políticas e regras aplicáveis da ICP-Brasil;
  - Compromisso de nunca divulgar informações sigilosas;
  - Conhecimento de PS, DPC, PC e outros documentos relativos à sua atividade.

Com relação à contratação, desligamento e acompanhamento de desempenho de funcionários, são verificados:

- Não contratação de estagiários;
- Na contratação de cada funcionário:
  - Antecedentes criminais;
  - Creditícios;
  - Histórico de empregos anteriores;
  - Comprovantes de escolaridade e residência.
- Realização de entrevistas na contratação e no desligamento de funcionários;
- Avaliações periódicas de desempenho.
- No desligamento:
  - Revogação de credencial, identificação, crachá;
  - Revogação de uso de equipamentos;
  - Revogação de uso de mecanismos e acesso físico;
  - Revogação de acesso lógico.

Com relação aos treinamentos técnico-operacionais são observados:

- Mecanismos de Segurança da Informação;
- Sistema Certificação da AC;
- Recuperação de Desastre;
- Reconhecimento de assinaturas e validade dos documentos apresentados;
- Treinamento específico para a função.

2.4.12.2.2 Segurança Física

Na segurança física são verificadas as condições de segurança física para a proteção da chave privada da entidade, do sistema de certificação da entidade e de outras informações críticas.

A auditoria para a segurança física é realizada verificando a manutenção da sala-cofre, sua estrutura de energia e ar condicionado, seu sistema de detecção e alarme de incêndio e sistema de combate a incêndio por gás. É verificado o controle de acesso físico por monitoramento e identificação nas passagens de nível. As condições ambientais são verificadas por monitoramento por câmara de vídeo e sala de segurança. São também verificados os inventários de bens de informação. Na auditoria também é verificada a capacidade de realizar os controles exigidos de forma manual ou através de equipamentos ou sistemas.

Para realizar essas auditorias são usadas as técnicas de análise documental, testes e observação direta.

Existem quatro níveis de proteção para o acesso ao *hardware* da Autoridade Certificadora e mais dois níveis de proteção para acesso à chave privada da Autoridade Certificadora. Em todos os níveis, pessoas que não fazem parte do pessoal da entidade só podem transitar acompanhadas e identificadas. Todos os níveis de segurança devem ser monitorados por câmeras de vídeo ligadas a um sistema de gravação 24 horas por dia, e o sistema de monitoramento das câmeras de vídeo e o sistema de notificação de alarmes devem permanentemente monitorados por guarda armado no nível de proteção três.

O indivíduo que entrar em uma área de nível um deve ser identificado e registrado por segurança armada. Para passar para o segundo nível deve ser exigida identificação por meio eletrônico e uso de crachá.

No terceiro nível também são controladas as entradas e saídas de pessoas autorizadas através de dois mecanismos de controle, como cartão eletrônico e identificação biométrica.

O quarto nível diz respeito à sala cofre. Neste nível, o piso e o teto deverão ser inteiriços, ou seja, uma célula estanque com proteção a ameaças de acesso

indevido, de água, de vapor, de gases e de fogo. Nesse nível também se utiliza dois mecanismos de controle de entradas e saídas de pessoas autorizadas, porém para acesso a esse ambiente é necessário a identificação de, no mínimo, duas pessoas autorizadas.

A célula estanque deve possuir sistemas de detecção de fumaça e de extinção de incêndio por gás. Deve possuir ar condicionado redundante, e seu sistema de alimentação elétrica deve possuir geradores principais e reserva e *no breaks*. Interior ao quarto nível encontra-se o quinto nível, que é um cofre ou um gabinete reforçado e trancado.

O sexto e último nível diz respeito à guarda da chave privada da Autoridade Certificadora. São depósitos localizados no interior do cofre do quinto nível, onde as chaves privadas ficam armazenadas quando não estão em operação.

2.4.12.2.3 Segurança Lógica

Na auditoria da segurança lógica são analisados os controles de acesso lógico; a geração, extração e guarda de *logs*; a geração extração e guarda de backups e o controle de *softwares*. As auditorias são realizadas através de técnicas de análise documental, testes e observação direta. Na auditoria pré-operacional, por ainda não haverem registros históricos, é verificada a capacidade da candidata a Autoridade Certificadora de realizar os controles exigidos.

Controle de acesso lógico:

- Análise das estratégias adotadas pela entidade para dividir funções e acessar os sistemas críticos;
- Como são guardadas as senhas de administrador dos sistemas e qual a sua periodicidade de troca;
- Utilização de *logins* individuais para acesso aos sistemas;
- Análise das listas de acesso lógico aos diversos sistemas para verificar se somente os funcionários encarregados das atividades possuem acesso.

Geração, extração e guarda de *logs*:

- Verificação dos procedimentos e scripts para extração dos *logs*;
- Verificação se todos os eventos de guarda obrigatória são registrados;
- Verificação do local de armazenamento e período de retenção dos *logs*.

Geração, extração e guarda de backups:

- Verificação se os backups extraídos são suficientes para recomposição dos sistemas em caso de falhas;
- Verificação da forma de guarda e período de retenção dos backups;
- Análise de outros itens de segurança.

Controle de *softwares*

- São analisados os procedimentos da AC para atualização dos *softwares* instalados, em especial quanto à homologação prévia das alterações e quanto à aplicação tempestiva de correções de segurança;
- Verificam-se os controles para evitar a instalação de *softwares* não autorizados nos equipamentos que fazem parte da rede da AC e atualizações de *softwares*.

2.4.12.2.4 Segurança de Rede

Para a segurança de rede, são verificados a segurança da rede da entidade e seu repositório, através de técnicas de análise documental, testes e observação direta.

Na segurança da rede da Autoridade Certificadora é verificado:

- A topologia da rede, sob o enfoque de segurança e disponibilidade, se:
    - A rede é segmentada, de forma a proteger o equipamento de certificação;
    - Existem equipamentos redundantes para evitar a perda de acesso;
    - Os links externos são contratados com operadoras diferentes;

    - O tráfego dentro de intranets e extranets é protegido por VPN.
- Os firewalls e sistemas de detecção de intrusos com relação a:
    - Monitoramento;
    - Regras e políticas implementadas;
    - Atualização de listas de vulnerabilidades;
    - Entre outros.

No repositório da Autoridade Certificadora é verificado:

- A contínua verificação pelas aplicações, que fazem uso dos certificados emitidos pela entidade, da lista de certificados revogados;
- Se as PC e DPC estão sempre disponíveis publicamente;
- Os mecanismos para verificação do índice de disponibilidade mensal do repositório, que deve ser de pelo menos 99%;
- Os procedimentos para publicação da Lista de Certificados Revogados e sua segurança.

2.4.12.2.5 Segurança da Informação

Para a auditoria da segurança da informação, usam-se técnicas de análise documental e observação direta, A auditoria desta área divide-se em sete subáreas:

- Classificação da informação;
- Geração, manuseio, guarda e destruição de documentos e arquivos;
- Auditorias de segurança das informações;
- Análise de Risco;
- Plano de Continuidade de Negócios;
- Plano de Extinção da AC;
- Gerenciamento de Mudanças e Administração da AC.

Na auditoria verifica-se se os procedimentos utilizados estão em conformidade com os documentos de:

- Sistema de Classificação da Informação;
- Gerenciamento de Risco;
- Teste no Plano de Continuidade de Negócios;
- Plano de Extinção da AC.

Na auditoria verifica-se ainda se a entidade está aparelhada para analisar pelo menos semanalmente os *logs* coletados e procura-se entender como será feito o controle e gerenciamento de todos os processos que devem ser obrigatoriamente realizados.

2.4.12.2.6 Gerenciamento de Chaves Criptográficas e do Certificado da Autoridade Certificadora

No gerenciamento de chaves criptográficas e do certificado da Autoridade Certificadora, a auditoria é realizada por análise documental, observação direta e simulação. Nesta auditoria são verificados os procedimentos e a capacidade dos sistemas instalados na entidade de gerenciar suas chaves criptográficas e seu próprio certificado, seguindo os requisitos definidos pela ICP Brasil.

A simulação durante a auditoria é realizada na:

- Geração de chaves criptográficas da AC;
- Solicitação de seu certificado à AC Raiz;
- Recepção do certificado e inserção no sistema;
- Solicitação de revogação de seu certificado.

A auditoria analisa também a guarda e a utilização da chave privada da Autoridade Certificadora em relação aos aspectos:

- A chave privada da entidade deve ser guardada sempre cifrada em *hardware* seguro;
- A decifração deve ocorrer envolvendo pelo menos duas pessoas;
- Essas pessoas devem assinar termo declarando ter conhecimentos da sua responsabilidade no processo;
- Cada uma dessas pessoas deve necessitar de pelo menos um elemento físico (cartão ou *token*) mais senha particular para ativação da chave privada;
- Os cartões ou *tokens* ficam armazenados em um cofre, cuja chave fica em poder de uma terceira pessoa.

2.4.12.2.7 Gerenciamento do Ciclo de Vida dos Certificados Emitidos

No gerenciamento do ciclo de vida dos certificados emitidos são verificados os procedimentos e a capacidade dos sistemas instalados na entidade para gerenciar o ciclo de vida dos certificados emitidos por ela de acordo com a normatização da ICP Brasil. Para isso utiliza-se de técnicas de análise documental, observação direta e simulação de:

- Geração de certificados de diferentes tipos, um para cada Política de Certificação;
- Geração de Lista de Certificados Revogados;
- Publicação de certificados e Lista de Certificados Revogados no repositório, com os requisitos de segurança definidos.

2.4.12.2.8 Procedimentos Finais

Nos procedimentos finais, para deixar o sistema preparado para a efetiva colocação em funcionamento, quando autorizado pelo Diretor-Presidente do ITI, são realizadas as seguintes medidas:

- Ao final das simulações, é solicitada a reinstalação do sistema operacional, do sistema de gerenciamento de banco de dados e do sistema de gerenciamento de certificados no equipamento ou partição que irá abrigar o servidor de certificação da AC, na presença de pelo menos um auditor;
- Essa reinstalação é filmada e os procedimentos realizados são registrados em *logs,* de modo que a comissão de auditoria tenha condições de detectar qualquer atividade não autorizada.

2.4.12.3 Auditoria Pré-Operacional de Autoridade de Carimbo de Tempo

Na auditoria pré-operacional de autoridade de carimbo de tempo, são verificados os documentos relativos à sua habilitação jurídica, à sua regularidade fiscal, à sua qualificação econômico-financeira e à sua qualificação técnica.

Relativos à sua habilitação jurídica são verificados:

- Ato constitutivo, devidamente registrado no órgão competente;
- Documentos da eleição de seus administradores, quando aplicável.

Relativos à sua regularidade fiscal são verificados:

- Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
- Prova de inscrição no cadastro de contribuintes estadual ou municipal relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei;
- Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

Relativos à sua qualificação econômico-financeira são verificados:

- Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI), afirmando que o candidato se encontra em boa situação financeira para a execução das atividades a que se propõe junto à ICP-Brasil;
- Certidão negativa de falência ou concordata expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente.

Relativos à sua qualificação técnica são verificados:

- Declaração de Práticas de Carimbo do Tempo (DPCT);
- Políticas de Carimbo de Tempo (PCT);
- Política de Segurança (PS).

2.4.12.4 Auditoria Pré-Operacional de Autoridade Registradora

Nas auditorias pré-operacionais em Autoridades de Registro são verificadas as áreas de Segurança Física, Lógica, de Rede, de Pessoal e a Segurança da Informação e o Ciclo de Vida dos Certificados. São mais simples do que as

auditorias em AC, pois as Autoridades de Registro utilizam ambientes físicos menores que não possuem tantos níveis de segurança de acesso; não utilizam servidores para as atividades, apenas estações de trabalho para acessar o sistema de certificação da AC; ocupam menos pessoas e; executam apenas as etapas do ciclo de vida dos certificados que dizem respeito à identificação dos usuários e a validação das requisições.

O ponto central da auditoria de AR é na verificação do treinamento e preparo dos agentes de certificação para a execução das atividades, pois o agente de validação é quem pode atestar que um dado certificado pertence efetivamente ao seu titular através da validação presencial. Além disso, também é o agente de validação que orienta o titular do certificado sobre o seu uso correto e as implicações decorrentes da guarda inadequada de sua chave privada.

2.4.12.5 Auditoria Pré-Operacional de Prestador de Serviços de Suporte

Na auditoria pré-operacional de Prestador de Serviços de Suporte, quando o PSS fornece mão de obra especializada, a auditoria apenas verifica os itens relativos à Segurança de Pessoal. No caso de o PSS fornecer também infraestrutura física e lógica, a auditoria compreende a verificação dos itens relativos à Segurança Física, Lógica, de Rede e da Informação. Quando o PSS fornece tanto a mão de obra quanto a infraestrutura, a auditoria compreende todos os itens descritos.

2.4.12.6 Auditoria Operacional de Autoridade Certificadora

Na auditoria operacional de Autoridade Certificadora são verificados os mesmos itens que na pré-operacional, com a diferença de que já existem registros históricos como:

- Certificados emitidos;
- Certificados revogados;
- *Logs* dos acessos aos ambientes físico e lógico;

- Entre outros.

Desse modo, através da análise dos registros, avalia-se se a entidade está realizando adequadamente os seus procedimentos. A situação econômico-financeira da empresa é analisada pelo último balanço patrimonial, pela atualização da apólice de seguros e pela realização de auditorias em entidades subordinadas no período que passou.

2.4.12.7 Auditoria Operacional de Autoridade de Carimbo do Tempo

Na auditoria operacional de Autoridade de Carimbo do Tempo são verificados os mesmos itens que na pré-operacional, com a diferença de que já existem registros históricos. Desse modo, através da análise dos registros, avalia-se se a entidade está realizando adequadamente os seus procedimentos.

2.4.12.8 Auditoria Operacional de Autoridade Registradora

A auditoria operacional de Autoridade de Registro foca na análise dos certificados emitidos, além dos itens verificados na auditoria pré-operacional, para evidenciar a qualidade dos processos de identificação e validação dos requisitantes de certificados.

Os documentos de identificação e outros termos devem estar armazenados pelos agentes de registro no ambiente da AR, para que a lista dos certificados emitidos pela entidade, fornecida à auditoria pela AC responsável, possa ser confrontada com eles.

2.4.12.9 Auditoria Operacional de Prestador de Serviços de Suporte

A auditoria operacional de Prestador de Serviços de Suporte é realizada simultaneamente à auditoria da AC ou AR à qual o PSS está vinculado e são verificados os mesmos itens já descritos.

2.4.12.10 Auditorias Operacionais Realizadas por Empresas de Auditoria Independentes

As auditorias operacionais realizadas por Empresas de Auditoria Independentes são realizadas em Autoridades Certificadoras que não sejam estejam imediatamente abaixo da AC Raiz. Essas empresas de auditoria independente podem ser contratadas para realizar também auditorias operacionais em Autoridades de Registro e Prestadores de Serviço de Suporte.

Como a quantidade de entidades credenciadas à ICP Brasil tende a crescer de forma não linear, não sendo possível a AC Raiz auditar diretamente todas elas, a delegação de serviços de auditoria a empresas de auditoria independentes descentraliza esse processo da AC Raiz de uma forma controlada.

O processo de auditoria por estas entidades envolve as seguintes fases:

- Cadastramento inicial da empresa de auditoria junto à AC Raiz, com comprovação da capacidade jurídico-fiscal e técnica;
- Solicitação de autorização à AC Raiz para executar missão de auditoria na entidade contratante, realizada a cada auditoria nova e acompanhada dos seguintes documentos:
    - Plano de auditoria;
    - Descrição dos procedimentos a serem usados nas verificações;
    - Relação dos auditores que irão executar a missão;
    - Modelo de relatório.
- Realização da auditoria e envio do relatório final para análise da AC Raiz.

2.4.12.11 Importância das Auditorias

A importância das auditorias na ICP Brasil é notada na contribuição para a manutenção da qualidade dos serviços e processos realizados pelas entidades da estrutura, servindo para evitar problemas graves, como (RIBEIRO *et al*, 2004):

- Utilização de sala-cofre sem os requisitos de estanqueidade necessários;
- Manutenção de bases de dados corrompidas;
- Não utilização de VPN para proteger o tráfego de dados para o servidor da AC;
- Alocação de pessoas despreparadas para executar a tarefa de Agentes de Registro;
- Não verificação da vulnerabilidade dos servidores, tendo, em decorrência, sistemas desatualizados e com graves brechas de segurança;
- Não realização da análise dos *logs* de eventos críticos;
- Perda de imagens dos ambientes pela falta de troca das fitas de vídeo em tempo hábil;
- Emissão de certificados a titulares sem a respectiva documentação.

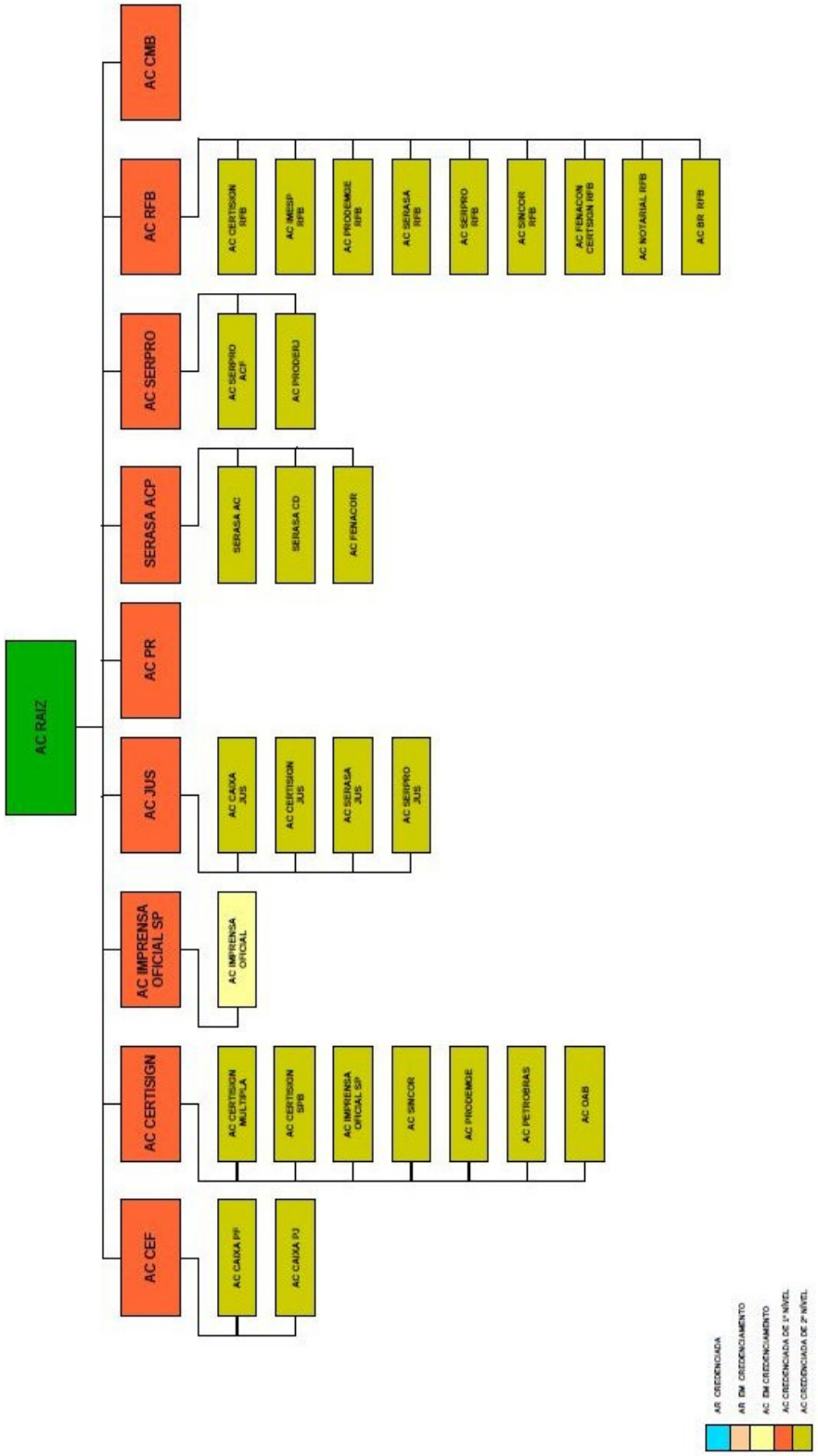

Ilustração 7 – Entidades da estrutura física da ICP-Brasil.
Uma imagem mais detalhada pode ser acessada por
<http://www.iti.gov.br/twiki/pub/Certificacao/EstruturaIcp/Estrutura_completa.pdf>

Fonte: ESTRUTURA DA ICP-BRASIL, 2010.

2.5 ORGANIZAÇÃO VIRTUAL

Neste tópico será mostrado o conceito de organização virtual, o que é e como funciona. O entendimento desse tipo de organização é necessário ao trabalho, pois o mesmo apresenta a proposta de um modelo de um sistema automatizado que será utilizado por diferentes organizações, cada uma atuando com a sua competência, e este sistema será controlado por um gestor. Estas são características das organizações virtuais.

Uma Organização Virtual pode ser entendida como uma rede temporária de organizações independentes, ligadas pela tecnologia da informação, e que se ligam a outras para formar uma cooperação, contribuindo com o que for de sua competência (BYRNE, 1993).

Uma definição bem completa de organizações virtuais é dada por Strausak (1998):

> Uma rede temporária de instituições independentes, negócios ou indivíduos especializados, que trabalham juntos, de um modo espontâneo, por meio da Tecnologia da Informação e Comunicação de forma a alcançar a ponta em uma competição existente. Eles integram-se verticalmente, unificam suas competências distintivas e funcionam como uma única organização ou unidade organizacional (STRAUSAK, 1998, p. 9-24).

Organizações virtuais são uma versão eletrônica de empresas tradicionais que buscam aproveitar novas oportunidades de mercado formando uma rede com outras empresas que possuem competências distintas (OPREA, 2003).

A organização virtual é uma alternativa estratégica para aumentar a competitividade e os ganhos das organizações que participam de uma cooperação. Para formá-las é necessário haver um grupo de organizações dispostas a cooperar entre si e compartilhar seus processos, recursos e habilidades, para buscar novas oportunidades de negócios.

Os tipos de organizações virtuais são (BULTJE e WIJK, 1998):

- Internas, quando uma organização utiliza para as operações de equipes internas;
- Estáveis, quando é uma cooperação de organizações diferentes coordenadas por uma empresa central que contrata e terceiriza as partes do processo;
- Dinâmicas, quando mantém uma cooperação temporária devido a oportunidades;
- *Web-company*, que são ágeis por serem redes temporárias de organizações especializadas suportadas pela Internet.

As principais características das organizações virtuais são (BAUER e KÖSZEGI, 2003; JAGERS; JANSEN; STEENBAKKERS, 1998; COSTA, 2009):

- São redes temporárias de indivíduos, empresas ou partes de corporações maiores que se unem com uma finalidade comum;
- Os participantes podem estar cada um em locais distintos;
- Cada participante colabora na rede com a sua competência principal;
- Possui uma utilização forte das tecnologias de informação e comunicação;
- A organização virtual pode ser composta por diferentes empresas a cada dia, de acordo com as necessidades e oportunidades de negócios que forem surgindo;
- Os membros têm um relacionamento igualitário, baseado na confiança mútua entre as partes;
- Devido à meta comum a ser seguida, os participantes atuam pro meio de autogestão e auto responsabilização;
- Apresentam uma única identidade aos clientes.

No entanto, uma série de dificuldades é percebida que impedem o avanço desde modelo organizacional com utilização de tecnologia da informação e comunicação para coordenar a integração das atividades, processos e informações conjuntas (FRANKE, 2002; HASSE e DE ROLT, 2006; COSTA, 2009), entre os quais estão:

- Dificuldade em encontrar organizações que dispõem de competências essenciais complementares para formar as organizações virtuais e

cadeias de valor consistentes;

- Falta de metodologias para a gestão de organizações virtuais;
- Necessidade de desenvolvimento de mecanismos legais e jurídicos de contratação;
- Falta de sinergia tecnológica e sociológica entre as organizações parceiras;
- Despreparo do administrador pela falta de experiência e de técnicas de administração de empresas em rede;
- Utilização de documentos eletrônicos sem segurança;
- Falta de confiança no compartilhamento de informações entre as empresas.

Para resolver estas questões, Goldman *et al* (1995) *apud* Franke (2002) apresentam o conceito organizacional de redes virtuais de organizações, com o objetivo de estruturar o processo de formação de organizações virtuais. Esse conceito é formado por três elementos que podem ser observados na ilustração 8:

- Plataforma Virtual;
- Corporação Virtual;
- Gestor Virtual.

A plataforma virtual é composta por uma rede dinâmica de empresas independentes, que através de pré-acordo cooperam umas com as outras e utilizam a tecnologia da informação, sob a coordenação de um Gestor Virtual (FRANKE, 2002; ROLT; SCHMITZ; SANTOS, 2005).

A corporação virtual é o resultado da cooperação temporária de algumas ou todas as organizações que formam a plataforma virtual, que formam uma aliança temporária a fim de atender um propósito específico, com o apoio de um Gestor Virtual (FRANKE, 2002; ROLT; SCHMITZ; SANTOS, 2005).

O gestor virtual atua como um facilitador da formação da corporação virtual temporária, e é responsável pelo início e coordenação das atividades suas atividades e pela manutenção da plataforma virtual de empresas (FRANKE, 2002).

2.5.1 Serviços compartilhados

O conceito de serviços compartilhados é definido como a prática organizacional em que unidades estratégicas de negócios da mesma organização ou de organizações diferentes compartilham um conjunto de serviços ao invés de tê-los como uma série de funções duplicadas (COOKE; QUINN; KRIS, 2000).

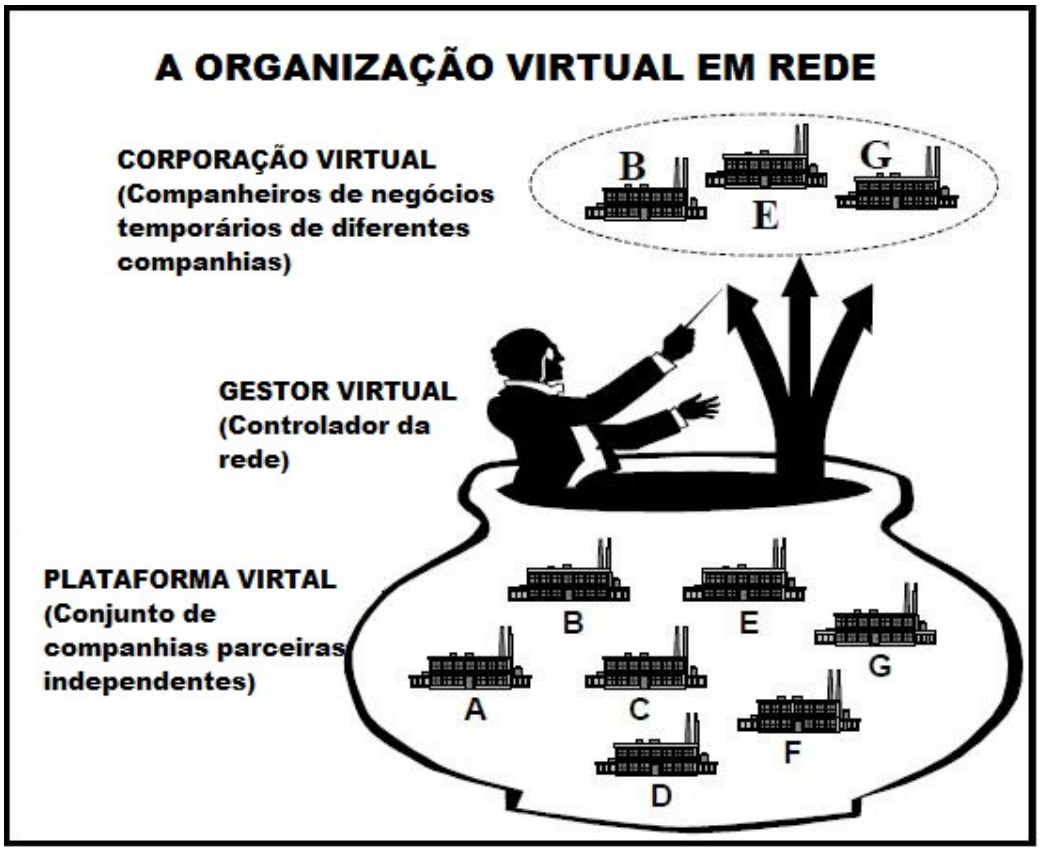

Ilustração 8 – A Organização virtual em rede.

Fonte: FRANZE e HICKMANN, 1999

Schulman *et al* (2001) define que o conceito é embasado pelo compartilhamento de elementos comuns a cada negócio ou organização com o objetivo de alcançar mais competitividade e eficiência na utilização de seus recursos.

A adoção de serviços compartilhados representa economia para as organizações, pois permite que haja a diminuição de serviços duplicados com a unificação dos serviços. Com isso, a organização pode focar na especialização da área que representa a sua competência central, o que a confere vantagens competitivas e desenvolvimento estratégico.

Crooks, Spatz e Warman (1995) definem os serviços compartilhados como um grupo de empresas privadas ou instituições públicas que formam uma cooperativa para prover um ou mais serviços que melhoram ou aumentam a competitividade de suas operações.

Quando os serviços que são providos por essas cooperativas são comparadas com quando são executados exclusivamente pelas organizações se não houvesse compartilhamento, eles apresentam um custo menor que o custo combinado da execução individual.

Para que o serviço seja adequado para ser compartilhado, ele deve ser transacional e operado por processos, ter processos comuns que possam ser compartilhados, deve ser executado em grande volume, deve ter independência geográfica, requer especialistas exclusivos para o serviço, deve apresentar alto nível de capital intensivo e esteja abaixo da quantidade crítica na demanda por uma única organização (FOTHERGILL; BINKS; RYAN-COLLINS, 2006).

A primeira área das organizações onde o conceito de serviços compartilhados foi utilizado foi a área financeira, devido a esse conceito apresentar a redução de custos já mencionada. Porém, outras áreas também são passíveis de terem esse conceito aplicado, como os processos de recursos humanos e departamento de pessoal, tecnologia da informação e comunicação, aspectos legais, marketing e administração de benefícios (IPF, 2006; SCHULMAN *et al*, 2001).

A gestão dos serviços compartilhados também pode ser realizada por organizações participantes da própria rede. Com isso, há mais controle sobre o serviço, pois nesse caso não é necessária a contratação de uma organização externa à rede que preste o serviço compartilhado que as organizações em rede necessitam (IPF, 2006).

A tecnologia da informação é um dos grandes propulsores na adoção dos

serviços compartilhados pelas organizações. Ela permite a estruturação dos serviços compartilhados, proporcionando a comunicação, a integração das unidades de negócios com as áreas de suporte e a automatização de procedimentos (COSTA, 2009).

2.6 MAPEAMENTO DE PROCESSOS

Em um ambiente organizacional, as decisões precisam ser eficientes e eficazes. O uso de ferramentas gerenciais que auxiliem os gestores a enxergar os pontos fortes e os pontos fracos da empresa auxilia a buscar esse objetivo. Com essa finalidade, é possível mapear os processos da organização e organizá-los de uma forma que possibilite a visão geral das operações e, com isso, seja possível fazer análises que ajudem a melhorar os processos existentes. A essa ferramenta gerencial dá-se o nome de Mapeamento de Processos.

Brache e Rumller (2007) definem processo como sendo várias etapas com várias funções que existem para a criação de um produto ou serviço e formam uma cadeia de agregação de valores. Nessa visão, segundo Cerqueira Neto (1994) *apud* Villela (2000) os primeiros processos a serem identificados são os processo de negócio, depois os processos de apoio aos processos de negócio e por fim os processos de controle gerencial. Os processos de negócios são os que são identificáveis pelo cliente, os processos de apoio colaboram com os processos de negócio junto aos clientes e os processos de controle gerencial coordenam os dois tipos anteriores de processo.

Hammer e Champy (1994) definem o processo como um conjunto de atividades realizadas em uma sequencia lógica para produzir um produto ou serviço específico para um grupo específico de clientes e Davenport (1994) define processo como uma estrutura de atividades ordenadas no tempo e no espaço, que possuem um começo e um fim e recebem insumos por entradas (*inputs*) e os devolvem acrescidos de valor por saídas (*outputs*).

Em um modo geral, a definição de processo pode ser tomada como um conjunto de atividades que por sua vez são formadas por tarefas e estas são

formadas por procedimentos, e recebem insumos por *inputs*, adicionam valor a ele e o fornecem através de *outputs* a um cliente específico (GONÇALVES, 2000).

Um processo não envolve apenas as operações de entrada, processamento e saída. Além destas operações há também envolvido na sua execução os recursos humanos e materiais e seus custos, o tempo de execução do processo, a documentação que tramita e a que é gerada pelo processo, a tecnologia utilizada, o volume de trabalho necessário para executá-lo e a área da organização envolvida.

Segundo Harrington (1993), os processos se dividem por uma hierarquia de acordo o nível de detalhamento com que o trabalho é descrito. Essa hierarquia é formada por macroprocesso, processo, subprocesso, atividade e tarefa. Um processo formado por um conjunto de processos e que, deste modo, envolve duas ou mais funções na estrutura da empresa é chamado de macroprocesso. Um processo, como já comentado, é um conjunto de atividades sequenciais que recebem um insumo, processam e o devolve acrescido de valor. Um subprocesso relaciona-se com outro subprocesso e realiza um objetivo específico em apoio ao macroprocesso. Uma atividade de um processo ou subprocesso define-se como os procedimentos que ocorrem dentro dele com o objetivo de produzir um resultado específico. Uma tarefa pode ser entendida como um elemento de uma atividade e que possui uma incumbência específica.

Segundo Garvin (1998), existem três categorias básicas de processos empresariais:

- Processos de negócios ou processos de cliente – caracterizam a atuação da empresa e são suportados por outros processos internos, resultando no produto ou serviço que é recebido por um cliente externo;
- Processos organizacionais ou de integração organizacional – são centralizados na organização em busca de seu desempenho geral, garantindo o suporte adequado aos processos de negócios;
- Processos gerenciais – são focalizados nos gerentes e suas relações e incluem ações de medição e ajuste do desempenho da organização.

Para realizar o Mapeamento dos processos da organização é necessário antes fazer o levantamento de quais e quantos eles são. As técnicas mais utilizadas

para o levantamento de processos são:

- Entrevista – Realizada através de conversação de forma planejada, sistemática e documentada, feita entre duas ou mais pessoas que têm interesse ou problemas em comum.
- Questionário - Série de questões ou perguntas previamente formuladas, podendo ser realizada de forma presencial ou à distância.
- Observação – Verificação pessoal do que acontece no ambiente em que se desenvolve o processo, realizado de forma não planejada e nem estruturada, ocorre de forma casual a partir de fatos que despertam interesse.
- Análise de documentos - Identificação, coleta e análise de toda a documentação a respeito do processo em estudo.

Para poder ter uma visão geral dos processos da organização que permita identificar os relacionamentos existentes entre eles e suas atividades e tarefas, os atores principais e seus papéis e responsabilidades e o fluxo de valor destes processos, é necessário realizar a modelagem dos processos em uma representação gráfica, depois de feito o levantamento. Essa representação gráfica auxiliará na análise e é feita na forma de um fluxograma, onde as atividades do processo são representadas em sequencia e é mostrado o que ocorre em cada etapa, o que entra e o que sai do processo, as decisões que são tomadas e os atores envolvidos. Este processo é chamado de Modelagem de Processo de negócios ou BPM (*Business Process Modeling*) na sigla em inglês.

Kettinger (2005) *apud* Dávalos (2010) diz que a modelagem dos processos serve de auxílio ao gerenciamento e construção de sistemas de integração de dados. Johansson (1995) lista uma variedade de áreas onde a modelagem de processos tem origens:

- Estudo de trabalho em fábricas para torná-las mais produtivas;
- Estudo de organizações e seus métodos para a eficiência do tempo;
- Controle de entradas no processo para controlar os seus resultados;
- Simulação de processos para testá-los a variadas condições de operação;
- Modelagem de negócios para o planejamento da empresa;

- Análise e engenharia de sistemas para a automação de processos.

Vernadat (1996) diz que as empresas alcançam a excelência profissional quando se concentram em dois pontos: otimização do modelo existentes e redefinição das operações. O mapeamento, modelagem e análise dos processos da organização auxiliam no aumento da eficiência, na redução de custos e no aumento da qualidade. Os principais benefícios dos modelos de processos de negócios são:

- Construção de uma cultura, visão e linguagem compartilhada;
- Formalização do conhecimento e práticas da empresa;
- Suportar decisões para melhoria e controle das operações da empresa.

Segundo Dávalos (2010) os modelos de processos de negócio formam uma infraestrutura de comunicação que pode auxiliar as empresas:

- A obter uma maior compreensão da empresa;
- A adquirir e registrar conhecimentos para uso posterior;
- A racionalizar e garantir o fluxo de informações;
- A projetar e especificar uma parte da empresa;
- A servir como base para análises de partes ou aspectos da empresa;
- Como base para a simulação do funcionamento da empresa;
- Como base para tomada de decisões sobre as operações e a organização da empresa;
- Como base para o desenvolvimento e implantação de *softwares* de forma integrada.

No modelo de processo de negócios de uma empresa é representado o funcionamento da empresa pelos seus processos, atividades, operações e eventos. Por ele é possível identificar os fluxos dos processos através do tempo e as decisões tomadas em cada ponto desse fluxo, bem como os dados que trafegam através do processo e os agentes envolvidos nele e a responsabilidade de cada um deles.

As finalidades do modelo de processos de negócios são variadas. Ajudam a entender o funcionamento da organização, possibilitam a análise e a melhoria dos seus processos, possibilitam a realização de simulações de decisões tomadas nos processos e servem de auxílio à administração da organização. Entendendo os processos da organização pode-se determinar como eles devem ser gerenciados

para aperfeiçoar o desempenho da organização.

Para melhorar o desempenho da organização é necessário realizar alterações na estrutura dos seus processos. Geralmente a implementação de sistemas automatizados fazem parte dessa mudança através da automação dos fluxos de trabalho, tornando-os mais ágeis, seguros e confiáveis.

A união da modelagem de processos de negócios com a tecnologia da informação define o conceito de gerenciamento de processo de negócios, que possui o foco na otimização dos resultados das organizações através da melhoria dos processos de negócio.

2.7 BPMN (*BUSINESS PROCESS MODELING NOTATION*)

Para a modelagem dos processos de negócio presentes neste trabalho, e propor o modelo a que este trabalho se dispõe, foi escolhida e utilizada a ferramenta de processos BPMN, a qual será explicada neste item.

O BPMN – *Business Process Modeling Notation* – foi desenvolvido pelo BPMI - *Business Process Management Initiative*. Em maio de 2004, foi lançada para o público a versão 1.0 do BPMN, após mais de dois anos de esforços do *BPMI Notation Working Group*.

O objetivo principal do BPMN é fornecer uma notação de fácil compreensão para todos os usuários de negócios, desde os analistas de negócio que criam os rascunhos iniciais dos processos, passando pelos desenvolvedores técnicos responsáveis pela aplicação da tecnologia que irá executar os processos, até para as pessoas que irão gerir e acompanhar os processos. Dessa maneira o BPMN cria um padrão que serve como uma ponte entre o projeto dos processos de negócio e a implementação deles.

O BPMN define um modelo de processos de negócios, ou BPD - *Business Process Diagram*, que é baseado em uma técnica de diagramação adaptada para a criação de modelos gráficos de operações de processos de negócio. O modelo de processos de negócio do BPMN é uma rede de objetos gráficos, divididos em

atividades e controles de fluxo que definem sua ordem de execução.

2.7.1 Noções básicas sobre BPMN

Um BPD é formado por um conjunto de elementos gráficos. Estes elementos permitem o desenvolvimento fácil de diagramas simples que parecem familiares para a maioria dos analistas de negócio, como um fluxograma. Os elementos foram escolhidos para serem distinguíveis uns dos outros e utilizam formas que são familiares à maioria dos modeladores.

Umas das motivações para o desenvolvimento do BPMN foi estabelecer um mecanismo simples para a criação de modelos de processos de negócios e ser ao mesmo tempo capaz de lidar com a complexidade inerente aos processos de negócio. A abordagem para lidar com esses dois requisitos conflitantes foi organizar os aspectos gráficos da notação em categorias específicas.

Isto proporcionou um pequeno conjunto de categorias de notação de modo que o leitor de um BPD reconhece facilmente os tipos básicos de elementos e consegue compreender o diagrama. Dentro das categorias básicas de elementos, podem ser adicionadas variações e informações para suportar os requisitos de complexidade sem alterar a simplicidade visual do diagrama. As quatro categorias básicas de elementos são:

- Objetos de Fluxo (*Flow Objects*)
- Objetos de conexão (*Connecting Objects*)
- Raias (*Swimlanes*)
- Artefatos (*Artifacts*)

2.7.1.1 Objetos de Fluxo (*Flow Objects*)

Um BPD tem um pequeno conjunto de elementos principais, formados por três objetos de fluxo, de modo que os modeladores não precisam aprender um grande número de formas diferentes. Os três objetos de fluxo são:

2.7.1.1.1 Evento (*Event*)

Um evento é representado por um círculo e representa algum acontecimento no fluxo de um processo de negócio. Estes eventos afetam o fluxo do processo e normalmente são uma causa inicial (*trigger*) ou um resultado final (*result*). Os eventos possuem a parte interna do círculo aberta, onde são definidos marcadores internos que diferenciam entre os diferentes tipos de *triggers* e de *results*. Há três tipos de eventos que dependem de onde eles afetam o fluxo: inicial (s*tart*), intermediário (*intermediate*) e final (*end*).

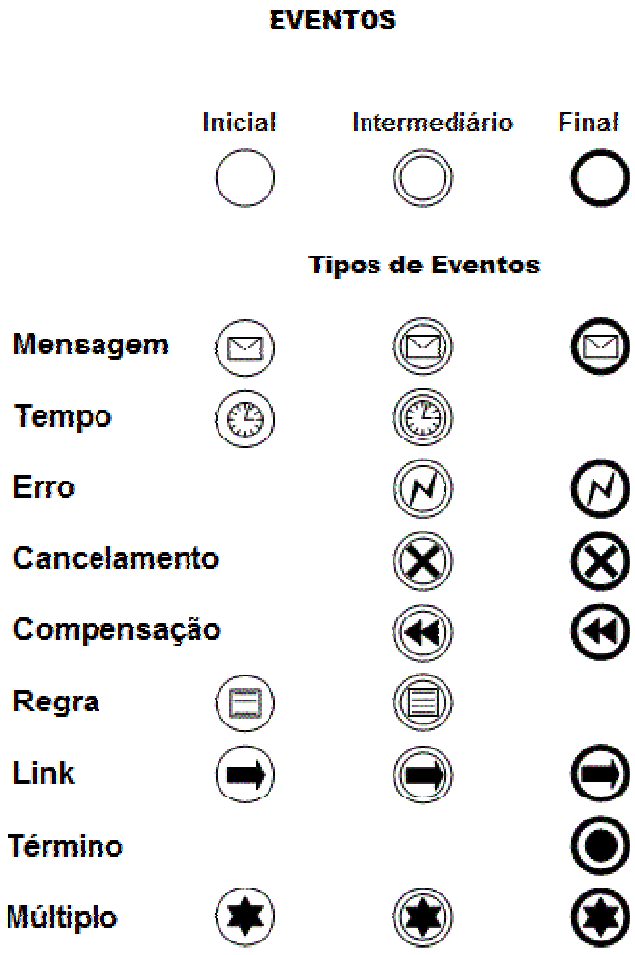

Ilustração 9 – Eventos do BPMN

Fonte: <http://www.bpmn.org>

O evento de início indica onde o fluxo de sequencia de um processo começará. Pode ser ativada por uma mensagem, uma data ou ciclo, uma condição, uma conexão ou por múltiplas razões.

O evento intermediário indica quando um evento acontece entre o início e o fim de um processo. Pode ser ativado por uma mensagem, uma data ou um ciclo, um tratamento de erro, o cancelamento de uma tarefa, um tratamento de compensação, uma condição, uma conexão ou por múltiplas razões.

O evento final indica o fim de um processo. O processo pode acabar com uma mensagem, com um erro, com cancelamento, com compensação, com um link, por múltiplas razões ou simplesmente chegar ao final.

2.7.1.1.2 Atividade (*Activity*)

Uma atividade é representada por um retângulo de bordas arredondadas e representa um trabalho que a empresa realiza em um processo. Uma Atividade pode ser única ou composta. Os tipos de atividades são: tarefa (*task*) e subprocesso (*sub-process*). O Subprocesso é distinguido por um pequeno sinal de mais (+) na parte central inferior do retângulo.

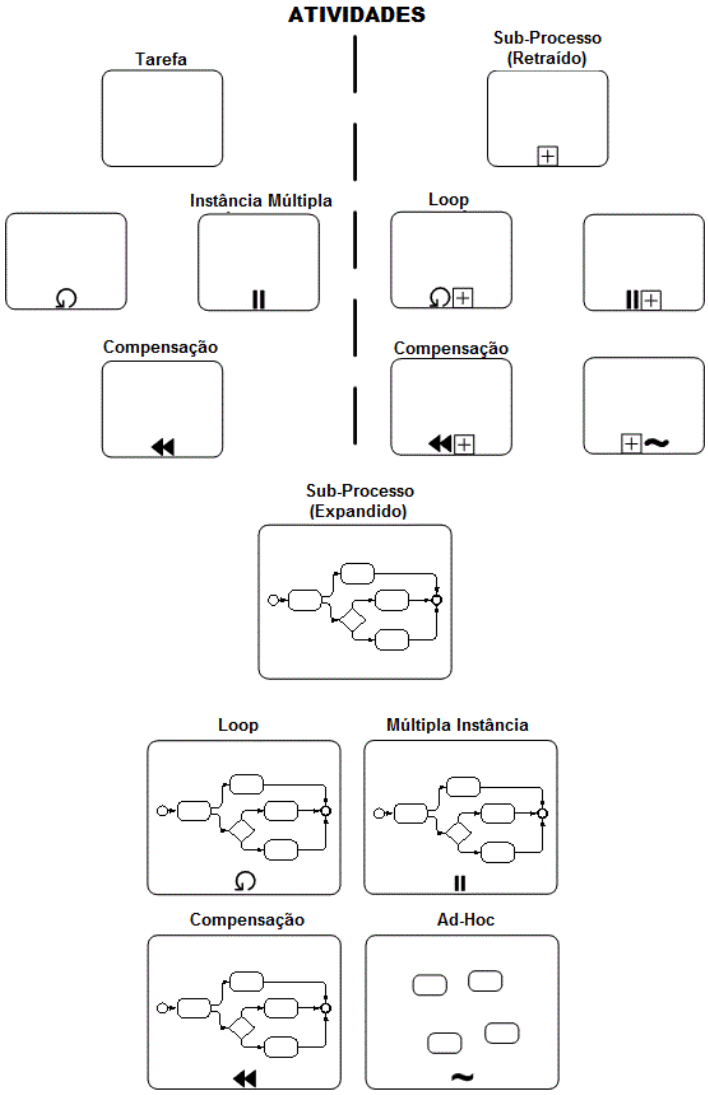

Ilustração 10 – Atividades do BPMN

Fonte: <http://www.bpmn.org>

Uma atividade pode ser uma tarefa simples ou conter várias tarefas. Quando é uma tarefa simples ela pode entrar em loop devido à avaliação de uma condição, devido a uma compensação ou por um número específico de vezes. Quando é uma tarefa composta, pode entrar em loop devido à avaliação de uma condição, devido a uma compensação, por um número específico de vezes ou pode ser definido para uma atividade específica de um participante do processo.

2.7.1.1.2 Portal (*Gateway*)

Um portal é representado na forma de um losango e é usado para controlar divergências e convergências de sequencia no fluxo. Determina decisões tradicionais como a bifurcação, fusão e união de caminhos. Marcadores internos no portal indicam o tipo de controle e de comportamento dele.

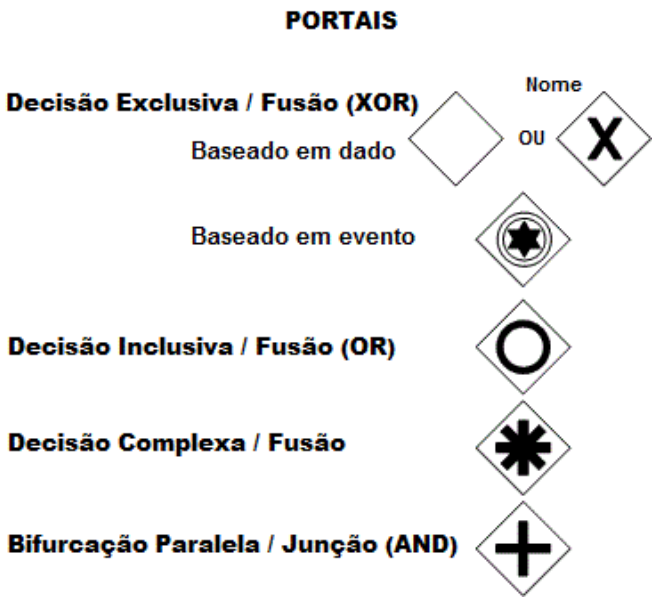

Ilustração 11 – Portais do BPMN

Fonte: <http://www.bpmn.org>

Quando o portal é do tipo XOR o fluxo do processo pode tomar apenas um dos caminhos que o portal possui. Quando é baseado em dados, a decisão de toma o caminho é pela expressão *booleana* contida no atributo da expressão. Quando é baseada em evento significa que é um evento que determinará para onde o fluxo do processo irá seguir.

Quando o portal é do tipo OR podem ser tomados de um até todas as opções de caminhos que o portal possui. Pode ser tomado tanto para bifurcação como para junção de caminhos de fluxo. Podem ser simples ou complexos, quando podem representar mais de uma decisão para o fluxo tomar um caminho.

Quando o portal é do tipo AND significa que o fluxo do processo tomará todos os caminhos indicados por ele.

2.7.1.2 Objetos de conexão (*Connecting Objects*)

Os Objetos de Fluxo são conectados juntos em um diagrama para criar a estrutura básica de um processo de negócio. Existem três objetos de conexão, os quais são:

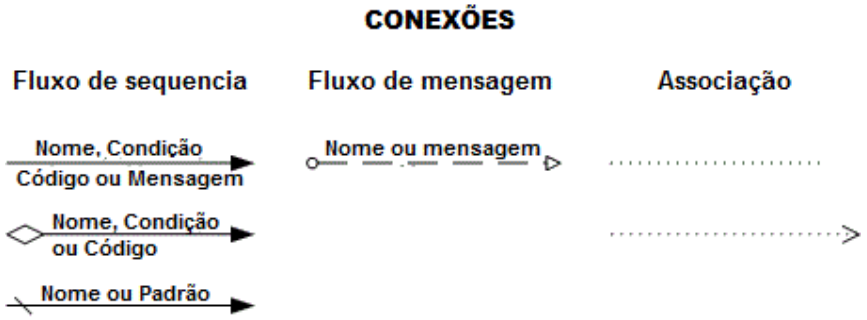

Ilustração 12 – Conexões do BPMN

Fonte: <http://www.bpmn.org>

2.7.1.2.1 Fluxo de Sequencia (*Sequence Flow*)

Um fluxo de sequencia é representado por uma linha sólida com uma seta sólida e é usado para mostrar a sequencia em que as atividades serão realizadas em um processo.

2.7.1.2.2 Fluxo de Mensagem (*Message Flow*)

Um fluxo de mensagem é representado por uma linha tracejada. Possui uma seta aberta e é usado para mostrar o fluxo de mensagens entre os dois participantes do processo, entidades empresariais ou papéis de negócio, que enviam e recebem

mensagens.

2.7.1.2.3 Associação (*Association*)

Uma associação é representada por uma linha pontilhada com uma seta e é usada para associar dados, textos e outros artefatos com os objetos de fluxo. As associações são utilizadas para mostrar as entradas e saídas das atividades.

Para modelistas que desejam ou necessitam de um baixo nível de precisão para criar modelos de processos para fins de documentação e comunicação, os elementos principais, além dos conectores, proporcionam a capacidade de criar diagramas facilmente compreensíveis. Para modelos que exigem um maior nível de precisão para criar modelos de processos, os detalhes adicionais de cada elemento podem ser utilizados.

2.7.1.3 Raias (*Swimlanes*)

Muitos processos de metodologias de modelagem utilizam o conceito de raias como um mecanismo para organizar atividades em diferentes categorias visuais, para ilustrar diferentes capacidades funcionais ou responsabilidades. O BPMN possui duas representações principais de raias, as quais são:

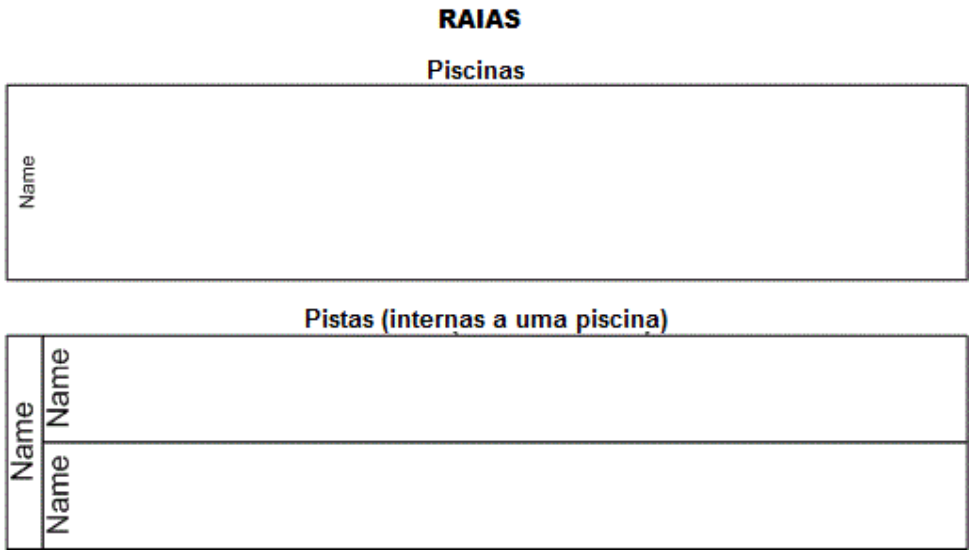

Ilustração 13 – Raias do BPMN

Fonte: <http://www.bpmn.org>

2.7.1.3.1 Piscina (*Pool*)

Uma piscina representa um participante no processo. Atua também como um *container* gráfico para o particionamento de um conjunto de atividades de outras piscinas.

2.7.1.3.2 Pista (*Lane*)

A pista é uma subpartição dentro de uma piscina e se estende em todo o comprimento da piscina, tanto verticalmente ou horizontalmente. Pistas são usadas para organizar e categorizar atividades.

Piscinas são utilizadas quando o diagrama envolve duas entidades ou participantes que são separados fisicamente no diagrama. As atividades dentro de grupos separados são processos particulares do grupo. O fluxo de sequencia não pode cruzar a fronteira de uma piscina. O fluxo de mensagens é utilizado como o mecanismo para mostrar a comunicação entre os dois participantes e, desse modo,

ele se liga entre duas piscinas ou entre objetos dentro das piscinas. Pistas são mais estreitamente relacionados com a tradicional metodologia de raias da modelagem de processos. Pistas são frequentemente usadas para separar as atividades associadas com um determinado papel ou função. As sequencia de fluxo podem atravessar as fronteiras das pistas dentro de uma piscina, mas a mensagem de fluxo não deve ser utilizada entre objetos de fluxo em pistas de uma mesma piscina.

2.7.1.4 Artefatos (*Artifacts*)

O BPMN foi projetado para permitir certa flexibilidade a modelos e ferramentas de modelagem, estendendo a base de notação e fornecendo capacidade adicional para o contexto adequado de uma modelagem de uma situação específica. Qualquer número de artefatos pode ser adicionado a um diagrama, se for apropriado para o contexto do processo de negócio que está sendo modelado. A versão atual da especificação BPMN define três tipos de artefatos, os quais são:

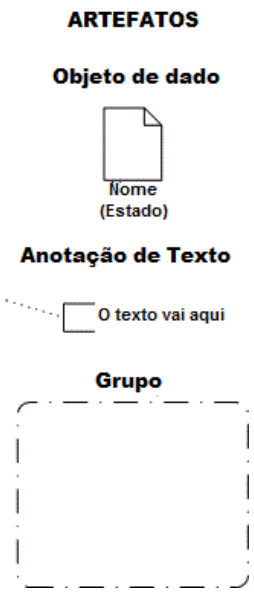

Ilustração 14 – Artefatos do BPMN

Fonte: <http://www.bpmn.org>

2.7.1.4.1 Objeto de dado (*Data Object*)

Objetos de dados são um mecanismo para mostrar como os dados são utilizados ou produzidos por atividades. Eles estão ligados a atividades através de associações.

2.7.1.4.2 Grupo (*Group*)

Um grupo é representado por um retângulo de canto arredondado desenhado com uma linha tracejada. O agrupamento pode ser usado para fins de documentação ou de análise. Não afeta a sequencia do fluxo.

2.7.1.4.3 Anotação (*Annotation*)

Anotações são um mecanismo para o modelador fornecer informações de texto adicionais para o leitor de um diagrama.

Os artefatos incluídos no modelo pelos modeladores acrescentam mais detalhes sobre como o processo é realizado, muitas vezes para mostrar as entradas e saídas das atividades no processo. No entanto, a estrutura básica do processo, conforme determinado pelas atividades, pontes e fluxos de sequencia, não são mudados com a adição de artefatos no diagrama.

3 PROCEDIMENTOS METODOLÓGICOS

A fundamentação teórica do capítulo anterior orienta a metodologia a aplicada para o estudo dos processos de realização de auditoria e de fiscalização da Infraestrutura de Chaves Públicas Brasileira e a automação dos mesmos.

A estrutura da ICP-Brasil e sua normatização são definidas seguindo padrões mundialmente seguidos. Portanto, a ICP-Brasil possui particularidades em sua normatização, mas os princípios que a orienta e permite a gerência e a fiscalização de seus processos são semelhantes a qualquer outra Infraestrutura de Chaves Públicas existente.

Desse modo, as conclusões a que se chegou com o estudo da ICP-Brasil podem ser estendidas e utilizadas como orientação no estudo de qualquer outra ICP que se deseje pesquisar.

3.1 CARACTERIZAÇÃO DA PESQUISA

Como já citado, o estudo baseia-se na proposta de automação dos processos de realização de auditoria e de fiscalização da Infraestrutura de Chaves Públicas Brasileira. Portanto, o objetivo deste estudo é apresentar a proposta de um modelo para a automação e o uso do documento eletrônico seguro nos processos de realização de auditoria e de fiscalização da ICP-Brasil, utilizando abordagens metodológicas adequadas para alcançá-lo.

A pesquisa foi dividida em quatro etapas, e em cada etapa ela teve uma abordagem diferente.

Na primeira etapa foi feita a revisão bibliográfica, onde se reuniu informações na literatura para o desenvolvimento da pesquisa do modo como o objeto em estudo é aplicado atualmente e de como é possível a forma de sua aplicação como se deseja propor. A abordagem nesta etapa foi teórico-empírica.

Na segunda etapa foi feita a análise do estado atual da arte. Neste ponto foram estudados os processos atuais que são executados pela Infraestrutura de

Chaves Públicas Brasileiras na auditoria e na fiscalização. A abordagem foi qualitativa, já que a análise e conclusões obtidas nessa etapa prouveram da coleta e organização de dados de funcionamento atual da ICP-Brasil através de sua normatização.

Segundo Chizotti, a investigação qualitativa tem o propósito de verificar a dinâmica entre a realidade e o sujeito na tentativa de relacionar modelos teóricos de decisão de investimentos à prática do mercado (CHIZZOTTI, 1991). Para Yin, o estudo de caso é uma investigação empírica que investiga um fenômeno contemporâneo dentro de seu contexto da vida real, especialmente quando os limites e o contexto não estão claramente definidos (YIN, 2002). A utilização de uma abordagem qualitativa por conhecimento teórico-empírico nestas duas primeiras etapas orientou a pesquisa para relacionar a dinâmica entre o mundo real e a subjetividade do sujeito de estudo, já que a investigação não foi baseada em dados quantificáveis, mas na coleta e organização de dados que forneçam informação para a construção de análises e conclusões (RICHARDSON, 1999).

Na terceira etapa foi proposto um novo modelo para a Infraestrutura de Chaves Públicas Brasileira automatizar e utilizar o documento eletrônico seguro nos seus processos de auditoria e fiscalização, tornando-os mais eficientes e dinâmicos. A abordagem nesta etapa foi avaliativa e indutiva.

Segundo Lakatos e Markoni, o método dedutivo é o método de abordagem que, partindo das teorias e leis, na maioria das vezes, prediz a ocorrência dos fenômenos particulares (LAKATOS, 1995), e é realizado em três etapas: a observação dos fenômenos; a descoberta da relação entre eles e a generalização da relação (LAKATOS, 2006). Este método orientou bem esta etapa da pesquisa.

Na última etapa foi comparado o modelo proposto com o estado atual da arte, para verificar quais seriam os possíveis impactos que o modelo proposto causaria se fosse utilizado no lugar do modelo atual. Nesta etapa a pesquisa adquire abordagem descritiva, explicativa e comparativa.

O método comparativo foi utilizado para desenvolver análises comparativas com a finalidade de verificar semelhanças e explicar divergências entre os dois modelos, o proposto e o atual. O método descritivo serviu para analisar e relacionar

os fatos e fenômenos observados e o método explicativo para identificar os fatores que determinam ou contribuem para a ocorrência dos fenômenos observados (GIL, 1991).

O estudo foi realizado com o detalhamento dos atuais processos de auditoria e de fiscalização da ICP-Brasil. As fontes de informações, os dados colhidos da normatização da ICP-Brasil e detalhamento do estado atual da arte guiaram este estudo.

3.2 TÉCNICAS DE COLETA E ANÁLISE DOS DADOS

Os dados que foram coletados para orientar a pesquisa foram diferentes a cada etapa.

Na primeira etapa foi utilizada a revisão teórica e o levantamento documental através de pesquisa bibliográfica e documental. Esta etapa da pesquisa serviu para colher todas as informações e dados possíveis na literatura acadêmica e técnica sobre que fatores orientaram as pesquisas e os desenvolvimentos das normas das ICPs até elas adquirirem a estrutura e a ideologia atuais. Esta etapa da pesquisa teve características objetivas, já que foi apenas coletado dados de documentos acadêmicos e técnicos.

Na segunda etapa foi utilizada a revisão teórica e a análise documental, através da análise bibliográfica e documental e de pesquisas na normatização da ICP-Brasil. Nesta etapa foram definidos os pontos da literatura acadêmica e documental que são importantes para se compreender o estado atual da arte dos processos de auditoria e fiscalização da ICP-Brasil, listando suas limitações e pontos fracos. Também foram definidos os pontos da literatura acadêmica e documental que orientaram na elaboração da proposta de automação e uso do documento eletrônico seguro pelos mesmos processos. Ao final foi feita a modelagem em BPMN do estado atual da arte do objeto de estudo. Esta etapa da pesquisa teve características subjetivas, com a interpretação pessoal da análise documental e teórica para verificar como se encontram atualmente os processos que são o foco da pesquisa.

Na terceira etapa foi utilizada a fundamentação teórica e documental, além da experiência própria do autor na área, para propor um modelo para a elaboração da proposta de automação e dos processos de auditoria e fiscalização da ICP-Brasil com o uso do documento eletrônico seguro. Para isso foi utilizada a análise do material recolhido nas etapas anteriores e a modelagem em BPMN do cenário proposto. Esta etapa da pesquisa teve características objetivas, com a análise da fundamentação técnica e acadêmica sobre o tema, e subjetiva, com a modelagem lógica de um possível cenário automatizado dos processos estudados. Nesta etapa foi feito o mapeamento, modelagem e análise dos processos pesquisados, para determinar o seu modelo de gestão e fiscalização do ponto de vista de seus processos de negócio (GONCALVES, 2000) e a adequação destes processos em um modelo onde eles estejam automatizados e utilizando o documento eletrônico seguro como substrato para guarda e troca de informações.

Na quarta e última etapa foi confrontado o estado atual da arte com o modelo proposto. Neste ponto da pesquisa foi analisado o impacto que o modelo proposto teria na estrutura, se fosse adotado. Esta etapa da pesquisa teve características objetivas e subjetivas, já que foram utilizados tanto o resultado de dados colhidos com a documentação acadêmica e técnica, que serviram de referencial teórico, quanto o resultado da percepção do autor de como pode ser feita a automação dos processos mapeados da estrutura atual.

O quadro abaixo ilustra os procedimentos metodológicos adotados:

	1ª Etapa	**2ª Etapa**	**3ª Etapa**	**4ª Etapa**
Objetivo	Revisão bibliográfica.	Análise do estado atual da arte.	Propor um novo modelo lógico.	Comparar modelo proposto com estado atual da arte.
Técnica	- Revisão	- Revisão	- Fundamentação	Estado atual da arte versus

	teórica; - Levantamento documental.	teórica; - Análise documental.	teórica; - Fundamentação documental; - Experiência própria.	modelo proposto.
Abordagem	- Teórica; - Empírica.	Qualitativa.	- Avaliativa; - Indutiva.	- Descritiva; - Explicativa; - Comparativa.
Instrumentos	- Pesquisa bibliográfica; - Pesquisa documental.	- Análise bibliográfica; - Análise documental; -Modelagem em BPMN.	- Análise; - Modelagem em BPMN.	- Modelo lógico proposto; - Estado atual da arte.
Característica	Objetiva.	Subjetiva.	- Objetiva; - Subjetiva.	- Objetiva; - Subjetiva.

Ilustração 15 – Procedimentos metodológicos adotados.

Com a elaboração do modelo proposto da terceira etapa da pesquisa e o resultado da comparação da quarta etapa da pesquisa, foi organizado o relatório final da pesquisa, abrangendo as considerações finais, as limitações encontradas e as propostas de estudos subsequentes.

3.4 LIMITAÇÕES DA PESQUISA

Por ser uma pesquisa inovadora, a literatura sobre uso de organizações virtuais, serviços compartilhados e automação de processos em ICPs é escassa. As pesquisas para melhorar a eficiência da gestão da estrutura de uma ICP é tema novo não apenas no Brasil, mas em âmbito global.

O cenário atual da estrutura da ICP-Brasil é determinada por entidades que detêm grandes poderes econômicos e políticos e se beneficiam da aplicação das regras de negócios no seu formato atual. Pode não ser interesse dessas entidades que exista uma proposta que automatize os processos de fiscalização e auditoria da ICP-Brasil e possibilite mais controle da AC Raiz sobre os mesmos.

A estrutura física da ICP-Brasil envolve muita segurança e controle. O acesso a ela é dificultoso por questões de segurança dos dados das entidades de sua estrutura.

O tempo disponível para realizar este estudo é curto para se estudar uma estrutura tão grande e complexa como a ICP-Brasil, quanto mais apresentar um modelo ideal de automação dos seus processos de auditoria e fiscalização. O resultado da pesquisa pode não ficar tão bom quanto poderia ser com mais tempo para se aprofundar no detalhamento funcional e normativo da ICP-Brasil.

4 APRESENTAÇÃO, ANÁLISE E INTERPRETAÇÃO DOS DADOS

A ICP-Brasil apresenta uma série de documentos em seu normativo que orientam as entidades que a compõe na execução da tarefa que cabe a cada uma no ciclo de vida dos certificados digitais emitidos. Esses documentos compõem o conjunto de documentos principais das normas da legislação da ICP-Brasil e cada um trata das normas de um tema específico dentro da variada gama de processos da estrutura. Completando essas normas existem os adendos, que são documentos que auxiliam na execução das normas das atividades que são descritas em cada um dos documentos principais do normativo.

As auditorias e as fiscalizações da ICP-Brasil são tratadas em três documentos de normas principais. Para a auditoria há um normativo específico, assim como para a fiscalização. No caso da auditoria, porém, há outro normativo que trata do credenciamento e descredenciamento de entidades na estrutura. Esse documento deve ser levado em consideração porque parte dos processos de pré-auditoria de entidades estão descritos nele.

Para a auditoria são os seguintes documentos:

- DOC-ICP-03 (ANEXO A);
- DOC-ICP-08 (ANEXO B);

E para a fiscalização é:

- DOC-ICP-09 (ANEXO C).

Além dos documentos há os adendos que os auxiliam, e que serão apresentados no decorrer da explicação dos processos.

O DOC-ICP-03 possui o título de “CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL” e encontra-se na sua versão 4.3, de 24 de novembro de 2009.

O DOC-ICP-08 possui o título de “CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES DA ICP-BRASIL” e encontra-se na sua versão 4.0, de 18 de novembro de 2009.

O DOC-ICP-09 possui o título de “CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL” e encontra-se na sua versão 3.0, de novembro de 2008.

As auditorias têm por objetivo avaliar se os processos, procedimentos,

atividades e controles estão em conformidade com as respectivas Políticas de Certificado, Declaração de Práticas de Certificação, Política de Segurança e demais normas e procedimentos estabelecidos pelo Comitê Gestor da ICP-Brasil (ANEXO B). Existem dois tipos de auditorias:

- Pré-operacionais – realizadas antes do início das atividades do candidato a Prestador de Serviço de Certificação;
- Operacionais – realizadas anualmente em todos os Prestadores de Serviço de Certificação para manutenção do credenciamento junto à ICP-Brasil.

O objetivo da Fiscalização é verificar a conformidade dos processos, procedimentos e atividades dos PSCs com suas Declarações de Práticas, Políticas e com as Resoluções e normas gerais estabelecidas para as entidades integrantes da ICP-Brasil (ANEXO C).

A norma DOC-ICP-08 trata de todos os processos de auditoria, inclusive os de credenciamento de entidades de auditoria. Para este trabalho foram focados apenas os processos de realização de auditorias nas entidades da ICP-Brasil. A norma DOC-ICP-03 possui os processos de como as auditorias pré-operacionais devem ser realizadas. Estes foram os processos utilizados na modelagem.

A norma DOC-ICP-09 trata de todos os processos de fiscalização e todos foram utilizados na modelagem.

4.1 PROCESSOS DE REALIZAÇÃO DE AUDITORIA

A auditoria pode ser iniciada por evento do credenciamento de uma entidade à estrutura, quando ela é pré-operacional, ou pode ser planejada, quando é operacional.

A AC Raiz realiza a auditoria:

- Pré-operacional de:
  - AC de primeiro nível e seus PSS;
  - AC subsequente e seus PSS;
  - ACT.
- Operacional de:
  - AC de primeiro nível e seus PSS;
  - AR no exterior.

Empresas de auditoria independente credenciadas junto ao ITI realizam auditoria:

- Pré-operacional de:
  - AR;
  - AR no exterior;
  - PSS de AR.
- Operacional de:
  - AC subsequente e seus PSS;
  - ACT;
  - AR;
  - AR no exterior;
  - PSS de AR.

A auditoria operacional também pode ser realizada por Auditoria Interna da respectiva AR credenciada junto ao ITI em:

- AR;
- AR no exterior;
- PSS de AR.

A AC Raiz recebe auditorias do Comitê Gestor ou seus prepostos, formalmente designados.

A ilustração 16 mostra o macroprocesso de realização de auditorias na ICP-Brasil.

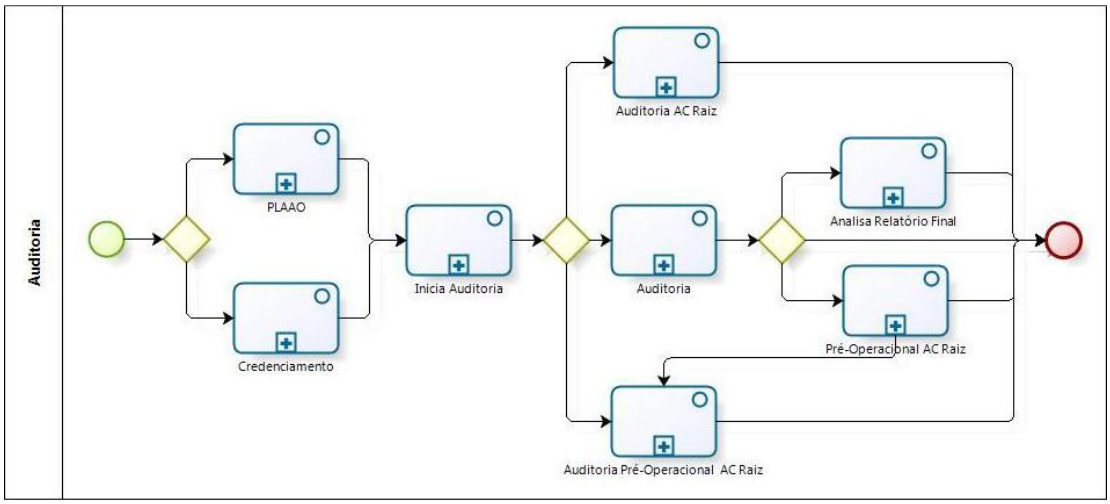

Ilustração 16 – Macroprocesso do fluxo de auditoria.

Quando a auditoria é planejada, a AC preenche um Plano Anual de Auditoria Operacional ADE-ICP-08.C (PLAAO) das entidades das quais ela é responsável (ANEXO E). O PLAAO precisa ser protocolado pela Diretoria de Auditoria, Fiscalização de Normalização (DAFN). Isso deve ser feito até o dia 15 de dezembro de cada ano para o ano civil seguinte.

Até o dia 15 de março de cada ano, para fins de manutenção de credenciamento na ICP-Brasil, a AC deve enviar à AC Raiz o cronograma das auditorias a serem realizadas, durante o ano todo, nas entidades que lhe sejam operacionalmente vinculadas.

A ilustração 17 mostra esse processo.

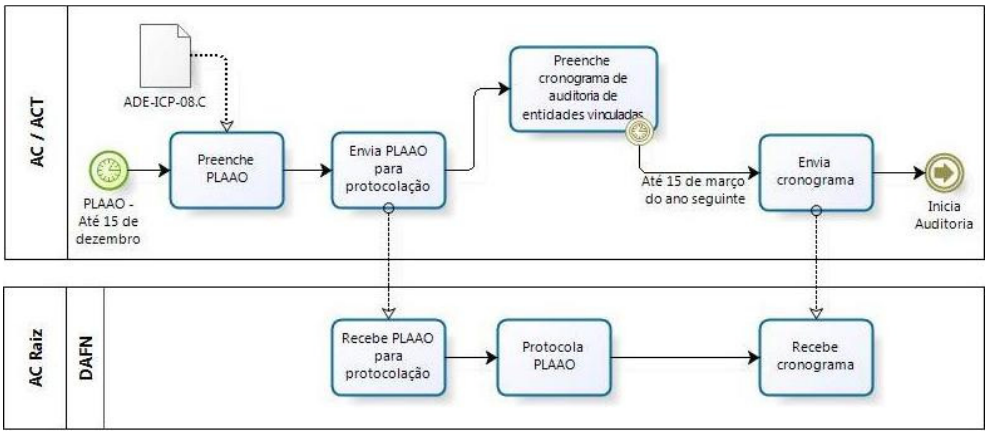

Ilustração 17 – Início de auditoria por um PLAAO.

Quando a auditoria é iniciada devido ao credenciamento de uma AC (e seus PSS) ou ACT, a entidade candidata deve preencher o formulário de requerimento de auditoria ADE-ICP-03.D (ANEXO D) e enviá-lo à AC Raiz, para dar início ao processo de auditoria. Quando é o credenciamento de uma AR ou PSS de AR, o Prestador de Serviço de Certificação (PSC) responsável por ela é que deve das início ao processo de auditoria.

A ilustração 18 mostra esse processo.

Quando a auditoria é iniciada, se ela for pré-operacional ou operacional de AR ou PSS de AR, o PSC responsável contrata uma empresa de auditoria independente credenciada ao ITI para realizá-la. Caso seja de AC subsequente, a empresa de

auditoria independente também é contrata pelo PSC responsável para realizar a auditoria.

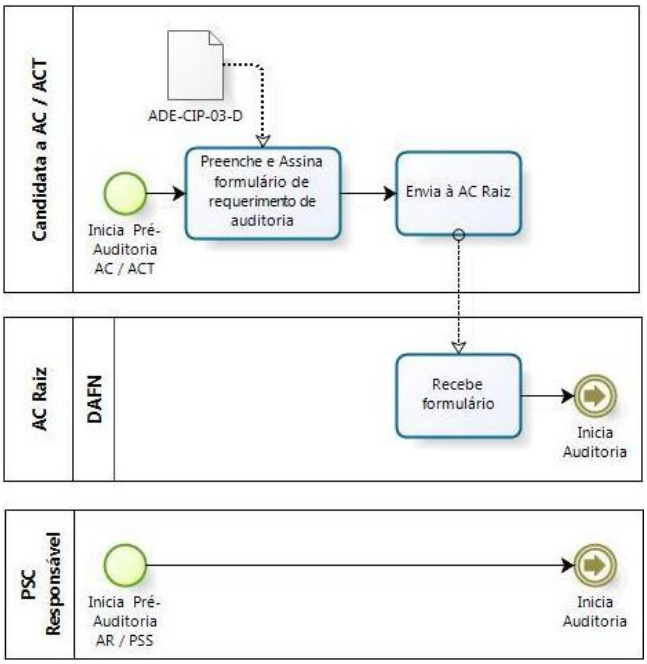

Ilustração 18 – Início de pré-auditoria por credenciamento

Caso seja de AC de primeiro nível (e seus PSS) ou ACT, a AC Raiz é quem realiza a auditoria. Caso seja uma auditoria pré-operacional, a AC Raiz tem até 15 dias para iniciar os processos.

A Ilustração 19 mostra esses processos.

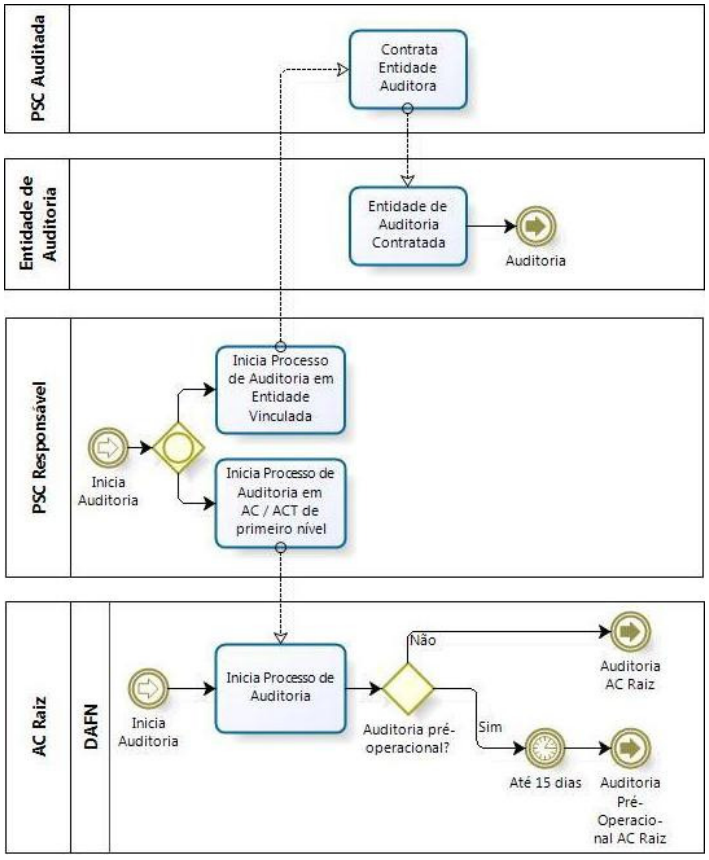

Ilustração 19 – Início de processos de auditoria e pré-auditoria.

Quando a auditoria é realizada por uma entidade auditora, se ela for pré-operacional será preciso avisar a AC Raiz do início da auditoria. Para isso deve-se utilizar o modelo de comunicação de início de trabalhos de auditoria ADE-ICP-08.D (ANEXO F) e a correspondência deve ser feita através de e-mail assinado, segundo os procedimentos para troca de correspondências entre as entidades e o ITI ADE-ICP-08.H (ANEXO J).

A auditoria é iniciada e realizada utilizando como base a descrição dos processos das entidades da ICP-Brasil ADE-ICP-08.E (ANEXO G) e, quando é pré-operacional, os requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICP-Brasil DOC-ICP-05.

Durante o processo de auditoria a entidade que está realizando a auditoria analisa os processos, procedimentos, atividades e controles com PCs, DPCs, PSs, normas e procedimentos da entidade auditada. Ela também pode solicitar documentação adicional e ter acesso aos ambientes físicos e lógicos da entidade

auditada. Estas atividades são realizadas até que a auditoria esteja finalizada.

Quando a auditoria é finalizada, a entidade de auditoria guarda o material utilizado na auditoria e elabora o relatório final, com base nos critérios para emissão de parecer de auditoria DOC-ICP-08.F (ANEXO H). O relatório deve ser enviado à entidade auditada e ao PSC responsável.

A ilustração 20 mostra estas atividades.

Em seguida serão verificadas irregularidades no processo de auditoria. Caso nenhuma irregularidade seja verificada, a entidade de auditoria emite o relatório final de auditoria.

Caso seja verificada alguma irregularidade, a entidade auditada e o PSC responsável recebem o aviso de que há irregularidades. A entidade auditada deve informar ao PSC responsável e à entidade de auditoria que recebeu o aviso e então deve corrigir as irregularidades dentro de um tempo determinado pela entidade de auditoria. Quando as irregularidades estiverem corrigidas, o PSC responsável e a entidade de auditoria devem ser avisados.

Acabando o tempo para a correção de irregularidades, a entidade de auditoria verificará se elas foram corrigidas. Caso tenham sido, uma nova auditoria será realizada, caso contrário a entidade auditada e o PSC responsável são avisados e o relatório final será elaborado. O PSC responsável deve avisar a AC Raiz sobre a não correção das irregularidades de acordo com o ANEXO J.

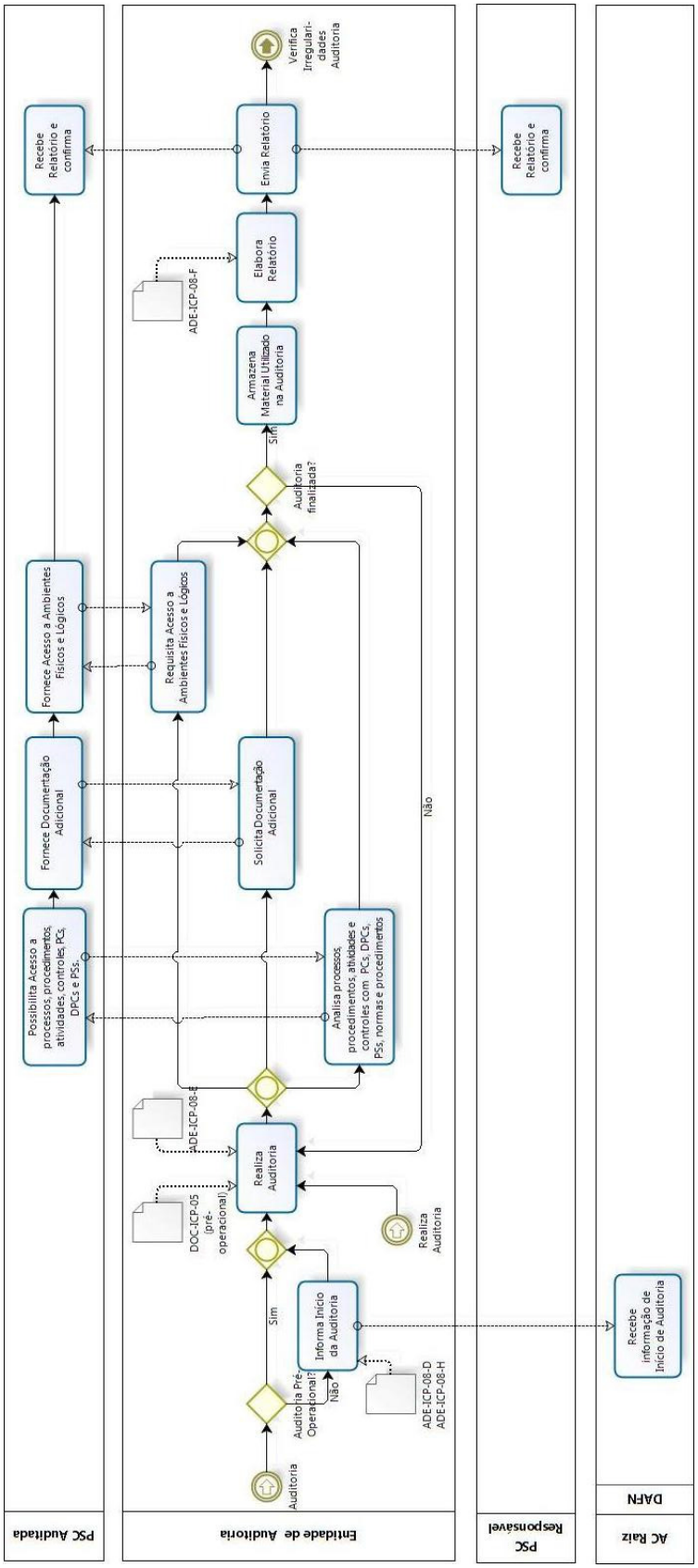

Ilustração 20 – Processo de auditoria por entidade auditora.

Quando o relatório final é gerado, ele é enviado à entidade auditada, ao PSC responsável e à AC Raiz de acordo com o ANEXO J. Se a auditoria for pré-operacional, o PSC responsável envia o relatório final junto com os documentos de credenciamento à AC Raiz, de acordo com o ANEXO J. Caso a auditoria seja operacional, a AC Raiz pode analisar o relatório final ou emitir parecer sobre ele.

A ilustração 21 mostra essas atividades.

Quando a auditoria é do tipo operacional e de AC de primeiro nível (e seus PSS) ou ACT, ela é realizada utilizando como base a descrição dos processos das entidades da ICP-Brasil ADE-ICP-08.E (ANEXO G).

Durante o processo de auditoria a AC Raiz analisa os processos, procedimentos, atividades e controles com PCs, DPCs, PSs, normas e procedimentos da entidade auditada. Ela também pode solicitar documentação adicional e ter acesso aos ambientes físicos e lógicos da entidade auditada. Estas atividades são realizadas até que a auditoria esteja finalizada.

Quando a auditoria é finalizada, a AC Raiz guarda o material utilizado na auditoria e elabora o relatório final, com base nos critérios para emissão de parecer de auditoria DOC-ICP-08.F (ANEXO H). O relatório deve ser enviado à entidade auditada.

A ilustração 22 mostra estas atividades.

Em seguida serão verificadas irregularidades no processo de auditoria. Caso nenhuma irregularidade seja verificada, a AC Raiz emite o relatório final de auditoria.

Caso seja verificada alguma irregularidade, a entidade auditada recebe o aviso de que há irregularidades. A entidade auditada deve informar à entidade AC Raiz que recebeu o aviso e então deve corrigir as irregularidades dentro de um tempo determinado pela AC Raiz. Quando as irregularidades estiverem corrigidas, a AC Raiz deve ser avisada.

Acabando o tempo para a correção de irregularidades, a AC Raiz verificará se elas foram corrigidas. Caso tenham sido, uma nova auditoria será realizada, caso contrário a entidade auditada é avisada e o relatório final será elaborado.

Quando o relatório final é gerado, ele é enviado à entidade auditada de acordo com o ANEXO J. A AC Raiz então emite o parecer sobre ele.

A ilustração 23 mostra essas atividades.

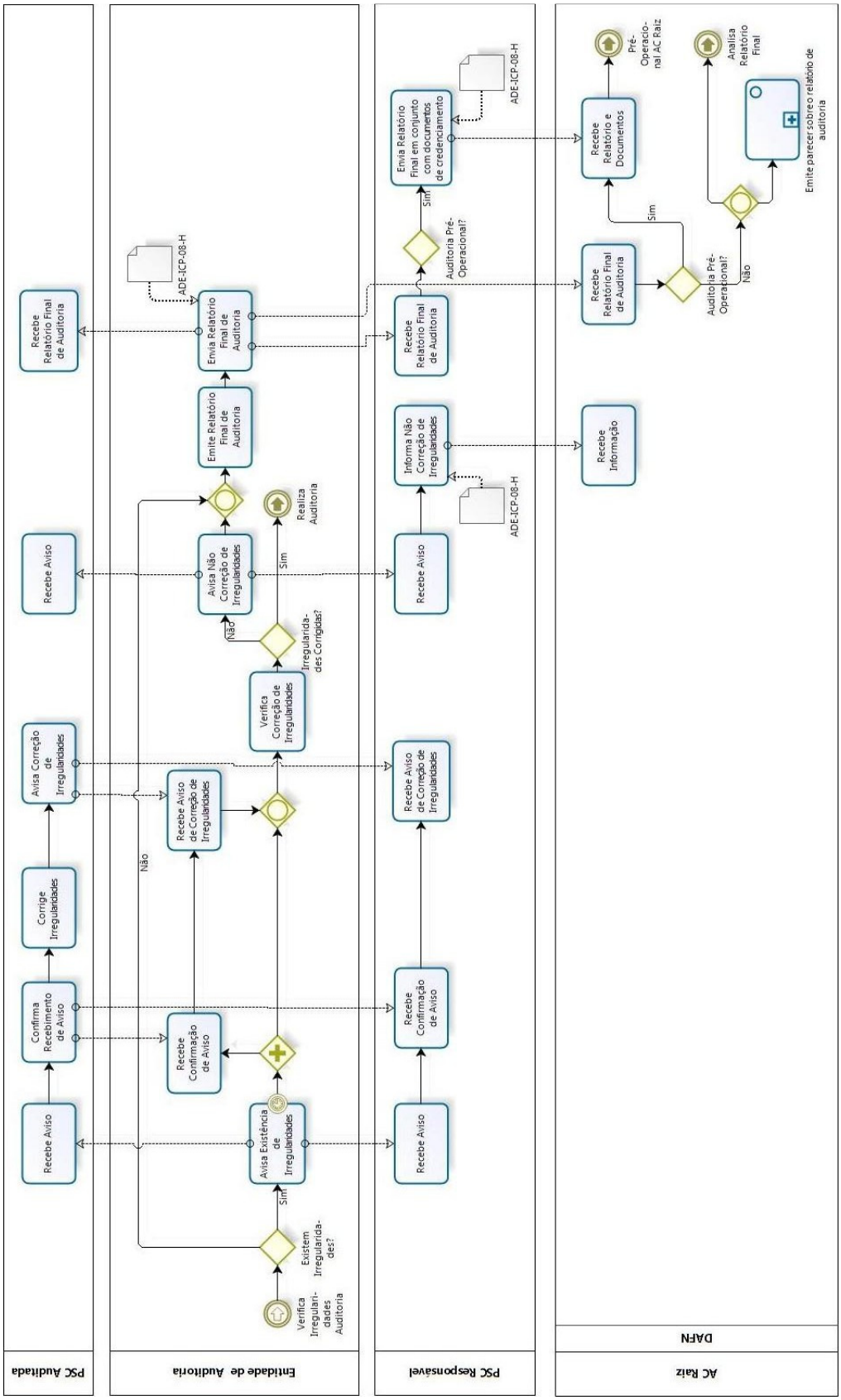

Ilustração 21 – Verificação de irregularidade encontrada na auditoria por entidade auditora.

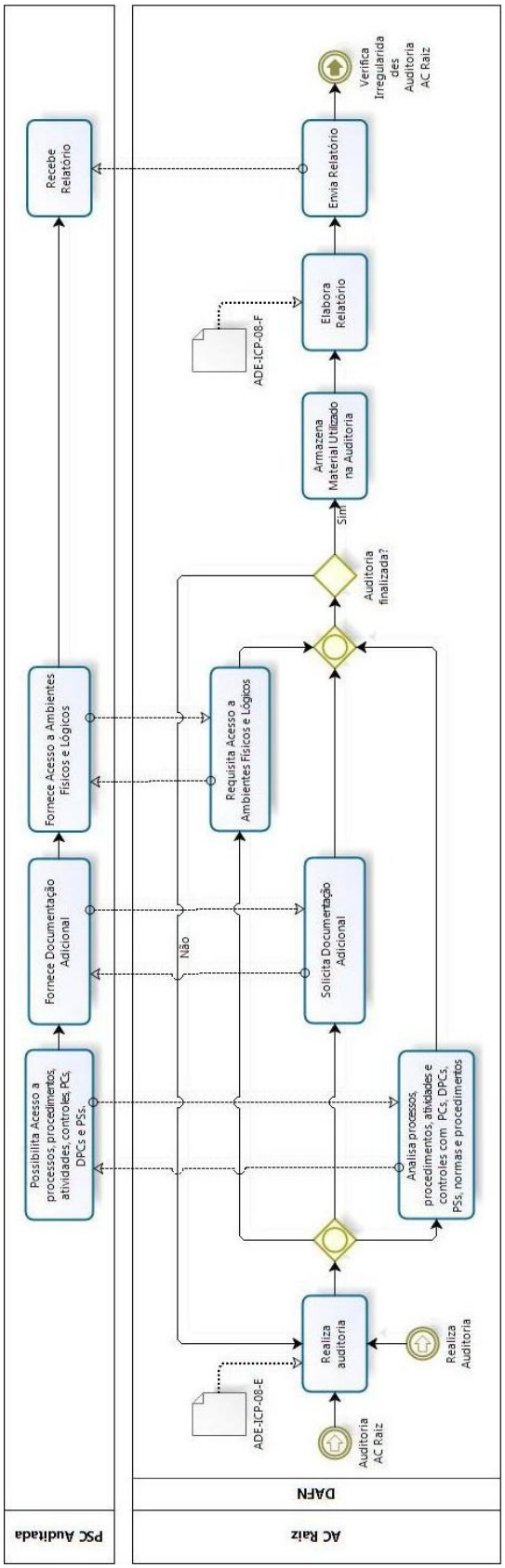

Ilustração 22 – Processo de auditoria realizada pela AC Raiz

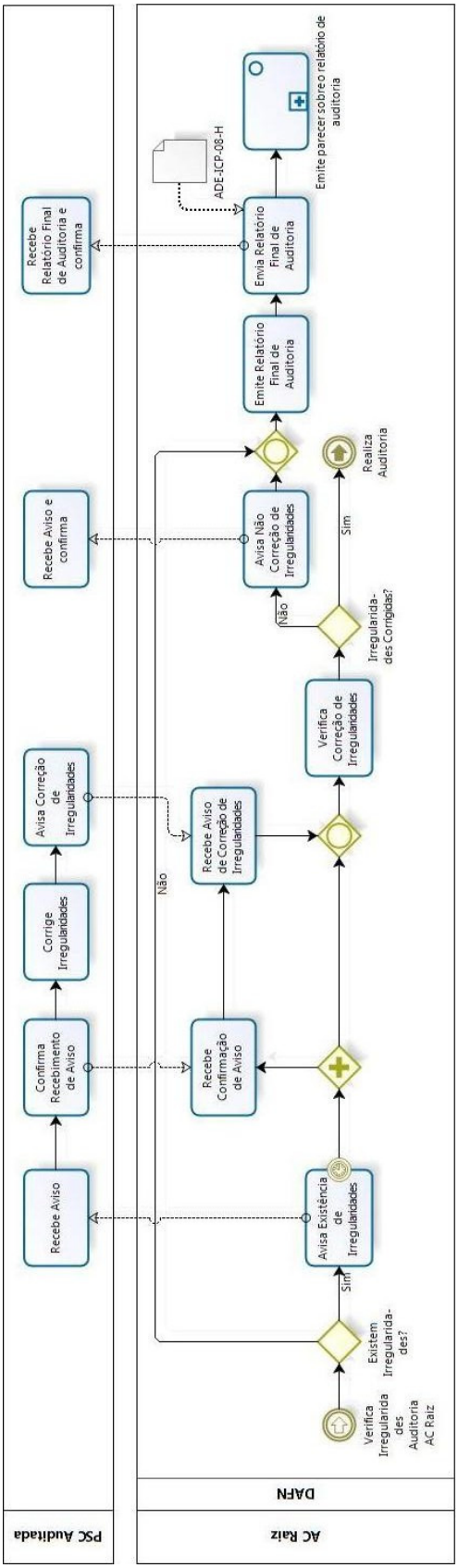

Ilustração 23 – Verificação de irregularidades encontradas na auditoria pela AC Raiz.

Quando a auditoria é pré-operacional de AC e primeiro nível (e seus PSS) ou ACT, ela é realizada utilizando como base a descrição dos processos das entidades da ICP-Brasil ADE-ICP-08.E (ANEXO G).

Durante o processo de auditoria a AC Raiz analisa os processos, procedimentos, atividades e controles com PCs, DPCs, PSs, normas e procedimentos da entidade auditada. Ela também pode solicitar documentação adicional e ter acesso aos ambientes físicos e lógicos da entidade auditada. Estas atividades são realizadas até que a auditoria esteja finalizada.

Quando a auditoria é finalizada, a AC Raiz guarda o material utilizado na auditoria e elabora o relatório final, com base nos critérios para emissão de parecer de auditoria DOC-ICP-08.F (ANEXO H). O relatório deve ser enviado à entidade auditada.

A ilustração 24 mostra estas atividades.

Em seguida serão verificadas irregularidades no processo de auditoria pré-operacional. Caso nenhuma irregularidade seja verificada, a AC Raiz emite o relatório final de auditoria.

Caso seja verificada alguma irregularidade, a entidade auditada recebe o aviso de que há irregularidades. A entidade auditada deve informar à entidade AC Raiz que recebeu o aviso e então deve corrigir as irregularidades dentro de um tempo determinado pela AC Raiz. Quando as irregularidades estiverem corrigidas, a AC Raiz deve ser avisada.

Acabando o tempo para a correção de irregularidades, a AC Raiz verificará se elas foram corrigidas. Caso tenham sido, será realizada uma auditoria complementar caso ainda não tenha sido realizada. Se a auditoria complementar já tiver sido realizada ou se as irregularidades não tiverem sido corrigidas o relatório final será elaborado.

Quando o relatório final é gerado, ele é enviado à entidade auditada e a AC Raiz terá 30 dias para emitir o parecer sobre ele.

A ilustração 25 mostra essas atividades.

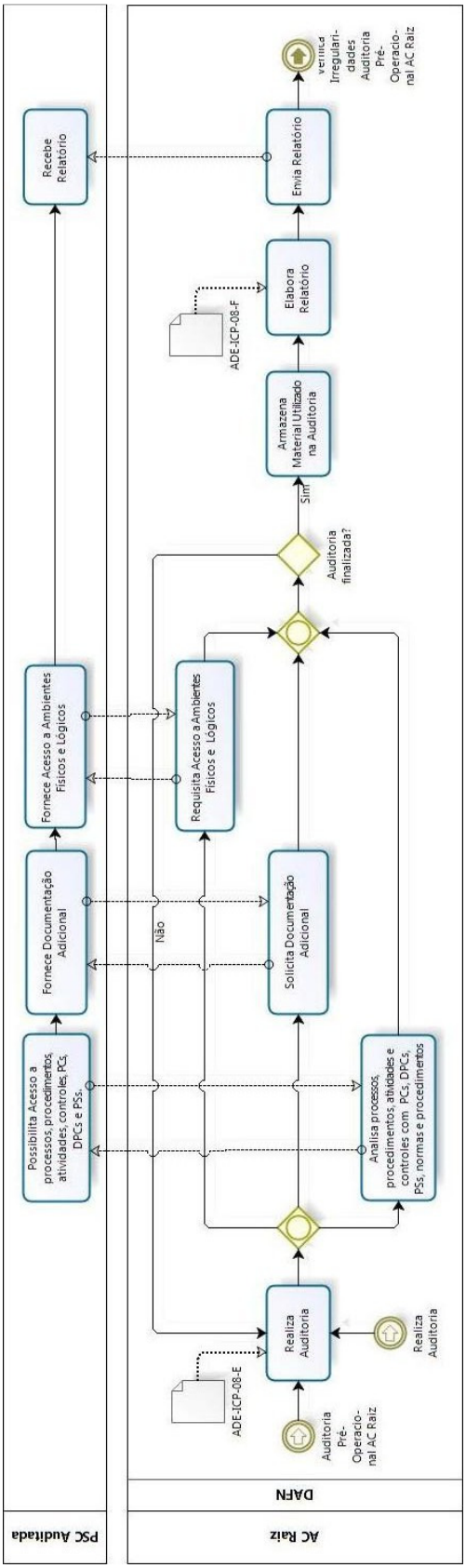

Ilustração 24 – Processo de auditoria pré-operacional realizada pela AC Raiz.

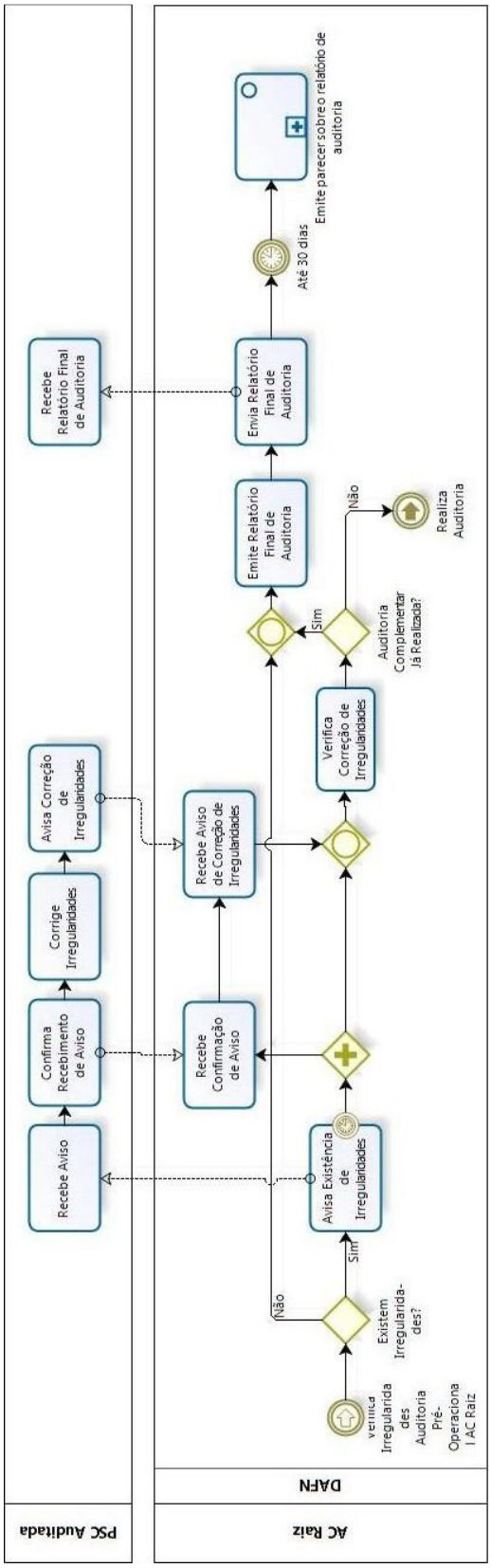

Ilustração 25 – Verificação de irregularidades encontradas na auditoria pré-operacional realizada pela AC Raiz.

Quando a auditoria é pré-operacional de AR ou PSS de AR, após a auditoria realizada por uma entidade auditora independente e credenciada ao ITI, a AC Raiz irá examinar a documentação para o credenciamento da entidade candidata, juntamente com o relatório de auditoria pré-operacional. Em 30 dias a AC Raiz pode se decidir por solicitar material utilizado na pré-auditoria e realizar ela mesmo a auditoria pré-operacional, que substituirá a auditoria já realizada. O processo dessa auditoria será o mesmo já descrito na ilustração 24.

Caso a AC Raiz decida manter a auditoria já realizada, ela irá emitir o parecer sobre o relatório de auditoria.

A ilustração 26 ilustra essas atividades.

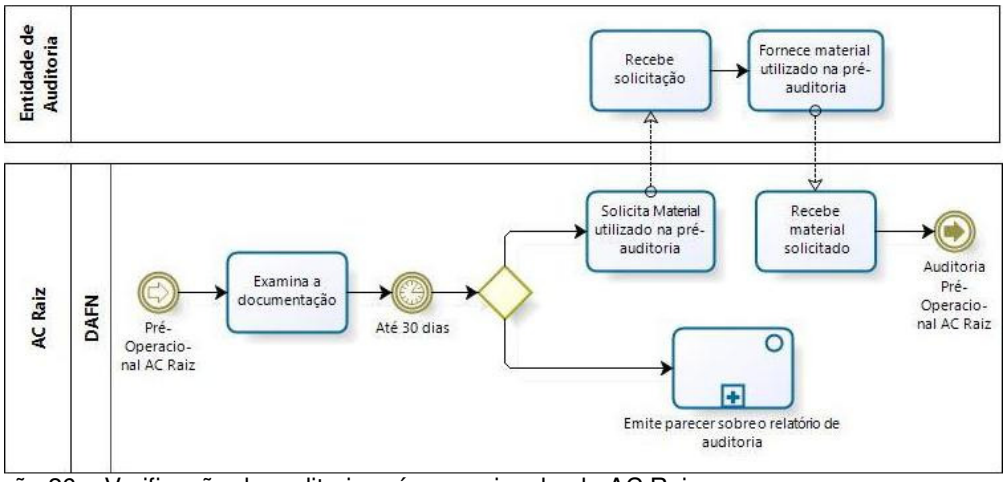

Ilustração 26 – Verificação de auditoria pré-operacional pela AC Raiz.

Quando a AC Raiz analisa um relatório final de auditoria, ela pode solicitar esclarecimentos ou documentos complementares tanto à entidade de auditoria quanto à entidade auditada, antes de começar a analisar a documentação, de acordo com a metodologia de auditoria da entidade de auditoria. Se nenhuma irregularidade for encontrada, o processo finaliza.

Caso seja encontrada alguma irregularidade, a AC Raiz avisa a entidade de auditoria e esta tem 15 dias para apresentar justificativas. Caso em 15 dias as justificativas não tenham sido apresentadas ou sejam insatisfatórias, a AC Raiz irá aplicar uma penalidade à entidade de auditoria de acordo com os critérios para

aplicação de penalidades a entidades credenciadas na ICP-Brasil ADE-ICP-08.G (ANEXO I).

A penalidade é enviada à entidade de auditoria e essa decide se aceita ou não a penalidade. Caso aceite, a AC Raiz publica a decisão de penalidade no DOU e o processo finaliza. Caso não aceite, ela solicita recurso ao diretor-presidente do ITI. Ele analisa o recurso e pode decidir por manter a penalidade ou indeferi-la. Se ele indeferir a penalidade, o processo finaliza, caso contrário ele pode pedir que a Procuradoria Federal Especializada subsidie a decisão dele, publica a penalidade no DOU e avisa a entidade de auditoria.

Recebendo a penalidade, em até 10 dias a entidade de auditoria pode decidir se aceita e então o processo finaliza, ou pode solicitar recurso ao Comitê Gestor da ICP-Brasil. O Comitê Gestor recebe o pedido de recurso e publica no DOU a sua decisão, finalizando o processo.

A ilustração 27 mostra esse processo.

Para emitir parecer sobre um relatório de auditoria, a AC Raiz analisa o relatório final de auditoria e, se for auditoria pré-operacional e credenciamento tiver sido indeferido, ela avisa o PSC responsável que, por sua vez, avisa ao PSC auditado. O PSC auditado decide se aceita ou não a penalidade, solicitando recurso ao Comitê Gestor, caso não aceite. Caso o credenciamento tenha sido deferido, são enviadas recomendações de auditoria à área de fiscalização da AC Raiz, caso seja necessário, e então o deferimento de credenciamento é publicado no DOU e o processo finaliza.

Se a auditoria realizada tiver sido operacional, são enviadas recomendações de auditoria à área de fiscalização da AC Raiz, caso seja necessário. Se o relatório de auditoria tiver recebido conceito 5 e for o segundo consecutivo, a entidade é descadastrada. Caso não tenha sido consecutivo, a entidade em suas operações suspensas. Caso o conceito tenha sido 3 ou 4, a entidade recebe penalidade. Caso o conceito tenha sido 1 ou 2, o processo finaliza.

Se o conceito tiver sido 3, 4 ou 5, a AC Raiz elabora o ofício de acordo com os fatos e normas descumpridas.

Esse processo todo se visualiza na ilustração 28.

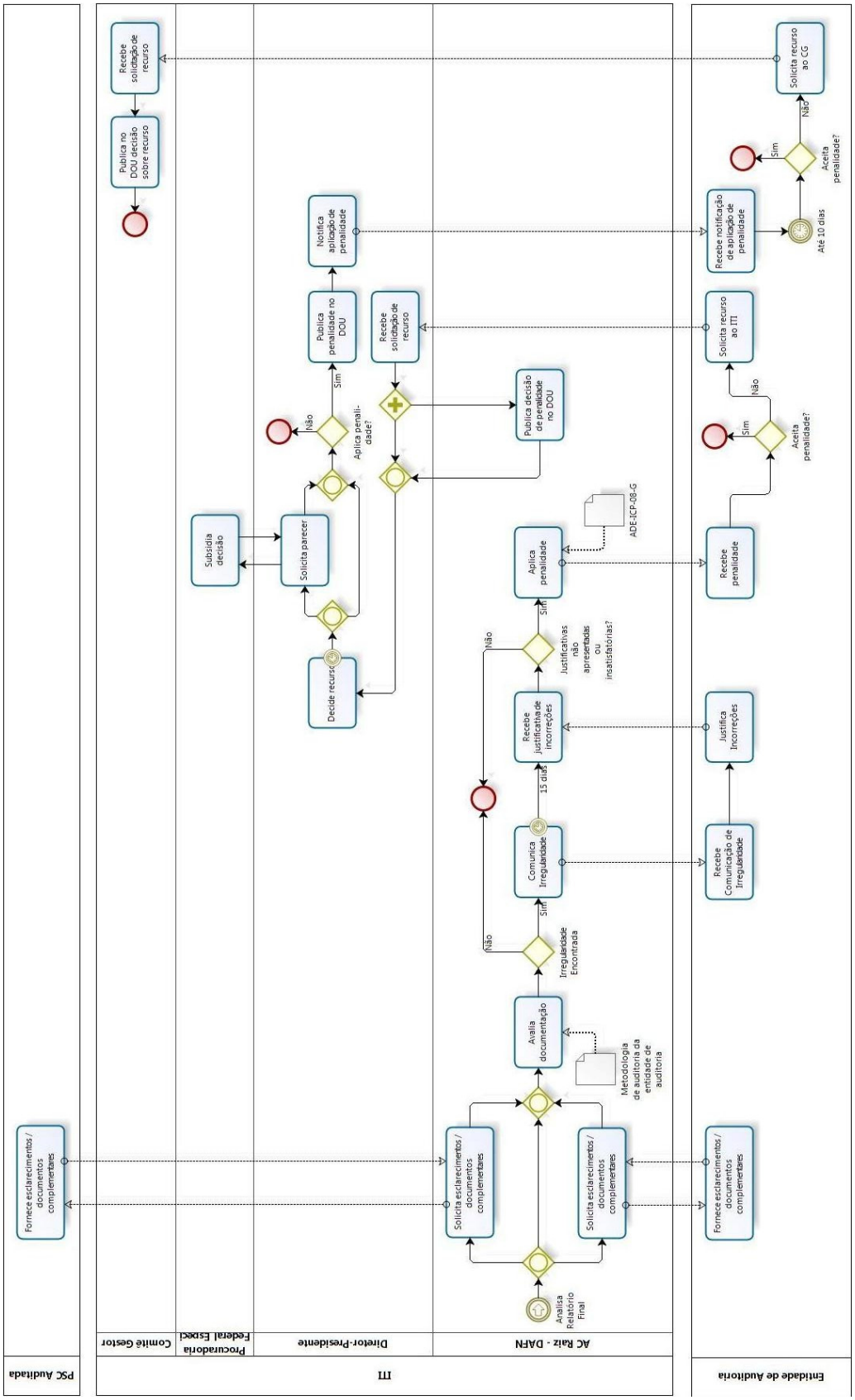

Ilustração 27 – Análise do relatório final de auditoria.

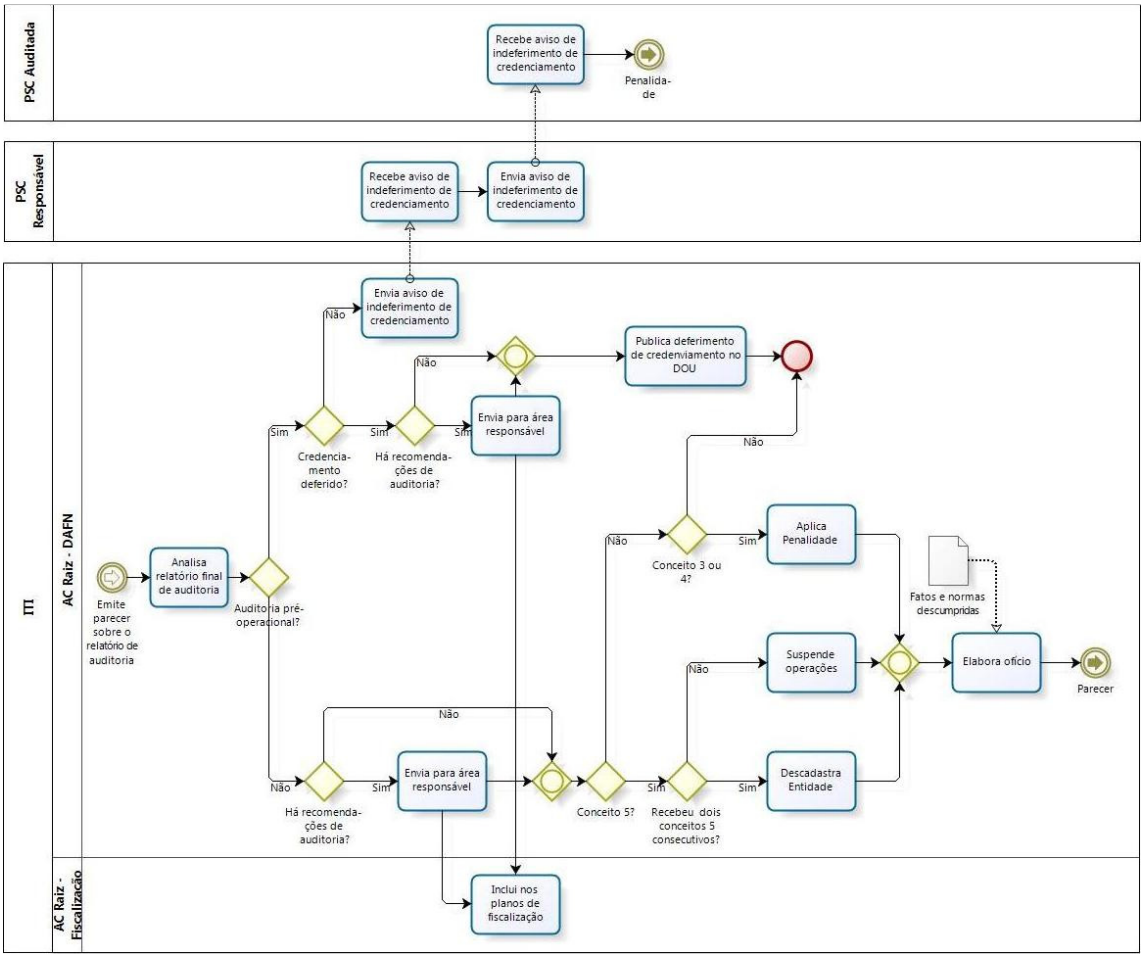

Ilustração 28 – Emissão de parecer sobre o relatório de auditoria

Após elaborar o ofício, a AC Raiz irá enviar o parecer de auditoria para a entidade auditada, que irá protocolar sua defesa utilizando justificativas e documentação para isso. A AC Raiz recebe a defesa e verifica se a aceita. Caso aceite, ela arquiva o processo e ele finaliza, senão ela notificará a penalidade à entidade auditada. Caso a entidade aceite a penalidade, o processo finaliza e a AC Raiz publica a decisão de penalidade no DOU, senão ela solicita recurso ao diretor-presidente do ITI. Ele analisa o recurso e pode decidir por manter a penalidade ou indeferi-la. Se ele indeferir a penalidade, o processo finaliza, caso contrário ele pode pedir que a Procuradoria Federal Especializada subsidie a decisão dele, publica a penalidade no DOU e avisa a entidade de auditoria.

Recebendo uma penalidade, em até 10 dias a entidade de auditoria pode decidir se aceita e então o processo finaliza, ou pode solicitar recurso ao Comitê

Gestor da ICP-Brasil. O Comitê Gestor recebe o pedido de recurso e publica no DOU a sua decisão, finalizando o processo.

A ilustração 29 mostra esse processo.

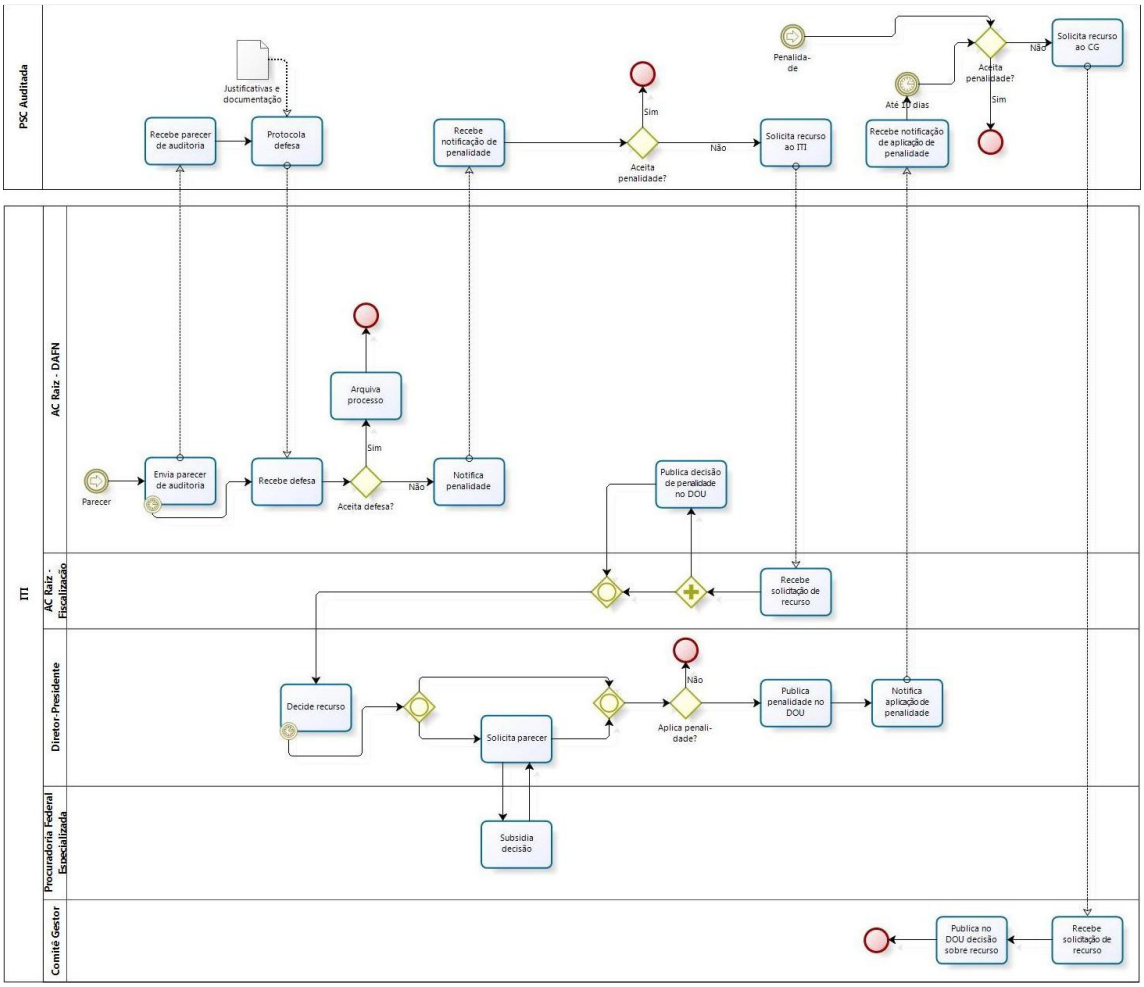

Ilustração 29 - Emissão de parecer sobre o relatório de auditoria – continuação.

4.2 PROCESSOS DE FISCALIZAÇÃO

O PFC iniciar-se-á através de planejamento de fiscalização semestral, recomendação obtida em Relatórios de Auditoria (Pré-Operacionais ou Operacionais), por denúncia feita por usuário de certificação digital da ICP-Brasil ou por constatação de ameaça à confiabilidade da ICP-Brasil (ANEXO C). Quem realiza os processos de fiscalização são os fiscais da AC Raiz. Ao iniciar um procedimento de fiscalização de certificação, é iniciado também um processo administrativo de fiscalização, onde será armazenada toda documentação.

A AC Raiz publica a abertura dos procedimentos de fiscalização de certificação e terá 120 dias para executar a ação de fiscalização de certificação. Ela pode prorrogar essa ação apenas uma vez por mais 120 dias. Ao finalizar a ação de fiscalização de certificação, a AC Raiz publica seu encerramento e elabora o relatório de fiscalização com base no documento ADE-ICP-09.E (ANEXO O).

Se tiver sido apresentada irregularidade no relatório de fiscalização, essas irregularidades serão corrigidas. Após as irregularidades serem corrigidas, a AC Raiz avisa ao PSC fiscalizado e ao PSC responsável o encerramento da fiscalização, e o processo finaliza. Esse macroprocesso da fiscalização pode ser visto na ilustração 30.

Na execução da ação de fiscalização de certificação, o diretor ou o coordenador geral da ação emite um termo de fiscalização inicial ADE-ICP-09.C (ANEXO M). Caso tenha necessidade, pode ser emitidos também termos de fiscalização extensivo e/ou complementar. Eles são incorporados ao termo de fiscalização inicial e ele é enviado ao PSC fiscalizado e ao PSC responsável.

O fiscal da ICP-Brasil então fiscaliza a entidade, tendo pleno acesso aos ambientes físicos e lógicos da entidade fiscalizada e podendo solicitar a ela informações complementares sempre que julgue necessário, usando como base o documento ADE-ICP-09.A (ANEXO K). Se não encontrar nenhuma infração, verifica se a ação de fiscalização de certificação já finalizou. Caso encontre alguma infração, ele irá emitir um auto de infração de certificação ADE-ICP-09.B (ANEXO L) e enviará ao PSC fiscalizado e ao PSC responsável. Se a ação de fiscalização já tiver finalizado, o direto ou coordenador geral da ação emitem um termo de fiscalização final e enviam ao PSC fiscalizado e o PSC responsável. Esse processo está representado na ilustração 31.

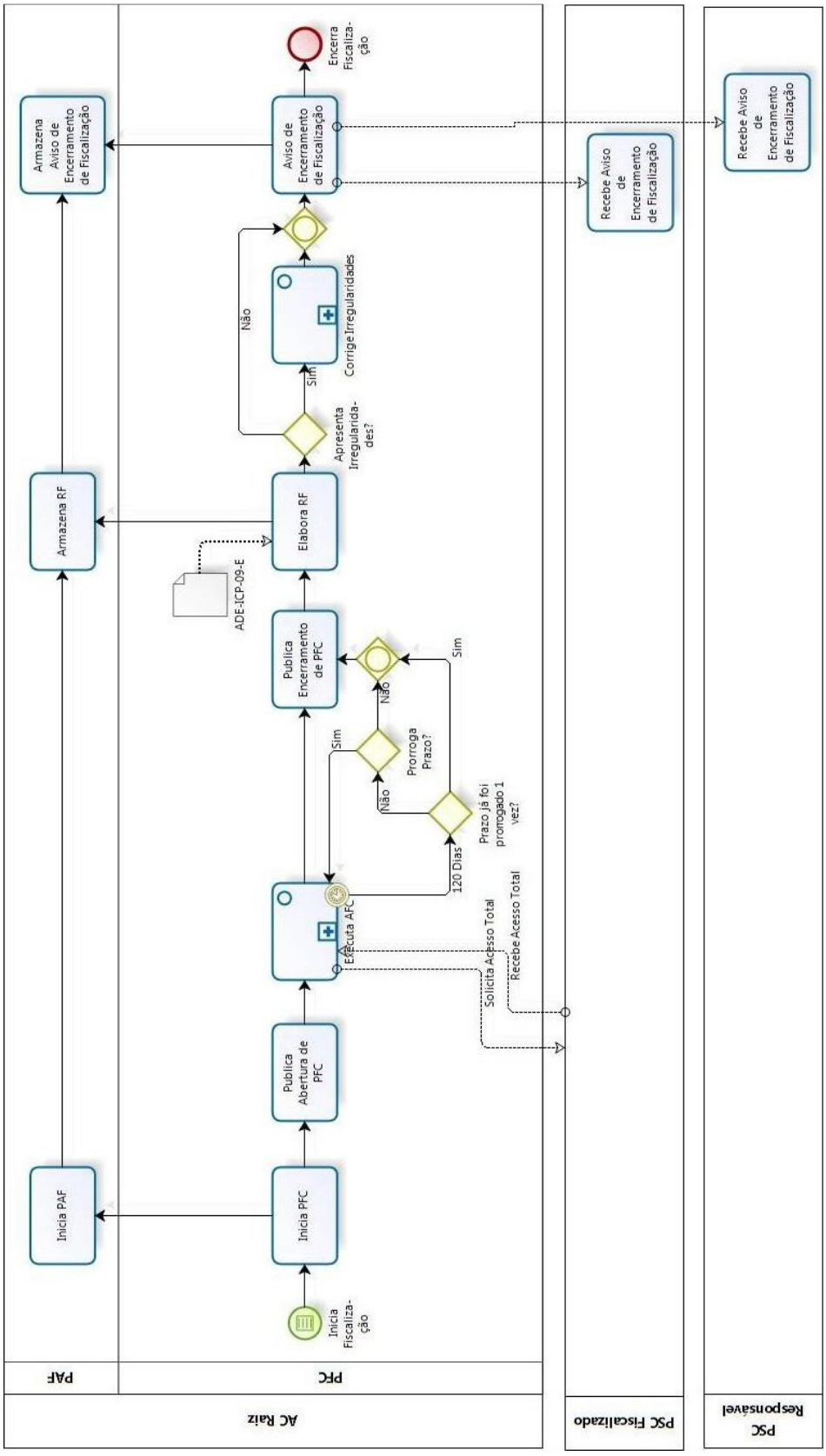

Ilustração 30 – Processo de fiscalização.

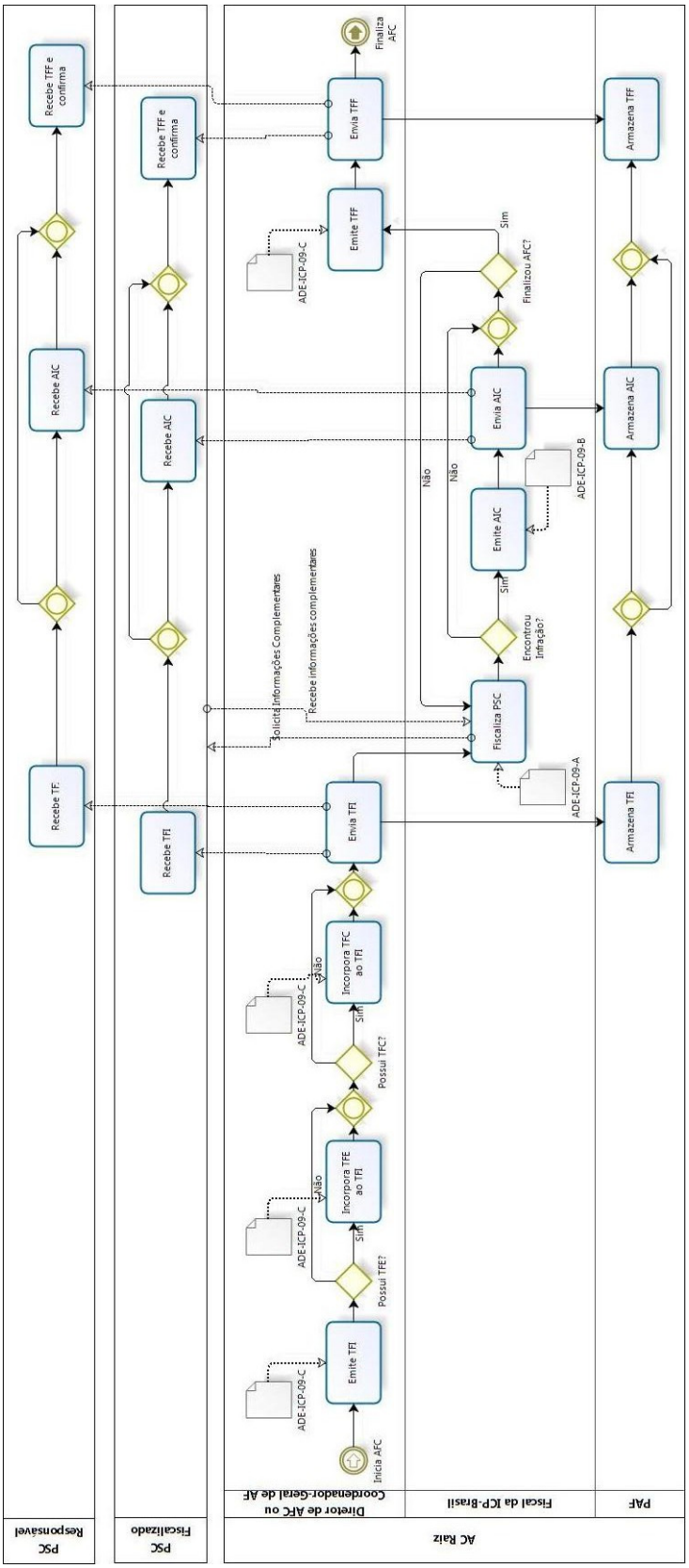

Ilustração 31 – Execução de ato de fiscalização de certificação.

Se alguma irregularidade foi encontrada durante a fiscalização, o diretor ou o coordenador geral da ação de fiscalização notifica a irregularidade por uma notificação de fiscalização de certificação ADE-ICP-09.D (ANEXO N) à entidade fiscalizada. Ela terá até 15 dias para apresentar a justificativa e defesa. Caso não apresente, o PSC responsável recebe a notificação e tem até 15 dias para apresentar a justifica e defesa. Não recebendo a justifica e defesa, a AC Raiz aplicará uma penalidade à entidade fiscalizada em até 20 dias.

Caso a defesa tenha sido apresentada, uma notificação de correção de irregularidades será enviada à entidade fiscalizada com um prazo para ser realizada. A entidade fiscalizada realiza as correções e avisa à AC Raiz. Após o prazo a AC Raiz verifica se a irregularidade foi corrigida e se tiver sido finaliza a verificação de irregularidades. Caso não tenha sido, ela aplicará penalidade à entidade fiscalizada em até 20 dias, de acordo com o documento ADE-ICP-09-01.

A entidade fiscalizada decide se aceita ou não a penalidade. Se aceitar o processo finaliza, senão ela tem até 20 dias para solicitar recurso à AC Raiz. A AC Raiz se reconsidera a penalidade. Caso reconsidere, ela encaminha a decisão sobre o recurso à entidade fiscalizada e o processo finaliza. Caso contrário, encaminha o recurso ao diretor presidente, que decide sobre ele com o subsídio da Procuradoria Federal Especializada e envia a decisão do recurso à AC Raiz, que encaminha para a entidade fiscalizada e finaliza o processo.

Os processos de irregularidade na fiscalização podem ser observados nas ilustrações 32 e 33.

Neste capítulo foi apresentada a modelagem em BPMN de como é realizado atualmente os processos de auditoria e fiscalização da ICP-Brasil. Esta modelagem serviu de base para a identificação dos pontos onde é possível utilizar o documento eletrônico seguro nestes processos. Também serviu de base para modelar os processos de forma que eles sejam executados centrados em um sistema automatizado. O próximo capítulo apresenta os resultados obtidos.

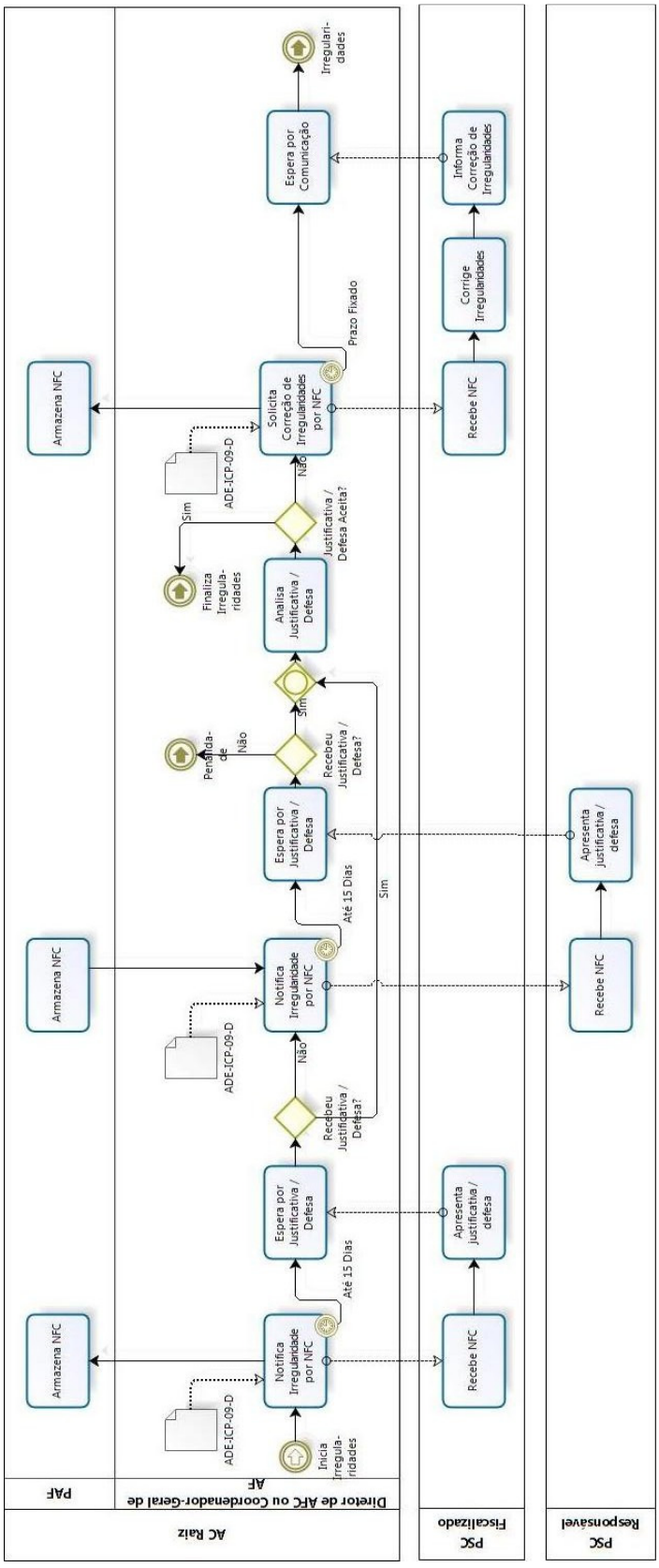

Ilustração 32 – Verificação de irregularidades.

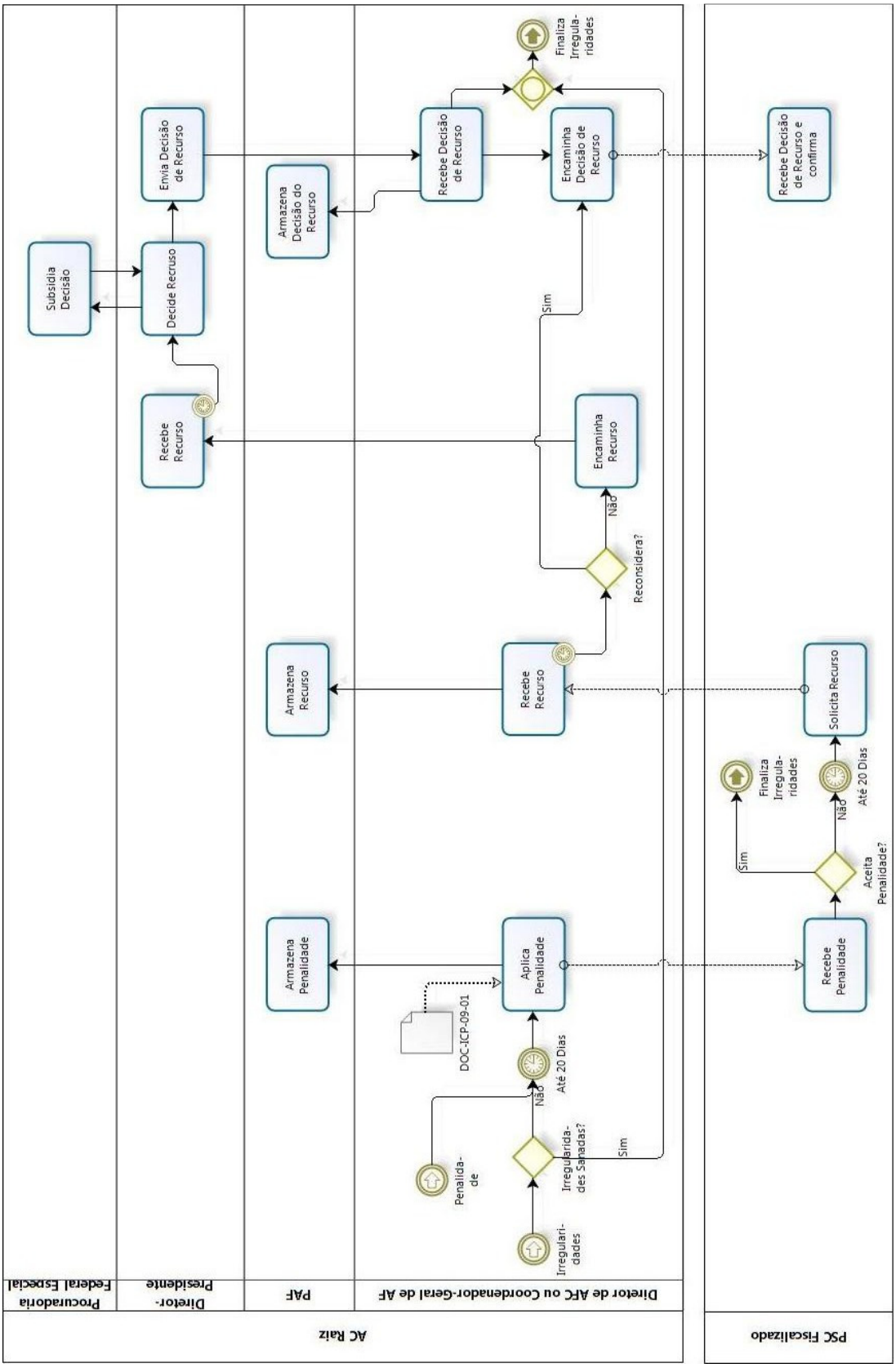

Ilustração 33 – Verificação de irregularidades – continuação.

5 APRESENTAÇÃO DO MODELO DE AUTOMAÇÃO PROPOSTO

Na apresentação dos dados, é possível perceber que há muitos pontos de comunicação entre entidades envolvidas nos processos de realização de auditoria e de fiscalização. Em vários pontos são gerados relatórios, termos, notificações, entre outras documentações. Em vários pontos é preciso que alguma entidade forneça documentação a outra.

Todos estes pontos foram mapeados e foi realizada a proposta de um modelo que automatize os processos que já foram apresentados, aumentando a eficiência do sistema, de modo que ele controle o fluxo de informações e comunicações entre as entidades. Nesse sistema também é utilizado o documento eletrônico seguro, de modo que os vários pontos onde documentação é gerada sejam substituídos por documentos eletrônicos seguros.

O sistema ainda controlará o nível de acesso de usuários, de modo que eles possam ter acesso apenas às atividades e informações que sejam de seu interesse. Para acessar o sistema, casa usuário dele o acessará através de identificação por certificação digital, o que permitirá identificar qual usuário específico que estará realizando uma determinada ação no sistema. Seu certificado também servirá para assinar qualquer documento eletrônico que ele produza no sistema, assim será possível relacioná-lo ao documento produzido. Toda ação no sistema que produza um documento eletrônico será ainda protocolada por Autoridades e/ou Sistemas de Carimbos de Tempo internos ao sistema.

O sistema gerará *log* e armazenará informações de toda atividade e evento ocorrido e quem esteve envolvido, bem como armazenará toda documentação eletrônica produzida em todo processo, identificando-as com os processos e com quem esteve envolvido em sua criação e quando aconteceu. Isso permitirá maior controle da AC Raiz sobre os processos de realização de auditorias e fiscalização nas entidades da ICP-Brasil.

Cada processo de auditoria e fiscalização no sistema será identificado e separado, para que as entidades possam executar suas tarefas nele de forma linear e correta.

5.1 PROCESSOS AUTOMATIZADOS PARA REALIZAÇÃO DE AUDITORIAS

Os processos de auditoria para melhor entendimento de como eles serão realizados de forma automatizada no sistema proposto, foram divididos entre as auditorias:

- Pré-operacionais de AC (e seus PSS) e ACT;
- Pré-operacionais de AR e PSS de AR;
- Operacionais de AC (e seus PSS) e ACT;
- Operacionais de AR e PSS de AR.

Cada um dos processos será apresentado em um tópico separado.

5.1.1 Auditoria Pré-Operacional de AC e ACT

Para solicitar a pré-auditoria, a AC ou ACT candidata acessa o sistema com um certificado digital previamente cadastrado nele. Ao acessar o sistema, a entidade preenche no próprio sistema o formulário de requerimento de auditoria e o salva. O sistema assinará o formulário com o certificado da entidade e o protocolará, armazenando as informações geradas e dando início a um processo de pré-auditoria em AC ou ACT, dependendo da entidade que estiver se candidatando.

O sistema então emite um aviso de requerimento de auditoria à AC Raiz, tanto por e-mail assinado pelo sistema quanto um status no próprio sistema que avise à AC Raiz quando ela o acessar. Enquanto a AC Raiz recebe o aviso e tem 15 dias para iniciar a auditoria, a entidade candidata realiza o *upload* no sistema de documentos digitalizados de seus processos, procedimentos, atividades, controles, PC, DPC e PSS, os quais serão assinados e protocolados pelo sistema e relacionados ao processo.

A AC Raiz acessa a documentação no sistema para iniciar a auditoria e caso ela não seja suficiente solicita documentação auxiliar ao sistema, que repassará a solicitação à entidade candidata. A entidade realiza o *upload* da documentação solicita no sistema, que a assina e protocola, e então o sistema avisa a AC Raiz que a documentação está disponível. A AC Raiz acessa o sistema e verifica a documentação.

Essas atividades são mostradas na ilustração 34.

Após finalizar a auditoria, a AC Raiz elaborará o relatório no próprio sistema,

que o assinará e protocolará e o relacionará ao processo. O sistema envia por e-mail o relatório à entidade candidata. Se a AC Raiz verificar irregularidade na auditoria, ela preenche a existência de irregularidades no sistema determinando um tempo para correção, que será assinado e protocolado, e o sistema avisa por e-mail à entidade candidata, que acessa o sistema e confirma o recebimento. A confirmação será assinada e protocolada e enviada à AC Raiz.

A entidade realiza as correções e quando estiverem corrigidas preenche o aviso de correção no sistema, que o assinará e protocolará e enviará o aviso à AC Raiz. A AC Raiz, quando receber o aviso irá verificar se já foi realizada auditoria complementar. Caso não tenha sido, ela realiza a auditoria complementar, senão elabora o relatório final de auditoria no sistema, que o assina e protocola e envia à entidade candidata. Em até 30 dias a AC Raiz elabora o parecer sobre o relatório de auditoria.

Essas atividades são mostradas na ilustração 35.

Caso a AC Raiz defira o credenciamento, se houver planos de fiscalização ela os preenche no sistema e o sistema avisa por e-mail a área de fiscalização da AC Raiz. A AC Raiz preenche então o deferimento no próprio sistema, que avisa a entidade candidata que ela passou na auditoria, e publica o deferimento de credenciamento no DOU.

Caso a AC Raiz indefira o credenciamento, ela preenche o indeferimento no sistema, que avisa a entidade candidata. A entidade candidata verifica se aceita ou não o indeferimento e caso aceite o processo finaliza. Caso não aceite, ela preenche uma solicitação de recurso no sistema, que o enviará ao Comitê Gestor e este preencherá a decisão do recurso no sistema e publica a decisão no DOU. O sistema avisará à entidade candidata da decisão do recurso e o processo finaliza.

Essas atividades são mostradas na ilustração 36.

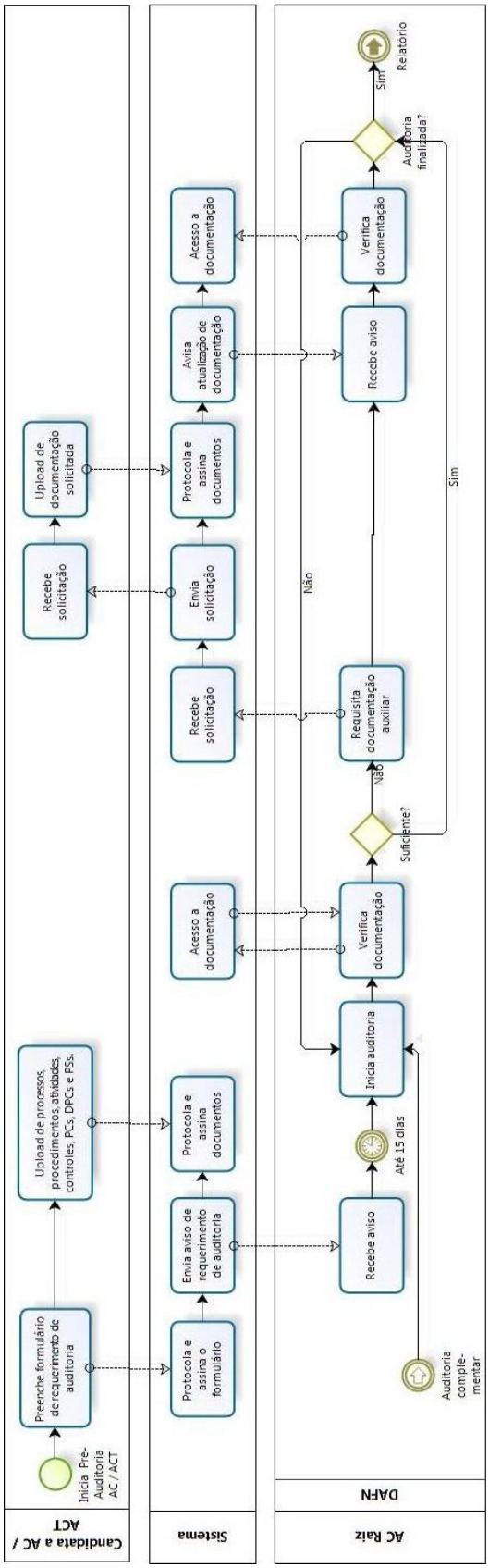

Ilustração 34 – Auditoria pré-operacional de AC e ACT.

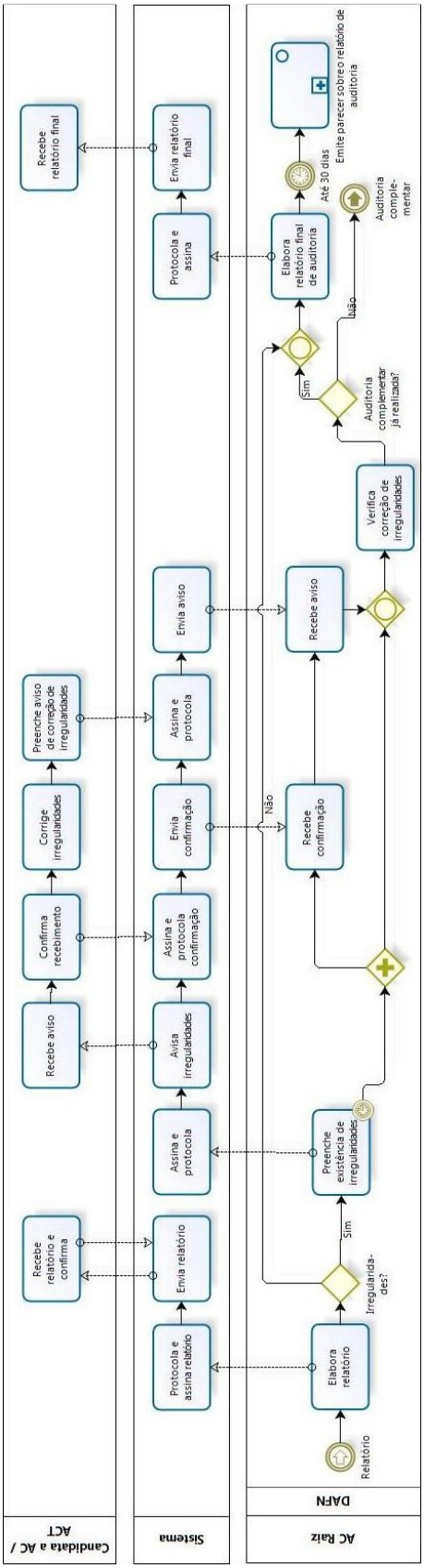

Ilustração 35 – Auditoria pré-operacional de AC e ACT – continuação.

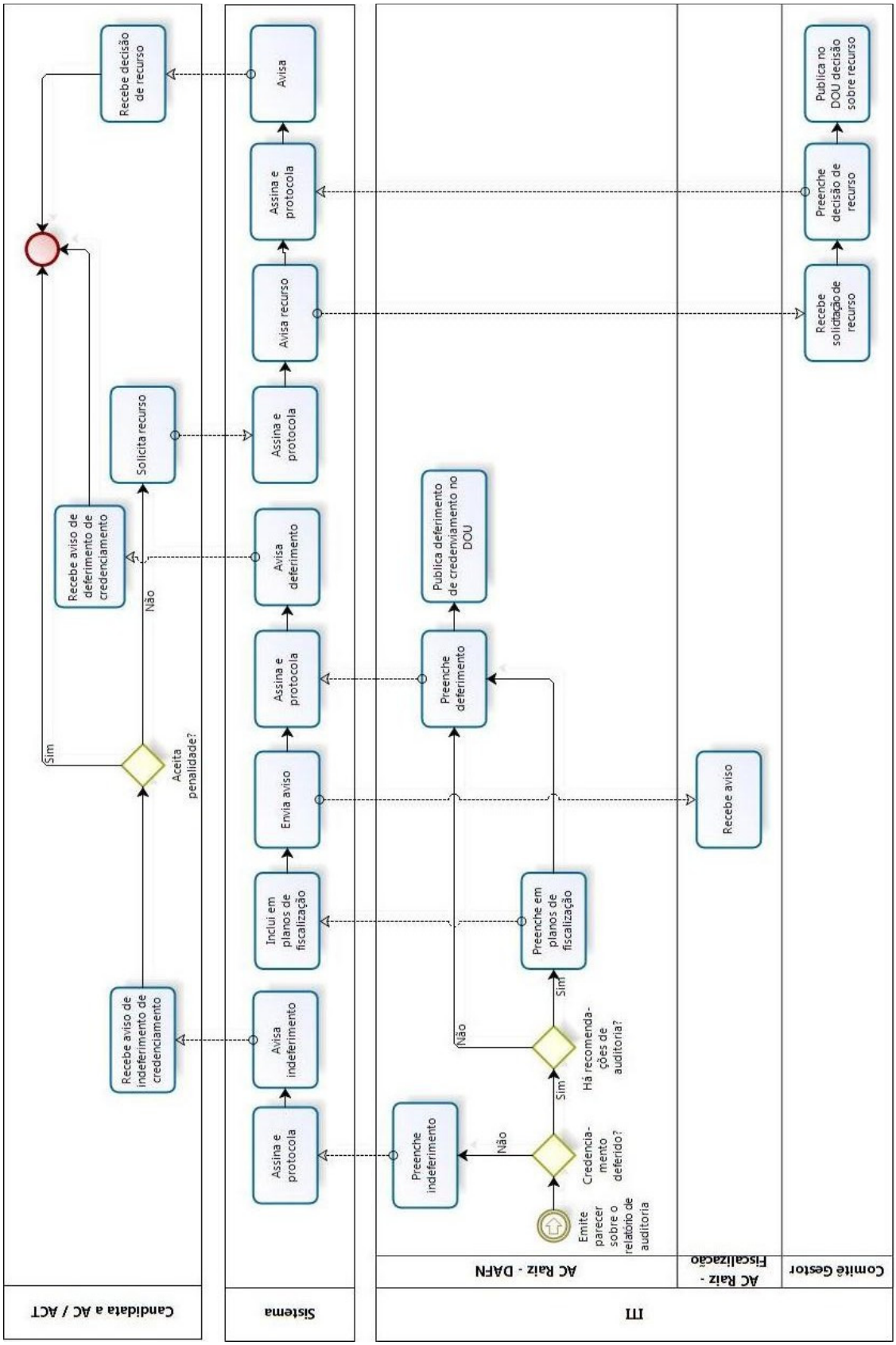

Ilustração 36 – Parecer sobre o relatório de auditoria.

5.1.2 Auditoria Pré-Operacional de AR e PSS de AR

O processo de pré-auditoria de AR e PSS de AR inicia com a entidade auditoria acessando o sistema e preenchendo o formulário de início de auditoria. O sistema assinará e protocolará o formulário e informará a entidade candidata e a entidade responsável do início do processo.

A entidade candidata realizará o *upload* dos processos, procedimentos, atividades, controles, PC, DPC e PS. A entidade responsável realizará o *upload* dos documentos de credenciamento. Todos os documentos devem estar digitalizados e são assinados e protocolados e relacionados ao processo.

A entidade auditora então acessa o sistema e inicia a auditoria, acessando a documentação. Caso ela não seja suficiente, ela solicita documentação auxiliar ao sistema, que avisa a entidade candidata para que ela realize o *upload* da documentação adicional. O sistema protocola e assina e avisa à entidade auditora, que acessa o sistema e verifica a documentação adicional.

Ao finalizar a auditoria, a entidade auditoria preenche o relatório no sistema, que será assinado e protocolado, e é enviado por e-mail assinado pelo sistema à entidade candidata e à entidade responsável.

Esses processos estão mapeados na ilustração 37.

Após elaborar o relatório, a entidade de auditoria verifica se foram identificadas irregularidades. Se não tiver sido, será elaborado o relatório final no sistema, caso contrário será preenchido no sistema o formulário de existência de irregularidades com tempo determinado para serem corrigidas, assinado e protocolado e enviado à entidade candidata e à entidade responsável.

A entidade candidata deve acessar o sistema e confirmar o recebimento do formulário. O sistema assina e protocola e avisa a entidade de auditoria e a entidade responsável. A entidade candidata corrige as irregularidades e preenche no sistema o formulário de correção de irregularidades. O sistema assina e protocola e avisa a entidade de auditoria e a entidade responsável.

A entidade de auditoria verifica se as correções forma feitas e caso tenham sido ele realiza nova auditoria. Caso não tenham sido ele elabora o relatório final de auditoria no sistema. O relatório final é assinado e protocolado enviado à entidade candidata, à entidade responsável e à AC Raiz. A entidade de auditoria então realiza no sistema o *upload* do material utilizado na auditoria.

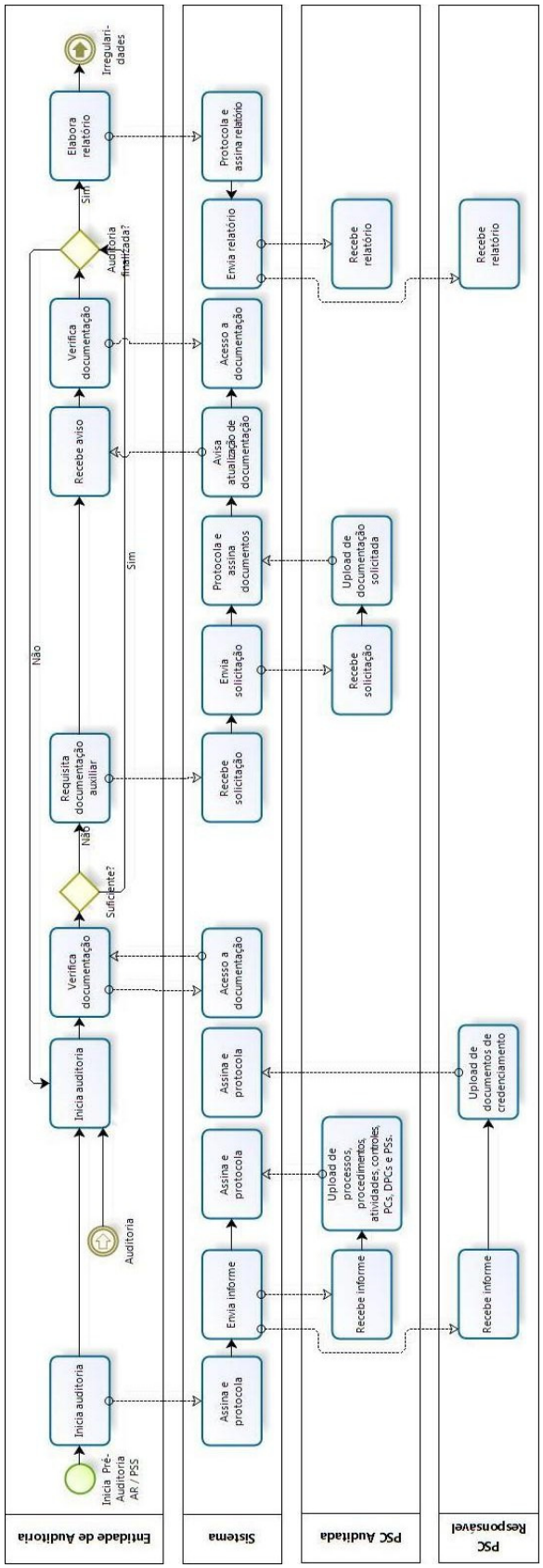

Ilustração 37 – Auditoria pré-operacional de AR e PSS de AR.

Quando a AC Raiz recebe o relatório final, ela acessa e verifica no sistema a documentação do processo relacionado àquele relatório e tem 30 dias para ou realizar sua própria auditoria, substituindo a já feita, ou emitir parecer sobre o relatório de auditoria.

Esses processos são visualizados na ilustração 38.

Se a AC Raiz decide realizar a pré-auditoria, ela acessa a documentação e o material utilizado na pré-auditoria anterior no sistema para iniciar a auditoria e caso ela não seja suficiente solicita documentação auxiliar ao sistema, que repassará a solicitação à entidade candidata. A entidade realiza o *upload* da documentação solicita no sistema, que a assina e protocola, e então o sistema avisa a AC Raiz que a documentação está disponível. A AC Raiz acessa o sistema e verifica a documentação.

Essas atividades são mostradas na ilustração 39.

Após finalizar a auditoria, a AC Raiz elaborará o relatório no próprio sistema, que o assinará e protocolará e o relacionará ao processo. O sistema envia por e-mail o relatório à entidade candidata. Se a AC Raiz verificar irregularidade na auditoria, ela preenche a existência de irregularidades no sistema determinando um tempo para correção, que será assinado e protocolado, e o sistema avisa por e-mail à entidade candidata, que acessa o sistema e confirma o recebimento. A confirmação será assinada e protocolada e enviada à AC Raiz.

A entidade realiza as correções e quando estiverem corrigidas preenche o aviso de correção no sistema, que o assinará e protocolará e enviará o aviso à AC Raiz. A AC Raiz, quando receber o aviso irá verificar se já foi realizada auditoria complementar. Caso não tenha sido, ela realiza a auditoria complementar, senão elabora o relatório final de auditoria no sistema, que o assina e protocola e envia à entidade candidata. Em até 30 dias a AC Raiz elabora o parecer sobre o relatório de auditoria.

Essas atividades são mostradas na ilustração 40.

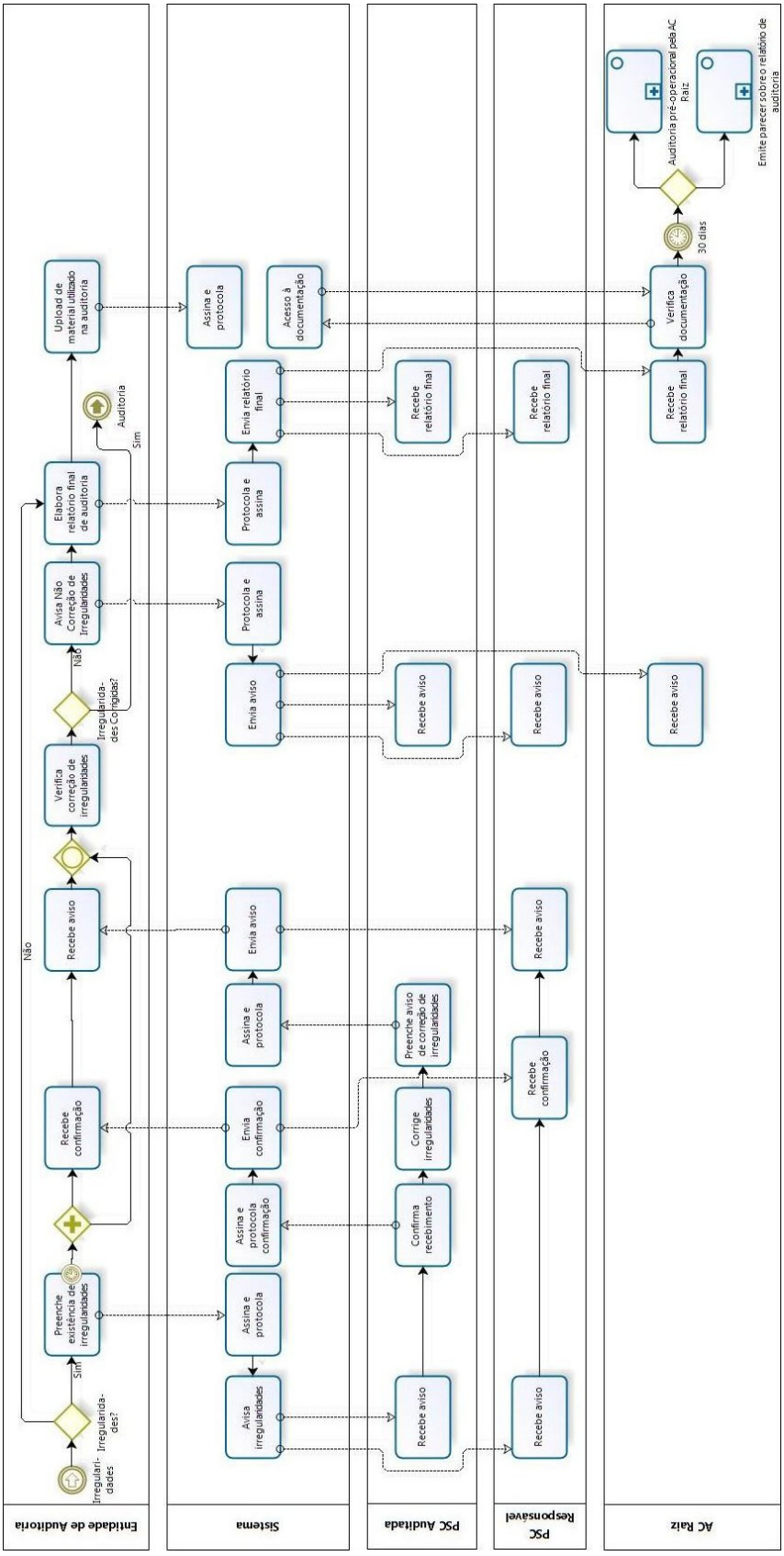

Ilustração 38 – Auditoria pré-operacional de AR e PSS de AR - continuação.

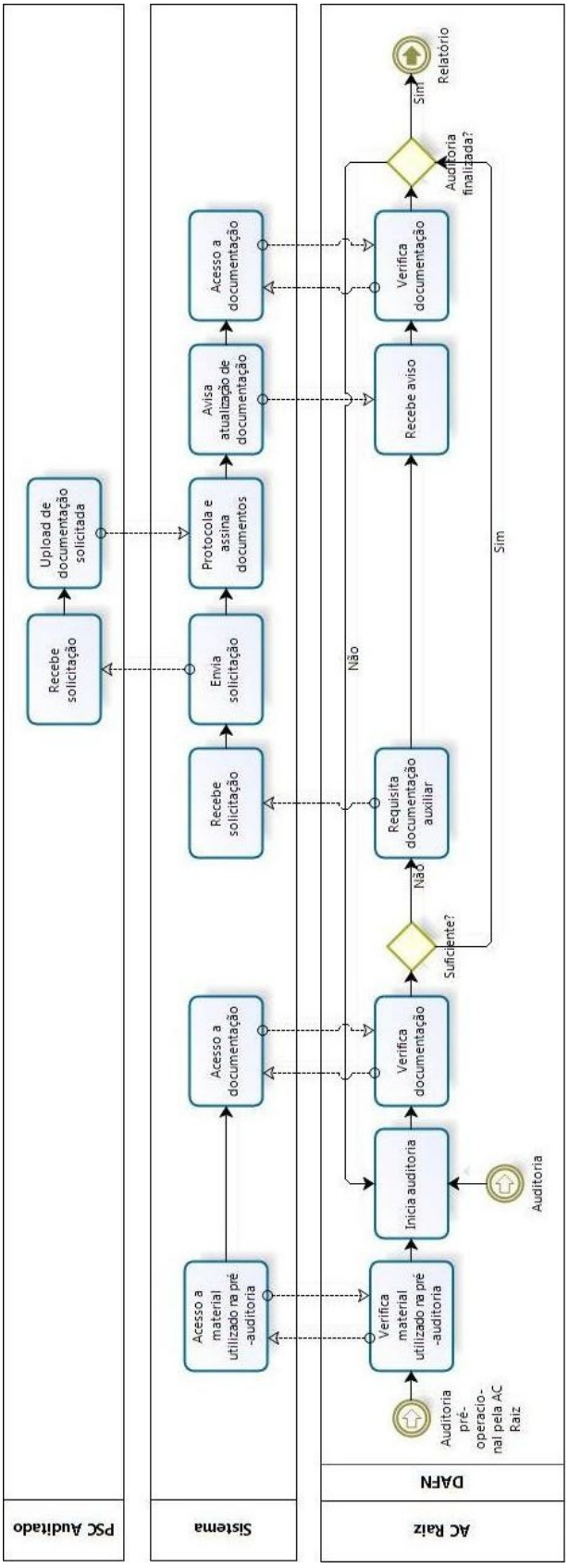

Ilustração 39 – Verificação de auditoria pré-operacional pela AC Raiz.

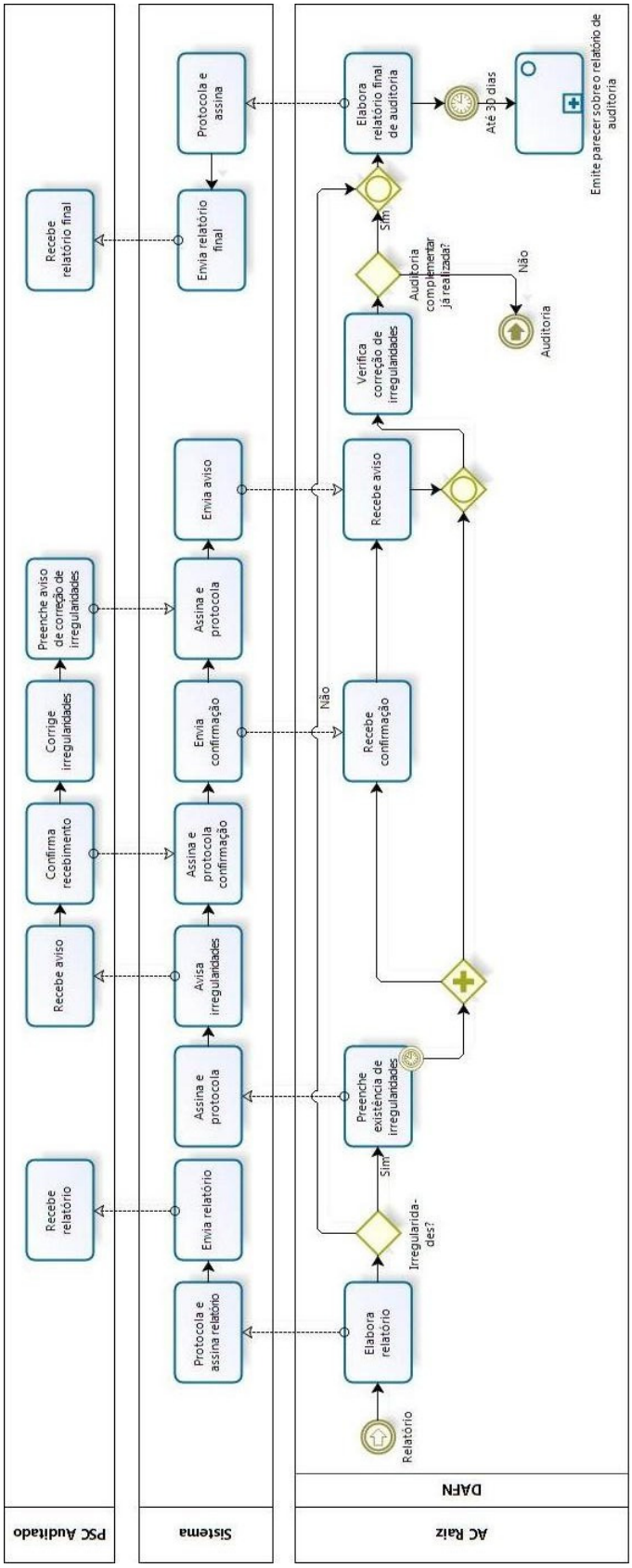

Ilustração 40 – Verificação de auditoria pré-operacional pela AC Raiz - continuação.

Caso a AC Raiz defira o credenciamento, se houver planos de fiscalização ela os preenche no sistema e o sistema avisa por e-mail a área de fiscalização da AC Raiz. A AC Raiz preenche então o deferimento no próprio sistema, que avisa a entidade candidata que ela passou na auditoria, e publica o deferimento de credenciamento no DOU.

Caso a AC Raiz indefira o credenciamento, ela preenche o indeferimento no sistema, que avisa a entidade candidata e a entidade responsável. A entidade candidata verifica se aceita ou não o indeferimento e caso aceite o processo finaliza. Caso não aceite, ela preenche uma solicitação de recurso no sistema, que o enviará ao Comitê Gestor e este preencherá a decisão do recurso no sistema e publica a decisão no DOU. O sistema avisará à entidade candidata da decisão do recurso e o processo finaliza.

Essas atividades são mostradas na ilustração 41.

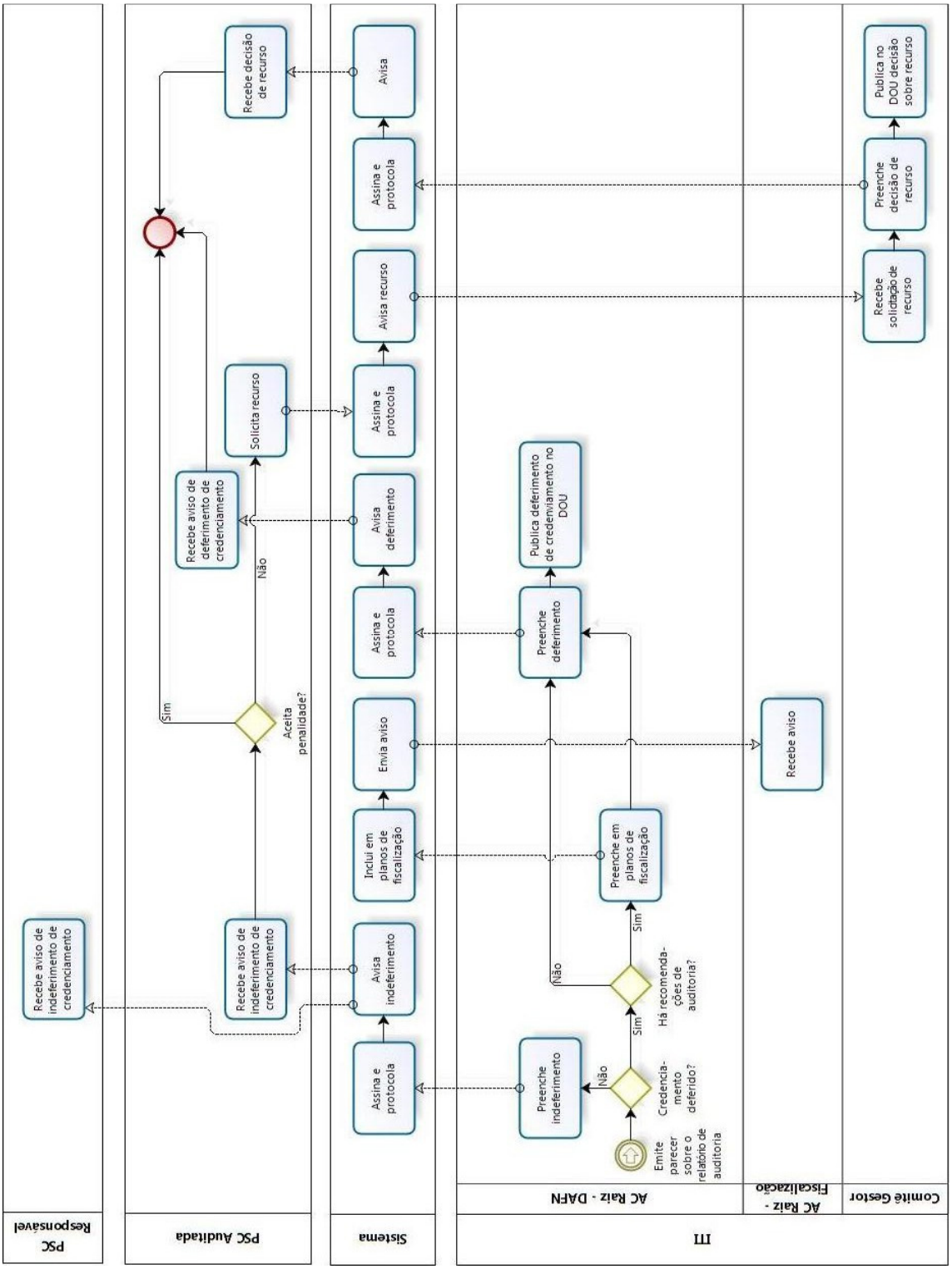

Ilustração 41 – Parecer sobre o relatório de auditoria.

5.1.3 Auditoria Operacional de AC e ACT

Até o dia 15 de março de cada ano, a AC ou ACT acessa o sistema e preenche o cronograma de auditorias de todas as entidades sob sua responsabilidade. O sistema assina e protocola o cronograma e o envia à AC Raiz. Quando estiver na data de uma auditoria ser realizada, conforme o cronograma, o sistema avisa à AC ou ACT e à AC Raiz.

A entidade realiza o *upload* no sistema dos processos, procedimentos, atividades, controle, PC, DPC e PS, os quais serão assinados e protocolados. A AC Raiz inicia a auditoria e acessa o sistema para verificar a documentação. Se for necessária documentação adicional, a AC Raiz a solicita pelo sistema, que envia a solicitação à entidade para que ela realize o *upload* no sistema, o qual assinará e protocolará a documentação adicional. O sistema avisará a AC Raiz que a documentação adicional está disponível para que ela o acesse e verifique.

Essas atividades são demonstradas na ilustração 42.

Após finalizar a auditoria, a AC Raiz elaborará o relatório no próprio sistema, que o assinará e protocolará e o relacionará ao processo. O sistema envia por e-mail o relatório à entidade auditada. Se a AC Raiz verificar irregularidade na auditoria, ela preenche a existência de irregularidades no sistema determinando um tempo para correção, que será assinado e protocolado, e o sistema avisa por e-mail à entidade auditada, que acessa o sistema e confirma o recebimento. A confirmação será assinada e protocolada e enviada à AC Raiz.

A entidade auditada realiza as correções e quando estiverem corrigidas preenche o aviso de correção no sistema, que o assinará e protocolará e enviará o aviso à AC Raiz. A AC Raiz, quando receber o aviso irá verificar se as correções foram realizadas. Caso tenham sido, ela realiza nova auditoria, senão ela preenche no sistema o aviso de não correção de irregularidades, que será assinado e protocolado e o sistema avisa à entidade candidata. A AC Raiz então elabora o relatório final de auditoria no sistema, que o assina e protocola e envia à entidade auditada. Em até 30 dias a AC Raiz elabora o parecer sobre o relatório de auditoria.

Essas atividades são mostradas na ilustração 43.

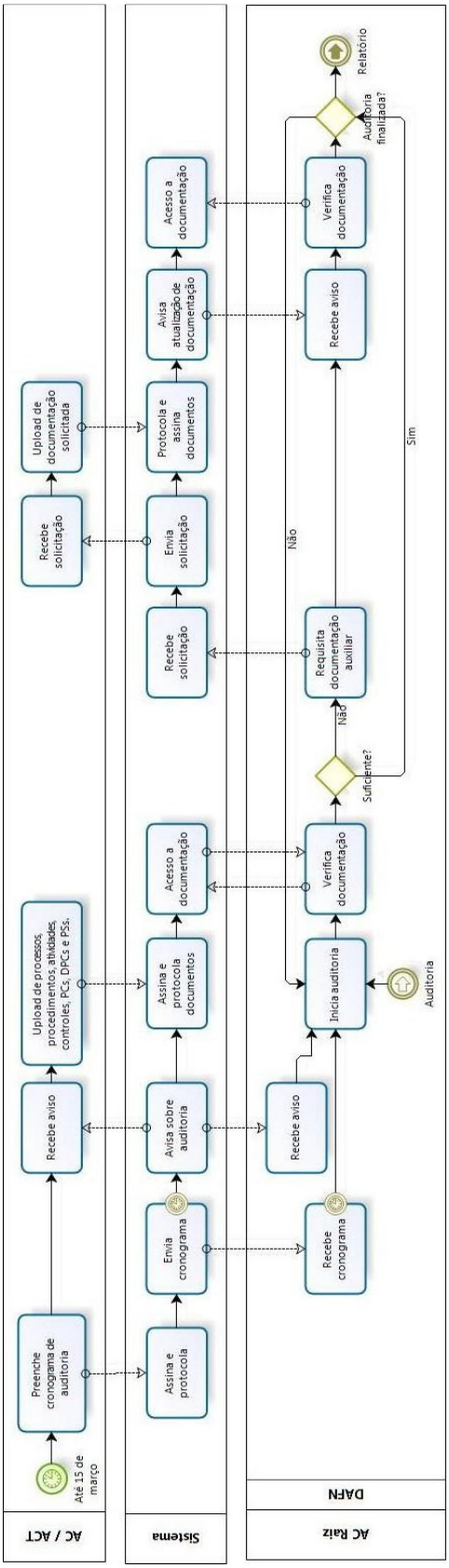

Ilustração 42 – Auditoria operacional de AC e ACT.

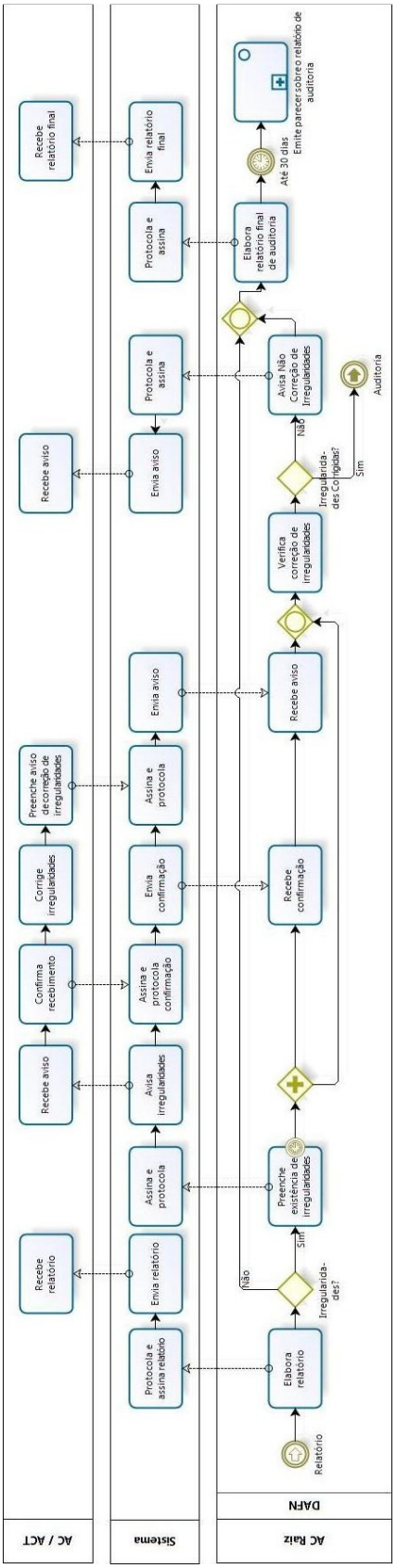

Ilustração 43 – Auditoria operacional de AC e ACT - continuação.

Para emitir o parecer sobre o relatório de auditoria a AC Raiz verifica se há recomendações de auditoria e, caso existam, ela preenche no sistema as recomendações em planos de fiscalizações, e o sistema avisa à área de fiscalização da AC Raiz.

Depois a AC Raiz verifica o conceito que foi dado no relatório de auditoria. Se o conceito for 1 ou 2, o processo finaliza. Se for 3 ou 4, aplica uma penalidade à entidade auditada. Se for 5 e não tiver sido consecutivo, suspende as operações da entidade auditada. Se tiver sido conceito 5 consecutivo, a entidade é descadastrada. Para aplicar penalidade, suspender operações ou descadastrar a entidade, a AC Raiz protocola e assina a sua decisão do processo no sistema.

Ao final da decisão, a AC Raiz elabora um ofício no sistema, que é protocolado e assinado e enviado à entidade auditada, a qual terá um prazo de 10 dias para apresentar defesa. A entidade assina e protocola a defesa no sistema, e o sistema a envia à AC Raiz. Se a AC Raiz aceitar a defesa, ela arquiva o processo e o finaliza, assinando e protocolando no sistema a decisão tomada. Caso contrário, ela aplicará a penalidade à entidade auditada.

Esse processo pode ser visto na ilustração 44.

A AC Raiz assina e protocola uma notificação de penalidade no sistema, que o enviará à entidade auditada que decidirá se aceita ou não a penalidade. Se ela aceitar, a AC Raiz publica a decisão de penalidade no DOU e o processo é finalizado, senão ela assina e protocola um pedido de recurso no sistema. O pedido de recurso é enviado à AC Raiz, para conhecimento, e ao diretor presidente do ITI.

O diretor presidente decide o recurso e assina e protocola no sistema. Caso julgue necessário, pode pedir subsídio à sua decisão no sistema, que avisará Procuradoria Federal Especializada e esta acessará o sistema para subsidiar a decisão, assinando e protocolando seu ato. Se o diretor presidente aplicou penalidade, ele a publica no DOU e finaliza o processo.

O sistema envia a decisão à entidade auditada e, se tiver sido aplicada penalidade, pode aceitá-la ou não. Se aceitá-la, o processo é finalizado, senão ela solicita recurso pelo sistema. O sistema assina e protocola o recurso e o envia ao Comitê Gestor, que assina e protocola sua decisão no sistema e a publica no DOU. O sistema envia a decisão do recuso à entidade auditada e o processo finaliza.

Essas atividades são visualizadas na ilustração 45.

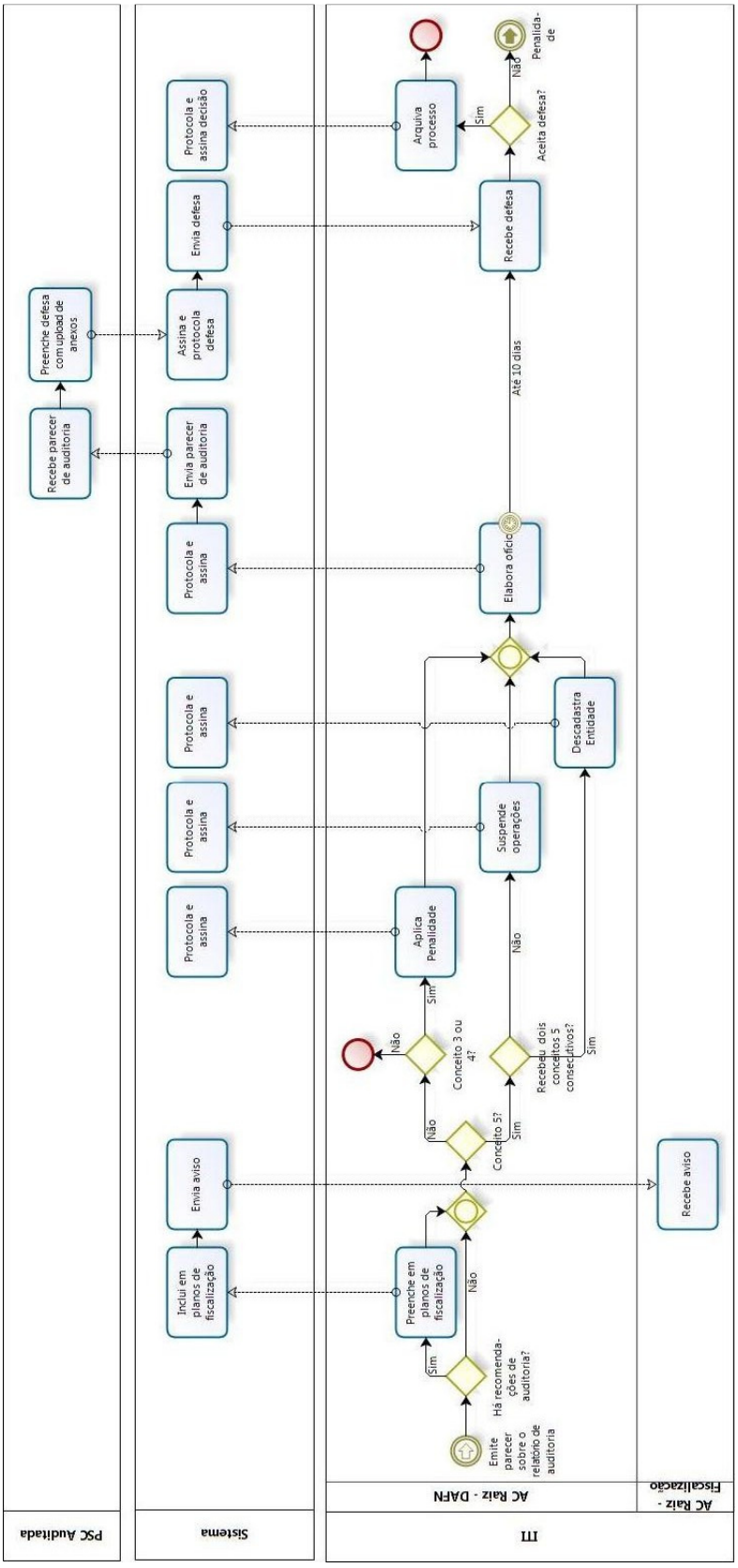

Ilustração 44 – Parecer sobre o relatório de auditoria.

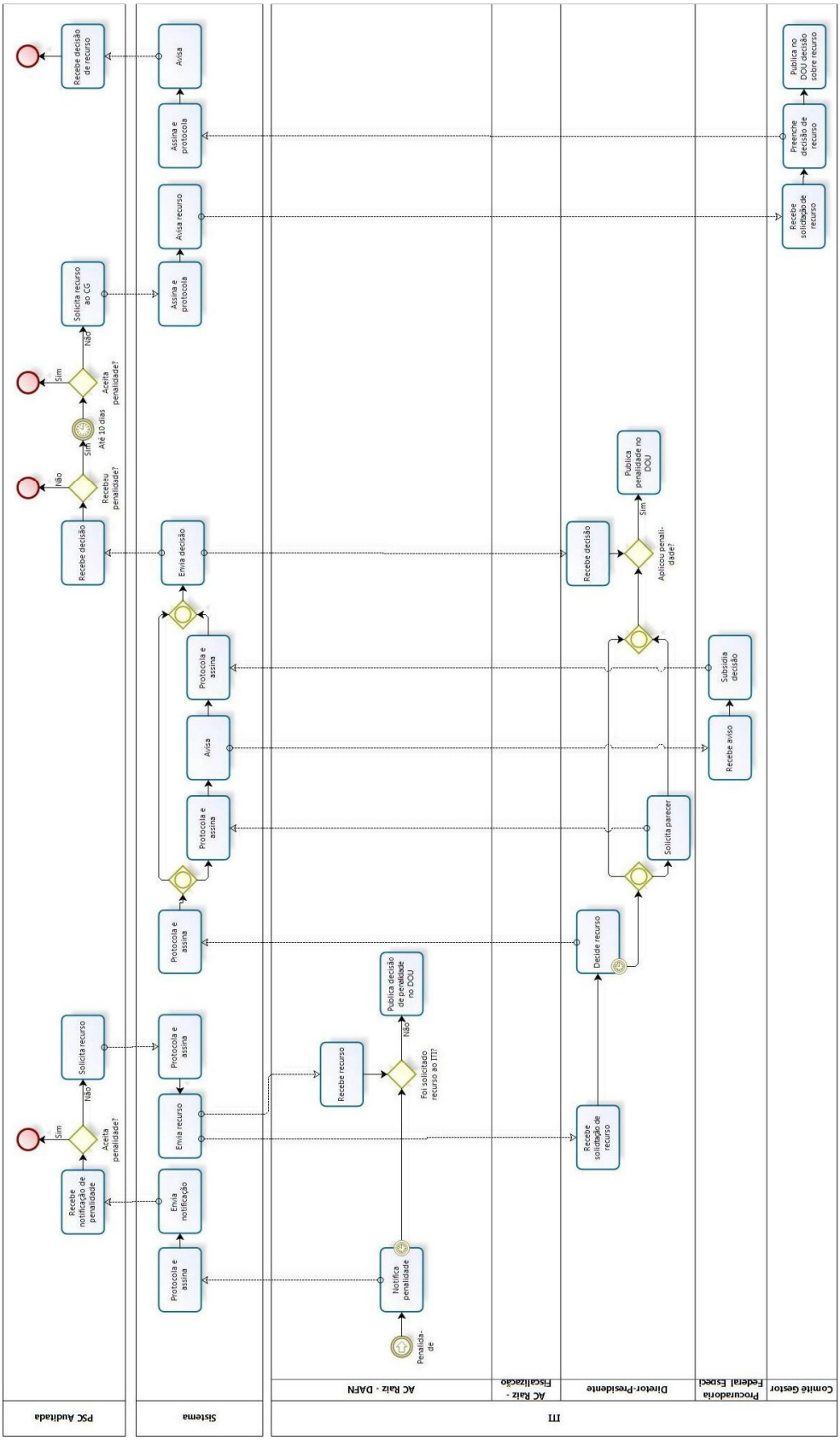

Ilustração 45 – Parecer sobre o relatório de auditoria - continuação.

5.1.4 Auditoria Operacional de AR, ACs subsequentes e PSS de AR

O PSC responsável preenche o PLAAO no sistema até o dia 15 de dezembro para o ano civil seguinte. O PLAAO é assinado e protocolado no sistema e enviado à AC Raiz. Até o dia 15 de março de cada ano, o PSC responsável acessa o sistema e preenche o cronograma de auditorias de todas as entidades sob sua responsabilidade. O sistema assina e protocola o cronograma e o envia à AC Raiz. Quando estiver na data de uma auditoria ser realizada, conforme o cronograma, o sistema avisa ao PSC responsável, à AC Raiz e ao PSC que será auditado.

A entidade a ser auditada realiza o *upload* no sistema dos processos, procedimentos, atividades, controle, PC, DPC e PS, os quais serão assinados e protocolados. O PSC responsável contrata uma entidade auditoria independente e cadastrada no ITI e ela inicia um processo de auditoria, acessando o sistema para verificar a documentação. Se for necessária documentação adicional, a entidade auditora a solicita pelo sistema, que envia a solicitação à entidade auditada para que ela realize o *upload* no sistema, o qual assinará e protocolará a documentação adicional. O sistema avisará a entidade auditora que a documentação adicional está disponível para que ela o acesse e verifique.

Essas atividades são demonstradas na ilustração 46.

Após finalizar a auditoria, a entidade auditora elaborará o relatório no próprio sistema, que o assinará e protocolará e o relacionará ao processo. O sistema envia por e-mail o relatório à entidade auditada e à entidade responsável. Se a entidade auditora verificar irregularidade na auditoria, ela preenche a existência de irregularidades no sistema determinando um tempo para correção, que será assinado e protocolado, e o sistema avisa por e-mail à entidade auditada e à entidade responsável. A entidade auditada acessa o sistema e confirma o recebimento. A confirmação será assinada e protocolada e enviada à entidade auditora e à entidade responsável.

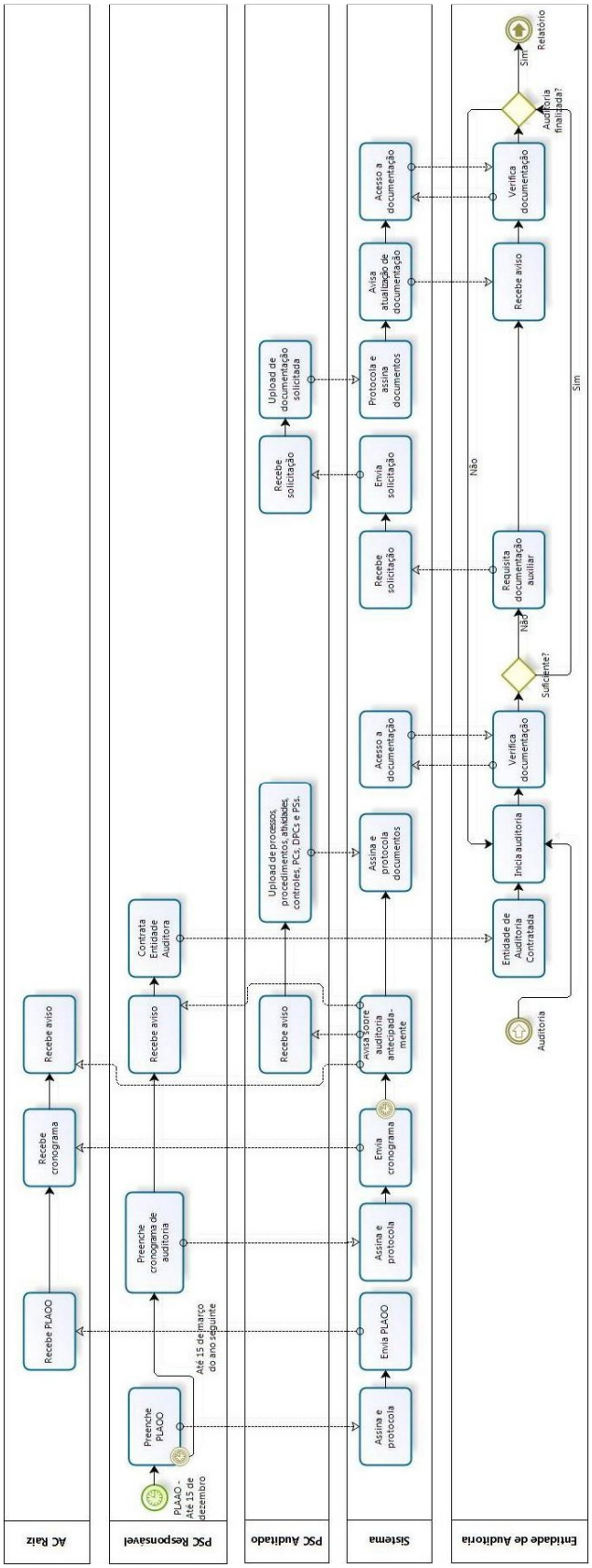

Ilustração 46 – Auditoria operacional de AR e PSS de AR.

A entidade auditada realiza as correções e quando estiverem corrigidas preenche o aviso de correção no sistema, que o assinará e protocolará e enviará o aviso à entidade auditora, à entidade responsável e à AC Raiz. A entidade auditora, quando receber o aviso, irá verificar se as correções foram realizadas. Caso tenham sido, ela realiza nova auditoria, senão ela preenche no sistema o aviso de não correção de irregularidades, que será assinado e protocolado e o sistema avisa à entidade auditada e à entidade responsável. A entidade auditora então elabora o relatório final de auditoria no sistema, que o assina e protocola e envia à entidade auditada, à entidade responsável e à AC Raiz. A AC Raiz recebe o relatório final, verifica a documentação da auditoria no sistema e, em até 30 dias analisa o relatório final e/ou emite o parecer sobre o relatório de auditoria.

Essas atividades são mostradas na ilustração 47.

A análise do relatório final de auditoria serve para a AC Raiz controlar a qualidade da auditoria realizada pela entidade de auditoria independente.

A AC Raiz, para avaliar a documentação, pode solicitar esclarecimentos e documentos complementares no sistema à entidade de auditora. A solicitação será assinada e protocolada e enviada à entidade de auditoria, que assinara e protocolará no sistema sua resposta e o sistema a enviará à AC Raiz.

Para avaliar a documentação, a AC Raiz pode também solicitar esclarecimentos e documentos complementares no sistema à entidade auditada. A solicitação será assinada e protocolada e enviada à entidade auditada, que assinara e protocolará no sistema sua resposta e o sistema a enviará à AC Raiz.

Se nenhuma irregularidade for encontrada, o processo finaliza. Caso contrário, a AC Raiz assina e protocola no sistema a comunicação de irregularidades e este o envia à entidade auditora, que justifica as irregularidades no sistema, assinando e protocolando a justificativa, e o sistema envia à AC Raiz. Isso deve ser feito em um prazo estabelecido pela AC Raiz.

Se a AC Raiz aceitar as justificativas, o processo finaliza, senão ela aplica penalidade à entidade auditora.

Esse processo é mostrado na ilustração 48.

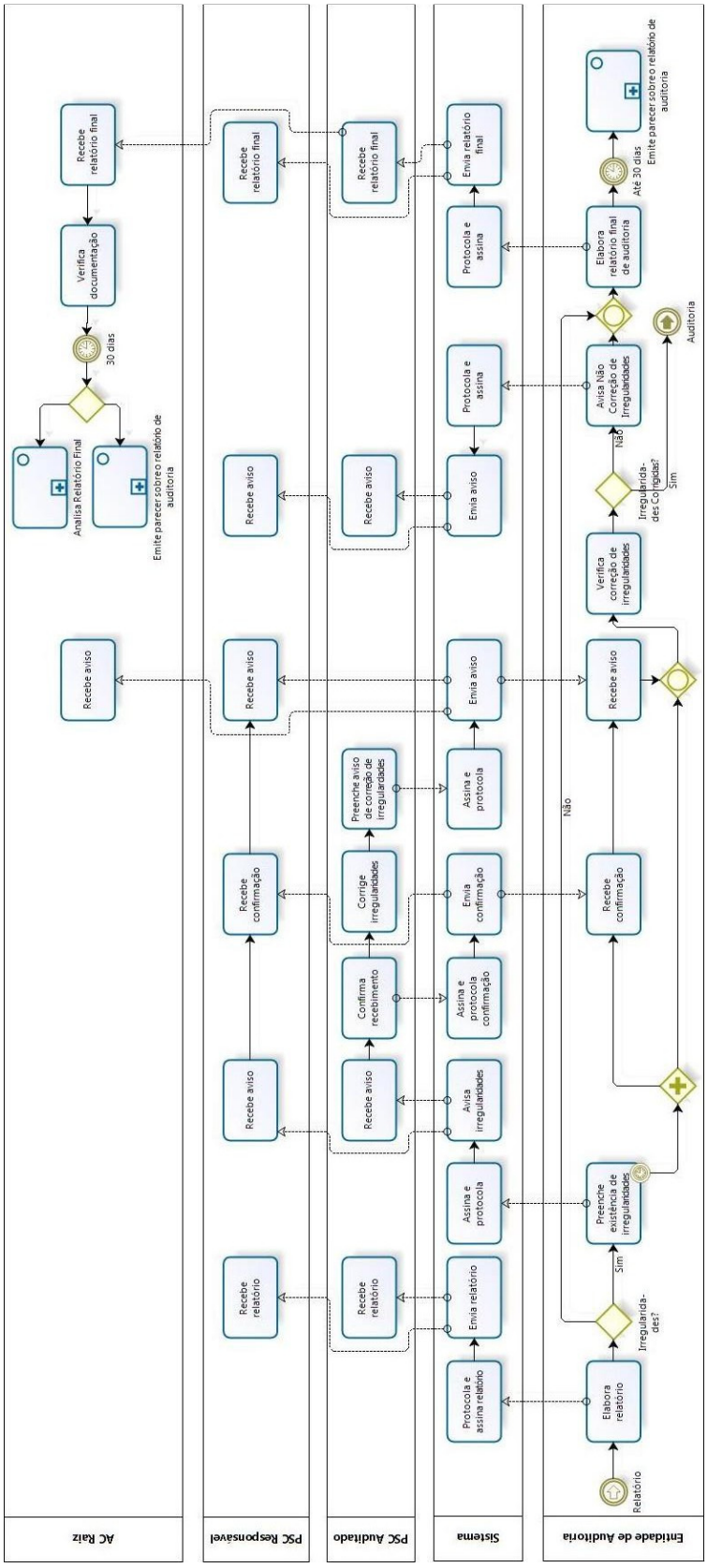

Ilustração 47 – Auditoria operacional de AR e PSS de AR – continuação.

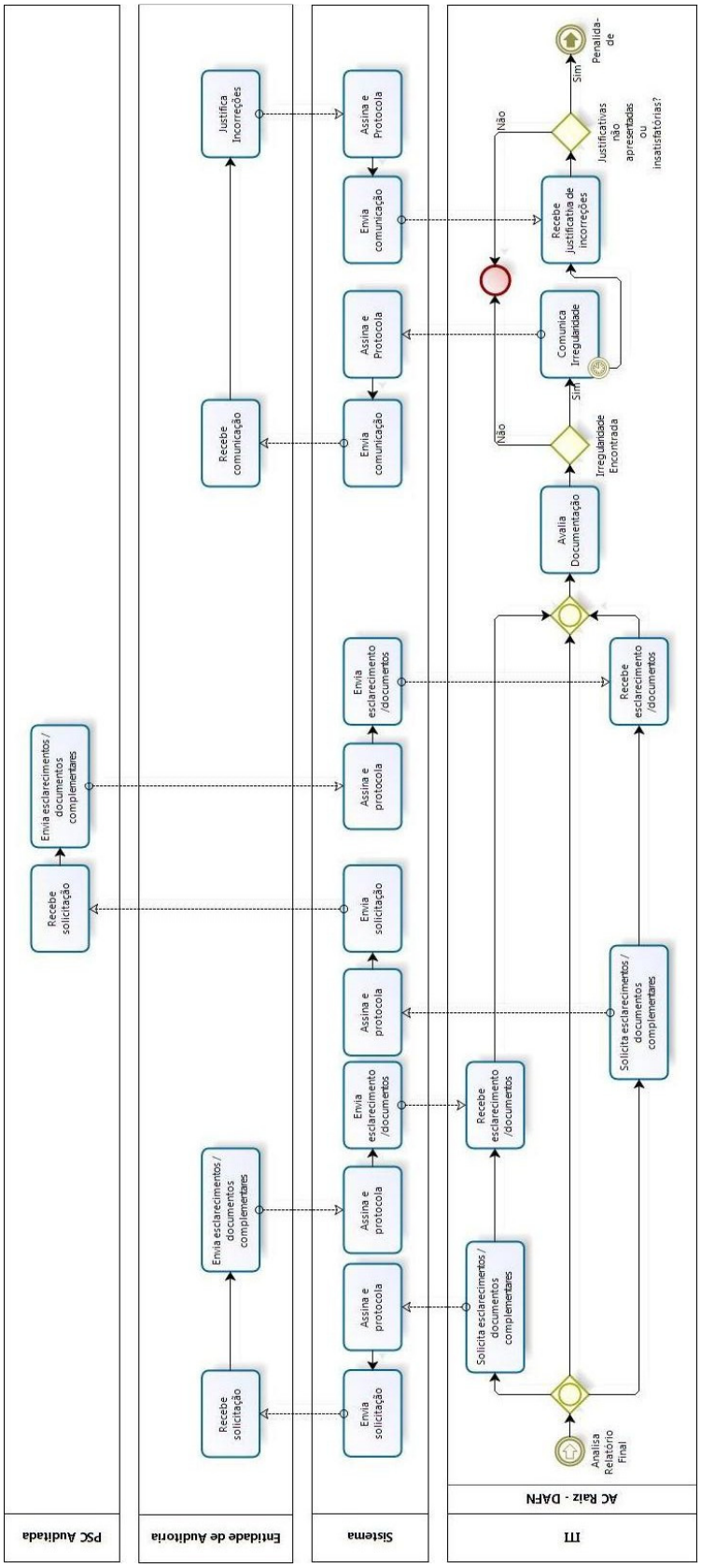

Ilustração 48 – Análise do relatório final.

A AC Raiz assina e protocola uma notificação de penalidade no sistema, que o enviará à entidade de auditoria, que decidirá se aceita ou não a penalidade. Se ela aceitar, a AC Raiz publica a decisão de penalidade no DOU e o processo é finalizado, senão ela assina e protocola um pedido de recurso no sistema. O pedido de recurso é enviado à AC Raiz, para conhecimento, e ao diretor presidente do ITI.

O diretor presidente decide o recurso e assina e protocola no sistema. Caso julgue necessário, pode pedir subsídio à sua decisão no sistema, que avisará a Procuradoria Federal Especializada e esta acessará o sistema para subsidiar a decisão, assinando e protocolando seu ato. Se o diretor presidente aplicou penalidade, ele a publica no DOU e finaliza o processo.

O sistema envia a decisão à entidade de auditoria e, se tiver sido aplicada penalidade, pode aceitá-la ou não. Se aceitá-la, o processo é finalizado, senão ela solicita recurso pelo sistema. O sistema assina e protocola o recurso e o envia ao Comitê Gestor, que assina e protocola sua decisão no sistema e a publica no DOU. O sistema envia a decisão do recuso à entidade de auditoria e o processo finaliza.

Essas atividades são visualizadas na ilustração 49.

Para emitir o parecer sobre o relatório de auditoria a AC Raiz verifica se há recomendações de auditoria e, caso existam, ela preenche no sistema as recomendações em planos de fiscalizações, e o sistema avisa à área de fiscalização da AC Raiz.

Depois a AC Raiz verifica o conceito que foi dado no relatório de auditoria. Se o conceito for 1 ou 2, o processo finaliza. Se for 3 ou 4, aplica uma penalidade à entidade auditada. Se for 5 e não tiver sido consecutivo, suspende as operações da entidade auditada. Se tiver sido conceito 5 consecutivo, a entidade é descadastrada. Para aplicar penalidade, suspender operações ou descadastrar a entidade, a AC Raiz protocola e assina a sua decisão do processo no sistema.

Ao final da decisão, a AC Raiz elabora um ofício no sistema, que é protocolado e assinado e enviado à entidade auditada, a qual terá um prazo de 10 dias para apresentar defesa. A entidade assina e protocola a defesa no sistema, e o sistema a envia à AC Raiz. Se a AC Raiz aceitar a defesa, ela arquiva o processo e o finaliza, assinando e protocolando no sistema a decisão tomada. Caso contrário, ela aplicará a penalidade à entidade auditada.

Esse processo pode ser visto na ilustração 50.

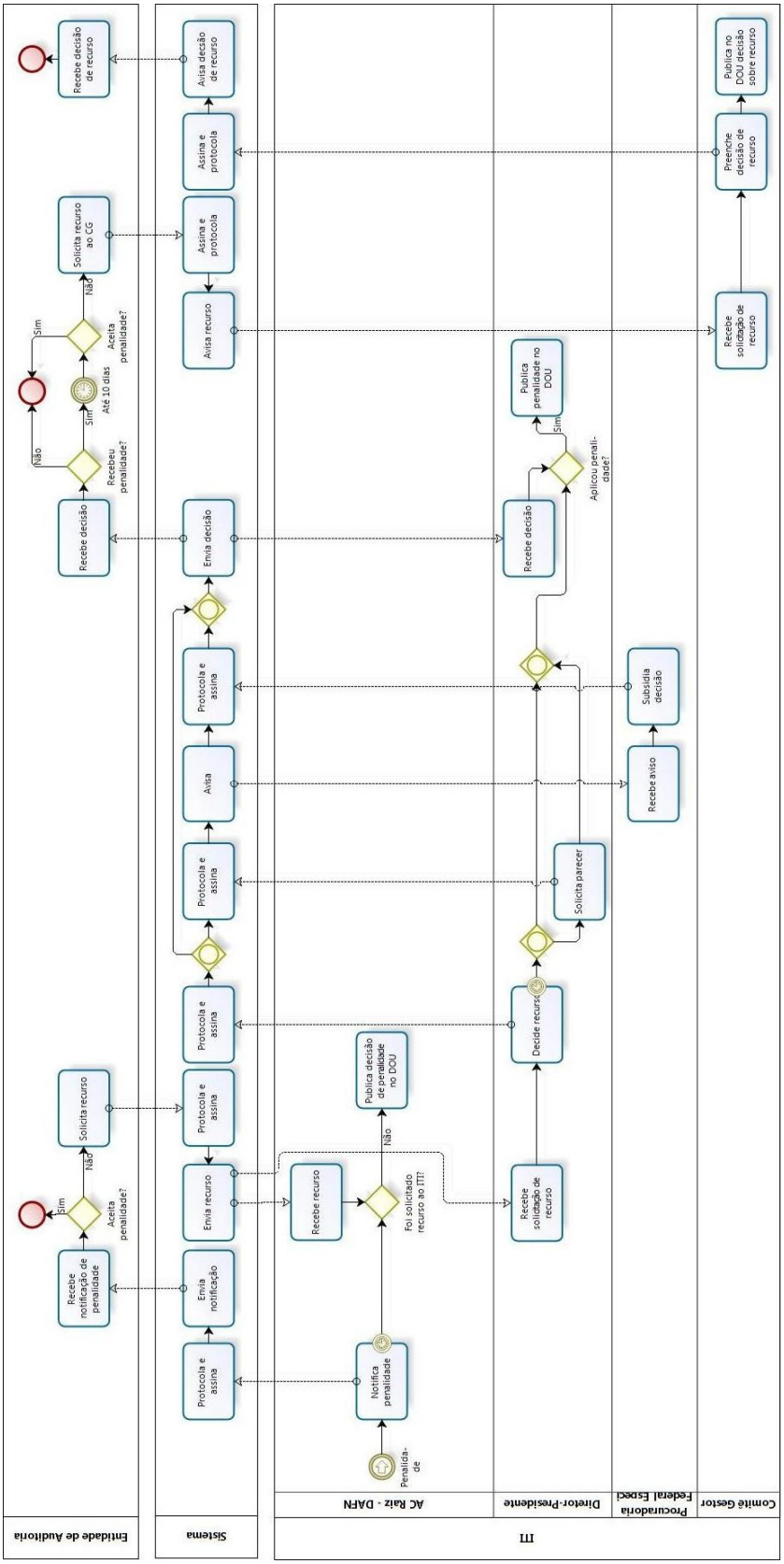

Ilustração 49 – Análise do relatório final - continuação.

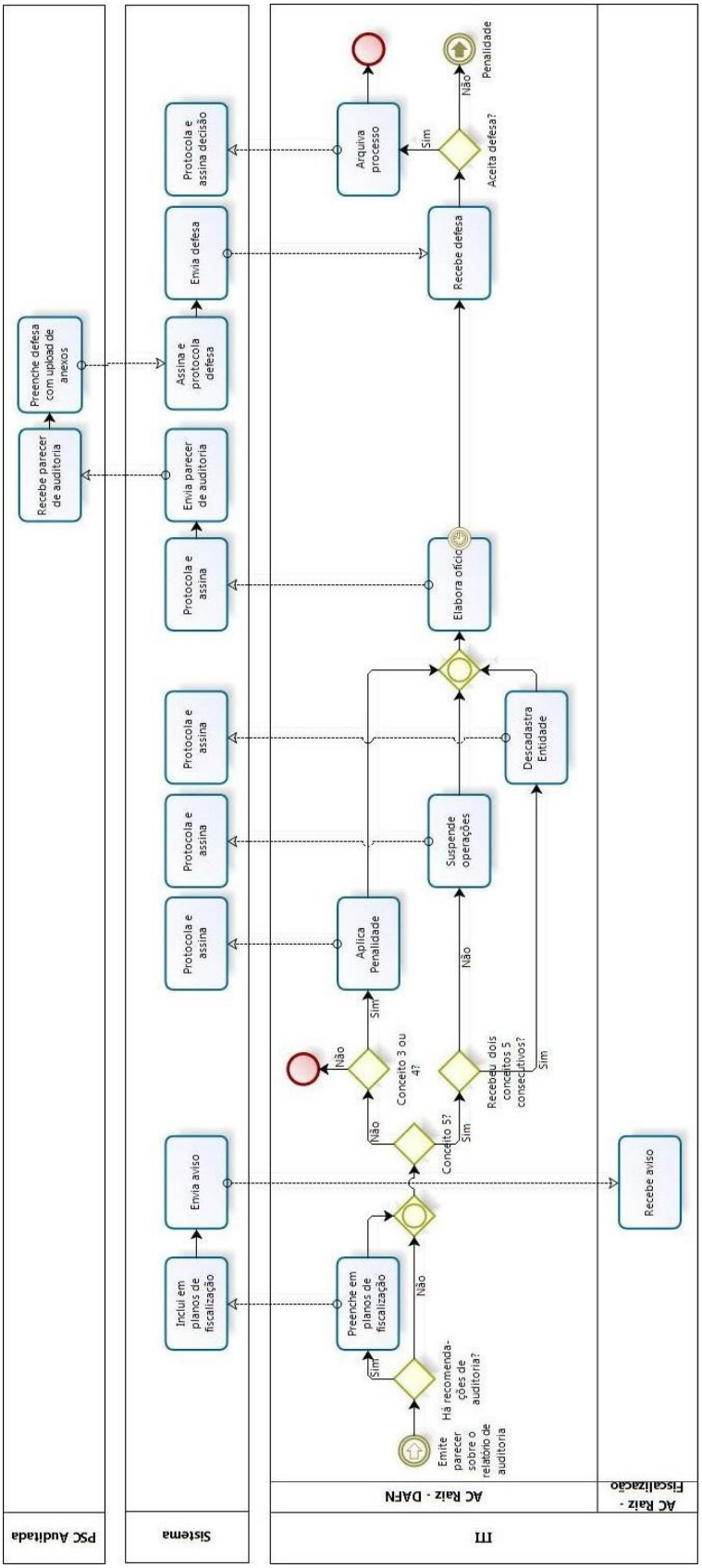

Ilustração 50 – Emissão do parecer sobre o relatório de auditoria.

A AC Raiz assina e protocola uma notificação de penalidade no sistema, que o enviará à entidade auditada que decidirá se aceita ou não a penalidade. Se ela aceitar, a AC Raiz publica a decisão de penalidade no DOU e o processo é finalizado, senão ela assina e protocola um pedido de recurso no sistema. O pedido de recurso é enviado à AC Raiz, para conhecimento, e ao diretor presidente do ITI.

O diretor presidente decide o recurso e assina e protocola no sistema. Caso julgue necessário, pode pedir subsídio à sua decisão no sistema, que avisará Procuradoria Federal Especializada e esta acessará o sistema para subsidiar a decisão, assinando e protocolando seu ato. Se o diretor presidente aplicou penalidade, ele a publica no DOU e finaliza o processo.

O sistema envia a decisão à entidade auditada e, se tiver sido aplicada penalidade, pode aceitá-la ou não. Se aceitá-la, o processo é finalizado, senão ela solicita recurso pelo sistema. O sistema assina e protocola o recurso e o envia ao Comitê Gestor, que assina e protocola sua decisão no sistema e a publica no DOU. O sistema envia a decisão do recuso à entidade auditada e o processo finaliza.

Essas atividades são visualizadas na ilustração 51.

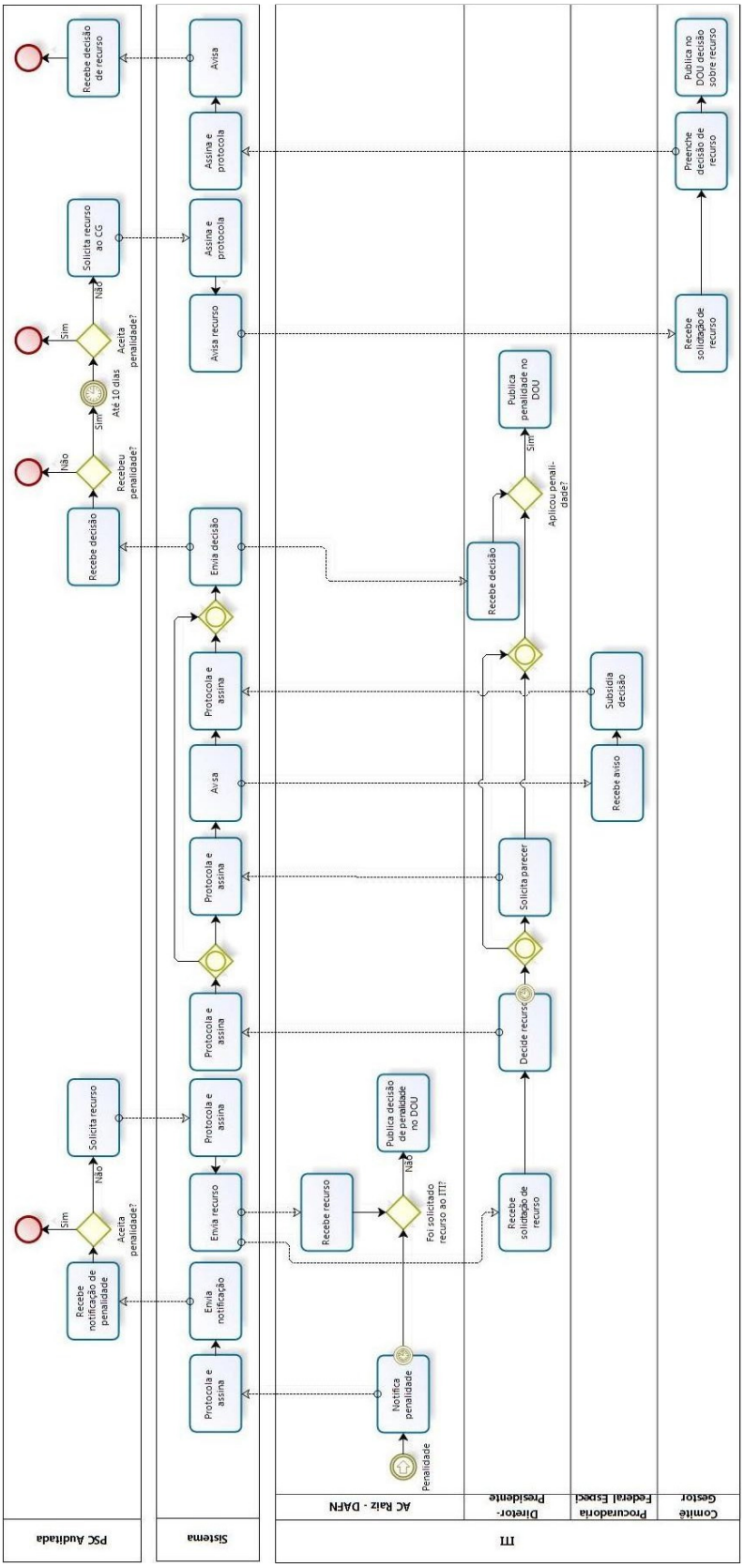

Ilustração 51 – Emissão do parecer sobre o relatório de auditoria - continuação.

5.2 PROCESSOS AUTOMATIZADOS PARA REALIZAÇÃO DE FISCALIZAÇÕES

Para iniciar o processo de fiscalização, a AC Raiz assina e protocola no sistema o início de um processo administrativo de fiscalização e torna público o procedimento de fiscalização de certificação. A ação de fiscalização de certificação é então executada entre o sistema, a AC Raiz e a entidade fiscalizada.

Após 120 dias, se a AC Raiz decidir prorrogar a fiscalização, ela assina e protocola a solicitação de prorrogação no sistema. O sistema verifica se a ação de fiscalização de certificação já foi prorrogada uma vez. Caso não tenha sido, avisa à AC Raiz que a ação será prorrogada, caso contrário avisa que não será prorrogada e fica esperando a AC Raiz assinar e protocolar no sistema a solicitação de final de processo de fiscalização de certificação.

Após a AC Raiz assinar e protocolar a solicitação de final de processo de fiscalização de certificação no sistema e tornar público essa decisão, ela verificará se foram encontradas irregularidades na fiscalização. Em caso negativo, ela preencherá no sistema a solicitação de finalização do processo administrativo de fiscalização. Em caso afirmativo, os procedimentos para corrigir as irregularidades serão executados entre o sistema, a AC Raiz e a entidade fiscalizada. Ao final a AC Raiz preencherá no sistema a solicitação de finalização do processo administrativo de fiscalização.

A solicitação de finalização do processo administrativo de fiscalização é assinada e protocolada pelo sistema e o aviso de finalização é enviado à AC Raiz e à entidade fiscalizada, e o processo é finalizado.

A ilustração 52 mostra este macroprocesso.

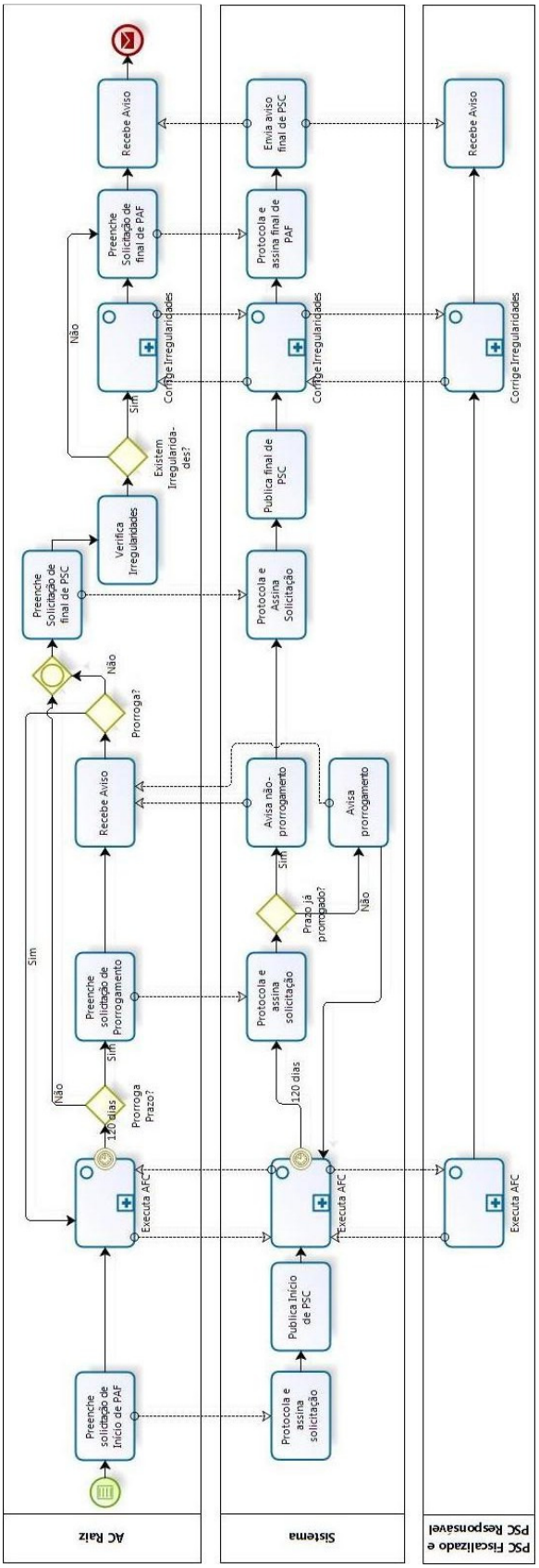

Ilustração 52 – Processo de fiscalização.

Na execução da ação de fiscalização de certificação, o diretor ou coordenador geral da ação de fiscalização preenche um termo de fiscalização inicial no sistema, que será assinado e protocolado. Caso tenha necessidade, pode ser preenchidos no sistema também termos de fiscalização extensivo e/ou complementar. Eles são incorporados ao termo de fiscalização inicial e assinados e protocolados no sistema. O sistema envia o termo de fiscalização inicial ao PSC fiscalizado, ao PSC responsável e à AC Raiz.

O fiscal da ICP-Brasil então fiscaliza a entidade. Se não encontrar nenhuma infração, verifica se a ação de fiscalização de certificação já finalizou. Caso encontre alguma infração, ele irá preencher no sistema um auto de infração de certificação, o qual será assinado e protocolado. O sistema enviará o auto de infração ao PSC fiscalizado, ao PSC responsável e à AC Raiz. Se a ação de fiscalização já tiver finalizado, o diretor ou coordenador geral da ação preenche no sistema um termo de fiscalização final. O sistema assina e protocola o termo e o envia ao PSC fiscalizado, ao PSC responsável e à AC Raiz.

Esse processo está representado na ilustração 53.

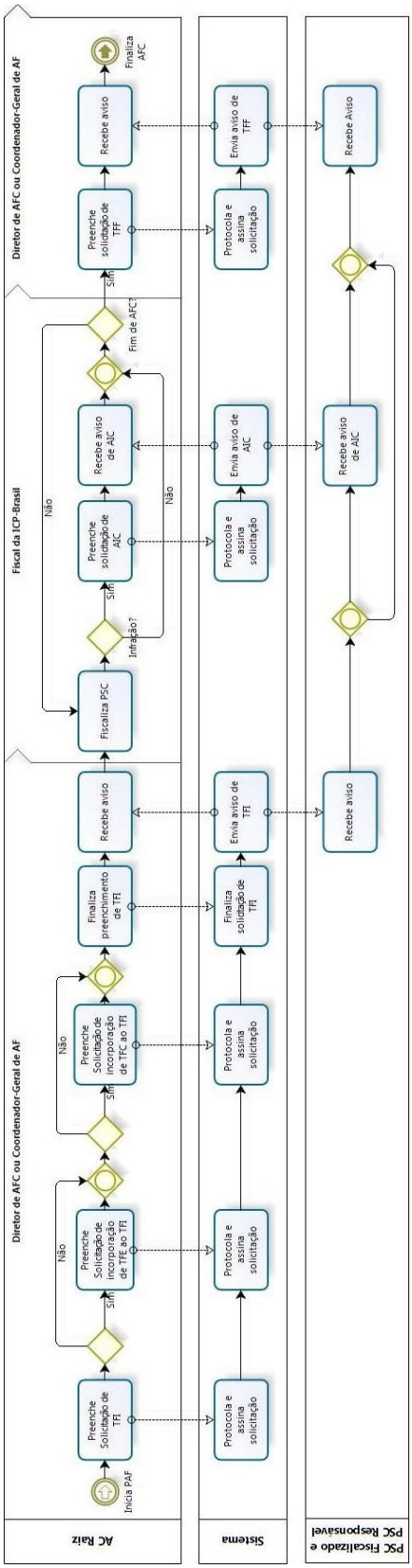

Ilustração 53 – Execução de ato de fiscalização de certificação.

Se alguma irregularidade foi encontrada durante a fiscalização, o diretor ou o coordenador geral da ação de fiscalização notifica a irregularidade preenchendo uma notificação de fiscalização de certificação no sistema. A notificação é assinada e protocolada e enviada à entidade fiscalizada e à entidade responsável. Ela terá até 15 dias para preencher a justificativa e defesa no sistema, que será assinada e protocolada e enviada à AC Raiz. Caso não apresente, a AC Raiz preenche, assina e protocola no sistema uma notificação, que o sistema envia ao PSC responsável. O PSC responsável tem até 15 dias para preencher a justifica e defesa no sistema, que a assinará e protocolará e enviará à AC Raiz. Não recebendo a justifica e defesa, a AC Raiz aplicará uma penalidade à entidade fiscalizada em até 20 dias.

Caso a defesa tenha sido apresentada, uma notificação de correção de irregularidades será preenchida, assinada e protocolada no sistema e o sistema a enviará à entidade fiscalizada com um prazo para ser realizada. A entidade fiscalizada realiza as correções e preenche o aviso de correção no sistema, o qual será assinado e protocolado e enviado pelo sistema à AC Raiz. Após o prazo a AC Raiz verifica se a irregularidade foi corrigida e, se tiver sido, finaliza a verificação de irregularidades. Caso não tenha sido, ela preencherá, assinará e protocolará no sistema uma penalidade, que o sistema enviará à entidade.

A entidade fiscalizada decide se aceita ou não a penalidade. Se aceitar o processo finaliza, senão ela tem até 20 dias para solicitar recurso pelo sistema, que assinará e protocolará o recurso e enviará à AC Raiz. A AC Raiz decide se reconsidera a penalidade. Caso reconsidere, ela assina e protocola no sistema a decisão sobre o recurso, que a envia à entidade fiscalizada, e o processo finaliza. Caso contrário, assina e protocola no sistema o encaminhamento do recurso, que o envia ao diretor presidente. Ele decide sobre o recurso e pode pedir o subsídio da Procuradoria Federal Especializada, que assina e protocola seu subsídio no sistema. Ele então preenche, assina e protocola a decisão do recurso no sistema e o sistema envia a decisão à entidade fiscalizada e finaliza o processo.

Os processos de irregularidade na fiscalização podem ser observados nas ilustrações 54 e 55.

Neste capítulo foi apresentada a modelagem de uma proposta de modernização dos processos de auditoria e fiscalização da ICP-Brasil, através de um sistema automatizado utilizando o documento eletrônico seguro.

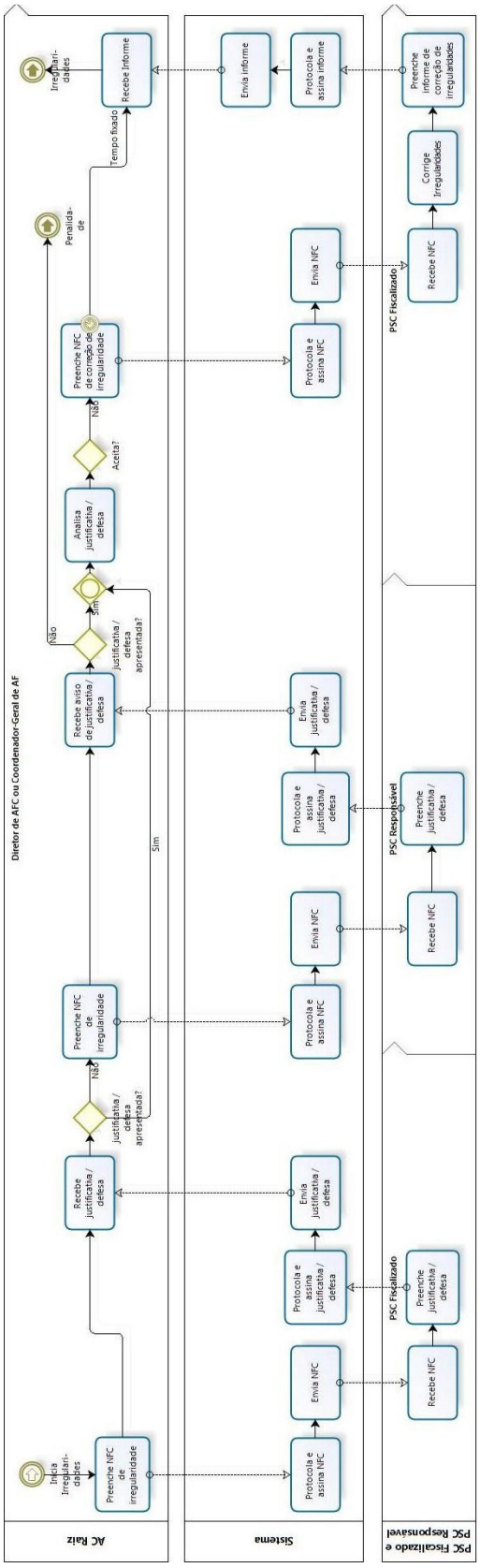

Ilustração 54 – Correção de irregularidades.

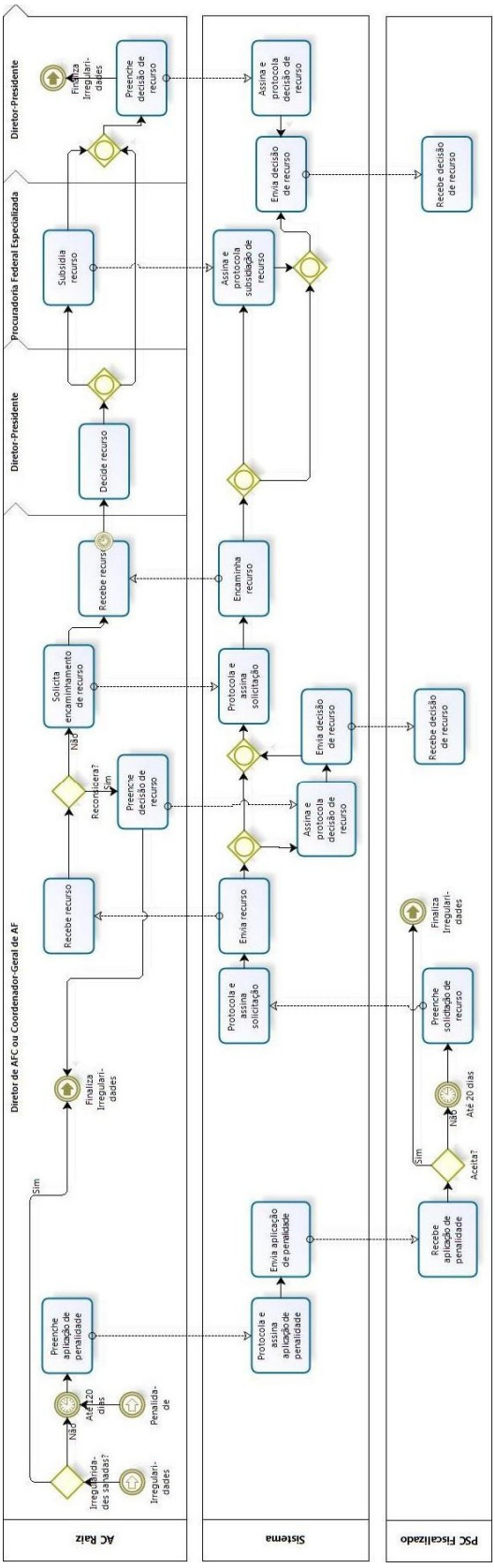

Ilustração 55 – Correção de irregularidades - continuação.

6 CONCLUSÕES E RECOMENDAÇÕES

Vivemos em uma era onde as tecnologias da informação e da comunicação estão presentes em todo tipo de relacionamento. Nas relações sociais, nas relações comerciais, nas relações diplomáticas, nas relações educacionais, nas relações empresarias, nas relações políticas, em todo tipo de relação que envolva algum tipo de troca de informação entre pessoas, os computadores estão presentes em algum ponto do processo.

A importância da tecnologia dos computadores cresceu tanto no decorrer do século XX e no início do século XXI que hoje é impossível imaginar o mundo sem os computadores. A sociedade mundial tornou-se dependente deles e instituiu um novo tipo de sociedade chamada de sociedade da informação. A sociedade onde as interações são ágeis e dinâmicas, devido aos processos automatizados pelas redes de computadores. A sociedade que tornou os fluxos e informações mais eficientes e, consequente, se tornou mais eficiente, já que uma sociedade não existe sem processos de troca de informações e de comunicações.

Entretanto, com a transferência do conhecimento e das transações humanas para dentro dos computadores, o substrato de papel se perde. Não existe mais o substrato que garante a autenticidade e a integridade da informação, caso alguém rasure o que está contido nele. O papel garante a identificação da pessoa responsável pela informação nele contida através de sua assinatura, e isso também se perde. O papel onde terceiras partes confiáveis garantem prova de que a informação contida nele é original, por quem foi escrita e quando foi escrita, já não existe mais.

Na sociedade informacional, onde é possível conectar tudo e todos por redes de computadores, a informação está armazenada principalmente em bits, que podem ser acessados e alterados sem que fiquem rastros da história da informação contida neles. Com isso nota-se que o documento eletrônico, por si só, não é seguro, não é confiável, como o documento em papel pode ser.

No papel, uma informação secreta poderia ser cifrada em código. No documento eletrônico, quem tiver acesso aos bits que formam a informação pode visualizar a informação a partir de um computador.

A falta de segurança da informação digital, em paralelo com o crescimento e uso cada vez mais frequente dos computadores nos mais variados processos no

decorrer do século XX, estimulou cientistas, principalmente matemáticos, a trabalharem em métodos para torná-lo seguro e confiável.

Com as técnicas de criptografia da informação digital e o conceito de infraestruturas de chaves públicas, foi possível dotar o documento eletrônico das mesmas características de segurança e confiabilidade que o documento em papel possuía. Todas essas técnicas resultaram no certificado digital, o documento eletrônico que garante que as pessoas, físicas e jurídicas, possam dotar as transações e informações digitais que criam com as características de autenticidade, integridade, não repúdio, tempestividade e sigilo. O documento em papel foi efetivamente superado.

No Brasil há uma infraestrutura de chaves públicas mantida por uma autarquia ligada ao governo federal e que é responsável por ser a terceira parte confiável nas informações e comunicações eletrônicas. Essa estrutura é composta de normas, procedimentos, regras e entidades que são responsáveis pelos documentos de identificação digitais para pessoas físicas e jurídicas em âmbito nacional: os certificados digitais da ICP-Brasil, a Infraestrutura de Chaves Públicas Brasileira.

Entretanto, muitos dos processos dessa estrutura ainda são feitos de forma manual e com o suporte do documento em papel. É uma contradição, uma vez que essa estrutura existe justamente para dar confiabilidade e permitir o uso das informações e comunicações digitais.

Nesse trabalho foram focados em alguns processos em particular, alguns dos mais importantes, responsáveis por manter a confiabilidade da própria estrutura: os processos de realização de auditorias e fiscalizações nas entidades da ICP-Brasil, para garantir que os certificados digitais fornecidos por ela, e o ciclo de vida deles, sejam seguros e confiáveis para serem utilizados por pessoas físicas e jurídicas no território brasileiro.

Para isso, foi feito o estudo, a pesquisa, o levantamento e o mapeamento de como os processos de realização de auditorias e de fiscalização são atualmente executados na ICP-Brasil. Com isso foi possível modelar estes processos e, no modelo, identificar os pontos onde a automação e o uso do documento eletrônico seguro seria possível, para então propor um modelo automatizado desses processos e utilizando o certificado digital como suporte de confiabilidade para as informações geradas e as comunicações realizadas, dando mais segurança até mesmo aos

processos modelados.

Comparando os dois modelos apresentados neste trabalho, é possível verificar que todos os processos apresentados atualmente são possíveis de serem automatizados. Também é possível observar que em vários dos pontos dos processos onde alguma informação seria gerada, ocasionando muitas vezes em geração de documentos em substrato físico, pode ser substituído pela geração de documentos eletrônicos assinados e protocolados por intermédio de certificados digitais.

O modelo automatizado proposto garante maior controle dos processos de realização de auditorias e de fiscalizações à AC Raiz. No modelo atual, a AC Raiz não pode controlar o fluxo da informação para saber em que ponto está o processo e quem são ou foram os responsáveis por cada atividade ou evento que acontece ou aconteceu. A partir do sistema automatizado, onde o sistema controla o fluxo da informação e a comunicação entre as entidades envolvidas, a AC Raiz pode saber exatamente o que aconteceu, está acontecendo e o que deve acontecer em cada ponto do processo.

Como cada entidade acessa o sistema utilizando certificado digital e deixa seu histórico nos *logs* e nas transações realizadas, a AC Raiz pode saber exatamente quem tem responsabilidade por cada ato que foi executado nos processos. A chave privada dessas pessoas é utilizada para assinar suas ações no sistema, e elas são ainda protocoladas por sistemas de carimbo do tempo digitais internos ao sistema, que permitem saber o tempo exato em que cada ação foi realizada.

O sistema permite que os processos se tornem mais eficientes. Com a automação do sistema, a rapidez do fluxo de dados também se torna maior. Os processos automáticos são executados assim que forem possíveis, não dependem da disponibilidade de uma pessoa para serem executados. Isso os torna mais ágeis e mais dinâmicos.

Esse ganho em eficiência, dinamismo e agilidade dos processos estudados, em conjunto com o maior controle e a maior confiança que eles teriam, é possível de ser observado no modelo automatizado proposto, onde vários processos manuais foram suprimidos e simplificados, sem perder sua segurança, ao contrário, aumentando-a. É possível observar no modelo proposto que o controle do fluxo de informações também ficou muito superior ao modelo atual, realizado de forma

manual.

Só estas vantagens já justificariam a adoção do modelo automatizado, mas há mais uma característica que pode ser observada comparando os dois modelos, a ausência da necessidade de fazer uso de documentos em papel ou qualquer outro substrato físico. O modelo automatizado extingue a necessidade do papel, CD, DVD, ou qualquer outro substrato que não sejam os bits do sistema.

O próprio sistema faz o controle de como a informação deve fluir, avisando a todos as entidades do processo quando eles devem fazer algo e o que devem fazer. Isso elimina a necessidade de impressão de manuais para saber como executar os processos pesquisados. Os documentos que devem ser gerados pelos participantes dos processos também não precisam mais de modelos em papel, já que o modelo deles está no sistema de forma eletrônica e o usuário o utiliza quando precisar. A comunicação é realizada por e-mail enviado única e exclusivamente pelo sistema automatizado, e ele guarda registros das comunicações efetuadas por ele, de forma assinada e protocolada por ele mesmo.

Com tantas vantagens se chega à conclusão que o sistema não é apenas possível de ser implementado, mas também necessário. A economia que este sistema proveria em função da simplificação, aumento da segurança e controle e eliminação da geração de documentos em substrato físico dos processos poderia ser sentido no produto final, o certificado digital.

O documento de identificação digital que é tão importante na sociedade da informação, mas ainda não é popularmente disseminado devido ao seu elevado custo, depende de tornar a estrutura responsável por seu ciclo de vida se tornar menos dispendiosa, e uma das maneiras de fazer isso é tornar seus processos mais eficientes, menos custosos e dotados de maior controle e simplicidade, através da automação pela tecnologia da informação e pelo uso dos documentos eletrônicos seguros.

6.1 TRABALHOS FUTUROS

A pesquisa deste trabalho se baseou no normativo da ICP-Brasil, já que ela contém as regras que toda entidade deve seguir à risca. Mas para melhorar o modelo proposto, a validação do modelo do estado atual da arte dos processos entre o maior número possível de entidades que fazem parte da Infraestrutura de

Chaves Públicas Brasileira e atuam nos processos de realização de auditoria e fiscalização ajudaria a identificar atividades que são realizadas no mundo real, mas não estão presentes nas normas.

Seria de grande valia para a melhoria do modelo proposto também uma simulação dos sistemas, para poder identificar o quanto de eficiência é capaz de se obter em função de economia de tempo e de recursos humanos. Para isso seria necessário realizar uma pesquisa, com base na modelagem do estado atual dos processos, no maior número possível de entidades que participam deles.

A pesquisa visaria recolher dados de tempo que cada atividade mapeada nos processos consome e qual o recurso humano que ela necessita para ser executada. Com as médias e desvios padrões de tempo e número de entes envolvidos em todas as atividades, seria possível inferi-las nos modelos e realizar uma simulação discreta de seus processos para ver quão mais rápidos e econômicos os processos automatizados seriam.

A simulação discreta é o emprego de técnicas matemáticas em computadores com o objetivo de imitar um processo ou operação do mundo real.

Por fim, a melhor maneira de observar a eficiência do sistema automatizado dos processos de realização de auditoria e de fiscalização da ICP-Brasil seria programá-lo e testá-lo no mundo real, melhorando-o com os estudos que seriam necessários realizar e os e dados a mais que surgiriam durante esse processo.

REFERÊNCIAS

ALTER, S. **Information Systems: a management perspective.** Addison-Wesley Publishing Co. Massachusetts, 1992.

BRASIL. **Medida Provisória 2.200-2**. Medida Provisória que instituiu a ICP-Brasil.

BAUER, R.; KÖSZEGI, S. T. Measuring the degree of virtualization. **Eletronic Journal of Organizational Virtualness**, vol. 5, n. 2, p. 26-46, 2003.

BRACHE, A. P.; RUMMLER, G. A. **Melhores desempenhos das empresas**: uma abordagem prática para transformar as organizações através da reengenharia. São Paulo: Makron Books, 2007.

BROCARDO, M. L.; DE ROLT, C. R.; FERNANDES, R**. Introdução à certificação digital:** Da criptografia ao carimbo de tempo. 2006. Disponível em: <http://www.tj.sc.gov.br/encontro/2006/palestras/certificacao.pdf>. Acesso em 17 nov. 2009.

BULDAS, A.; LIPMAA, H.; SCHOENMAKERD, B. **Optimally efficient accountable time-stamping.** Public Key Cryptography '2000, LNCS 1751, [S.l.], 2000.

BULTJE, R.; WIJK, J.V. Taxonomy of Virtual Organisations, based on definitions, characteristics and typology. In: **VoNet: The Newsletter,** v. 2, n. 3, p. 16. 1998.

BYRNE, J.A. The virtual corporation. In: **Business Week**, February, 1993.

CASTELLS, Manuel. **A sociedade em rede: a era da informação: economia, sociedade e cultura.** v. 1; 8. ed. São Paulo: Paz e Terra, 1999. 698p.

CARLOS, M. C. **Topologias dinâmicas de Infra-estrutura de Chaves Públicas**. 2007. 112 p. Dissertação (Mestrado em Ciência da Computação) - Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2007.

CHIZZOTTI, A. **Pesquisa em ciências humanas e sociais.** São Paulo: Cortez, 1991.

COOKE; Robert; QUINN; Barbara; KRIS; Andrew. **Shared services: Mining for corporate gold**. EUA: Financial Times Prentice Hall, 1999.

COSTA, T. da. **Modernização dos Serviços de Registro Público do Brasil:** Proposta da Averbação Eletrônica da Penhora de Imóveis. 2009. 136 p. Dissertação (Mestrado em Administração) Programa de Pós-Graduação em Administração, Universidade do Estado de Santa Catarina, Florianópolis, 2009.

CROOKS , A. C.; SPATZ, K. J. WARMAN, M. **Basics of organizing a shared-services cooperative**. Rural Business and Cooperative Development Service (RBCDS), 1995. [on line] Disponível em <http://www.rurdev.usda.gov/rbs/pub/SR46.pdf >. Acesso em: 17 mar. 2010.

DÁVALOS, R. V. **Modelagem de processos**: livro didático / Ricardo Villarroel Dávalos ; design instrucional Dênia Falcão de Bittencourt, Viviane Bastos ; [assistente acadêmico Leandro Rocha]. – 4. ed. rev. e atual. – Palhoça : Unisul Virtual, 2010. 186 p.

DAVENPORT, H. T. **Reengenharia de processos**: como inovar na empresa através de tecnologia de informação. Rio de Janeiro, Campus, 1994, 391 p.

DE ROLT, C. R.; SCHMITZ, L. C.; SANTOS, I. A. **Taxonomia das organizações virtuais**. 2005.

DIAS, J. da S. **Confiança no Documento Eletrônico**. 2004. 141 p. Tese (Doutorado em Engenharia de Produção e Sistemas) – Programa de Pós Graduação em Engenharia de Produção, Universidade Federal de Santa Catarina, Florianópolis, 2004.

DIFFIE, W.; HELLMAN, M. **New directions on cryptographic techniques.** Proceedings of the AFIPS National Computer Conference, [S.l.], 1976.

FEDERAL, G. **Decreto Lei 4.264**.

FEISTEL, H. **Block cipher cryptographic system**, U.S. Patent # 3,798,359, 19 Mar 1974.

FEISTEL, H. **Step code ciphering system**, U.S. Patent # 3,798,360, 19 Mar 1974.

FOTHERGILL, J.; BINKS, J.; RYAN-COLLINS, J. **Transformation through shared services:** improving quality, increasing efficiency. CBI, 2006. [on line] Disponível em <http://www.cbi.org.uk/ndbs/positiondoc.nsf/1f08ec61711f29768025672a0055f7a8/A472C8AC387689F68025719500361928/$file/sharedservices0606.pdf >. Acesso em: 17 mar. 2010.

FRANKE, U. J. The Competence-Based View on the Management of Virtual Web Organizations. In: FRANKE, U. **Managing Virtual Web Organizations in the 21st Century:** Issues and Challenges, Hershey, 2002.

Franke, U. J.; Hickmann B. **Is the Net-broker an entrepreneur? What role does the net-broker play in virtual Webs and virtual corporations?** Workshop: Organizational Virtualness and Electronic Commerce, Zurich, Switzerland. Proceedings of the 2nd International VoNet-Workshop, September, 1999, p. 117-134.

GARVIN, David. The processes of organization and management. Sloan Management Review, v. 39, n. 4, Summer 1998.

GIL, A. C. **Como elaborar projetos de pesquisa.** São Paulo: Atlas, 1991.

GONÇALVES, J. E. L. **As empresas são grandes coleções de processos.** RAE – Revista de Administração de Empresas, V. 40, n 1. São Paulo - SPG, Jan/Mar 2000. p. 6-19.

GONÇALVES, J. E. L. **Processo, que processo?** Revista de Administração de Empresas (RAE). São Paulo: FGV, v. 40 . n. 4 . p. 8-19, Out./Dez. 2000.

HABER, S.; STORNETTA, S. **How to time-stamp a digital document.** Journal of Cryptology, [S.l.], v.3, p.99–112, 1991.

HAMMER, M.; CHAMPY, J. **Reengenharia revolucionando a empresa em função dos clientes, da concorrência e das grandes mudanças da gerência**. Rio de Janeiro, Campus, 1994, 189 p.

HARRINGTON, J. **Aperfeiçoando processos empresariais.** São Paulo: Makron Books, 1993.

HASSE, D.; DE ROLT, C. R. **Modelo de Incubadora Virtual utilizando a Teoria das Organizações Virtuais**. In: Simpósio de Gestão da Inovação Tecnológica da ANPAD, 24. 2006, Gramado. Anais... Gramado, 2006.

HENDERSON, J.C. & VENKATRAMAN, N. **Strategic Alignment: Leveraging Information Technology For Transforming Organizations.** IBM Systems Journal. v.32, n.1, p.4-16, 1993.

HOUSLEY, R.; POLK, T. **Planning for PKI**. 1. ed. [S.l.]: Wiley, 2001.

ESTRUTURA DA ICP-BRASIL. [on line] Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/EstruturaIcp/Estrutura_da_ICP-Brasil_-_site.pdf> Acesso em 27 mar. 2010.

ICP-BRASIL, C. G. D. **RESOLUCÃO Nº 16**. Resolucão que determina o Observatório Nacional como fornecedor da hora legal brasileira para a ICP-Brasil.

INSTITUTE OF PUBLIC FINANCE (IPF). **Shared services:** the opportunities and issues for public sector organizations. Jun. 2006. [on line] Disponível em: <http://www.ipf.com/fileupload/ upload/Shared_services187200611542.pdf> Acesso em 17 mar. 2010.

INTERNATIONAL TELECOMMUNICATION UNION – STANDARDIZATION SECTOR (ITU-T). **Recommendation X.509 – Information Technology – Open Systems Interconnection – The Directory:** Authentication Framework. [S.l.], 1988.

INTERNATIONAL TELECOMMUNICATION UNION – STANDARDIZATION SECTOR (ITU-T). **Recommendation X.509 (11/93) – Information Technology – Open Systems Interconnection – The Directory:** Authentication Framework. [S.l.], 1993.

INTERNATIONAL TELECOMMUNICATION UNION – STANDARDIZATION SECTOR (ITU-T). **Recommendation X.509 (1997 E) – Information Technology – Open Systems Interconnection - The Directory:** Authentication Framework. [S.l.], Junho 1997.

JÄGERS, H.; JANSEN, W.; STEENBAKKERS, W. Characteristics of Virtual Organizations. In: SIEBER, P.; GRIESE, J. Organizational virtualness and electronic commerce. **Proceedings of the 2nd VoNet** - workshop, Bern: Simowa Verlag, Zurich, p. 65-76, sep. 1998.

JOHANSSON, H. J.; McHUGH, P.; PEDLEBURY, A. J.; WHELLER A. W. **Processos de negócios**: como criar sinergia entre a estratégia de mercado e a excelência operacional. São Paulo: Pioneira, 1995, 227 p.

KEEN, P.G.W. **Information Technology And The Management Theory: The Fusion Map.** IBM Systems Journal, v.32, n.1, p.17-38, 1993.

KOHNFELDER, L. **Towards a pratical public-key cryptosystem.** MIT laboratory for Computer Systems. Master thesis, 1978.

LAKATOS, E. M.; MARCONI, M. A. **Metodologia do trabalho científico.** São Paulo: Atlas, 1995.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos da metodologia científica.** São Paulo: Atlas, 2006.

LAUDON, K. C. **Sistemas de Informações gerenciais : administrando a empresa digital.** São Paulo: Prentice Hall, 2004.

LUFTMAN, J.N.; LEWIS, P.R. & OLDACH, S.H. **Transforming The Enterprise: The Alignment Of Business And Information Technology Strategies**. IBM Systems Journal, v.32, n.1, p.198-221, 1993.

MCCULLAGH, A.; LITTLE, P.; CAELLI, W., **Electronic signatures: understand the past to develop the future.** University of New South Wales Law Journal, 452, 1998.

OPREA, M. Coordination in an agent-based virtual enterprise. **Studies in informatics and Control.** v.12, n.3, p. 215-225, set. 2003.

O QUE É CERTIFICAÇÃO DIGITAL. [on line] Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf> Acesso em 14 out. 2009.

PADOVEZE, C. L. **Sistemas de informações contábeis: fundamentos e análise.** São Paulo: Atlas, 2004.

PEREIRA, C. D.; PANTOJA, A. V.; ZWIEREWICZ, M.; COPPETE, M. C.; BORGES, M. K. **Sociedade da Informação, Educação Digital e Inclusão.** 1 ed. Florianópolis: Insular, 2007.

PORTER, Michael E. **Competição: estratégias competitivas essenciais.** 2.ed. Rio de Janeiro: Editora Campus Ltda, 1999.

QUINN, B.; COOKE, R.; KRIS, A., **Shares Services: Mining for corporate gold.** London: Financial TimesPrentice Hall, 2000.

RFC 3161, **Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)**, D. Pinkas Integris, R. Zuccherat Entrust August, 2001

RIBEIRO, A. M. et al. **A Infraestrutura de Chaves Públicas Brasileira e suas Bases para a Auditoria em Segurança da Informação**. Diretoria de Auditoria, Fiscalização e Normalização, Instituto Nacional de Tecnologia da Informação, Brasília, 2004.

RICHARDSON, R. J. **Pesquisa social: métodos e técnicas.** São Paulo: Atlas, 1999.

RIVEST, R.; SHAMIR, A.; ADLEMAN, L. **A method for obtaining digital signatures and public key cryptosystems**. Communications of the ACM, [S.l.], February, 1978.

SCHEIBELHOFER, K. **Signing XML Documents and the Concept of "What You See Is What You Sign"**. 2001. 118 p. Dissertação (Master's Thesis in Telematics) - Institute for Applied Information Processing and Communications, Graz University of Technology, Austria, 2001.

SCHULMAN, D. et al. **Shared services**: adding value to the business units. New York: John Wiley & Sons, 2001.

STRAUSAK, N. Resumée of VoTalk. In: SIEBER, Pascal, GRIESE, Joachim (eds). **Organizational Virtualness**. Proceedings of the VoNet - Workshop, April 27-28, 1998. Bern, Simona Verlag Bern, 1998, p. 9-24.

TAPSCOT, D., WILLIAMS,A. **Wikinomics: como a colaboração em massa pode mudar o seu negócio.** Rio de Janeiro: Nova Fronteira, 2007.

VERNADAT, F. B. **Enterprise modeling and integration**: principles and applications. London: Chapman & Hall, 1996.

VILLELA, C. da S. S. **Mapeamento de processos como ferramenta de reestruturação e aprendizado organizacional.** 2000. 182 p. Pós-Graduação (Engenharia da Produção) – Universidade Federal de Santa Catarina, Florianópolis, 2000.

WEIL, P. **The Relationship Between Investment In Information Technology And Firm Performance: A Study Of The Valve Manufacturing Sector.** Information Systems Research, v.3, n.4, p.307-333, Dec. 1992.

YIN, R. K. **Estudo de caso: planejamento e métodos.** 2ª ed. São Paulo: Bookman, 2002.

ANEXOS

ENTRE AS ENTIDADES DE AUDITORIA E O ITI

ANEXO K – REQUISIÇÃO DE INFORMAÇÕES COMPLEMENTARES

ANEXO L – AUTO DE INFRAÇÃO

ANEXO M – TERMO DE FISCALIZAÇÃO

ANEXO N – NOTIFICAÇÃO

ANEXO O – RELATÓRIO DE FISCALIZAÇÃO

ANEXO A - CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL

Infra-Estrutura de Chaves Públicas Brasileira

CRITÉRIOS E PROCEDIMENTOS

PARA CREDENCIAMENTO DAS

ENTIDADES INTEGRANTES DA ICP-

BRASIL DOC-ICP-03 - versão 4.3

24 de novembro de 2009

Infra-Estrutura de Chaves Públicas Brasileira

Sumário

CONTROLE DE ALTERAÇÕES

Resolução que aprovou alteração	*Item Alterado*	*Descrição da Alteração*
Resolução 52, de 19.11.2008 (Versão 4.0)	1, 2.1.3, 2.1.4.1, 2.1.4.2, 2.2.1.5, 2.2.4, 2.2.5.1.2, 2.2.5.3, 3.3, 3.4, 4.3, 4.4.2.1, 4.4.2.2, Anexo IV	Inclusão de referências a Autoridades de Carimbo de Tempo
Resolução 47, de 23.11.2007 (versão 3.0)	2.1.2	Alterados os documentos a serem apresentados caso a instalação técnica de uma AR se localize em endereço diferente do de sua sede administrativa
	3.1.d	Alterada a data para apresentação do cronograma anual de auditoria das ACs para 15 de março
	3.2.1	Inclusão dos subitens 3.2.1.1 e 3.2.1.3 e renumeração dos demais
	Item 3.a dos Anexos I, II e III	Substituição da exigência de apresentação de balanço contábil por apresentação de parecer de contador com registro no CNAI.
Resolução 40, de 18.04.2006 (Versão 2.0)	Diversos	Criação do DOC-ICP-03, consolidando documentos anteriores

Infra-Estrutura de Chaves Públicas Brasileira

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora
AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil
AR - Autoridades de Registro
CG - Comitê Gestor
CPF - Cadastro de Pessoas Físicas
DPC - Declaração de Práticas de Certificação
ICP-Brasil - Infra-Estrutura de Chaves Públicas Brasileira
PC - Políticas de Certificado
PS - Política de Segurança
PSS - Prestadores de Serviço de Suporte

Infra-Estrutura de Chaves Públicas Brasileira

1. INTRODUÇÃO

Este documento estabelece os critérios e procedimentos a serem observados para o credenciamento, manutenção do credenciamento e descredenciamento de Autoridades Certificadoras (ACs), de Autoridades de Registro (ARs), de Autoridades de Carimbo do Tempo (ACTs) e de Prestadores de Serviço de Suporte (PSSs), no âmbito da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil.

2. CREDENCIAMENTO

2.1 Critérios

Os candidatos ao credenciamento na ICP-Brasil devem atender aos seguintes critérios:
a) ser órgão ou entidade de direito público ou pessoa jurídica de direito privado;
b) estar quite com todas as obrigações tributárias e os encargos sociais instituídos por lei;
c) atender aos requisitos relativos à qualificação econômico-financeira estabelecidos, conforme a atividade a ser desenvolvida, nos anexos I, II e III; e
d) atender às diretrizes e normas técnicas da ICP-Brasil relativas à qualificação técnica, constantes dos documentos relacionados no Anexo I, aplicáveis aos serviços a serem prestados.

2.1.1 Critérios para credenciamento de AC

Os candidatos ao credenciamento como AC devem ainda:
a) apresentar, no mínimo, uma entidade operacionalmente vinculada, candidata ao credenciamento para desenvolver as atividades de AR, ou solicitar o seu próprio credenciamento como AR;
b) apresentar a relação de eventuais candidatos ao credenciamento para desenvolver as atividades de PSS;
c) ter sede administrativa localizada no território nacional; e
d) ter instalações operacionais e recursos de segurança física e lógica, inclusive sala-cofre, compatíveis com a atividade de certificação, localizadas no território nacional, ou contratar PSS que as possua.

2.1.2 Critérios para credenciamento de AR

Os candidatos ao credenciamento como AR devem ainda:
a) estar operacionalmente vinculados a, pelo menos, uma AC ou candidado a AC. A AR em operação está apta a operar em todas as Políticas de Certificados credenciadas pela AC vinculada.
b) ter sede administrativa, instalações operacionais e recursos de segurança física e lógica compatíveis com a atividade de registro.
c) apresentar a relação de eventuais candidatos a PSS; e
d) caso a instalação técnica se localize em endereço diferente do de sua sede administrativa, apresentar, cumulativamente:
   i) no caso de entidade privada:
      1. certidão atualizada da junta comercial ou do registro civil de pessoas jurídicas, conforme sua natureza;
      2. alvará de funcionamento, se houver;
      3. CNPJ;
   ii) no caso de pessoa jurídica da administração direta, indireta, ou órgão público:
      1. ato administrativo que autorize a operação naquele endereço;
   iv) no caso de serviços notariais e de registro:

1. cópia do ato de outorga da delegação;
2. CNPJ

2.1.3 Critérios para credenciamento de ACT

Os candidatos ao credenciamento como ACT devem ainda:
a) apresentar a relação de eventuais candidatos ao credenciamento para desenvolver as atividades de PSS;
b) ter sede administrativa localizada no território nacional; e
c) ter instalações operacionais e recursos de segurança física e lógica compatíveis com a atividade de emissão de carimbos do tempo, localizadas no território nacional, ou contratar PSS que as possua.

2.1.4 Critérios para credenciamento de PSS

2.1.4.1 Para efeito dos processos tratados neste documento, considera-se PSS aquele que desempenha atividade descrita nas Políticas de Certificado (PC) e na Declaração de Práticas de Certificação (DPC) da AC a que estiver vinculado, diretamente ou por intermédio da AR, ou nas Políticas de Carimbo do Tempo (PCT) e na Declaração de Práticas de Carimbo do Tempo (DPCT) da ACT a que estiver vinculado. classificando-se, conforme o tipo de atividade prestada, em três categorias:
(1) disponibilização de infra-estrutura física e lógica;
(2) disponibilização de recursos humanos especializados; ou
(3) disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

2.1.4.2 Os candidatos ao credenciamento como PSS devem:
a) estar operacionalmente vinculados a, pelo menos, uma AC ou candidato a AC, ou uma AR ou candidato a AR ou a uma ACT ou candidato a ACT;
b) ter sede administrativa, instalações operacionais e recursos de segurança física e lógica compatíveis com as atividades a serem desempenhadas.

2.2 Procedimentos

2.2.1 Diretrizes Gerais

2.2.1.1 O processo de credenciamento obedece a procedimentos específicos, relacionados com a natureza da atividade a ser desenvolvida no âmbito da ICP-Brasil.
2.2.1.2 Todas as comunicações e requerimentos à AC Raiz, deverão ser encaminhados por intermédio da cadeia de AC, ou candidatos a AC, operacionalmente vinculados. Inicia-se a tramitação pela AC, ou candidato a AC, de nível imediatamente superior ao do interessado. A tramitação prossegue, a partir daí, respeitando a hierarquia de AC, ou candidatos a AC, operacionalmente vinculados, até chegar à AC Raiz.
2.2.1.3 As ACs serão responsáveis por comunicar as decisões do CG da ICP-Brasil ou da AC Raiz às entidades que lhes estejam operacionalmente vinculadas, respeitando a hierarquia de AC.
2.2.1.4 As ACTs se comunicarão diretamente com a AC Raiz.
2.2.1.5 O deferimento do pedido de credenciamento será publicado no Diário Oficial da União e importará a autorização para funcionamento no âmbito da ICP-Brasil e, no caso de AC e ACT, a emissão do seu certificado.
2.2.1.6 Em cada etapa da tramitação, a entidade que receber a solicitação de credenciamento de AC, AR, ou ACT tem prazo de até 30 (trinta) dias corridos para analisá-la e encaminhá-la à entidade de nível imediatamente superior, caso a solicitação seja acatada ou, se recusada, devolvê-la ao postulante com fundamentação da recusa.

2.2.1.7 Havendo recusa ou findo o prazo estabelecido no item 2.2.1.6, caberá recurso do postulante a AC Raiz.

2.2.2 Procedimentos para credenciamento de AC

2.2.2.1 Solicitação

2.2.2.1.1 As solicitações dos candidatos ao credenciamento como AC na ICP-Brasil serão encaminhadas à AC Raiz mediante a apresentação dos documentos a seguir relacionados:

a) formulário SOLICITAÇÃO DE CREDENCIAMENTO DE AC [1] devidamente preenchido e assinado pelo representante legal do candidato a AC;
b) documentos relacionados no Anexo I;
c) formulário SOLICITAÇÃO DE CREDENCIAMENTO DE AR [2] devidamente preenchido e assinado pelos representantes legais dos candidatos a AC e AR;
d) documentos relacionados no Anexo II, exceto na hipótese de o candidato a AR ser o próprio candidato a AC e indicar o mesmo endereço de instalação técnica; e
e) se for o solicitado o credenciamento de PSS:
    i. formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS [3], devidamente preenchido e assinado pelos representantes legais dos candidatos a AC e a PSS, bem como, do candidato a AR, se houver por parte do candidato a PSS intenção de vinculação operacional ao candidato a AR;
    ii. documentos relacionados no Anexo III; e
    iii. documento indicando as atividades específicas para as quais postula o credenciamento como PSS, selecionando uma dentre as seguintes opções: (1) disponibilização de infra-estrutura física e lógica; (2) disponibilização de recursos humanos especializados; ou (3) disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

2.2.2.1.2 A solicitação de credenciamento será protocolada perante o Protocolo-Geral da AC Raiz e recebida, em até 30 (trinta) dias, por intermédio de despacho fundamentado.

2.2.2.1.3 Caso a solicitação de credenciamento não contenha todos os documentos relacionados nos anexos I, II ou III, quando for o caso, a AC Raiz determinará a intimação da candidata para que, sob pena de arquivamento do processo. supra as irregularidades no prazo máximo de 30 (trinta) dias, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.

2.2.2.2 Auditoria Pré-Operacional

2.2.2.2.1 Após a publicação do despacho de recebimento, o candidato a AC deverá remeter à AC Raiz, no prazo máximo de 30 (trinta) dias, o formulário de REQUERIMENTO DE AUDITORIA [4], devidamente preenchido, declarando estar em conformidade com todos os requisitos exigidos pelas resoluções do CG da ICP-Brasil relacionados à atividade de autoridade certificadora e pronto para ser auditado no prazo de 15 (quinze) dias a contar daquele momento.

2.2.2.2.2 Tal requerimento deverá ser preenchido e assinado pelos representantes legais do candidato a AC.

2.2.2.2.3 Durante as diligências de auditoria a AC Raiz poderá exigir documentação adicional contendo especificações sobre equipamentos, produtos de *hardware* e *software*, procedimentos técnicos e operacionais adotados pela candidata.

2.2.2.2.4 Caso o relatório de auditoria aponte o não-cumprimento de quaisquer dos critérios para credenciamento exigidos pelo item 2.1, a AC Raiz intimará a candidata para que os cumpra no prazo que fixar, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.

2.2.2.2.5 Após a comunicação da candidata de que atendeu os critérios de credenciamento apontados como não cumpridos no relatório de auditoria, a AC Raiz intimará a candidata, por meio de ofício enviado com comprovação de recebimento pelo destinatário, determinando a realização de auditoria complementar, de modo a verificar as medidas adotadas.

2.2.2.2.6 A desistência de solicitação de credenciamento em tramitação poderá ser requerida até a data em que for recebido na AC Raiz o REQUERIMENTO DE AUDITORIA [4].
2.2.2.2.7 Apresentado o relatório final de auditoria, a AC Raiz manifestar-se-á sobre o deferimento ou indeferimento da solicitação de credenciamento, no prazo máximo de 30 (trinta) dias.
2.2.2.2.8 Sobre a decisão de indeferimento de solicitação de credenciamento caberá recurso administrativo da candidata ao Comitê Gestor da ICP-Brasil.
2.2.2.3 Ato de credenciamento
2.2.2.3.1 O credenciamento limita-se às PCs indicadas no formulário referido na alínea "a" do item 2.2.1.1 e poderá não contemplar todas as PCs propostas.
2.2.2.3.2 O deferimento total ou parcial, ou o indeferimento do credenciamento, será fundamentado e comunicado ao candidato a AC. É considerado deferimento parcial aquele que não contemplar todas as PCs propostas pelo candidato a AC.
2.2.2.3.3 O ato de credenciamento da AC condicionará a emissão do certificado pela AC Raiz ou pela AC de nível imediatamente superior, conforme o caso:

a) ao pagamento da tarifa estabelecida nas DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [5], no caso de a credenciada ser AC de nível imediatamente subseqüente à AC Raiz.
b) à apresentação, pela AC credenciada à AC Raiz, no prazo máximo de 10 (dez) dias após o deferimento do credenciamento, de apólice de contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades;

2.2.2.3.4 A Administração Direta da União, dos Estados, do Distrito Federal e dos Municípios está dispensada do pagamento da tarifa e da apresentação da apólice previstas no item anterior.
2.2.2.3.5 O credenciamento se consuma com a emissão do certificado da AC. Após o deferimento do credenciamento, a AC de nível imediatamente superior emitirá no máximo em 10 (dez) dias o certificado da AC credenciada, que terá um prazo máximo de 60 (sessenta) dias para entrar em operação.

2.2.3 Procedimentos para credenciamento de AR:

2.2.3.1 Solicitação
2.2.3.1.1 As solicitações dos candidatos ao credenciamento como AR na ICP -Brasil serão encaminhadas à AC ou candidato a AC a que o candidato a AR esteja operacionalmente vinculado, por intermédio de formulário SOLICITAÇÃO DE CREDENCIAMENTO DE AR [2]. A AC ou candidato a AC que receber a solicitação deverá manter cópia sob sua guarda e encaminhar para a AC Raiz os seguintes documentos:

a) o formulário SOLICITAÇÃO DE CREDENCIAMENTO DE AR [2], devidamente preenchido e assinado pelos representantes legais do candidato a AR e da AC ou do candidato a AC a que esteja operacionalmente vinculado;
b) documentos relacionados no Anexo II, exceto na hipótese de o candidato a AR ser a própria AC ou candidato a AC e indicar o mesmo endereço de instalação técnica.
c) identificação do local onde será guardada a documentação relativa aos certificados gerados pela AR;
d) relatório final de auditoria pré-operacional da AR, realizada observando o disposto no item 2.7 do documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [10]; ou declaração de que o referido relatório será encaminhado pela cadeia de AC para o endereço eletrônico auditoria@iti.gov.br ou perante o Protocolo-Geral da AC Raiz, assinada pelos responsáveis legais da AC; e
e) se for solicitado o credenciamento de PSS:
    i. formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS [3], devidamente preenchido e assinado pelos representantes legais dos candidatos a AR e a PSS;

ii. documentos relacionados no Anexo III; e
iii. documento indicando as atividades específicas para as quais postula o credenciamento como PSS, selecionando uma dentre as seguintes opções: (1) disponibilização de infra-estrutura física e lógica; (2) disponibilização de recursos humanos especializados; ou (3) disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

2.2.3.1.2 A solicitação de credenciamento será protocolada perante o Protocolo-Geral da AC Raiz e recebida, em até 30 (trinta) dias, por intermédio de despacho fundamentado.
2.2.3.1.3 Caso a solicitação de credenciamento não contenha todos os documentos relacionados nos anexos II ou III, quando for o caso, a AC Raiz determinará a intimação da candidata para que, sob pena de arquivamento do processo. supra as irregularidades no prazo máximo de 30 (trinta) dias, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.
2.2.3.2 Auditoria
2.2.3.2.1 Após a publicação do despacho de recebimento, a Diretoria de Auditoria, Fiscalização e Normalização examinará a documentação apresentada e poderá, caso julgue necessário, no prazo máximo de 30 (trinta) dias:

a) solicitar vista do material utilizado na auditoria (documentos, registros históricos e demais elementos materiais que deram subsídios à elaboração do relatório);
b) exigir documentação adicional contendo especificações sobre equipamentos, produtos de *hardware* e *software*, procedimentos técnicos e operacionais adotados pela candidata;
c) realizar auditoria pré-operacional por seu quadro próprio, elaborando relatório que prevalecerá sobre o apresentado pela candidata; ou
d) indeferir o pedido, caso não seja apresentado o relatório final de auditoria na forma descrita no item 2.2.3.1.1.

2.2.3.2.2 Com base no(s) relatório(s) finais de auditoria, a AC Raiz manifestar-se-á sobre o deferimento ou indeferimento da solicitação de credenciamento. Relatório final é aquele emitido quando a auditoria não detectar não-conformidades ou quando as não-conformidades apontadas em relatório preliminar já estiverem regularizadas e certificadas pela empresa que realizou o trabalho de auditoria.
2.2.3.2.3 Sobre a decisão de indeferimento de solicitação de credenciamento caberá recurso administrativo da candidata ao Comitê Gestor da ICP-Brasil.
2.2.3.3 Ato de credenciamento
2.2.3.3.1 O credenciamento do candidato a AR está condicionado ao credenciamento da AC a que está operacionalmente vinculado.
2.2.3.3.2 O deferimento ou o indeferimento do credenciamento será fundamentado e comunicado à AC que deu encaminhamento ao requerimento.
2.2.3.3.3 Caso a AR já esteja credenciada na ICP-Brasil e deseje se vincular a qualquer outra AC também credenciada, deve ser realizado procedimento de credenciamento simplificado, que consiste no encaminhamento de correspondência ao endereço eletrônico auditoria@iti.gov.br ou ao Protocolo-Geral da AC-Raiz, assinada pelos responsáveis legais da AC imediatamente subseqüente a AC Raiz, informando o que se segue:

- a data em que a AR iniciará as operações junto à AC subordinada;
- o local onde a AR irá armazenar os Termos de Titularidade correspondentes a esse novo credenciamento; e
- qual o instrumento legal, a exemplo de contrato ou convênio, utilizado para descrever as responsabilidades desse vínculo entre as entidades envolvidas.

2.2.5 Procedimentos para credenciamento de ACT

2.2.4.1 Solicitação

2.2.4.1.1 As solicitações dos candidatos ao credenciamento como ACT na ICP-Brasil serão encaminhadas à AC Raiz mediante a apresentação dos documentos a seguir relacionados:

a) formulário SOLICITAÇÃO DE CREDENCIAMENTO DE ACT [13] devidamente preenchido e assinado pelo representante legal do candidato a ACT;
b) documentos relacionados no Anexo IV;
c) se for o solicitado o credenciamento de PSS:
   i) formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS [3], devidamente preenchido e assinado pelos representantes legais dos candidatos a ACT e a PSS;
   ii) documentos relacionados no Anexo III; e
   iii) documento indicando as atividades específicas para as quais postula o credenciamento como PSS, selecionando uma dentre as seguintes opções: (1) disponibilização de infra-estrutura física e lógica; (2) disponibilização de recursos humanos especializados; ou (3) disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

2.2.4.1.2 A solicitação de credenciamento será protocolada perante o Protocolo-Geral da AC Raiz e recebida, em até 30 (trinta) dias, por intermédio de despacho fundamentado.

2.2.4.1.3 Caso a solicitação de credenciamento não contenha todos os documentos relacionados nos anexos IV ou III, quando for o caso, a AC Raiz determinará a intimação da candidata para que, sob pena de arquivamento do processo, supra as irregularidades no prazo máximo de 30 (trinta) dias, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.

2.2.4.2 Auditoria Pré-Operacional

2.2.4.2.1 Após a publicação do despacho de recebimento, o candidato a ACT deverá remeter à AC Raiz, no prazo máximo de 30 (trinta) dias, o formulário de REQUERIMENTO DE AUDITORIA [4], devidamente preenchido, declarando estar em conformidade com todos os requisitos exigidos pelas resoluções do CG da ICP-Brasil relacionados à atividade de autoridade certificadora e pronto para ser auditado no prazo de 15 (quinze) dias a contar daquele momento.

2.2.4.2.2 Tal requerimento deverá ser preenchido e assinado pelos representantes legais do candidato a ACT.

2.2.4.2.3 Durante as diligências de auditoria a AC Raiz poderá exigir documentação adicional contendo especificações sobre equipamentos, produtos de *hardware* e *software*, procedimentos técnicos e operacionais adotados pela candidata.

2.2.4.2.4 Caso o relatório de auditoria aponte o não-cumprimento de quaisquer dos critérios para credenciamento exigidos, a AC Raiz intimará a candidata para que os cumpra no prazo que fixar, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.

2.2.4.2.5 Após a comunicação da candidata de que atendeu os critérios de credenciamento apontados como não cumpridos no relatório de auditoria, a AC Raiz intimará a candidata, por meio de ofício enviado com comprovação de recebimento pelo destinatário, determinando a realização de auditoria complementar, de modo a verificar as medidas adotadas.

2.2.4.2.6 A desistência de solicitação de credenciamento em tramitação poderá ser requerida até a data em que for recebido na AC Raiz o REQUERIMENTO DE AUDITORIA [4].

2.2.4.2.7 Apresentado o relatório final de auditoria, a AC Raiz manifestar-se-á sobre o deferimento ou indeferimento da solicitação de credenciamento, no prazo máximo de 30 (trinta) dias.

2.2.4.2.8 Sobre a decisão de indeferimento de solicitação de credenciamento caberá recurso administrativo da candidata ao Comitê Gestor da ICP-Brasil.

2.2.4.3 Ato de credenciamento

2.2.4.3.1 O deferimento ou o indeferimento do credenciamento será fundamentado e comunicado ao candidato a ACT.

2.2.4.3.2 O ato de credenciamento da ACT será publicado pela AC Raiz no Diário Oficial da União e condicionará a emissão do(s) certificado(s) para os seus equipamentos:

a) ao pagamento da tarifa estabelecida nas DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [5];

b) à apresentação, pela ACT credenciada à AC Raiz, no prazo máximo de 10 (dez) dias após o deferimento do credenciamento, de apólice de contrato de seguro de cobertura de responsabilidade civil decorrente da atividade de emissão de carimbos do tempo, com cobertura suficiente e compatível com o risco dessa atividade.

2.2.4.3.3 A Administração Direta da União, dos Estados, do Distrito Federal e dos Municípios está dispensada do pagamento da tarifa e da apresentação da apólice previstas no item anterior.
2.2.4.3.4 O credenciamento se consuma com a emissão do(s) certificado(s) para os equipamentos da ACT, por AC credenciada na ICP-Brasil. Após o deferimento do credenciamento, a ACT terá um prazo máximo de 60 (sessenta) dias para entrar em operação.

2.2.5 Procedimentos para credenciamento de PSS

2.2.5.1 Solicitação
2.2.5.1.1 As solicitações dos candidatos ao credenciamento como PSS na ICP-Brasil serão encaminhadas à AC ou candidato a AC a que o candidato a PSS esteja operacionalmente vinculado, diretamente ou por intermédio de AR ou de candidato a AR, por meio do formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS [3].
2.2.5.1.2 A AC ou ACT ou candidato a AC que receber a solicitação deverá manter cópia sob sua guarda e encaminhar para a AC Raiz os seguintes documentos:

a) o formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS [3], devidamente preenchido e assinado pelos representantes legais da AC ou candidato a AC e da AR, ACT, se houver, por parte do candidato a PSS, intenção de vinculação operacional a uma AR;
b) relatório final de auditoria pré-operacional do PSS, realizada observado o disposto no item 2.7 do documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [10];
c) documentos relacionados no Anexo III; e
d) documento indicando as atividades específicas para as quais postula o credenciamento como PSS, selecionando uma dentre as seguintes opções:
   (1) disponibilização de infra-estrutura física e lógica;
   (2) disponibilização de recursos humanos especializados; ou
   (3) disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

2.2.5.1.3 A solicitação de credenciamento será protocolada perante o Protocolo-Geral da AC Raiz e recebida, em até 30 (trinta) dias, por intermédio de despacho fundamentado.
2.2.5.1.4 Caso a solicitação de credenciamento não contenha todos os documentos relacionados no anexo III, a AC Raiz determinará a intimação da candidata para que, sob pena de arquivamento do processo, supra as irregularidades no prazo máximo de 30 (trinta) dias, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.
2.2.5.2 Auditoria
2.2.5.2.1 Após a publicação do despacho de recebimento, a Diretoria de Auditoria, Fiscalização e Normalização examinará a documentação apresentada e poderá, caso julgue necessário:

a) solicitar vista do material utilizado na auditoria (documentos, registros históricos e demais elementos materiais que deram subsídios à elaboração do relatório);
b) exigir documentação adicional contendo especificações sobre equipamentos, produtos de *hardware* e *software*, procedimentos técnicos e operacionais adotados pela candidata; ou
c) realizar auditoria pré-operacional por seu quadro próprio, elaborando relatório que terá prevalência sobre o apresentado pela candidata.

2.2.5.2.2 Com base no(s) relatório(s) de auditoria, a AC Raiz manifestar-se-á sobre o deferimento ou indeferimento da solicitação de credenciamento, em até 30 (trinta) dias, por meio de despacho fundamentado.
2.2.5.2.3 Sobre a decisão de indeferimento de solicitação de credenciamento caberá recurso administrativo da candidata ao Comitê Gestor da ICP-Brasil.
2.2.5.3 Ato de credenciamento. O credenciamento do candidato a PSS estará condicionado ao credenciamento da AC, ACT ou da AR a que esteja operacionalmente vinculado. O deferimento ou o indeferimento do credenciamento será fundamentado e comunicado à AC ou ACT que deu encaminhamento ao requerimento.
2.2.5.4 Vedações ao credenciamento. É vedado o credenciamento e a contratação, pelas ARs, de PSS para executar as atividades de identificação e autenticação da identidade dos titulares e responsáveis pelo certificados previstas no item 3 do documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [10].

3. MANUTENÇÃO DO CREDENCIAMENTO

As entidades credenciadas deverão manter atendidos os critérios definidos no item 2.1.

3.1 Manutenção de credenciamento de AC

A entidade credenciada para desenvolver as atividades de AC deverá:
a) comunicar, desde logo, à AC Raiz ou à AC a que está subordinada:
   i. qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores;
   ii. desvinculação de AC, de AR ou de PSSs credenciados; ou
   iii. violação, de que tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil, cometida pelas ACs, ARs ou pelos PSSs que lhe sejam operacionalmente vinculados.
b) solicitar à AC Raiz autorização para alterar sua DPC**,** suas PCs ou sua Política de Segurança - PS, constantes dos documentos relacionados no Anexo I.
c) manter os titulares dos certificados informados acerca de eventual sucessão de AC ou AR operacionalmente vinculadas;
d) encaminhar à AC Raiz, até o dia 15 (quinze) de março de cada ano, cronograma das auditorias a serem realizadas, durante o ano, nas entidades que lhe sejam operacionalmente vinculadas;
e) encaminhar à AC Raiz relatórios de auditorias realizadas nas entidades que lhe sejam operacionalmente vinculadas, até 30 (trinta) dias após sua conclusão.

3.2 Manutenção de credenciamento de AR

A entidade credenciada para desenvolver as atividades de AR deverá:
a) comunicar, desde logo, à AC a que está operacionalmente vinculada:
   i. qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores;
   ii. desvinculação de PSS credenciado;
   iii. violação, de que tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil, por parte dos PSSs que lhe sejam operacionalmente vinculados;
b) observar a DPC, as PCs e a PS da AC a que estiver vinculada;
c) observar os procedimentos seguintes para abertura e extinção de instalações técnicas, postos provisórios e para celebração de acordos operacionais com outras ARs, quando for o caso.

3.2.1 Abertura de nova instalação técnica

3.2.1.1 Considera-se instalação técnica o ambiente físico de uma AR, cujo funcionamento foi autorizado pelo ITI, por tempo indeterminado, onde serão realizadas as atividades de validação e verificação da solicitação de certificados.
3.2.1.2 A AR já credenciada na ICP-Brasil poderá abrir novos endereços de instalações técnicas desde que encaminhe à AC Raiz solicitação de funcionamento, acompanhada dos seguintes documentos:

a) o formulário SOLICITAÇÃO DE FUNCIONAMENTO DE NOVOS ENDEREÇOS DE INSTALAÇÕES TÉCNICAS DE AR [6] devidamente preenchido e assinado pelos representantes legais da AR e da AC a que esteja operacionalmente vinculada;
b) indicação dos procedimentos que serão adotados quanto aos aspectos de segurança e operacionais;
c) nome e CPF das pessoas responsáveis por cada uma das novas instalações técnicas da AR;
d) nome e CPF dos agentes de registro que atuarão nas novas instalações técnicas da AR;
e) certidão da junta comercial ou alvará de funcionamento referente ao estabelecimento onde se localizará a instalação técnica e, nos casos de entidades públicas, cópia de publicação do ato que autoriza a operação naquele endereço; e
f) identificação do local onde será guardada a documentação relativa aos certificados gerados em cada instalação técnica.

3.2.1.3 Os serviços notariais e de registro, nos termos do art. 236 da Constituição Federal, desde que formalmente vinculados a uma AR já credenciada, poderão ser autorizados a funcionar como instalação técnica e seus delegados, prepostos e funcionários a atuar como agentes de registro.
3.2.1.3.1 A autorização para que os serviços notariais e de registro funcionem como instalação técnica de uma AR, requer:

a) celebração de contrato com uma AR, que deverá conter, no mínimo, as seguintes cláusulas:
   i) qualificação da AR credenciada e do titular da delegação do serviço notarial e de registro;
   ii) objeto detalhado das atividades a serem desenvolvidas;
   iii) designação do local onde será guardada a documentação relativa aos certificados gerados na instalação técnica;
   iv) responsabilidade objetiva e solidária do titular da delegação e da AR pelas atividades de validação e verificação da solicitação de certificados;
   v) compromisso de respeitar todas as regras da ICP-Brasil;
   vi) obrigação de a AR verificar a conformidade dos processos executados na instalação técnica;
   vii) prazo de vigência;
b) apresentação dos documentos previstos no subitem 3.2.1.2

3.2.1.4 Estando a documentação regular, a AC Raiz autorizará, em até 30 (trinta) dias, o funcionamento das novas instalações técnicas mediante intimação da AC solicitante, que a partir desse momento disponibilizará os novos endereços de instalações técnicas na página *web* da AC.
3.2.1.5 A AC Raiz poderá, a qualquer tempo, verificar a conformidade dos procedimentos e atividades das novas instalações técnicas das ARs com as práticas e regras estabelecidas pela ICP-Brasil. Quando constatada não conformidade em uma dessas instalações técnicas, a AC Raiz aplicará as sanções legais previstas no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7].

3.2.2 Extinção de Instalação Técnica

3.2.2.1 A extinção de uma instalação técnica de AR poderá se dar por determinação da AC Raiz ou por iniciativa da AC ou da AR vinculada.

3.2.2.2 Em qualquer dos casos, a AC à qual a AR esteja vinculada deverá realizar os seguintes procedimentos e manter os registros de sua execução para futuras auditorias de conformidade:

a) enviar ofício à AC Raiz informando a extinção da instalação técnica, a data de encerramento de suas atividades e a identificação da instalação técnica da AR que guardará a documentação relativa aos certificados gerados por aquela extinta;
b) guardar relatório com os nomes completos de todos os agentes de registro que emitiram certificados na instalação técnica extinta;
c) revogar, no sistema de certificação, as autorizações dos agentes de registro, caso não sejam aproveitados em outra instalação técnica da AR;
d) inventariar os certificados emitidos na instalação técnica;
e) transferir, de forma segura, a documentação dos certificados gerados na instalação técnica extinta para a instalação identificada na alínea a);
f) publicar, na página *web* da AC, informações sobre a extinção da instalação técnica da AR vinculada; e
g) enviar à AC Raiz, no prazo máximo de 60 (sessenta) dias da data de extinção informada na alínea "a", relatório descrevendo todos os procedimentos adotados.

3.2.2.4 Importante observar, que no caso de a AR possuir um único endereço de instalação técnica, a extinção deste, sem a abertura concomitante de um novo endereço de instalação técnica, implicará, automaticamente, o descredenciamento da AR, devendo ser observados os procedimentos definidos para tal caso.

3.2.3 Abertura de Posto Provisório

3.2.3.1 A AR já credenciada na ICP-Brasil poderá abrir postos provisórios de instalações técnicas com prazo máximo de 120 (cento e vinte) dias para funcionamento, renovável por igual período, desde que encaminhe à AC Raiz solicitação de funcionamento com no mínimo 10 (dez) dias de antecedência, acompanhada dos seguintes documentos:

a) Formulário SOLICITAÇÃO DE FUNCIONAMENTO DE POSTOS PROVISÓRIOS DE INSTALAÇÕES TÉCNICAS DE AR [8], devidamente preenchido e assinado pelos representantes legais da AR e da AC a que esteja operacionalmente vinculada;
b) indicação dos procedimentos que serão adotados quanto aos aspectos de segurança e operacionais;
c) indicação da pessoa responsável pelo posto provisório;
d) relação dos agentes de registro que trabalharão no posto provisório; e
e) identificação da instalação técnica da AR que guardará a documentação relativa aos certificados gerados pelo posto provisório, após o encerramento de suas atividades.

3.2.3.2 Estando a documentação regular, a AC Raiz autorizará o funcionamento do posto provisório mediante intimação da solicitante.

3.2.3.3 Não é necessário a autorização da AC Raiz para a AR já credenciada na ICP-Brasil que deseje abrir postos provisórios com prazo máximo de 15 (quinze) dias de funcionamento, sem período renovável, bastando para isso que seja encaminhada à AC Raiz, pela cadeia de AC, correspondência contendo as informações descritas no item 3.2.3.1, para o endereço eletrônico auditoria@iti.gov.br ou perante o Protocolo-Geral da AC Raiz, com no mínimo 5 (cinco) dias de antecedência.

3.2.4 Encerramento de Posto Provisório

Após o encerramento das atividades do posto provisório, deve ser enviado à AC Raiz relatório contendo:

a) quantidade de certificados emitidos pelo posto provisório e respectivos subtotais, categorizados por tipo de certificado;

b) nomes completos de todos os agentes de registro que efetivamente emitiram certificados no posto provisório.
c) outras informações sobre o evento, julgadas relevantes.

3.2.5 Celebração de Acordo Operacional

3.2.5.1 A AR já credenciada na ICP-Brasil poderá celebrar acordo operacional com outra AR também credenciada na ICP-Brasil, para que esta última execute, em nome da primeira, as seguintes atividades:

a) Confirmação da identidade do titular ou do responsável pelo certificado – processo realizado mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos;
b) Validação da solicitação de certificado - conferência dos dados da solicitação de certificado com os constantes dos documentos necessários para autenticação da identidade de um indivíduo ou de uma organização;
c) Aprovação da solicitação de certificado - confirmação da validação realizada e liberação da emissão do certificado no sistema da AC.

3.2.5.2 Para tanto, as ACs que possuem vínculos com as ARs que firmarem acordos operacionais, deverão comunicar a AC-Raiz, no prazo de 10 (dez) dias úteis, as seguintes informações:

a) A Identificação das ARs (nome da AR contratante/AC e nome da AR contratada/AC vinculada);
b) Validade do Acordo (dd/mm/aaaa até dd/mm/aaaa).

3.2.5.3 As ARs convenentes deverão manter cópia dos Acordos Operacionais firmados e as ACs às quais estas ARs estão vinculadas deverão publicar à lista de ARs que participam de Acordos Operacionais.
3.2.5.4 A AC Raiz poderá, a qualquer tempo, verificar a conformidade dos procedimentos e atividades das ARs com as práticas e regras estabelecidas pela ICP-Brasil. Quando constatada não conformidade, a AC Raiz aplicará as sanções legais previstas no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7].

3.3 Manutenção de credenciamento de ACT

A entidade credenciada para desenvolver as atividades de ACTs deverá:

a) comunicar, desde logo, à AC Raiz:
   i) qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores;
   ii) desvinculação de PSSs credenciados; ou
   iii) violação, de que tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil, cometida pelos PSSs que lhe sejam operacionalmente vinculados.
b) solicitar à AC Raiz autorização para alterar sua DPCT**,** suas PCTs ou sua Política de Segurança (PS), constantes dos documentos relacionados no Anexo IV.
c) encaminhar à AC Raiz, até o dia 15 (quinze) de março de cada ano, cronograma das auditorias a serem realizadas, durante o ano, nas suas instalações técnicas;
d) encaminhar à AC Raiz relatórios de auditorias realizadas nas suas instalações técnicas, até 30 (trinta) dias após a conclusão das mesmas.

3.4 Manutenção de credenciamento de PSS

A entidade credenciada para desenvolver as atividades de PSS deverá:

a) Comunicar à ACT ou AC a que estiver operacionalmente vinculada, diretamente ou por intermédio de AR, qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores;
b) Observar a DPC, as PCs e a PS da AC a que estiver vinculada, diretamente ou por intermédio de AR, ou a DPCT, as PCTs ou PS da ACT.

4. DESCREDENCIAMENTO

4.1 Descredenciamento de AC

4.1.1 Requisitos Gerais para o descredenciamento de AC

4.1.1.1 O descredenciamento de uma AC pode ocorrer em relação a todas as PCs para qual tenha sido credenciada ou em relação a PC específicas.
4.1.1.2 O descredenciamento de uma AC para todas as PCs credenciadas enseja a revogação do correspondente certificado e o descredenciamento de todas as entidades que lhe sejam operacionalmente vinculadas: AC subseqüentes, AR ou PSS.

4.1.2 Hipóteses para o descredenciamento de AC

a) Quando da expiração do prazo de validade de certificado da AC, sem que haja a emissão de novo certificado para substituí-lo;
b) Quando do descredenciamento da AC de nível imediatamente superior;
c) Quando do descredenciamento de AR única vinculada, sem que haja a solicitação de credenciamento de nova AR;
d) Quando do descredenciamento de PSS único vinculado, que desempenhe atividades descritas nas DPCs e PCs da AC, de modo a inviabilizar a continuidade de operação da AC, sem que haja a solicitação de credenciamento de novo PSS e sem que a AC passe a desempenhar, ela própria, as atividades antes executadas pelo PSS;
e) A pedido da própria AC, mediante requerimento, em relação às suas atividades;
f) Por determinação da AC Raiz, em razão de descumprimento de qualquer dos critérios e procedimentos exigidos para o seu funcionamento, após o decurso do prazo para regularização, sem que a entidade tenha sanado a irregularidade e mediante processo administrativo.

4.1.3 Procedimentos para descredenciamento de AC

4.1.3.1 Descredenciamento solicitado pela própria AC
Na hipótese de o descredenciamento ser solicitado pela própria AC, deverão ser obedecidos os seguintes procedimentos:

a) a AC comunicará, com 120 (cento e vinte) dias de antecedência, diretamente à AC Raiz e às entidades a ela vinculadas, e publicará em sua página *web*, para conhecimento dos titulares de certificados emitidos, a decisão de encerrar suas atividades de emissão de certificados no âmbito da ICP-Brasil ou de não mais emitir certificados sob as PCs especificadas; e
b) a AC divulgará, pelos 90 (noventa) dias imediatamente anteriores à expiração do certificado, em sua página *web*, a decisão de encerrar suas atividades no âmbito da ICP-Brasil ou de não mais emitir certificados sob as PCs especificadas.

4.1.3.2 Descredenciamento por determinação da AC Raiz
Na hipótese de descredenciamento da AC por determinação da AC Raiz, deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz comunicará à AC o seu descredenciamento, com relação às PCs que especificar;
b) as ACs descredenciadas sob esta hipótese ficam impedidas de apresentar novo pedido de credenciamento pelo prazo de 6 (seis) meses contados da publicação de que trata o item 4.1.2.2.a.

4.1.3.3 Descredenciamento por qualquer das hipóteses previstas

Em qualquer das hipóteses de descredenciamento de AC deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz divulgará o fato, logo após a consumação da respectiva hipótese, no Diário Oficial da União e em sua página *web;*
b) As ACs subseqüentes, ARs e PSSs operacionalmente vinculados deverão cessar, em relação às PCs objeto do descredenciamento, suas atividades de emissão de certificados no âmbito da ICP-Brasil, imediatamente após a comunicação de que trata a alínea anterior
c) Em caso de descredenciamento total de uma AC:
   i. As chaves públicas dos certificados por ela emitidos deverão ser armazenadas por outra AC, após aprovação da AC Raiz;
   ii. Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas aquela indicada pela AC que encerra as suas atividades;
   iii. A AC que encerra as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas; e
   iv. Caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.

4.2 Descredenciamento de AR

O descredenciamento de uma AR enseja o descredenciamento de PSS que lhe seja operacionalmente vinculado e implicará a paralisação automática das operações de todas as suas instalações técnicas.

4.2.1. Hipóteses para o descredenciamento de AR

São as seguintes as hipóteses para descredenciamento de AR:

a) Quando do descredenciamento da AC a que esteja operacionalmente vinculada;
b) Quando da extinção do endereço de instalação técnica único da AR, sem que haja a solicitação de abertura de um novo endereço de instalação técnica;
c) Quando do descredenciamento de PSS único vinculado operacionalmente à AR, que desempenhe atividades descritas na DPC e PCs da AC à qual a AR esteja operacionalmente vinculada, de modo a inviabilizar a continuidade de operação da AR, sem que haja a solicitação de credenciamento de novo PSS;
d) A pedido da AC à qual a AR esteja operacionalmente vinculada, mediante requerimento, em relação às atividades da AR; ou
e) Por determinação da AC Raiz, em razão do descumprimento dos critérios e procedimentos exigidos para o seu funcionamento, após o decurso do prazo para regularização, sem que a entidade tenha sanado a irregularidade e mediante processo administrativo.

4.2.2 Procedimentos para descredenciamento de AR

4.2.2.1 Descredenciamento solicitado pela própria AC

4.2.2.1.1 Na hipótese de descredenciamento de AR a pedido da AC à qual a AR esteja operacionalmente vinculada, a AC enviará o respectivo requerimento à AC Raiz, informando:

a) O motivo do descredenciamento;
b) A data de encerramento das atividades da AR; e
c) A identificação da AC ou AR que guardará a documentação relativa aos certificados gerados por aquela extinta.

4.2.2.1.2 Caso necessário realizar a guarda da documentação relativa aos certificados emitidos em local ou entidade que não pertença à ICP-Brasil, deverá ser solicitada autorização ao Comitê Gestor da ICP-Brasil.
4.2.2.2 Descredenciamento por determinação da AC Raiz.
Na hipótese de descredenciamento da AR por determinação da AC Raiz, deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz comunicará à AC e à AR o seu descredenciamento;
b) as ARs descredenciadas por determinação da AC Raiz ficam impedidas de apresentar novo pedido de credenciamento pelo prazo de 6 (seis) meses contados da publicação de que trata a alínea 4.2.2.3.a;
c) nos casos de reincidência de descredenciamento por determinação da AC Raiz, as ARs descredenciadas ficam impedidas de apresentar novo pedido de credenciamento pelo prazo de 5 anos, contados da data da publicação de que trata a alínea 4.2.2.3.a.

4.2.2.3 Descredenciamento por qualquer das hipóteses previstas
Em qualquer das hipóteses de descredenciamento de AR deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz divulgará o fato, logo após a consumação da respectiva hipótese, no Diário Oficial da União e em sua página *web;*
b) imediatamente após a publicação referida na alínea anterior, a AC à qual a AR descredenciada estava operacionalmente vinculada deverá adotar os seguintes procedimentos, mantendo a guarda de toda a documentação comprobatória em seu poder:
   i. revogar, no sistema de certificação, as autorizações dos agentes de registro da AR descredenciada;
   ii. inventariar os certificados emitidos pela AR;
   iii. transferir, de forma segura, a documentação dos certificados gerados pela AR descredenciada para o local identificado no requerimento de descredenciamento;
   iv. publicar, em sua página *web*, informação sobre o descredenciamento da AR; e
   v. enviar à AC Raiz, no prazo máximo de 60 (sessenta) dias da publicação referida na alínea 4.2.2.3.a. relatório descrevendo todos os procedimentos adotados.

4.3 Descredenciamento de ACT

4.3.1 Requisitos Gerais para o descredenciamento de ACT

4.3.1.1 O descredenciamento de uma ACT pode ocorrer em relação a todas as PCTs para as quais tenha sido credenciada ou em relação a PCT específicas.
4.3.1.2 O descredenciamento de uma ACT para todas as PCTs credenciadas enseja a revogação dos correspondentes certificados e o descredenciamento de todos os PSSs que lhe sejam operacionalmente vinculados.

4.3.2 Hipóteses para o descredenciamento de ACT

a) A pedido da própria ACT, mediante requerimento, em relação às suas atividades;
b) Quando do descredenciamento de PSS único vinculado, que desempenhe atividades descritas na DPCT e PCTs da ACTs, de modo a inviabilizar a continuidade de operação da ACT, sem que haja a solicitação de credenciamento de novo PSS e sem que a ACT passe a desempenhar, ela própria, as atividades antes executadas pelo PSS;
c) Por determinação da AC Raiz, em razão de descumprimento de qualquer dos critérios e procedimentos exigidos para o seu funcionamento, após o decurso do prazo para regularização, sem que a entidade tenha sanado a irregularidade e mediante processo administrativo.

4.3.3 Procedimentos para descredenciamento de ACT

4.3.3.1 Descredenciamento solicitado pela própria ACT
Na hipótese de o descredenciamento ser solicitado pela própria ACT, deverão ser obedecidos os seguintes procedimentos:

a) a ACT comunicará, com 120 (cento e vinte) dias de antecedência, diretamente à AC Raiz e às entidades a ela vinculadas, e publicará em sua página *web*, para conhecimento dos subscritores, a decisão de encerrar suas atividades de emissão de carimbo do tempo no âmbito da ICP-Brasil ou de não mais emitir carimbos sob as PCTs especificadas; e
b) a ACT divulgará, pelos 90 (noventa) dias imediatamente anteriores ao encerramento, em sua página *web*, a decisão de encerrar suas atividades no âmbito da ICP-Brasil ou de não mais emitir certificados sob as PCTs especificadas.

4.3.3.2 Descredenciamento por determinação da AC Raiz
Na hipótese de descredenciamento da ACT por determinação da AC Raiz, deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz comunicará à ACT o seu descredenciamento, com relação às PCTs que especificar;
b) as ACTs descredenciadas sob esta hipótese ficam impedidas de apresentar novo pedido de credenciamento pelo prazo de 6 (seis) meses contados da publicação de que trata o item 4.4.3.2.a.

4.3.3.3 Descredenciamento por qualquer das hipóteses previstas
Em qualquer das hipóteses de descredenciamento de ACT deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz divulgará o fato, logo após a consumação da respectiva hipótese, no Diário Oficial da União e em sua página *web;*
b) Os PSSs operacionalmente vinculados deverão cessar, em relação às PCT objeto do descredenciamento, suas atividades de emissão de carimbos do tempo no âmbito da ICP-Brasil, imediatamente após a comunicação de que trata a alínea anterior
c) Em caso de descredenciamento total de uma ACT:
   i) A ACT ou a AC Raiz, conforme o caso, solicitará à AC emitente a revogação do(s) certificados(s) digital(is) do(s) equipamento(s) de carimbo do tempo da ACT descredenciada;
   ii) A ACT que encerra as suas atividades transferirá os documentos e *logs* de auditoria gerados durante sua operação para outra ACT interessada ou, na falta dessa, à AC Raiz, para guarda pelo período estipulado nos regulamentos da ICP-Brasil.

4.4 Descredenciamento de PSS

4.4.1 Hipóteses para o descredenciamento de PSS

a) Quando do descredenciamento da AC ou AR a que esteja operacionalmente vinculado;
b) A pedido da AC ou AR à qual esteja operacionalmente vinculado, mediante requerimento, em relação às atividades do PSS; ou
c) Por determinação da AC Raiz em razão de descumprimento de qualquer dos critérios e procedimentos exigidos para o seu funcionamento.

4.4.2 Procedimentos para descredenciamento de PSS

4.4.2.1 Descredenciamento solicitado pela própria AC ou ACT
Na hipótese de descredenciamento de PSS a pedido da AC ou ACT à qual o PSS esteja operacionalmente vinculado, a AC ou ACT enviará o respectivo requerimento à AC Raiz, informando:

a) o motivo do descredenciamento e
b) a data de encerramento das atividades do PSS.

4.4.2.2 Descredenciamento por determinação da AC Raiz.
Na hipótese de descredenciamento de PSS por determinação da AC Raiz, deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz comunicará à AC ou ACT e ao PSS o seu descredenciamento;
b) Os PSSs descredenciados por determinação da AC Raiz ficam impedidos de apresentar novo pedido de credenciamento pelo prazo de 6 (seis) meses contados da publicação de que trata a alínea 4.4.2.b;
c) Nos casos de reincidência de descredenciamento por determinação da AC Raiz, os PSSs descredenciados ficam impedidos de apresentar novo pedido de credenciamento pelo prazo de 5 anos, contados da data da publicação de que trata a alínea 4.3.2.c.

4.3.2.3 Descredenciamento por qualquer das hipóteses previstas
Em qualquer das hipóteses de descredenciamento de PSS deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz divulgará o fato, logo após a consumação da respectiva hipótese, no Diário Oficial da União e em sua página *web*;
b) Imediatamente após a publicação referida na alínea anterior, a AC à qual o PSS descredenciado estava operacionalmente vinculado, diretamente ou por intermédio de AR, deverá adotar os seguintes procedimentos, mantendo a guarda de toda a documentação comprobatória em seu poder:
   i. publicar, em sua página *web*, informação sobre o descredenciamento do PSS e o credenciamento de novo PSS, se for o caso; e
   ii. enviar à AC Raiz, no prazo máximo de 60 (sessenta) dias da publicação referida na alínea 4.3.2.3.a, relatório descrevendo todos os procedimentos adotados.

4.5 Obrigações Subsistentes

As ACs, as ARs e os PSSs operacionalmente vinculados têm o dever de observar as diretrizes e normas técnicas da ICP-Brasil, inclusive as obrigações que subsistirem após o encerramento das atividades de emissão de certificados.

5. DOCUMENTOS REFERENCIADOS

5.1 Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	*Nome do documento*	*Código*
[5]	DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06
[7]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[10]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[11]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[12]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02

5.2 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	*Nome do documento*	*Código*
[9]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL	DOC-ICP-03.01

5.3 Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br.

Ref.	*Nome do documento*	*Código*
[1]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE AC	ADE-ICP-03.A
[2]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE AR	ADE-ICP-03.B
[3]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS	ADE-ICP-03.C
[4]	Formulário REQUERIMENTO DE AUDITORIA	ADE-ICP-03.D
[6]	Formulário SOLICITAÇÃO DE FUNCIONAMENTO DE NOVOS ENDEREÇOS DE INSTALAÇÕES TÉCNICAS DE AR	ADE-ICP-03.E
[8]	Formulário SOLICITAÇÃO DE FUNCIONAMENTO DE POSTOS PROVISÓRIOS DE INSTALAÇÕES TÉCNICAS DE AR	ADE-ICP-03.F
[13]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE ACT	ADE-ICP-03.G

ANEXO I - DOCUMENTOS PARA CREDENCIAMENTO DE AC

O candidato a desenvolver as atividades de AC deve entregar à AC Raiz os seguintes documentos atualizados:

1. Relativos a sua habilitação jurídica:
   a) Ato constitutivo, devidamente registrado no órgão competente; e
   b) documentos da eleição de seus administradores, quando aplicável;

2. Relativos a sua regularidade fiscal:
   a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;
   b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
   c) Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e
   d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

3. Relativos a sua qualificação econômico-financeira:
   a) Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI) [1], afirmando que o candidato se encontra em boa situação financeira para a execução das atividades a que se propõe, junto à ICP-Brasil.
   b) Certidão negativa de falência ou concordata expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente.

4. Relativos a sua qualificação técnica:
   a) Declaração de Práticas de Certificação - DPC, atendendo às condições mínimas estabelecidas pelo documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [10];
   b) Políticas de Certificado (PC), atendendo às condições mínimas estabelecidas pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [11];
   c) Política de Segurança - PS, atendendo às condições mínimas estabelecidas na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[12]; e
   d) Documento indicando se pretende emitir certificados para AC de nível imediatamente subseqüente ao seu e, nesse caso, incluir os critérios e procedimentos de auditoria que pretende adotar em relação a essas ACs.

NOTA 1: Na hipótese de o candidato já estar credenciado como AC em relação a outra PC, o documento a apresentar fica restrito àquele descrito no item 4, alínea “b”. Nessa mesma hipótese, todos os demais documentos deverão ser reapresentados apenas se modificados em relação às versões anteriormente entregues.

NOTA 2: Na hipótese de o candidato a AC ser pessoa jurídica de direito público deverá apresentar a seguinte documentação, se aplicável:
a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;
b) Ato constitutivo;
c) Prova de regularidade junto às Fazendas Públicas Federal, Estaduais e Municipais do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

1 O Cadastro Nacional de Auditores Independentes (CNAI) está regulamentado pela Resolução CFC nº 1.019, de 18 de fevereiro de 2005

d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

NOTA 3: As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores – SICAF, registro cadastral oficial do Poder Executivo Federal, poderão, para fins do disposto no item 2, apresentar seu extrato.

NOTA 4: As ACs que estiverem se credenciando com o objetivo de emitir certificados exclusivamente para AC subseqüentes ficam dispensadas da apresentação de PC, devendo, todavia, a DPC incorporar todas as informações que deveriam constar na PC.

ANEXO II - DOCUMENTOS PARA CREDENCIAMENTO DE AR

O candidato a desenvolver as atividades de AR deve entregar à AC Raiz, por intermédio da AC ou candidato a AC a que esteja operacionalmente vinculado, os seguintes documentos atualizados:

1. Relativos a sua habilitação jurídica:
   a) ato constitutivo, devidamente registrado no órgão competente; e
   b) documentos da eleição de seus administradores, quando aplicável.

2. Relativos a sua regularidade fiscal:
   a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;
   b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
   c) Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e
   d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

3. Relativos a sua qualificação econômico-financeira:
   a) Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI) [2], afirmando que o candidato se encontra em boa situação financeira para a execução das atividades a que se propõe, junto à ICP-Brasil.
   b) Certidão negativa de falência ou concordata expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente.

4. Relativos aos contratos:
   a) Minuta do contrato ou do convênio com a AC a que está operacionalmente vinculada;
   b) Minuta do contrato ou do convênio com o PSS operacionalmente vinculado, se for o caso;
   c) Minuta dos termos de titularidade.

NOTA 1: Fica dispensado da entrega dos documentos descritos neste Anexo o candidato já credenciado como AR em relação a outra PC, exceto quando houver modificação dos mesmos em relação às versões anteriormente entregues.

NOTA 2: Na hipótese de o candidato a AR ser pessoa jurídica de direito público deverá apresentar a seguinte documentação, se aplicável:
a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;
b) Ato constitutivo;
c) Prova de regularidade junto às Fazendas Públicas Federal, Estaduais e Municipais do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e
d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

NOTA 3: As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores – SICAF, registro cadastral oficial do Poder Executivo Federal, poderão, para fins do disposto no item 2, apresentar seu extrato.

2 O Cadastro Nacional de Auditores Independentes (CNAI) está regulamentado pela Resolução CFC nº 1.019, de 18 de fevereiro de 2005

ANEXO III - DOCUMENTOS PARA CREDENCIAMENTO DE PSS

O candidato a desenvolver as atividades de PSS deve entregar à AC Raiz, por intermédio da AC ou candidato a AC a que esteja operacionalmente vinculado, os seguintes documentos atualizados:

1. Relativos a sua habilitação jurídica:
   a) ato constitutivo, devidamente registrado no órgão competente; e
   b) documentos da eleição de seus administradores, quando aplicável.

2. Relativos a sua regularidade fiscal:
   a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;
   b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
   c) Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e
   d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

3. Relativos a sua qualificação econômico-financeira:
   a) Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI) [3], afirmando que o candidato se encontra em boa situação financeira para a execução das atividades a que se propõe, junto à ICP-Brasil.
   b) Certidão negativa de falência ou concordata expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente.

NOTA 1: Fica dispensado da entrega dos documentos descritos neste Anexo o candidato já credenciado como PSS em relação a outra PC, exceto quando houver modificação dos mesmos em relação às versões anteriormente entregues.

NOTA 2: Na hipótese de o candidato a PSS ser pessoa jurídica de direito público deverá apresentar a seguinte documentação, se aplicável:
a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;
b) Ato constitutivo;
c) Prova de regularidade junto às Fazendas Públicas Federal, Estaduais e Municipais do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e
d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

NOTA 3: As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores – SICAF, registro cadastral oficial do Poder Executivo Federal, poderão, para fins do disposto no item 2, apresentar seu extrato.

3 O Cadastro Nacional de Auditores Independentes (CNAI) está regulamentado pela Resolução CFC nº 1.019, de 18 de fevereiro de 2005

ANEXO IV - DOCUMENTOS PARA CREDENCIAMENTO DE ACT

O candidato a desenvolver as atividades de ACT deve entregar à AC Raiz os seguintes documentos atualizados:

1. Relativos a sua habilitação jurídica:
   a) Ato constitutivo, devidamente registrado no órgão competente; e
   b) documentos da eleição de seus administradores, quando aplicável;

2. Relativos a sua regularidade fiscal:
   a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
   b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
   c) Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e
   d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

3. Relativos a sua qualificação econômico-financeira:
   a) Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI) [4], afirmando que o candidato se encontra em boa situação financeira para a execução das atividades a que se propõe, junto à ICP-Brasil.
   b) Certidão negativa de falência ou concordata expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente.

4. Relativos a sua qualificação técnica:
   a) Declaração de Práticas de Carimbo do Tempo (DPCT), atendendo às condições mínimas estabelecidas pelo documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DE TEMPO DA ICP- BRASIL [15];
   b) Políticas de Carimbo de Tempo (PCT), atendendo às condições mínimas estabelecidas pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DE TEMPO NA ICP-BRASIL [16]; e
   c) Política de Segurança (PS), atendendo às condições mínimas estabelecidas na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[12].

NOTA 1: Na hipótese de o candidato já estar credenciado como ACT em relação a outra PCT, o documento a apresentar fica restrito àquele descrito no item 4, alínea "b". Nessa mesma hipótese, todos os demais documentos deverão ser reapresentados apenas se modificados em relação às versões anteriormente entregues.

NOTA 2: Na hipótese de o candidato a ACT ser pessoa jurídica de direito público deverá apresentar a seguinte documentação, se aplicável:
a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
b) Ato constitutivo;
c) Prova de regularidade junto às Fazendas Públicas Federal, Estaduais e Municipais do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e
d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de

4 O Cadastro Nacional de Auditores Independentes (CNAI) está regulamentado pela Resolução CFC nº 1.019, de 18 de fevereiro de 2005

Serviço (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

NOTA 3: As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores (SICAF), registro cadastral oficial do Poder Executivo Federal, poderão, para fins do disposto no item 2, apresentar seu extrato.

ANEXO B - CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES DA ICP-BRASIL

Infra-Estrutura de Chaves Públicas Brasileira

CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES DA ICP-BRASIL (DOC-ICP-08)

Versão 4.0

18 de novembro de 2009

Infra-Estrutura de Chaves Públicas Brasileira

RESUMO

Infra-Estrutura de Chaves Públicas Brasileira

LISTA DE ACRÔNIMOS

AC – Autoridade Certificadora
AC Raiz – Autoridade Certificadora Raiz da ICP-Brasil **ACT –** Autoridade de Carimbo de Tempo
AR – Autoridade de Registro
AUDIBRA –Instituto dos Auditores Internos do Brasil
CD – *Compact Disc*
CG – Comitê Gestor da ICP-Brasil
CFC – Conselho Federal de Contabilidade
CGU – Controladoria Geral da União
CGAF – Coordenação Geral de Auditoria e Fiscalização
CMMI – *Capability Maturity Model Integration*
CNPJ – Cadastro Nacional de Pessoas Jurídicas
COBIT – *Control Objectives for Information and related Technology* **COSO –** *Committee of Sponsoring Organizations*
CVM – Comissão de Valores Mobiliários
DAFN – Diretoria de Auditoria, Fiscalização e Normalização **DOU –** Diário Oficial da União
DVD – *Digital Versatile Disc*
FGTS – Fundo de Garantia do Tempo de Serviço **IBRACON –** Instituto dos Auditores Independentes do Brasil **ICP-Brasil –** Infra-Estrutura de Chaves Públicas Brasileira
IIA – *Institute of Internal Auditors*
ISACA – *Information Systems Audit and Control Association*
IEC – *International Electrotechnical Commission*
ISO – *International Organization for Standardization*
ITIL – *Information Technology Infrastructure Library*
MPS-BR – Melhoria de Processo do Software Brasileiro
PDF – *Portable Document Format*
PLAAO – Plano Anual de Auditoria Operacional
PSC – Prestadores de Serviço de Certificação
PSS – Prestadores de Serviço de Suporte
SHA – *Secure Hash Algorithm*
SICAF – Sistema de Cadastramento Unificado de Fornecedores
TAR – *Tape Archive*
TCU – Tribunal de Contas da União

1. DISPOSIÇÕES GERAIS

e) Este documento regula, no âmbito da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, as atividades de auditoria, a serem realizadas em sua cadeia de certificação digital.
f) O código de ética e os princípios éticos para o exercício das atividades de auditoria interna e independente estabelecidos pelos diversos órgãos reguladores ou de classe (TCU, CGU, CFC, CVM, IBRACON, ISACA, AUDIBRA e IIA), integram, para todos os fins este normativo. As demais normas emitidas pelos citados órgãos serão observadas naquilo em que não conflitarem com este documento.
e) No presente documento o conceito de ***METODOLOGIA*** de auditoria se refere a todo o instrumental necessário à realização de trabalhos de auditoria como: manuais, roteiros, papéis de trabalho, mapa de riscos, procedimentos, técnicas, formulários, relatórios e modelos.
f) Toda correspondência tratada neste documento deve ser formalizada, preferencialmente, por meio de correio eletrônico, endereçado à Diretoria de Auditoria, Fiscalização e Normalização (auditoria@iti.gov.br), em conformidade com o ADE-ICP-08-H[9], ou na sua impossibilidade, por ofício da autoridade competente.
g) Todas as comunicações e requerimentos á AC Raiz, deverão ser encaminhados por intermédio da cadeia de AC, ou candidatos a AC, operacionalmente vinculados. Inicia-se a tramitação pela AC de nível imediatamente superior ao do interessado. A tramitação prossegue, a partir daí, respeitando a hierarquia de AC, operacionalmente vinculados, até chegar á AC Raiz.
h) As notificações e intimações de que trata este documento serão realizadas, preferencialmente, por correio eletrônico assinado digitalmente, ou na sua impossibilidade, por ofício da autoridade competente.

2. TIPOS DE AUDITORIA

2.1 As auditorias são classificadas em **PRÉ-OPERACIONAIS** e **OPERACIONAIS**, a saber:

a) **Pré-operacionais**: são as auditorias realizadas antes do início das atividades do candidato a Prestador de Serviço de Certificação (PSC), quer seja Autoridade Certificadora (AC), Autoridade de Carimbo do Tempo (ACT), Autoridade de Registro (AR) ou Prestador de Serviço de Suporte (PSS).

b) **Operacionais**: são as auditorias realizadas anualmente – considerado o ano civil –, em todos os PSC para manutenção do credenciamento junto à ICP -Brasil. Tais auditorias ocorrerão a partir do primeiro ano civil seguinte à data do DOU que publicar o credenciamento do PSC.

3. ENTIDADES QUE PODEM REALIZAR AUDITORIAS

3.1 As auditorias na cadeia da ICP-Brasil são realizadas exclusivamente pelo Comitê Gestor da ICP-Brasil, pelo Instituto Nacional de Tecnologia da Informação (ITI) ou por entidades credenciadas para o fim, observada a seguinte tabela:

Entidade	EXECUTOR DA AUDITORIA	
	Pré-operacional	**Operacional**
AC Raiz	Comitê Gestor da ICP-Brasil ou seus prepostos, formalmente designados	Comitê Gestor da ICP-Brasil ou seus prepostos, formalmente designados
AC de 1º Nível [1], e seus PSS	ITI/DAFN/CGAF	ITI/DAFN/CGAF
AC subseqüente [2] e seus PSS	ITI/DAFN/CGAF	Empresa de Auditoria Independente credenciada junto ao ITI
ACT	ITI/DAFN/CGAF	Empresa de Auditoria Independente credenciada junto ao ITI
AR	Empresa de Auditoria Independente credenciada junto ao ITI	Auditoria Interna da respectiva AR credenciada junto ao ITI Empresa de Auditoria Independente credenciada junto ao ITI
AR no Exterior	ITI/DAFN/CGAF ou, a seu critério, Empresa de Auditoria Independente credenciada junto ao ITI	Empresa de Auditoria Independente credenciada junto ao ITI Auditoria Interna da respectiva AR credenciada junto ao ITI
PSS de AR	Empresa de Auditoria Independente credenciada junto ao ITI	Empresa de Auditoria Independente credenciada junto ao ITI Auditoria Interna da respectiva AR credenciada junto ao ITI

e) O ITI poderá, a seu exclusivo critério ou por determinação do Comitê Gestor, executar auditorias pré-operacionais e operacionais em quaisquer das entidades integrantes ou candidatas a integrar a ICP-Brasil, utilizando servidores do quadro próprio do ITI/DAFN/CGAF, devidamente qualificados.
f) As auditorias operacionais realizadas pelo ITI com base na prerrogativa do item anterior, não supre a exigência de realização de auditoria operacional a ser realizada em conformidade com o item 2.1.”b” acima.

4. CREDENCIAMENTO DE EMPRESAS DE AUDITORIA INDEPENDENTE E ÓRGÃOS DE AUDITORIA INTERNA

4.1 São dois (2) os tipos de entidades credenciadas para realizar auditoria na cadeia da ICP-Brasil:
a) Tipo 1: entidades autorizadas a realizar auditoria em AC, ACT, AR e respectivos PSS, este tipo é destinado às empresas de Auditoria Independente cadastradas junto ao CNAI.
b) Tipo 2: entidades autorizadas a realizar auditoria somente em AR e respectivos PSS, este tipo é destinado às empresas enquadradas na alínea anterior e às unidades de Auditoria Interna formalmente instituídas.

1 Aquela cujo certificado é emitido pela AC Raiz

2 Aquela cujo certificado não é emitido pela AC Raiz

4.2 As entidades de auditoria independente candidatas a realizar trabalhos de auditoria na cadeia da ICP-Brasil, indicarão o tipo a que pleiteiam e apresentarão o formulário ADE-ICP-08.A[1], anexando:

2 documentação demonstrando que a estrutura organizacional e a metodologia de auditoria são claras e, formalmente definidas, para permitir a realização de trabalhos de auditoria;

3 documentação indicando que o sistema de controle de qualidade formalmente estabelecido atende às normas profissionais vigentes e são adotados procedimentos que garantam o seu cumprimento na realização dos trabalhos de auditoria;

4 comprovação de constituição legalmente registrada; onde conste a atividade de auditoria de sistemas ou de tecnologia da informação no objeto social da candidata;

5 comprovação de inscrição no Cadastro Nacional da Pessoa Jurídica;

6 comprovação de inscrição estadual e municipal, relativo ao domicílio sede da candidata;

7 certidões negativas de débitos junto as fazendas Federal, Estadual e Municipal; inclusive Seguridade Social e ao Fundo de Garantia do Tempo de Serviço;

8 certidão negativa de falência e de recuperação judicial;

9 certidão negativa de execução patrimonial;

10 declaração de que não está cumprindo nenhuma penalidade da Administração Pública Federal, Estadual e Municipal;

11 declaração de que não foi declarada inidônea nas esferas de Governo Federal, Estadual e Municipal;

12 currículo dos sócios, dos diretores e dos responsáveis técnicos que integram o quadro de auditores com poderes para emitir e assinar relatório de auditoria em nome da candidata;

13 atestado de capacidade técnica, emitido por pessoa jurídica que comprove a execução de serviços em auditoria de software ou de sistemas de informação, bem como comprove a quantidade de horas de serviços de auditoria prestada;

14 rol dos trabalhos realizados nos últimos 2 (dois) anos, contendo tabela indicando:

I. a classificação dos serviços realizados;

II. a quantidade de auditores alocados em cada serviço; e,

III. a quantidade de horas de auditoria em cada trabalho;

2.1.5 cópia de dois trabalhos de auditoria realizados em ambiente de TI, que tenham sido realizados nos dois últimos anos, contendo relatórios e respectivos papéis de trabalho;

2.1.4.1 caso a empresa esteja impedida de apresentar a documentação por força de sigilo profissional, poderá dar vistas ao ITI aos dois últimos trabalhos; ou,

II. apresentar relatório de avaliação executado por outra empresa de auditoria, no programa de avaliação pelos pares, denominado Comitê Administrador do Programa de Revisão Externa de Qualidade (CRE);

o) comprovação de inscrição no CNAI – Cadastro nacional de Auditores Independentes

4.3 As entidades de auditoria interna candidatas a realizar trabalhos de auditoria na cadeia da ICP-Brasil, só poderão pleitear o credenciamento para o tipo 2, e apresentarão o formulário ADE-ICP-08.B[2], anexando:

a) a documentação estabelecida nas alíneas “a”, “b”, “k”, “m” e “n” do item 4.2 anterior;

b) comprovação de estar formalmente constituída, com vinculação direta ao principal órgão administrador ou controlador da empresa onde estiver inserida ou instituída por força de dispositivo legal.

4.4 As unidades de auditoria interna credenciadas só poderão realizar trabalhos de auditoria no âmbito da própria empresa onde inseridas, isto é, que possuam o mesmo CNPJ ou radical de CNPJ.

4.5 As empresas de auditoria independente autorizadas a realizar auditorias no âmbito da ICP-Brasil atenderão aos seguintes requisitos mínimos, que serão avaliados e considerados quando do exame do pedido de credenciamento:

a) para o tipo 1: experiência comprovada de pelo menos 2 (dois) anos em:

I) áreas de segurança da informação (ambiente físico e lógico), criptografia, infra-estrutura de chaves públicas, segurança patrimonial e sistemas de processamento eletrônico de informações;

II) utilização de pelo menos um dos padrões de auditoria reconhecidos internacionalmente, como por exemplo: COBIT, "*Webtrust*", ABR ou COSO;

b) para o tipo 2: deverão possuir corpo técnico de auditores com experiência comprovada de pelo menos 2 (dois) anos em:
   I) segurança da informação, segurança patrimonial e nível básico de sistemas de processamento eletrônico de informações;
   II) utilização de pelo menos um dos padrões reconhecidos internacionalmente de avaliação gerencial ou de gestão, como por exemplo: COBIT, COSO ou ABR.

4.6 Para as empresas de auditoria candidatas ao credenciamento para o tipo 1, é desejável que o corpo técnico de auditores possua alguma certificação internacional (CISA-*Certified Information System Auditor*; CISM-*Certified Information Security Manager*, CISSP-*Certified Information Systems Security Professional*, etc.).

4.7 O pedido de credenciamento será protocolado no ITI, por meio de correspondência impressa assinada pela entidade candidata, anexando arquivos eletrônicos observado o ADE-ICP-08-H[9].

4.8 Quanto aos aspectos legais, o processo de credenciamento será submetido à Procuradoria Federal Especializada, que manifestar-se-á, em até 30 (trinta) dias, sobre o acolhimento do pedido de credenciamento.

4.9 O prazo será suspenso, caso a Procuradoria solicite a complementação da documentação em até 15 dias, só voltando a ser contado a partir do recebimento do que for solicitado. O processo será arquivado, mediante despacho da Procuradoria, caso não haja complementação do solicitado até o prazo concedido.

4.10 A documentação apresentada pela candidata para credenciamento constituirá processo específico e será acondicionada em arquivo próprio pela AC-Raiz, por prazo não inferior a 5 (cinco) anos, exceto quanto à eventual documentação de auditorias realizadas, que será considerada confidencial, ficando à disposição apenas dos próprios solicitantes do credenciamento.

4.11 Acolhido, pela Procuradoria, o pedido de credenciamento ou, recebido, na DAFN, o pedido de renovação, o Diretor da DAFN, por meio de despacho fundamentado, poderá:

a) deferir o pedido;
b) notificar a candidata para, no prazo máximo de 15 (quinze) dias corridos, complementar a documentação apresentada;
c) indeferir o pedido se, vencido o prazo da alínea "b", não forem cumpridas as exigências constantes da notificação retro mencionada;
d) indeferir o pedido que não atenda aos requisitos técnicos estabelecidos.

4.12 O credenciamento será publicado no DOU (Diário Oficial da União) e será renovado a cada cinco (5) anos, a contar da data da publicação do respectivo credenciamento ou renovação.

4.13 Nas renovações, mediante solicitação à DAFN, a entidade de auditoria anexará a mesma documentação apresentada para o credenciamento inicial, podendo, para os documentos que não sofreram alteração desde o último deferimento, serem substituídos por declaração expressa do Representante Legal, sob as penas da lei. Nestes casos, serão renovadas as certidões negativas fisco-tributárias exigíveis.

4.14 As empresas cadastradas no SICAF – Sistema Unificado de Cadastramento de Fornecedores, registro oficial do Poder Executivo Federal, poderão, para fins de comprovação da situação tributária federal, apresentar seu extrato em substituição às respectivas certidões negativas exigíveis, que será complementado pelas certidões estaduais e municipais exigíveis, se for o caso.

4.15 Qualquer alteração ocorrida, quer seja em atos constitutivos, estatuto, contrato social, organograma ou vinculação da entidade, quer seja dos dirigentes ou da equipe técnica de auditores, será submetida imediatamente à aprovação da DAFN, mediante formalização protocolada no ITI e que fará parte do processo de credenciamento da respectiva entidade de auditoria. Nestes casos será reavaliada a manutenção das condições exigidas para o credenciamento, observadas as regras para as renovações, podendo ser dispensada a apresentações de certidões ainda não exigíveis.

4.16 A apresentação de documentos para fins de credenciamento ou descredenciamento será sempre por meio eletrônico, com assinatura digital da cadeia da ICP-Brasil.

4.17 É responsabilidade das entidades de auditoria credenciadas, a solicitação à AC-Raiz da atualização de seus dados e certidões no Cadastro de entidades de Auditoria Credenciadas.

4.18 A entidade de auditoria credenciada poderá solicitar o descredenciamento à AC-Raiz, a qualquer tempo.
4.19 Indeferido o pedido de credenciamento ou de renovação de credenciamento, a DAFN notificará diretamente ao interessado, por meio de ofício, procedendo aos ajustes cabíveis nos registros de empresas de auditoria credenciadas.
4.20 A AC-Raiz deverá, no prazo de 15 (quinze) dias corridos, a contar do deferimento do credenciamento, da renovação ou do recebimento do pedido de descredenciamento, atualizar o Cadastro de Auditorias Independentes, disponível no endereço http://www.iti.gov.br.

5. PLANO ANUAL DE AUDITORIA OPERACIONAL (PLAAO)

5.1 Cada AC e ACT protocolará no ITI, até o dia 15 (quinze) de dezembro de cada ano, para aprovação da DAFN, seu PLAAO para o ano civil seguinte, contemplando todos os PSC diretamente subordinados (AC subseqüente, AR e respectivos PSS), por meio do formulário ADE-ICP-08-C[4].
5.2 As auditorias operacionais serão realizadas anualmente nos seguintes PSC:
a) AC credenciada e respectivos PSS;
b) ACT credenciada e respectivos PSS
c) AR, respectivas instalações técnicas e PSS, no caso daquelas que possuam até três (3) instalações técnicas credenciadas.

5.3 Para os casos de AR que possua mais de três (3) endereços de instalação técnica, é facultado à AC subordinante, especificamente para essa AR, propor um cronograma anual de auditoria com cobertura parcial de suas instalações técnicas, desde que:
a) cada instalação técnica seja auditada pelo menos uma vez a cada dois (2) anos;
b) sejam auditados anualmente, no mínimo, 40% (quarenta por cento) de suas instalações técnicas; e,
c) a AC apresente os critérios e justificativas aplicadas na seleção das instalações técnicas distribuídas pelo período de auditoria proposto.

6. REALIZAÇÃO DAS AUDITORIAS

6.1 Aspectos Gerais da Realização das Auditorias

6.1.1 As auditorias têm por objetivo avaliar se os processos, procedimentos, atividades e controles estão em conformidade com as respectivas Políticas de Certificado, Declaração de Práticas de Certificação, Política de Segurança e demais normas e procedimentos estabelecidos pelo Comitê Gestor da ICP-Brasil. O documento ADE-ICP-08-E[6] detalha os processos que compõem a cadeia de certificação e deverá nortear as auditorias realizadas na cadeia da ICP-Brasil.
6.1.2 Cada PSC manterá dossiê de auditoria, preferencialmente em meio digital, organizado e constituído de pastas, contendo cada uma:
a) os relatórios de auditoria pré e operacionais,
b) as evidências de regularização das não-conformidades identificadas e apontadas em relatórios de auditoria,
c) as correspondências trocadas sobre a regularização de inconformidades.

6.1.3 Os relatórios de auditoria deverão concluir sobre os processos e procedimentos de responsabilidade do PSC sob avaliação, manifestando sobre a suficiência dos controles executados para mitigação dos riscos existentes. O documento ADE-ICP-08-F[7] apresenta os critérios para emissão do Parecer de Auditoria que constará do Relatório de Auditoria.
6.1.4 A entidade de auditoria, no exercício de suas atividades no âmbito da ICP-Brasil, deve cumprir e fazer cumprir, por seus prepostos e empregados, as normas da ICP-Brasil, observadas ainda as normas

para o exercício da profissão de auditor independente ou interno, conforme o caso.
2.2.4.2.9 As auditorias serão executadas em conformidade e aderência com a metodologia que deu base ao credenciamento da entidade responsável pela execução da auditoria.
2.2.4.2.10 Os serviços de auditoria serão executados diretamente pela entidade de auditoria credenciada junto à ICP-Brasil, vedada a subcontratação total ou parcial dos serviços.
2.2.4.2.11 O auditor, no exercício de suas funções, terá livre acesso a todas as dependências da entidade auditada, assim como aos documentos e registros indispensáveis ao cumprimento de suas atribuições, não lhe podendo ser sonegado, sob qualquer pretexto, documentos, acessos ou informações.
2.2.4.2.12 A entidade auditada deve fornecer ao auditor todos os elementos e condições necessárias ao perfeito desempenho de suas funções.
2.2.4.2.13 Os Papeis de Trabalho, registros e demais elementos materiais que deram subsídio à elaboração dos relatórios ficarão sob a guarda da entidade executante da auditoria, pelo prazo mínimo de 5 (cinco) anos. A AC-Raiz, a qualquer tempo e a seu critério, poderá solicitar cópia do material, fixando prazo para entrega, preferencialmente por meio eletrônico, observado o ADE-ICP-08.H[9].
2.2.4.2.14 O relatório final de auditoria será emitido com com a seguinte destinação:

a original, entidade auditada;
b cópia, AC subordinante, se for o caso, ou a ACT responsável;
c cópia à AC de primeiro nível, se for o caso; e,
d cópia, ITI.

2.2.4.2.15 A cópia do relatório de auditoria destinada ao ITI será entregue à Diretoria de Auditoria, Fiscalização e Normalização do ITI, observado o ADE-ICP-08-H[9], diretamente pela entidade de auditoria.
6. Pré-relatórios ou relatórios parciais não devem ser encaminhados ao ITI.

6.2 Aspectos específicos das Auditorias Pré-operacionais

6.2.1 Também nos relatórios de auditoria pré-operacional, serão emitidos conceitos de auditoria para os candidatos a PSC em conformidade com os critérios constantes do ADE-ICP-08-F[7].
6.2.2 Nos casos em que for identificada qualquer não conformidade, o relatório de auditoria só será encaminhado ao ITI após a certificação, pela entidade de auditoria, da regularização das inconformidades encontradas. A entidade de auditoria deverá anexar as evidências das regularizações ao relatório de auditoria pré-operacional.

6.3 Aspectos específicos das Auditorias Operacionais

6.3.1 O relatório de auditoria conterá avaliação do PSC e respectivos PSS, podendo estender-se às AR vinculadas – quando se tratar de auditoria em AC –, e conceituará o PSC auditado, em conformidade com os critérios constantes do ADE-ICP-08-F[7].
6.3.2 Considerando o nível de exposição aos riscos, a entidade de auditoria poderá excluir processos ou sub-processos das avaliações de auditoria, de forma justificada. Tais exclusões e justificativas constarão do corpo do relatório de auditoria ou de anexo específico, a critério da entidade de auditoria e em conformidade com a metodologia apresentada quando do credenciamento da entidade de auditoria.
6.3.3 Nas auditorias operacionais nas AC, o relatório de auditoria deverá informar se são atendidos os critérios de realização de auditorias operacionais nas AR subordinadas e se são adotados controles para acompanhamento daquelas auditorias.
6.3.4 Iniciados os trabalhos de campo da auditoria operacional em qualquer PSC, a entidade responsável pela execução da auditoria informará o fato ao ITI, por correio eletrônico (auditoria@iti.gov.br), utilizando o modelo constante do ADE-ICP-08-D[5]; na data de início dos trabalhos, ou com antecedência máxima de dois dias úteis.
6.3.5 Nos casos de auditoria em AR com diversas IT-Instalações Técnicas, embora possa ser emitido relatório por IT, deverá ser consolidado relatório da AR e será atribuído conceito ao PSC, observado o ADE-ICP-08-F.

6.3.6 Nos casos de AR onde exista acordo operacional, a entidade de auditoria deverá apresentar anexo específico, descrevendo os procedimentos adotados em cada acordo operacional, informando a responsabilidade por eventuais não-conformidades identificadas no cumprimento do respectivo acordo.

a) Cópia deste anexo será destinada a outra AR participante do acordo operacional, que a manterá no dossiê de auditorias realizadas.
b) Cada AR regularizará, nos prazos indicados, as não-conformidades a que tiver dado causa, comunicando o fato a AC à qual estiver vinculada.

7. RELAÇÃO ENTRE OS AUDITORES E AS ENTIDADES AUDITADAS

7.1 Aplica-se ao auditor, no que couber, as regras de suspeição e impedimento estabelecidas nos artigos 134 e 135 do Código de Processo Civil; além das demais normas para o exercício da profissão de auditor independente ou interno.

7.2 A empresa de Auditoria Independente ou qualquer de seus auditores serão declarados impedidos de realizar auditoria, quando:

a) houver motivo íntimo declarado;
b) for amigo íntimo ou inimigo capital de membros da entidade auditada;
c) for credor ou devedor da entidade auditada ou de um de seus membros;
d) tiver recebido, nos últimos 5 (cinco) anos, da entidade auditada, pagamentos referentes à prestação de serviços, excetuando-se os recebimentos de valores referentes à prestação de auditoria;
e) tiver interesse no resultado da auditoria a ser realizada; e,
f) houver relacionamento, de fato ou de direito, como cônjuge, parente, consangüíneo ou afim, com algum dos membros da entidade auditada, em linha direta ou na colateral até o terceiro grau.
   I) Entende-se como membros da entidade auditada todas as pessoas que de alguma forma participem do capital social ou tenham influência na gestão do PSC auditado.

7.3 A empresa de auditoria independente e respectivos auditores que participarem dos trabalhos de auditoria no âmbito da ICP-Brasil, firmarão declaração, sob as penas da lei, de que não se enquadram em qualquer das causas de impedimento tratadas neste documento.

7.4 As declarações previstas neste documento constarão como anexos obrigatórios ao relatório de auditoria a ser entregue ao ITI.

7.5 Exceto quanto as entidades de Auditoria Interna, será obrigatória a rotação da equipe de auditoria (responsável técnico, diretor, gerente e qualquer outro integrante) e das empresas de Auditoria Independente a intervalos menores ou iguais a cinco anos consecutivos; observado o intervalo mínimo de três (3) anos para o retorno.

7.6 As entidades de auditoria independente contratadas por entes da administração pública direta ou indireta (Federal, Estadual ou Municipal) que estejam impedidas do rodízio previsto no item anterior, por força de dispositivo legal, para atenderem a rotatividade estabelecida; quando completarem os cinco anos e durante os próximos três anos dos prazos estabelecidos no item anterior, deverão submeter seus trabalhos à revisão por outra entidade de auditoria, que emitirá relatório circunstanciado sobre a correta aplicação das normas profissionais e técnicas utilizadas nestes trabalhos, encaminhando-o ao ITI.

7.7 Ocorrendo o impedimento da entidade de auditoria, esta deverá concluir os trabalhos cujas atividades de campo já tenham iniciado e tenham sido comunicadas ao ITI por meio do ADE-ICP-08-D[5]; estando impedida de iniciar novos trabalhos de campo.

2.2.5.1.5 Eventuais relatórios de auditoria recebidos em desacordo com o caput serão sumariamente arquivados e não terão qualquer validade perante o ITI, no que se refere ao cumprimento da obrigatoriedade de realização de auditorias.

8. ANÁLISE DO RELATÓRIO DE AUDITORIA PELO ITI

8.1 O relatório de auditoria será analisado pela Diretoria de Auditoria, Fiscalização e Normalização da AC Raiz, que poderá solicitar esclarecimentos ou documentos complementares aos executantes da auditoria ou aos respectivos PSC auditados.
8.2 A documentação de auditoria será avaliada em comparação com a metodologia de auditoria aprovada no credenciamento da entidade de auditoria.
8.3 Se, a qualquer tempo, a Diretoria de Auditoria, Fiscalização e Normalização constatar que o relatório de auditoria entregue apresenta incorreções, omissões ou descumprimento de norma profissional de auditoria, comunicará o fato à entidade que executou a auditoria. Neste caso, a entidade de auditoria deverá justificar as incorreções no prazo de 15 dias da data do recebimento da notificação.
8.4 Caso a entidade de auditoria não apresente as justificativas ou estas sejam consideradas insatisfatórias, o Diretor da DAFN poderá aplicar penalidade, de conformidade com o ADE-ICP-08.G[8], notificando a entidade de auditoria.
8.5 Em caso de reincidência no mesmo tipo de ocorrência, mesmo em outro PSC, o ITI poderá aplicar penalidades de acordo com os critérios estabelecidos no ADE-ICP-08.G[8], com base em despacho fundamentado do Diretor da DAFN.

9. NÃO-CONFORMIDADES EM RELATÓRIOS DE AUDITORIA

9.1 Cabe à entidade auditada cumprir, no prazo estipulado no relatório de auditoria, as recomendações para corrigir as não-conformidades com a legislação ou com as políticas, normas, práticas e regras estabelecidas. Tais regularizações serão comunicadas formalmente à entidade a que se vincula o PSC auditado, na data de vencimento do prazo concedido no relatório de auditoria.
9.2 Cabe à entidade subordinante do PSC controlar o cumprimento das recomendações de auditoria das entidades vinculadas, comunicando ao ITI, o não cumprimento de recomendações de auditoria, mantendo registros formais do acompanhamento.
9.3 Caso qualquer recomendação não seja cumprida no prazo estabelecido no relatório de auditoria, o PSC subordinante comunicará o fato ao ITI, anexando cópia de correspondências trocadas, evidências da inconformidade e das ações adotadas até o momento para mitigação do risco envolvido. Esta comunicação será preferencialmente por correio eletrônico assinado por representante legal do PSC com certificado da ICP-Brasil, observando o ADE-ICP-08-H[9].
9.4 O cumprimento e efetivação das recomendações de auditoria e de sugestões de melhoria acaso existentes no relatório de auditoria, devem ser objeto de análise e manifestação na auditoria subseqüente.
9.5 As entidades encarregadas da execução das auditorias manifestarão sobre o atendimento das recomendações da auditoria imediatamente anterior, em documento anexo ao relatório de auditoria a ser emitido.
9.6 No ITI, os casos de não-conformidade que ensejaram recomendações de auditoria serão encaminhadas para a área da AC-Raiz responsável pela Fiscalização e incluídos nos planos de trabalho da mesma, observados os procedimentos previstos no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL (DOC-ICP-09)[1].
9.7 Cabe à AC Raiz tomar todas as medidas cabíveis a fim de garantir a segurança e a confiabilidade da ICP-Brasil, podendo descredenciar a entidade auditada, mediante decisão motivada.
9.8 O ITI, em casos de iminente dano irreparável ou de difícil reparação a terceiros, suspenderá cautelarmente, no todo ou em parte, a emissão de certificado e/ou carimbo do tempo pelo respectivo PSC, podendo a suspensão ser também estendida ao PSC de nível imediatamente subseqüente ou superior àquele.
9.9 Se a entidade auditada for considerada INACEITÁVEL o ITI suspenderá imediatamente suas operações até que as não-conformidades sejam solucionadas.
9.10 Nos casos de auditorias em AR com diversas instalações técnicas-IT, embora possa ser emitido relatório por IT, deverá ser consolidado relatório da AR onde será atribuído conceito geral ao PSC.
9.11 A entidade cujo conceito atribuído seja cinco (5) – INACEITÁVEL – em duas auditorias operacionais

consecutivas, será descredenciada da ICP-Brasil, não podendo mais ter seu pedido de credenciamento aceito pelo ITI pelo período mínimo de dois (2) anos.
9.12 O descredenciamento será publicado no Diário Oficial da União, em consonância com os demais procedimentos de descredenciamento descritos nas normas da ICP-Brasil.
9.13 Toda vez que um PSC receber um conceito 3 ou 4 no relatório de auditoria operacional, poderá sofrer uma das penalidades previstas no ADE-ICP-08-G[8].

10. DOS PROCESSOS ADMINISTRATIVOS E DOS RECURSOS

10.1 Todas as penalidades referentes aos processos de auditoria serão aplicadas pelo Diretor de Auditoria, Fiscalização e Normalização (DAFN), com base em decisão fundamentada, quer se trate de PSC ou entidade de auditoria credenciada.
10.2 A entidade infratora será notificada pelo Diretor da DAFN, cujo ofício listará os fatos e as normas descumpridas.
10.3 A entidade notificada terá o prazo de até 10 (dez) dias, da data do recebimento da notificação da DAFN, para protocolar defesa, apresentando as justificativas e documentação que julgar conveniente para sua defesa.
10.4 Recebida a defesa, o Diretor da DAFN, poderá: arquivar o processo de aplicação da penalidade; ou, indeferir a defesa, mantendo a anterior decisão, fundamentadamente.
10.5 Indeferida a defesa, a entidade será notificada e penalizada de conformidade com o ADE-ICP-08.G[8].
10.6 A entidade notificada, na forma do item anterior, poderá interpor recurso ao Diretor-Presidente do ITI contra a aplicação da penalidade, no prazo de 10 dias da data em que for notificada da aplicação da penalidade pelo Diretor da DAFN.
10.7 Caso não seja apresentado recurso contra a decisão do Diretor da DAFN, a penalidade será publicada no DOU.
10.8 Protocolado recurso contra decisão do Diretor da DAFN, o Diretor-Presidente do ITI decidirá, com base em despacho fundamentado, em 15 dias da data da interposição do recurso contra aplicação de penalidade. Caso julgue necessário, o Diretor-Presidente solicitará parecer da Procuradoria Federal Especializada do ITI que subsidie a decisão quanto a aplicação da penalidade.
10.9 Da aplicação de penalidade imposta pelo Diretor-Presidente do ITI, caberá recurso ao Comitê-Gestor – instância máxima de decisão administrativa no âmbito da ICP-Brasil –, no prazo de 10 dias da data do recebimento da notificação da aplicação da penalidade.
10.10 As penalidades aplicadas pelo Diretor-Presidente serão publicadas no DOU.
10.11 Os recursos interpostos contra as decisões de que trata este item 10 não gozarão de efeito suspensivo, nos termos da lei nº 9.784/99, art. 61.
10.12 A decisão do Comitê Gestor que reformular penalidade aplicada pelo Diretor-Presidente do ITI será publicada no DOU.

11.DISPOSIÇÕES FINAIS

11.1 É de inteira responsabilidade da entidade de auditoria credenciada, a veracidade das informações e documentos apresentados ao ITI.
11.2 A não declaração de fato superveniente que possa desconstituir o teor de documentação já apresentada ou a falsa declaração, pela entidade credenciada ou por qualquer dos auditores que realizaram a auditoria, sujeita-os às penalidades cabíveis.
11.3 A empresa estrangeira que não tenha filial ou representante legal no País atenderá às exigências estabelecidas mediante a apresentação de documentos equivalentes autenticados pelo respectivo consulado e traduzido por tradutor juramentado.

12. DOCUMENTOS REFERENCIADOS

12.1 O documento abaixo é aprovado por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterado, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada do documento e as Resolução que o aprovou.

Ref.	Nome do documento	Código
[1]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09

12.2 Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br.

Ref.	Nome do documento	Código
[1]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE EMPRESA DE AUDITORIA ESPECIALIZADA E INDEPENDENTE	ADE-ICP.08.A
[2]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE ÓRGÃO DE AUDITORIA INTERNA	ADE-ICP.08.B
[4]	Modelo de PLAAO – PLANO ANUAL DE AUDITORIA OPERACIONAL	ADE-ICP.08.C
[5]	Modelo de COMUNICAÇÃO DE INÍCIO DE TRABALHOS DE AUDITORIA	ADE-ICP.08.D
[6]	Descrição dos PROCESSOS DAS ENTIDADES DA ICP-BRASIL	ADE-ICP.08.E
[7]	CRITÉRIOS PARA EMISSÃO DE PARECER DE AUDITORIA	ADE-ICP.08.F
[8]	CRITÉRIOS PARA APLICAÇÃO DE PENALIDADES A ENTIDADES CREDENCIADAS NA ICP-BRASIL	ADE-ICP.08.G
[9]	PROCEDIMENTOS PARA TROCA DE CORRESPONDÊNCIAS ENTRE AS ENTIDADES DE AUDITORIA E O ITI	ADE-ICP.08.H

ANEXO C - CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL

Infra-Estrutura de Chaves Públicas Brasileira

CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL

DOC-ICP-09 - versão 3.0

CONTROLE DE ALTERAÇÕES

Resolução que aprovou alteração	***Item Alterado***	***Descrição da Alteração***
Resolução 57, de 19.11.2008 (Versão 3.0)	1.1.j, 8.1	Inclusão de referências a Autoridades de Carimbo de Tempo
Resolução 45, de 18.04.2006 (Versão 2.0)	Diversos	Criação do DOC-ICP-09, consolidando documentos anteriores.

SIGLAS

AC - Autoridade Certificadora
AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil
ACT – Autoridade de Carimbo do Tempo
AFC - Ação de Fiscalização de Certificação
AIC - Auto de Infração de Certificação
AR - Autoridade de Registro
DPC - Declaração de Práticas de Certificação
ICP-Brasil - Infra-Estrutura de Chaves Públicas Brasileira
NFC - Notificação da Fiscalização de Certificação
PAF - Processo Administrativo de Fiscalização
PC - Políticas de Certificado
PFC - Procedimento de Fiscalização de Certificação
PS - Política de Segurança
PSC - Prestador de Serviço de Certificação
RF - Relatório de Fiscalização
RIC - Requisição de Informações Complementares
TF - Termo de Fiscalização
TFC - Termo de Fiscalização Complementar
TFE - Termo de Fiscalização Extensivo
TFF - Termo de Fiscalização Final
TFI – Termo de Fiscalização Inicial

1. DISPOSIÇÕES GERAIS

1.1. Para os fins deste documento, entende-se como:

a)AÇÃO DE FISCALIZAÇÃO DE CERTIFICAÇÃO (AFC) - Procedimentos preparatórios, levantamento de informações, ações presenciais ou à distância, levantamento de evidências, pedidos de complementação de informações através do documento REQUISIÇÃO DE INFORMAÇÕES COMPLEMENTARES (RIC) [1] e atividades do fiscal que devem estar relatadas no documento RELATÓRIO DE FISCALIZAÇÃO (RF) [5];

b)AUTORIDADE OUTORGANTE – Autoridade competente e empossada no cargo de Diretor de Auditoria, Fiscalização e Normalização da AC Raiz, sendo, pela legislação, autorizado a praticar, todos os atos necessários à realização do Procedimento de Fiscalização de Certificação (PFC) e que expede documentos relativos ao mesmo;

c)AUTO DE INFRAÇÃO DE CERTIFICAÇÃO (AIC) [2] – Documento preenchido pelo Fiscal da ICP-Brasil ao constatar infração por Prestador de Serviço de Certificação (PSC) durante a fiscalização;

d)FISCAL DA ICP-BRASIL – Servidor vinculado e lotado na Diretoria de Auditoria, Fiscalização e Normalização da AC Raiz, e no exercício das funções de fiscal, conforme indicado no documento TERMO DE FISCALIZAÇÃO (TF) [3];

e)FISCALIZAÇÃO – Atividade de controle e inspeção sistemática do cumprimento das resoluções, normas, procedimentos e atividades dos Prestadores de Serviço de Certificação (PSC) com a finalidade de examinar se as operações de cada um deles, isolada ou conjuntamente, se mantêm em conformidade com suas Declarações de Práticas, Políticas e com as Resoluções e normas gerais estabelecidas para as entidades integrantes da ICP-Brasil.

f)INFRAÇÃO

i - Não atendimento a qualquer disposição legal da ICP-Brasil ou normas complementares estabelecidas pela AC Raiz;

g) - Não-conformidade constatada a partir de fiscalização;

h) - Obstrução, omissão ou má-fé por parte do PSC tendente a prejudicar a ação fiscalizadora da AC Raiz;

g)INSTALAÇÃO TÉCNICA – Endereço físico de uma entidade integrante da ICP-Brasil que conste no formulário SOLICITAÇÃO DE CREDENCIAMENTO [6];

h)NOTIFICAÇÃO DA FISCALIZAÇÃO DE CERTIFICAÇÃO (NFC) [4] - Documento pelo qual a Autoridade Outorgante dá ciência à Entidade Fiscalizada e a sua responsável hierárquica para que faça ou deixe de fazer alguma coisa;

i)OBJETO DA FISCALIZAÇÃO – Descrição do ponto de controle sob verificação. É um item das resoluções, um conjunto de itens, ou itens de resoluções associados;

j)PRESTADOR DE SERVIÇO DE CERTIFICAÇÃO (PSC) – Qualquer entidade credenciada para operar na ICP-Brasil, como: as Autoridades Certificadoras (AC); as Autoridades de Registro (AR); as Autoridades de Carimbo do Tempo (ACT), os Prestadores de Serviço de Suporte (PSS); ou entidade vinculada, como o Laboratório de Ensaios e Auditoria (LEA) e outros que executem ou determinem a execução de itens de certificação presentes nas resoluções da ICP-Brasil;

k)PROCEDIMENTO DE FISCALIZAÇÃO DE CERTIFICAÇÃO (PFC) - Conjunto de ações que objetivam a verificação do cumprimento das normas, por parte das entidades credenciadas na ICP-Brasil, incluídos os atos administrativos de início e finalização e as ações de aplicação de penas, ampla defesa e comunicação de fiscalizações realizadas e dadas como conformes;

l)PROCESSO ADMINISTRATIVO DE FISCALIZAÇÃO (PAF) - Processo onde são arquivados todos os documentos e relatórios relativos ao Procedimento de Fiscalização de Certificação;

m)RELATÓRIO DE FISCALIZAÇÃO (RF) - Documento no qual o fiscal descreve o que constatou no Prestador de Serviço de Certificação, como foram as atividades e suas prescrições, subsidia o TFF e

retrata todo a AFC, atividades executadas e constatações obtidas pelo Fiscal da ICP-Brasil;
n)REQUISIÇÃO DE INFORMAÇÕES COMPLEMENTARES (RIC) [1] - Documento no qual o fiscal ou auditor solicita informações complementares necessárias à condução do processo de fiscalização ou auditoria;
o)TERMO DE FISCALIZAÇÃO (TF) – Documento-base para a fiscalização e que indica a sua finalidade. Pode ser um TERMO DE FISCALIZAÇÃO INICIAL (TFI), TERMO DE FISCALIZAÇÃO EXTENSIVO (TFE), TERMO DE FISCALIZAÇÃO COMPLEMENTAR (TFC) ou TERMO DE FISCALIZAÇÃO FINAL (TFF).

1.2. No que se refere aos prazos citados neste documento, entende-se que:

a)Os prazos serão contínuos, excluindo-se na sua contagem o dia do início e incluindo-se o do vencimento;
b)Os prazos só se iniciam ou vencem no dia de expediente normal no órgão em que corra o processo ou devam ser praticado os atos.

2. OBJETIVO DA FISCALIZAÇÃO

2.1. O objetivo da Fiscalização é verificar a conformidade dos processos, procedimentos e atividades dos PSCs com suas Declarações de Práticas, Políticas e com as Resoluções e normas gerais estabelecidas para as entidades integrantes da ICP-Brasil.

3. PROCEDIMENTOS DE FISCALIZAÇÃO DE CERTIFICAÇÃO

i) O PFC iniciar-se-á através de planejamento de fiscalização semestral, recomendação obtida em Relatórios de Auditoria (Pré-Operacionais ou Operacionais), por denúncia feita por usuário de certificação digital da ICP-Brasil ou por constatação de ameaça à confiabilidade da ICP-Brasil.
j) O PFC alcançará o exame de documentos, ambientes físico e lógico do PSC, bem como seu próprio pessoal, podendo acarretar a aplicação de uma ou mais penalidades.
k) A AFC será realizada pela AC Raiz por intermédio de seus fiscais.
l) O objeto da AFC estará associado a atividades diretamente vinculadas ao ciclo de vida dos certificados digitais da ICP-Brasil. Em caso de denúncia, por solicitação do Presidente da AC Raiz ou do Secretário Executivo do Comitê Gestor da ICP-Brasil a fiscalização poderá atuar sobre qualquer item ou regulamento previstos nas resoluções em vigor.
m) A AFC será instaurada mediante ordem específica denominada TFI.
n) No caso de flagrante constatação de irregularidade ou qualquer outra prática de infração às normas da ICP-Brasil, em que o retardo do início do procedimento coloque em risco a segurança ou confiabilidade dessa infra-estrutura, pela possibilidade de subtração de prova ou outro risco de eliminação ou dificuldades na obtenção de evidências que comprovem a irregularidade, a fiscalização será iniciada por fiscal habilitado e a Autoridade Outorgante terá prazo de 5 (cinco) dias para lavrar o TF.
o) Em caso de impedimento da realização da AFC por parte do Fiscal designado no TF, este poderá ser substituído ou ter a cooperação de outro fiscal, sendo que, em ambos os casos, deverá sempre haver um fiscal principal responsável pela AFC identificado no PAF.
p) Durante o AFC, o fiscal poderá emitir Autos de Infração de Certificação (AIC) quantos forem necessários, e cópia do mesmo deverá ser enviada para a AC responsável pelo pedido de credenciamento do PSC fiscalizado.
q) Uma AFC deverá conter prazo de execução que poderá ser de até 120 (cento e vinte) dias, podendo ser prorrogado uma única vez por igual período, por ato da Autoridade Outorgante, a requerimento do Fiscal responsável ou por motivo superveniente devidamente apresentado e descrito no PAF.
r) Será dada publicidade do PFC, no momento da abertura, por meio de um resumo do mesmo,

contendo o número do Processo Administrativo de Fiscalização (PAF), a sigla do PSC e o objeto do PFC. 3.11. O PFC se extingue:

a)pelo término do mesmo, registrado em TF específico; ou

b)pelo encerramento do prazo da AFC a que se refere o parágrafo 3.9.

3.12. Será dada publicidade do encerramento do PFC, acrescentando-se aos dados referenciados no item 3.10 o resultado da fiscalização.

4. PROCESSO ADMINISTRATIVO DE FISCALIZAÇÃO

4.1. Cada PFC ensejará a abertura de um PAF, que seguirá os procedimentos estabelecidos neste documento e observados os regulamentos de Processo Administrativo da AC Raiz.

4.2. Todos os documentos do PFC, inclusive o próprio PAF poderão ser suportados por mídia magnética desde que assinados eletronicamente por intervenientes devidamente qualificados e autorizados para responderem pela Fiscalização e pelos PSCs.

5. DOCUMENTOS DO PROCEDIMENTO DE FISCALIZAÇÃO

5.1. O Termo de Fiscalização deve conter:

a)a numeração de identificação e controle seqüencial e com ano de referência; b)tipo da TF (Inicial, Complementar, Extensivo ou Final)

c)os dados identificadores do PSC;

d)o objeto do procedimento de fiscalização;

e)o prazo para a realização da AFC;

f)o nome e a matrícula do fiscal responsável pela execução da fiscalização;

g)o nome e o número do telefone do Coordenador de Fiscalização; e

h)o nome, a matrícula e a assinatura da autoridade outorgante e, na hipótese de delegação de competência, a indicação do respectivo ato.

5.2. O TF será emitido, observadas suas respectivas atribuições regimentais, pelas seguintes autoridades: a)Diretor de Auditoria, Fiscalização e Normalização; ou

b)Coordenador-Geral de Auditoria e Fiscalização, nos impedimentos eventuais e temporários do primeiro.

5.3. O TF deverá ter os seguintes destinatários:

a)Prestador de Serviço de Certificação (PSC) a ser fiscalizado;

b)Processo Administrativo de Fiscalização (PAF); e

c)Prestador de Serviço de Certificação (PSC) de primeiro nível, responsável pelo pedido de credenciamento do PSC a ser fiscalizado, quando for o caso.

5.4. Todo PFC deverá ter, obrigatoriamente, um Termo de Fiscalização Inicial (TFI) e um Termo de Fiscalização Final (TFF). Adicionalmente, poderá ter um ou mais Termos de Fiscalização Complementar (TFC) e Termos de Fiscalização Extensivo (TFE).

a)O Termo de Fiscalização Complementar (TFC) deve ser incorporado ao TFI para o mesmo PSC e com objeto de fiscalização diferenciado;

b)O Termo de Fiscalização Extensivo (TFE) dever ser incorporado ao TFI para um PSC diferente mas com objeto relacionado ao objeto do TFI original;

c)O Termo de Fiscalização Final deve ser usado para encerrar todo procedimento aberto e executado por um TFI.

g) Havendo necessidade de realizar fiscalização em objeto e entidades diferentes o Fiscal deve solicitar a abertura de um novo TF.
h) O AIC é um documento informativo, dirigido ao PSC, de uma infração verificada pelo fiscal.
i) A AFC e as diligências realizadas em virtude de cada TF serão registradas em RF com os mesmos dados que identificam o TF no que se refere à entidade fiscalizada.
j) Apontada alguma irregularidade no RF, o PSC será notificado pela autoridade que expediu o TFI, através de uma NFC, fixando-se prazo de 15 (quinze) dias para que o PSC fiscalizado apresente, diretamente e formalmente, justificativa ou defesa à AC Raiz naquilo que foi argüido.
k) Caso o PSC não apresente, tempestivamente, justificativa ou defesa, será expedida uma NFC à AC responsável pelo pedido de credenciamento do PSC fiscalizado, sem prejuízo do regular seguimento do PFC.
l) Após análise da justificativa ou defesa apresentada, a Autoridade Outorgante poderá, mediante uma NFC, determinar que o PSC sane as irregularidades no prazo que fixar.
m) Após sanadas as irregularidades, o PSC deverá comunicar à Autoridade Outorgante as soluções adotadas.
n) Caso não seja apresentada a defesa ou não sejam sanadas as irregularidades, a Autoridade Outorgante decidirá em 20 (vinte) dias sobre a aplicação de penalidade.
o) Um Aviso de Encerramento deverá ser enviado aos interessados para dar ciência do encerramento da fiscalização.

6. PENALIDADES

6.1. Por infração, a entidade fiscalizada ficará sujeita às seguintes penalidades, independentemente de sua ordem de enumeração:

a) Advertência;
b) Restrição da realização de atividades relacionadas ao objeto da fiscalização até que sejam sanadas as irregularidades apontadas no RF;
c) Proibição de credenciamento de novas PCs até que sejam sanadas as irregularidades apontadas no RF;
d) Suspensão da emissão de novos certificados por prazo determinado ou até que sejam sanadas as irregularidades apontadas no RF;
e) Descredenciamento.

4.2 As penalidades poderão ser aplicadas isoladas ou cumulativamente.

4.3 A aplicação de uma penalidade não impede a aplicação de outra mais grave em caso de seu descumprimento.
6.4. Na aplicação das penalidades serão consideradas a natureza, a gravidade da infração cometida, a reincidência e a relevância do serviço para o ciclo de vida do certificado da ICP-Brasil, estando essa aplicação regulamentada pelo documento CRITÉRIOS PARA APLICAÇÃO DE PENALIDADES NO ÂMBITO DA ICP-BRASIL [7].
6.5. As penalidades serão aplicadas pelo Diretor de Auditoria, Fiscalização e Normalização.
6.6. Da decisão que impõe qualquer penalidade estabelecida no parágrafo 6.1 caberá recurso no prazo de 20 (vinte) dias, com efeito suspensivo.
6.7. O recurso será dirigido à autoridade que aplicou a penalidade, a qual, se não a reconsiderar, no prazo de 5 (cinco) dias o encaminhará ao Diretor-Presidente da AC Raiz para julgamento e avaliação de recurso.
6.8. O Diretor-Presidente da AC Raiz poderá encaminhar o PAF à Procuradoria Federal Especializada da

AC Raiz para emissão de parecer que subsidie a decisão do Diretor-Presidente.
6.9. O recurso deverá ser decidido pelo Diretor-Presidente, no prazo máximo de 15 (quinze) dias.

7. DISPOSIÇÕES FINAIS

7.1. A AC Raiz, por intermédio de seus gestores administrativos, garantirá o pleno e inviolável exercício das atribuições do Fiscal responsável pela execução do PFC.

8. DOCUMENTOS REFERENCIADOS

8.1. Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br .

Ref.	Nome do documento	Código
[1]	REQUISIÇÃO DE INFORMAÇÕES COMPLEMENTARES (RIC)	ADE-ICP-09.A
[2]	AUTO DE INFRAÇÃO DE CERTIFICAÇÃO (AIC)	ADE-ICP-09.B
[3]	TERMO DE FISCALIZAÇÃO (TF)	ADE-ICP-09.C
[4]	NOTIFICAÇÃO DA FISCALIZAÇÃO DE CERTIFICAÇÃO (NFC)	ADE-ICP-09.D
[5]	RELATÓRIO DE FISCALIZAÇÃO (RF)	ADE-ICP-09.E
[6]	SOLICITAÇÃO DE CREDENCIAMENTO (para AC ou AR, PSS ou ACT)	ADE-ICP-03.A ADE-ICP-03.B ADE-ICP-03.C ADE-ICP-03.G

8.2. Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[7]	CRITÉRIOS PARA APLICAÇÃO DE PENALIDADES NO ÂMBITO DA ICP-BRASIL	DOC-ICP-09.01

ANEXO D - FORMULÁRIO DE REQUERIMENTO DE AUDITORIA PARA AUTORIDADES CERTIFICADORAS DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

Infra-Estrutura de Chaves Públicas Brasileira

FORMULÁRIO DE REQUERIMENTO DE AUDITORIA PARA AUTORIDADES CERTIFICADORAS DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

1. IDENTIFICAÇÃO DA ENTIDADE SOLICITANTE

1.1 NOME (Razão Social):	1.2 CNPJ:
1.3 NOME DA AC NA ICP-BRASIL:	1.4 CÓDIGO DA ENTIDADE – a ser preenchido pelo ITI:

1.5 ENDEREÇO (das instalações técnicas - SITE PRINCIPAL):

RUA: Nº : COMPLEMENTO:

BAIRRO: CEP: MUNICÍPIO: UF:

DDD: TELEFONE: FAX: ENDEREÇO ELETRÔNICO:

1.6 ENDEREÇO (instalações técnicas – SITE BACKUP):

RUA: Nº : COMPLEMENTO:

BAIRRO: CEP: MUNICÍPIO: UF:

DDD: TELEFONE: FAX: ENDEREÇO ELETRÔNICO:

1.7 REPRESENTANTE LEGAL:

NOME: RG: CPF:

CARGO:

DDD: TELEFONE: FAX: ENDEREÇO ELETRÔNICO: CELULAR:

2. SOLICITAÇÃO

Solicitamos à Autoridade Certificadora Raiz a realização de auditoria pré-operacional nas nossas instalações técnicas supra citadas, _____ cujo credenciamento está sendo solicitado junto à ICP-Brasil conforme processo(s) número(s) .

3. DECLARAÇÃO

Declaramos que todos os dados informados neste formulário são verdadeiros e que as instalações técnicas para as quais estamos solicitando auditoria se encontram inteiramente prontas para ser auditadas, em relação às práticas descritas em nossa Política de Segurança, Declaração de Práticas de Certificação e Políticas de Certificado.

Local e data.

_____

(Assinatura do(s) Representante(s) Legal(ais) da Autoridade Certificadora)

ANEXO E - PLANO ANUAL DE AUDITORIA OPERACIONAL

PLANO ANUAL DE AUDITORIA OPERACIONAL

1. Modelo a ser preenchido pela AC, quanto às auditorias em AC subordinadas.

Nome da AC Vinculante	Nome da AC Subordinada	Localização da IT Principal ou de contingência	Período		Observações
			Início	Fim	
(A)	(B)	(C)	(D)	(E)	(F)

a) Instruções de Preenchimento:

– Nome da AC responsável pelo preenchimento do formulário.

B – Nome da AC subordinada à AC que está preenchendo o formulário.

C – Localização da instalação técnica do sítio principal. Deverá ser incluída uma linha com a informação do local da instalação técnica do sítio de contingência. Será incluída uma linha para cada PSS da AC.

D – Data prevista para o início da auditoria na respectiva instalação técnica.

E – Data prevista para entrega do relatório de auditoria pela entidade responsável pela execução da

auditoria. F – Informações adicionais que a AC julgar conveniente apresentar.

PLANO ANUAL DE AUDITORIA OPERACIONAL

3. Modelo a ser preenchido pela AC, quanto às auditorias em AR diretamente vinculadas.

Nome da AC	Nome da AR	Localização da instalação técnica	Período		Critérios / Observações
			Início	Fim	
(A)	(B)	(C)	(D)	(E)	(F)

4. Instruções de Preenchimento:

A – Nome da AC que subordina as AR vinculadas.

B – Nome da AR vinculada.

C – Localização de cada instalação técnica da AR subordinada. Deverá ser incluída uma linha para cada instalação técnica da AR. D – Data prevista para o início da auditoria na respectiva instalação técnica.

E – Data prevista para entrega do relatório de auditoria pela entidade responsável pela execução da auditoria. F – Critérios e justificativas utilizados para distribuição das instalações técnicas selecionadas em cada ano.

ANEXO F - MODELO DE E-MAIL COMUNICANDO INÍCIO DE TRABALHOS DE AUDITORIA

Infra-Estrutura de Chaves Públicas Brasileira
ADE ICP-08.D

MODELO DE ***e-mail*** COMUNICANDO INÍCIO DE TRABALHOS DE AUDITORIA

Para: CGAF/DAFN/ITI (auditoria@iti.gov.br)
Local e Data: Brasília (DF), dd.mm.aaaa

Informamos o início das atividades de campo da auditoria operacional no PSC (nome).

PSC: (1)
Entidade vinculante: (2)
Data de início dos trabalhos de campo: dd.mm.aaaa
Data prevista para entrega do relatório de auditoria: dd.mm.aaaa

Entidade de Auditoria (3)
Auditores (4)

Instruções de preenchimento:
i) – informar o nome da entidade que está sendo auditada.
j) – Informar a entidade à qual a unidade auditada se vincula.
k) – Nome da entidade responsável pela execução da auditoria.
l) – Nome dos auditores responsáveis pela execução da auditoria. dd.mm.aaaa – data no formato dia.mês.ano (01.01.2001)

ANEXO G - MAPA DE PROCESSOS IDENTIFICADOS NA ICP-BRASIL

MAPA DE PROCESSOS IDENTIFICADOS NA ICP-Brasil

1. Os processos nas AC – Autoridades Certificadoras estão assim distribuídos:

1.1. Executar fases do ciclo de vida de certificados digitais, composto pelos sub-processos:

m) Registrar solicitação

Os certificados admitidos no âmbito da ICP-Brasil devem manter conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

II) O padrão de formato para solicitação de certificados às AC emitentes deve ser PKCS#10.

III) A solicitação de geração de novo par de chaves antes da expiração do atual, quando por meio eletrônico, só é permitida para titulares pessoa física, limitado a uma ocorrência sucessiva.

IV) A solicitação de geração de novo par de chaves antes da expiração do atual, quando por meio eletrônico, para pessoas físicas, deve ser assinada digitalmente com o uso de certificado vigente de mesmo nível de segurança.

V) A solicitação de revogação de certificados digitais deve ser efetuada somente por pessoa autorizada.

VI) As circunstância para solicitação de revogação devem ser somente as previstas nas normas.

VII) O solicitante da revogação de um certificado deve ser identificado.

VIII) A solicitação de revogação de certificado deve conter justificativa documentada e armazenada.

b) Tratar validação

I) As etapas do processo de validação e verificação da solicitação de certificado devem ser registradas e assinadas digitalmente pelo executante, na solução de certificação disponibilizada pela AC.

II) O aplicativo que faz interface entre a AR e o sistema de certificação da AC deve possuir controle de acesso com autenticação por meio do certificado digital do agente de registro, no mínimo do tipo A3.

2.1.4 O aplicativo que faz interface entre a AR e o sistema de certificação da AC deve permitir acesso somente de equipamentos autenticados.

IV) O aplicativo que faz interface entre a AR e o sistema de certificação da AC deve possuir mecanismo de timeout de sessão de acordo com a análise de risco da AC.

b O aplicativo que faz interface entre a AR e o sistema de certificação da AC deve utilizar VPN, SSL ou outra tecnologia de igual ou superior nível de segurança.

VI) A verificação da solicitação de certificado deve ser executada por agente distinto do que executou a etapa de validação.

c) Tratar verificação

I) A verificação da solicitação de certificado deve ser executada antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

II) O aplicativo que faz interface entre a AR e o sistema de certificação da AC deve registrar eletronicamente em arquivo de auditoria todos os eventos relacionados a validação e verificação das solicitações de certificados, bem como as solicitações de revogação.

2.2.2.1.4 Tratar revogação

a) Certificados digitais devem ser revogados quando caracterizadas as circunstâncias definidas no item 4.4.1 da DOC-ICP-05.

O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos os tipos de certificado previsto pela ICP-Brasil é de 12 (doze) horas.

e) Emitir LCR

I) A freqüência para emissão de LCR deve atender ao estabelecido em sua respectiva DPC, não podendo ultrapassar 6 (seis) horas.

II) A LCR gerada pela AC deve implementar a versão 2 do padrão ITU X.509, de acordo com o estabelecido na RFC 3 280.

III) As ACs que disponibilizam verificação da situação de certificado por meio do protocolo OCSP (On-line Certificate Status Protocol) devem manter conformidade com o padrão estabelecido na RFC 2560.

IV) Antes de publicadas, todas as LCR geradas pela AC devem ser checadas quanto à consistencia de seu conteúdo.

f) Emitir certificados

2.2.2.3.6 O padrão de formato para entrega de certificados emitidos pela AC deve ser PKCS#7.

f) O algoritmo criptográfico e tamanho das chaves para geração de chaves assimétricas de AC devem ser RSA e 2048 bits, respectivamente.

III) O algoritmo criptográfico e tamanho das chaves para geração de chaves assimétricas de usuário final devem ser respectivamente RSA e 1024bits para certificados do tipo A1 a S3 e 2048 bits para A4 e S4.

IV) O algoritmo criptográfico para assinatura de certificado de AC deve ser

SHA-1 com RSA.

V) O algoritmo criptográfico para assinatura de certificado de usuário final deve ser SHA-1 com RSA ou DSA.

VI) O algoritmo simétrico para guarda da chave privada da entidade titular e de seu backup deve ser 3-DES, IDEA ou SAFER+.

VII) O módulo criptográfico de geração e armazenamento de chaves assimétricas de usuário final deve atender ao padrão obrigatório ou transitório.

VIII) O módulo criptográfico de geração e armazenamento de chaves assimétricas de AC deve atender ao padrão obrigatório ou transitório.

IX) A chave privada da AC deve trafegar cifrada entre o dispositivo gerador e a mídia utilizada para seu armazenamento.

X) As mídia armazenadora de chaves criptográficas devem atender aos requisitos mínimos de acordo com o tipo de certificado conforme tabela 2 do item 6.1.1.7 do DOC-ICP-04.

XI) A chave privada da AC deve ser utilizada apenas para assinatura de certificados por ela emitidos e de sua LCR.

XII) Propósito de uso em certificados de assinatura digital podem ter somente os bits de "*digitalSignature*", "*nonRepudiation*" e "*keyEncipherment*" ativados, sendo os restantes obrigatoriamente desativados.

XIII) Propósito de uso em certificados de sigilo podem ter somente os bits de "*keyEncipherment*" e "*dataEncipherment*" ativados, sendo os restantes obrigatoriamente desativados.

XIV) No âmbito da ICP-Brasil, não é permitido que terceiros possam legalmente obter a chave privada sem o consentimento de seu titular.

XV) A AC não deve manter cópia de segurança (backup) de chave privada de titular de certificado de assinatura digital por ela emitido.

XVI) Cópia de segurança de chave privada, quando for o caso, deve ser protegida com um nível de segurança não inferior àquele definido para a chave original.

XVII) O arquivamento de chave privada na AC, quando for o caso, deve ser condizente com o especificado em sua respectiva Política de Certificado.

XVIII) As ACs emissoras de certificados de assinatura digital e LCR devem armazenar permanentemente as chaves públicas e as LCR para uso futuro.

XIX) As ACs não devem emitir certificados com validade superior ao período máximo definido na ICP-Brasil.

2.2.3.1.4 Os certificados emitidos pela AC deve implementar a versão 3 definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 3280.

XXI) Os certificados ICP-Brasil emitidos para usuários finais devem contemplar as extensões de certificados definidas como obrigatórias.

XXII) Em certificados ICP-Brasil, o nome do titular do certificado, constante do campo "*Subject*", deve adotar o "*Distinguished Name*" (DN) do padrão ITU X.509/ISO 9594.

XXIII) Chaves privadas de AC devem trafegar cifradas entre o módulo gerador e a mídia utilizada para o seu armazenamento.

XXIV) O controle múltiplo ("n" de "m") para utilização da chave privada da AC deve requerer pelo menos 2 (dois) detentores de partição de chave formalmente designados.

XXV) A AC deve manter cópia de segurança de sua própria chave privada com armazenamento cifrado, protegido e nível de segurança não inferior àquele definido para a chave original.

XXVI) As chaves privadas de sigilo, quando cabível, devem manter o nível de segurança não inferior àquele definido para a chave original.

XXVII) O método de ativação e desativação de chave privada da AC deve atender ao estabelecido em sua respectiva DPC.

XXVIII) Os certificados ICP-Brasil de AC devem contemplar as extensões de certificados definidas como obrigatórias.

1.2. Manter repositórios, composto pelos sub-processos:

a) Manter DPC, PC e PS

I) As alterações nas DPC, PC e PS devem ser autorizadas pela AC RAIZ.

II) Toda PC e DPC elaborada no âmbito da ICP-Brasil deve observar requisitos e estrutura do DOC-ICP-04/DOC-ICP-05.

III) Toda PC e DPC elaborada no âmbito da ICP-Brasil deve indicar no item 1.2 o tipo de certificado, o nome da instituição e o OID atribuído para a respectiva PC.

IV) Toda PC e DPC elaborada no âmbito da ICP-Brasil deve indicar no item 1.3 informações das entidades envolvidas e a aplicabilidade dos certificados.

b Toda PC e DPC elaborada no âmbito da ICP-Brasil deve indicar no item 6.1 a descrição dos requisitos e os procedimentos para geração e instalação do Par de Chaves referentes ao certificado que define.

VI) Toda PC e DPC elaborada no âmbito da ICP-Brasil deve indicar no item 7 a descrição de perfis do certificado que define.

VII) Toda DPC elaborada no âmbito da ICP-Brasil deve indicar no item 2 as disposições gerais conforme estabelecido no DOC-ICP-05.

VIII) Toda DPC elaborada no âmbito da ICP-Brasil deve indicar no item 3 os

requisitos de identificação e autenticação.

IX) Toda DPC elaborada no âmbito da ICP-Brasil deve indicar no item 4 os requisitos operacionais.

X) Toda DPC elaborada no âmbito da ICP-Brasil deve indicar no item 5 os controles de segurança física, procedimental e de pessoal.

XI) Toda PC e DPC elaborada no âmbito da ICP-Brasil deve indicar no item 6 os Controles Técnicos de Segurança.

XII) Toda PC e DPC elaborada no âmbito da ICP-Brasil deve indicar no item 7 os perfis de certificados e LCR.

b) Manter publicação de Instalações Técnicas de AR e PSS e Acordos Operacionais

I) A AC deve manter em seu repositório, localizado no endereço da página web indicado no item 1.3.2 e 1.3.3 de sua PC ou DPC, a publicação de dados referentes às Autoridades de Registro e PSS sob sua hierarquia.

c) Manter publicação de DPC, PC e PS

I) A publicação de repositório da AC devem estar disponível no mínimo 99,5% do mês, 24 horas por dia, 7 dias por semana.

• A AC deve manter em seu repositório, localizado no endereço da página web indicado no item 2.6 de sua DPC, as informações descritas no item 2.6.1.2 do DOC-ICP-05.

2.2.4.1.4 Manter publicação de LCR e do certificado da AC

a) A AC deve implementar recursos necessários para a segurança dos dados armazenados em seus respectivos repositórios.

II) A frequência de publicação de LCR e certificado da AC deve assegurar a disponibilização sempre atualizada de seus conteúdos.

1.3. Manter segurança lógica, composto pelos sub-processos:

a) Manter equipamentos protegidos de ameaças

I) O tráfego das informações no ambiente de rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos, incluindo-se o "*Efeito Tempest*".

II) Deve ser providenciado firewall no perímetro externo da rede.

III) Os sistemas de certificação devem ser dispostos em segmentos de rede que devem ser isolados por meios diversos, como por exemplo: a) utilizando virtual "*lans"* ("*vlan"*); b) utilizando "*firewall*" na conexão externa do segmento; c) utilizando artifícios de roteamento.

IV) Ativos de processamento da rede, a exemplo de " *switches*" e roteadores, quando possuírem recursos básicos de segurança como acesso mediante senhas e outros, devem ser configurados para utilizá-los, visando reforçar seus controles de segurança.

8. As configurações de ativos de rede devem ser corrigidas quando da ativação dos equipamentos

VI) Nos computadores pessoais, devem ser adotadas medidas para combate de vírus, realização de backups, controle de acesso e uso de software não autorizado.

VII) Em todos os equipamentos devem ser sistematizados procedimentos para combate a processos destrutivos (virus, "*worms"* e cavalos-de-tróia).

VIII) Implementar nos servidores da AC envolvidos diretamente com os processos de emissão, expedição distribuição, revogação ou gerenciamento de certificados, controles de segurança.

b) Manter *logs* e trilhas de auditoria

I) Informações de segurança não geradas pelo sistema de certificação devem ser registradas.

II) Registrar e avaliar periodicamente violações de segurança.

III) Definir, analisar periodicamente e proteger devidamente arquivos de *logs* de sistemas.

IV) Validações e verificações de solicitações de certificados devem ser registradas.

c) Manter cópias de segurança e restauração

I) Descrever na DPC os procedimentos para recuperação de recursos computacionais corrompidos

d) Manter controle de acesso lógico

I) Nos sistemas, registrar acessos lógicos em *logs*, mantendo-os por períodos definidos.

d) O ambiente operacional dos sistemas deve ser monitorado.

9.14 Manter controle técnico de segurança

Definir procedimentos formais para a eliminação segura de mídias desnecessárias.

f) Nos ambientes de rede, registrar e avaliar periodicamente eventos de segurança.

III) Para os sistemas de controle de acesso lógico, registrar e avaliar periodicamente eventos de segurança.

IV) Manter os equipamentos sincronizados com a hora legal brasileira, distribuída pelo Observatório Nacional, de forma segura.

1.4. Manter infra-estrutura, composto pelos sub-processos:

a) Manter ar-condicionado

I) O sistema de ar-condicionado deve possuir redundância.

II) O sistema de climatização deve atender às condições ambientais estabelecidas na Norma NBR 11515.

III) A temperatura ambiente atendida pelo sistema de climatização deve ser permanentemente monitorada por sistema de notificação e alarme.

IV) O sistema de ar-condicionado em ambiente de nível 4 deve ser interno. b)

Manter energia elétrica

I) A alimentação elétrica da rede local de computadores deve ser separada da rede elétrica convencional.

II) A energia elétrica para a infra-estrutura da AC deve possuir sistemas e dispositivos que garantam o fornecimento ininterrupto.

III) Todos os cabos elétricos devem estar protegidos por tubulações ou dutos apropriados.

IV) Sistema de aterramento deve ser implantado.

V) Tubulações, dutos, calhas, quadros e caixas - de passagem, distribuição e terminações - devem ser construídos de forma a facilitar vistorias e a detecção de tentativas de violações.

VI) Todos os cabos devem ser catalogados e vistoriados no mínimo a cada 6 (seis) meses.

VII) Deve ser mantida atualizada a topologia de rede de cabos.

VIII) Instalações elétricas provisórias, fiações expostas e conexões inadequadas devem ser evitadas.

c) Manter equipamentos de computação

I) Módulo criptográfico para geração de chaves assimétricas de usuário final e armazenamento da chave privada de titular de certificado deve possuir certificação padrão FIPS 140-1.

II) Módulo criptográfico para geração de chaves assimétricas de AC e armazenamento da chave privada de AC deve possuir certificação padrão FIPS 140-1 level 2.

III) Materiais criptográficos, tais como, chaves, dados de ativação, suas cópias e equipamentos criptográficos devem ser armazenados em ambiente de nível 5 (cinco) ou superior.

d) Manter sistema de combate a incêndio

I) Sistema de prevenção contra incêndio nos ambientes da AC devem possuir alarme preventivo acionado por detectores de fumaça/partículas.

II) Sala-cofre de nível 4 (quatro) deve possuir sistema de extinção de incêndio por gás.

III) A sala-cofre de nível 4 (quatro) deve possuir resistência ao fogo em

conformidade com a norma NBR 15247.

e) Manter controle de acesso físico

I) Acesso aos componentes de infra-estrutura física como quadro de energia, comunicações e cabeamentos deve ser restrito ao pessoal autorizado.

II) Todas as passagens entre os níveis de acesso, bem como os ambientes de nível 4 e o ambiente do sistema de monitoração devem possuir sistemas de CTFV, 24x7.

III) O uso de equipamentos não autorizados nas instalações da AC só podem ser utilizados após autorização formal e sob supervisão.

IV) Todas as pessoas que transitam nas instalações integrantes da ICP-Brasil devem utilizar alguma forma visível de identificação (por exemplo: crachá).

V) Acesso de visitantes aos ambientes da AC devem ser registrados e supervisionados.

VI) Todas as portas de passagens do nível 2 para o nível 3 e do nível 3 para o nível 4 devem ser monitoradas por sistema de notificação de alarmes.

VII) O ambiente de nível 4 deve possuir alarme de detecção de movimento permanentemente ativo enquanto não for satisfeito o critério de acesso ao ambiente.

VIII) A localização das instalações da AC não deve ser publicamente identificada.

IX) Sistemas de segurança para acesso físico deverão ser instalados para controlar e auditar o acesso aos sistemas de certificação.

X) Controles duplicados sobre o inventário e cartões/chaves de acesso deverão ser estabelecidos. Uma lista atualizada do pessoal que possui cartões/chaves deverá ser mantida.

XI) Chaves criptográficas sob custódia do responsável deverão ser fisicamente protegidas contra acesso não autorizado, uso ou duplicação.

XII) Perdas de cartões/chaves de acesso deverão ser imediatamente comunicadas ao responsável pela gerência de segurança da entidade. Ele deverá tomar as medidas apropriadas para prevenir acessos não autorizados.

XIII) Os sistemas de AC deverão estar localizados em área protegida ou afastada de fontes potentes de magnetismo ou interferência de rádio freqüência.

XIV) Recursos e instalações críticas ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Elas devem ser fisicamente protegidas de acesso não autorizado, dano, ou interferência. A proteção

fornecida deve ser proporcional aos riscos identificados.

XV) A entrada e saída, de instalações críticas, sensíveis ou partes dedicadas, deverão ser automaticamente registradas com data e hora definidas e serão revisadas diariamente pelo responsável pela gerência de segurança da informação nas entidades da ICP-Brasil e mantidas em local adequado e sob sigilo.

XVI) Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos.

XVII) A infra-estrutura de interligação lógica deve estar protegida contra danos mecânicos e conexão não autorizada.

XVIII) Componentes críticos da rede local devem ser mantidos em salas protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries.

XIX) Sistemas que executam a função de certificação deverão estar isolados para minimizar a exposição contra tentativas de comprometer o sigilo, a integridade e a disponibilidade das funções de certificação.

2 A chave de certificação das AC (ativação da AC) deve estar protegida fisicamente de acesso desautorizado, para garantir seu sigilo e integridade.

XXI) Equipamentos que executem operações sensíveis devem receber proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou componentes).

XXII) A AC deve registrar, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação como os registros de acessos físicos.

XXIII) Não deverá haver identificação pública externa das instalações e, internamente, não deverão ser admitidos ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações deverão ser segregadas em compartimentos fechados e fisicamente protegidos.

XXIV) A AC deve possuir pelo menos 4 (quatro) níveis de acesso físico aos diversos ambientes da AC responsável, e mais 2 (dois) níveis relativos à proteção da chave privada da AC.

XXV) As salas-cofre deverão ser construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas deverão ser sanadas por normas internacionais pertinentes.

XXVI) Não existem limitações de ambientes de quarto nível necessários para abrigar os equipamentos off-line, on-line, e os ativos de rede ("*firewall*", roteadores, "*switches"* e servidores).

XXVII) A Autoridade Certificadora deve possuir um cofre (quinto nível) com

capacidade de armazenar chaves criptográficas, materiais de ativação, suas cópias e equipamentos criptográficos.

XXVIII) Para garantir a segurança do material armazenado, o cofre ou o gabinete deverá ser feito em aço ou material de resistência equivalente; e, possuir tranca com chave.

XXIX) O sexto nível - ou nível 6 - deve se consistir de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos deve dispor de fechadura individual. Os dados de ativação da chave privada da AC deverão ser armazenados nesses depósitos.

XXX) O primeiro nível - ou nível 1 - deverá situar-se após a primeira barreira de acesso às instalações da AC. Para entrar em uma área de nível 1, cada indivíduo deverá ser identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da AC deverão transitar devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC deverá ser executado nesse nível.

XXXI) O segundo nível - ou nível 2 - será interno ao primeiro e deverá requerer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse será o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC. A passagem do primeiro para o segundo nível deverá exigir identificação por meio eletrônico, e o uso de crachá.

XXXII) Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações da AC, a partir do nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, terão sua entrada controlada e somente poderão ser utilizados mediante autorização formal e supervisão.

XXXIII) O terceiro nível - ou nível 3 - deverá situar-se dentro do segundo e será o primeiro nível a abrigar material e atividades sensíveis da operação da AC. Qualquer atividade relativa ao ciclo de vida dos certificados digitais deverá estar localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não deverão ter permissão para acesso a esse nível. Pessoas que não possuam permissão de acesso não poderão permanecer nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

XXXIV)No terceiro nível deverão ser controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle deverão ser requeridos para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica.

XXXV) Telefones celulares, bem como outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC, não serão admitidos a partir do nível 3.

XXXVI) No quarto nível - ou nível 4 -, interior ao terceiro, é onde deverão ocorrer atividades especialmente sensíveis da operação da AC, tais como a emissão e revogação de certificados e a emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades deverão estar localizados a partir desse nível. O nível 4 deverá possuir os mesmos controles de acesso do nível 3 e, adicionalmente, deverá exigir, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas deverá ser exigida enquanto o ambiente estiver ocupado.

XXXVII) No quarto nível, todas as paredes, piso e teto deverão ser revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto deverão ser inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não deverão permitir a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 - que constituem as chamadas salas-cofre - deverão possuir proteção contra interferência eletromagnética externa.

XXXVIII) Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, deverão ser monitoradas por câmeras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmeras não deverão permitir a recuperação de senhas digitadas nos controles de acesso.

XXXIX) As fitas de vídeo resultantes da gravação 24x7 deverão ser armazenadas por, no mínimo, 1 (um) ano. Elas deverão ser testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, 1 (uma) fita referente a cada semana. Essas fitas deverão ser armazenadas em ambiente de terceiro nível.

XL) Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente deverão ser monitoradas por sistema de notificação de alarmes. Onde houver, a partir do nível 2, vidros separando níveis de acesso, deverá ser implantado um mecanismo de alarme de quebra de vidros, que deverá estar ligado ininterruptamente.

XLI) Em todos os ambientes de quarto nível, um alarme de detecção de movimentos deverá permanecer ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais empregados, o critério mínimo de ocupação deixar de ser satisfeito, deverá ocorrer a reativação automática dos sensores de presença.

XLII) O sistema de notificação de alarmes deverá utilizar pelo menos 2 (dois) meios de notificação: sonoro e visual.

XLIII) O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, deverão ser permanentemente monitorados

por guarda armado e estar localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, deverão ser monitoradas por câmeras de vídeo cujo posicionamento deverá permitir o acompanhamento das ações do guarda.

XLIV) Mecanismos específicos deverão ser implantados pela AC para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos deverão permitir o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos deve acionar imediatamente os alarmes de abertura de portas.

XLV) Todo empregado da AC terá sua identidade e perfil verificados antes de: a) ser incluído em uma lista de acesso às instalações da AC; b) ser incluído em uma lista para acesso físico ao sistema de certificação da AC; c) receber um certificado para executar suas atividades operacionais na AC; e d) receber uma conta no sistema de certificação da AC.

XLVI) Todos os servidores e elementos de infra-estrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda o sistema de certificação da AC, deverão estar localizados e operar em ambiente de nível, no mínimo, 4..

f) Manter disponibilidade da planta

I) A estrutura inteiriça do ambiente de nível 4, construído na forma de célula estanque, deverá prover proteção física contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.

1.5. Manter sítio de contingência, composto pelos sub-processos:

a) Manter integridade dos dados

I) O processo de transporte de chaves criptográficas e demais parâmetros do sistema de criptografia da ICP-Brasil devem ter a integridade e o sigilo assegurados.

II) Recurso de VPN ((Virtual Private Networks - redes privadas virtuais), baseada em criptografia, deve ser adotada para a troca de informações entre o sítio principal e o sítio de contingência.

III) Uma segunda cópia de todo o material arquivado pela AC deve ser mantido em local externo ao sítio principal.

IV) A AC responsável pela DPC deve verificar a integridade das cópias de segurança armazenada no sítio de contingência, no mínimo, a cada 6 (seis) meses.

b) Ativar sítio de contingência

I) A instalação de backup (sítio de contingência) deve entrar em operação em condições idênticas ao principal em no máximo 48 (quarenta e oito) horas quando ocorrer sinistro que torne inoperante a instalação principal.

II) Os procedimentos de ativação do sítio de contingência devem ser regularmente testados, de modo a garantir a disponibilidade.

c) Ativar retorno ao sítio principal

I) Os procedimentos de retorno do sítio de contingência para o sítio principal devem ser regularmente testados, de modo a garantir a disponibilidade.

d) Manter infra-estrutura

I) Sistemas e dispositivos redundantes devem estar disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna.

II) Os controles estabelecidos no processo "4 - Manter Infra-estrutura" devem ser aplicados sob o contexto do sítio de contingência.

e) Manter segurança lógica

I) Os controles estabelecidos no processo "3 - Manter Segurança Logica" devem ser aplicados sob o contexto do sítio de contingência.

1.6. Manter sistemas aplicativos, composto pelos sub-processos:

a) Manter sistema de AR

I) As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis nas entidades.

II) A documentação dos sistemas deve ser mantida atualizada. III) A

cópia de segurança deve ser testada e mantida atualizada.

IV) Os sistemas devem ser avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção.

4.1.1.3 As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas.

VI) Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (time-out).

VII) O aplicativo que faz a interface entre a AR e AC deve possuir registro em log de auditoria dos eventos citados no item 4.5.1 do DOC-ICP-05.

VIII) O aplicativo que faz a interface entre a AR e AC deve possuir histórico da inclusão e exclusão dos Agentes de Registro no sistema e das permissões concedidas ou revogadas.

IX) O aplicativo que faz a interface entre a AR e AC deve possuir registro em

log, para em cada certificado emitido, informando se a validação da solicitação de certificados foi executada interna ou externamente ao ambiente da AR.

4.1.4 O aplicativo que faz a interface entre a AR e AC deve possuir mecanismo para revogação automática dos certificados digitais emitidos fora do ambiente da AR e que não tenham sido verificados pelo segundo Agente de Registro, mediante cópia da documentação apresentada na etapa de validação, até o momento do início da validade do certificado.

XI) Para atendimento do previsto no item 6.1 do DOC-ICP-05, esse aplicativo deve: a) ter sido desenvolvido com documentação formal; b) ter mecanismos para controle de versões; c) ter documentação dos testes realizados em cada versão; d) ter documentação comprovando a homologação de cada versão em ambiente com as mesmas características do que será usado em produção, sendo esses ambientes, porém, obrigatoriamente apartados entre si; e) ter aprovação documentada do gerente da AC, ou responsável designado, para colocar cada versão em ambiente de produção.

XII) A AR deve encaminhar as solicitações de emissão ou de revogação de certificados à AC utilizando VPN (Virtual Private Network - rede privativa virtual), SSL (Secure Socket Layer - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade.

XIII) Todas as etapas dos processos de validação e verificação da solicitação de certificado devem ser registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3.

XIV) Os registros de todas as etapas do processo de validação e verificação devem feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

XV) A AC responsável pela DPC deverá registrar em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Entre outros, os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria: a) iniciação e desligamento do sistema de certificação; b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC; c) mudanças na configuração da AC ou nas suas chaves; d) mudanças nas políticas de criação de certificados; e) tentativas de acesso (login) e de saída do sistema (logoff); f) tentativas não-autorizadas de acesso aos arquivos de sistema; g) geração de chaves próprias da AC ou de chaves de seus usuários finais; h) emissão e revogação de certificados; i) geração de LCR; j) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves; k) operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e l) operações de escrita nesse repositório, quando aplicável.

b) Manter sistema de AC

I) Os algoritmos de criação e de troca das chaves criptográficas utilizados no sistema criptográfico da ICP-Brasil devem ser aprovados pelo CG ICP-Brasil.

II) Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*).

III) A DPC deve observar que quando um evento for registrado pelo conjunto de sistemas de auditoria da AC responsável, nenhuma notificação deverá ser enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

IV) Neste item, quando cabível, deve ser definida a forma de controle múltiplo, do tipo “n” pessoas de um grupo de “m”, requerido para a utilização das chaves privadas. A DPC deve estabelecer a exigência de controle múltiplo para a utilização da chave privada da AC responsável. Pelo menos 2 (dois) detentores de partição de chave, formalmente designados pela AC, deverão ser requeridos para a utilização de sua chave privada.

2 Os dados de ativação da chave privada da AC responsável serão únicos e aleatórios.

VI) Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, serão únicos e aleatórios.

VII) A geração do par de chaves da AC responsável será realizada off-line, para impedir acesso remoto não autorizado.

VIII) Cada computador servidor da AC responsável, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, deverá implementar, entre outras, as seguintes características: a) controle de acesso aos serviços e perfis da AC; b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC; c) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações; d) geração e armazenamento de registros de auditoria da AC; e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e f) mecanismos para cópias de segurança (backup).

IX) Os processos de projeto e desenvolvimento conduzidos pela AC deverão prover documentação suficiente para suportar avaliações externas de segurança dos componentes da AC.

X) Devem ser descritas as ferramentas e os procedimentos empregados pela AC responsável e pelas ARs vinculadas para garantir que os seus sistemas e redes operacionais implementem os níveis configurados de segurança.

XI) Uma metodologia formal de gerenciamento de configuração deverá ser

usada para a instalação e a contínua manutenção do sistema de certificação da AC.

c) Manter sistemas básicos

I) Os aplicativos e equipamentos utilizados nos processos de certificação digital devem possuir certificado FIPS ou NSH (Nível de Segurança de Homologação) compatível emitido pelo LEA.

II) Devem ser adotados procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração do Sistema Operacional e de outros arquivos críticos. Os eventos devem ser armazenados em relatórios de segurança (logs) de modo que sua análise permita a geração de trilhas de auditoria a partir destes registros.

III) As máquinas devem estar sincronizadas para permitir o rastreamento de eventos.

IV) A versão do Sistema Operacional, assim como outros softwares básicos instalados em máquinas servidoras, devem ser mantidos atualizados, em conformidade com as recomendações dos fabricantes.

V) Devem ser utilizados somente softwares autorizados pela própria entidade nos seus equipamentos. Deve ser realizado o controle da distribuição e instalação dos mesmos.

VI) Devem ser adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede.

VII) A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação.

VIII) A AC responsável pela DPC deverá registrar, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como: a) registros de acessos físicos; b) manutenção e mudanças na configuração de seus sistemas; c) mudanças de pessoal e de perfis qualificados; d) relatórios de discrepância e comprometimento; e e) registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

IX) As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (patches), disponibilizadas pelos respectivos fabricantes deverão ser implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.

d) Manter bases de dados

I) Todo parâmetro crítico, cuja exposição indevida comprometa a segurança do sistema criptográfico da ICP-Brasil, deve ser armazenado cifrado.

II) O processo de transporte de chaves criptográficas e demais parâmetros do sistema de criptografia da ICP-Brasil devem ter a integridade e o sigilo assegurados, por meio do emprego de soluções criptográficas específicas.

4.3 Os dados, as informações e os sistemas de informação das entidades e sob sua guarda, devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

IV) Informações sigilosas, corporativas ou que possam causar prejuízo às entidades devem estar protegidas e não devem ser enviadas para outras redes, sem proteção adequada.

V) As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, devendo ser adotados procedimentos de *backup*, definidos em documento específico.

VI) As LCRs e os certificados de assinatura digital deverão ser retidas permanentemente, para fins de consulta histórica.

VII) as cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 30 (trinta) anos a contar da data de expiração ou revogação do certificado.

VIII) As demais informações, inclusive arquivos de auditoria, deverão ser retidas por, no mínimo, 6 (seis) anos.

IX) Devem ser estabelecidos os formatos e padrões de data e hora contidos em cada tipo de registro.

1.7. Manter recursos humanos, composto pelos sub-processos:

a) Avaliar desempenho

I) Acompanhar o desempenho e avaliar periodicamente os empregados ou servidores com o propósito de detectar a necessidade de atualização técnica e de segurança.

II) Dar aos empregados ou servidores das entidades acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança.

III) Deve ser realizado processo de avaliação de desempenho da função que documente a observação do comportamento pessoal e funcional dos empregados, a ser realizada pela chefia imediata dos mesmos.

IV) Deverão ser motivo de registro atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do empregado.

V) Os comportamentos incompatíveis, ou que possam gerar

comprometimentos à segurança, deverão ser averiguados e comunicados à chefia imediata.

VI) As chefias imediatas assegurarão que todos os empregados ou servidores tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor.

b) Manter capacitação de pessoas

I) Todo o pessoal deve receber as informações necessárias para cumprir adequadamente o que está determinado na PS.

II) Um programa de conscientização sobre segurança da informação deverá ser implementado para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações das entidades. Especialmente, o pessoal envolvido ou que se relaciona com os usuários deve estar treinado sobre ataques típicos de engenharia social, como proceder e como se proteger deles.

III) Deve ser definido um processo pelo qual será apresentada aos empregados, servidores e prestadores de serviço esta PS e as normas e procedimentos relativos ao trato de informações e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento.

IV) Nos itens seguintes da DPC devem ser descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC responsável e nas ARs a ela vinculadas, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, deve também ser estabelecido o número de pessoas requerido para sua execução.

4.4 Todo o pessoal da AC responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá receber treinamento documentado, suficiente para o domínio dos seguintes temas: a) princípios e mecanismos de segurança da AC e das ARs vinculadas; b) sistema de certificação em uso na AC; c) procedimentos de recuperação de desastres e de continuidade do negócio; d) reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.1.9 e 3.1.10 e 3.1.11; e e) outros assuntos relativos a atividades sob sua responsabilidade.

VI) Todo o pessoal da AC responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá ser mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC ou das ARs.

c) Manter habilitação de pessoas

I) Os processos que envolvem as chaves criptográficas utilizadas nos sistemas criptográficos da ICP-Brasil deverão ser executados por um número mínimo e essencial de pessoas, assim como devem estar submetidos a mecanismos de controle considerados adequados pelo CG ICP-Brasil.

II) As pessoas, a que se refere o item anterior, deverão ser formalmente designadas pela chefia competente, conforme as funções a serem desempenhadas e o correspondente grau de privilégios, assim como terem suas responsabilidades explicitamente definidas.

III) Todo pessoal envolvido com o PCN deve receber um treinamento específico para poder enfrentar estes incidentes.

IV) Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado.

V) Devem ser adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros das entidades integrantes da ICP-Brasil, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade das entidades.

VI) Nenhuma entidade participante da ICP-Brasil admitirá estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados.

VII) O empregado, funcionário ou servidor assinará termo de compromisso assumindo o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos das entidades integrantes da ICP-Brasil.

VIII) Todos os empregados da AC deverão estar identificados por uma credencial de segurança de acordo com a informação e, consequentemente, com o grau de sigilo compatível ao cargo e/ou a função a ser desempenhada. Deverá existir um responsável designado para emitir as credenciais de segurança, e esse profissional deve possuir o conhecimento necessário para verificar que tipo de credencial deve ser emitida. As credenciais de segurança deverão ter prazo de expiração e deverão ter mecanismos de renovação desses prazos.

IX) As responsabilidades pela segurança física dos sistemas das entidades deverão ser definidos e atribuídos a indivíduos claramente identificados na organização.

X) Os usuários e administradores do sistema de controle de acesso devem ser formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso.

XI) Todo Agente de Registro, na ocasião de sua admissão, deve receber

treinamento documentado, com carga horária mínima de 16 horas, sobre os seguintes temas: a) princípios e mecanismos de segurança da AR; b) sistema de certificação em uso na AC; c) procedimentos de recuperação de desastres e de continuidade do negócio; d) reconhecimento de assinaturas e validade dos documentos apresentados; e) outros assuntos relativos a atividades sob sua responsabilidade.

XII) Somente após o recebimento da solicitação de habilitação do Agente de Registro e da declaração prevista no item anterior, a AC ou AR (nos casos previstos no item 2.1.3) pode incluí-lo nas bases de dados e conceder as permissões de acesso no sistema de certificação, sendo necessária para isso prévia autorização documentada do Gerente da AC ou do responsável por ele designado.

XIII) Na DPC devem ser descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC responsável e nas ARs a ela vinculadas, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, deve também ser estabelecido o número de pessoas requerido para sua execução.

XIV) A AC responsável pela DPC deverá garantir a separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize indevidamente o seu sistema de certificação sem ser detectado. As ações de cada empregado deverão estar limitadas de acordo com seu perfil.

XV) A AC deverá estabelecer um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

XVI) Todos os operadores do sistema de certificação da AC deverão receber treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso serão determinados, em documento formal, com base nas necessidades de cada perfil.

XVII) Todas as tarefas executadas no ambiente onde estiver localizado o equipamento de certificação da AC deverão requerer a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC poderão ser executadas por um único empregado.

XVIII) Procedimentos de verificação de antecedentes.

XIX) Requisitos de treinamento.

d) Admitir pessoas

I) Todo o pessoal da AC responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá ser admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. A AC responsável poderá definir requisitos adicionais para a admissão.

II) Todo o pessoal da AC responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá ser contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. A AC responsável poderá definir requisitos adicionais para a contratação.

e) Suspender, movimentar e desligar pessoas

I) Os procedimentos deverão ser documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos, remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados.

II) Suspensão e Desligamento.

III) Quando um empregado se desligar da AC, suas permissões de acesso deverão ser revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro da AC, deverão ser revistas suas permissões de acesso. Deverá existir uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC no ato de seu desligamento.

1.8. Manter credenciamento de AC, composto pelos sub-processos:

a) Manter contrato de seguro

I) Manter contrato de seguro de responsabilidade civil vigente.

b) Manter histórico de agentes de registro

I) A AR deve enviar à AC a relação atualizada dos Agentes de Registro em atividade, seus perfis qualificados e suas necessidades de acesso a informações do gerenciamento de ciclo de vida dos certificados. A AC deve manter essa informação atualizada, organizada e consolidada por instalação técnica, inclusive com o histórico das alterações realizadas, à disposição do ITI para os procedimentos de auditoria e fiscalização.

c) Regularizar não-conformidades identificadas

I) Cabe à entidade auditada cumprir, no prazo estipulado no relatório de auditoria, as recomendações para corrigir os casos de não-conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas.

d) Comunicar mudanças operacionais e violação de normas

I) A AC deve comunicar formalmente e imediatamente as mudanças operacionais ocorridas em seu ambiente de certificação e qualquer violação de normas da ICP-Br.

II) Os acordos operacionais realizados pelas AR vinculadas devem possuir

claramente a obrigação da execução de, pelo menos, uma das tarefas abaixo: a) Confirmação da identidade do titular ou do responsável pelo certificado – processo realizado mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos; b) Validação da solicitação de certificado - conferência dos dados da solicitação de certificado com os constantes dos documentos necessários para autenticação da identidade de um indivíduo ou de uma organização; c) Aprovação da solicitação de certificado - confirmação da validação realizada e liberação da emissão do certificado no sistema da AC.

III) Deve existir procedimentos formais para suspensão de acessos (físico e lógico) para empregados sob suspeita e para instauração de processos administrativos com as seguintes características: a) relato da ocorrência com "modus operandis "; b) identificação dos envolvidos; c) eventuais prejuízos causados; d) punições aplicadas, se for o caso; e e) conclusões.

e) Manter requisitos de manutenção de credenciamento

I) A AC deve possuir os seguintes procedimentos, quando necessário: a) comunicar, desde logo, à AC Raiz ou à AC a que está subordinada: i). qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores; ii). desvinculação de AC, de AR ou de PSSs credenciados; ou iii). violação, de que tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil, cometida pelas ACs, ARs ou pelos PSSs que lhe sejam operacionalmente vinculados. b) solicitar à AC Raiz autorização para alterar sua DPC, suas PCs ou sua Política de Segurança – PS, constantes dos documentos relacionados no Anexo I. c) manter os titulares dos certificados informados acerca de eventual sucessão de AC ou AR operacionalmente vinculadas; d) encaminhar à AC Raiz, até o dia 15 (quinze) de março de cada ano, cronograma das auditorias a serem realizadas, durante o ano, nas entidades que lhe sejam operacionalmente vinculadas; e) encaminhar à AC Raiz relatórios de auditorias realizadas nas entidades que lhe sejam operacionalmente vinculadas, até 30 (trinta) dias após sua conclusão.

f) Manter condições fisco-tributárias e econômico-financeiras

I) A AC deve manter as mesmas condições de qualificação quando do credenciamento, quais sejam: Relativos a sua regularidade fiscal: a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual; c) Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei. Relativos

a sua qualificação econômico-financeira: a) Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI), afirmando que o candidato se encontra em boa situação financeira para a execução das atividades a que se propõe, junto à ICP-Brasil. b) Certidão negativa de falência ou concordata expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente.

g) Manter e cumprir PS de AC

2 Todos os empregados devem possuir conhecimento da PS da AC que a deve divulgar.

II) Os empregados, as chefias e os prestadores de serviços devem conhecer os deveres e as responsabilidades definidas na PS.

III) Os procedimentos de combate a processos destrutivos (vírus, cavalo-de-tróia e worms) devem estar sistematizados e devem abranger máquinas servidoras, estações de trabalho, equipamentos portáteis e microcomputadores *stand alone*.

1.9. Credenciar e manter PSC, composto pelos sub-processos:

a) Auditar PSC

I) Auditorias de conformidade deve ser realizada conforme frequência estabelecida na DOC-ICP-08 em todas as entidades operacionalmente vinculadas à AC sob avaliação.

II) As AC devem encaminhar à AC RAIZ, no prazo estabelecido pela DOC-ICP-08, cronograma das auditorias a serem realizadas, durante o ano, nas entidades que lhe sejam operacionalmente vinculada.

III) As AC devem encaminhar à AC RAIZ relatórios de auditorias realizadas nas entidades que lhe sejam operacionalmente vinculada até 30 (trinta) dias após sua conclusão.

IV) A AC deverá incluir cláusula contratual exigindo da entidade de auditoria independente que o trabalho de auditoria seja realizado por corpo técnico com pelo menos 2 (dois) anos de experiência na área de segurança da informação (ambiente físico e lógico), criptografia, infra-estrutura de chaves públicas e sistemas críticos.

V) A AC deverá incluir cláusula contratual exigindo da entidade de auditoria independente que o trabalho de auditoria seja realizado por com pelo menos 2 (dois) anos de experiência em serviços de auditoria em TI ou similares.

VI) A equipe de auditoria contratada pela AC para realizar auditoria em seu âmbito ou cadeia deve ser totalmente independente da entidade auditada, aplicando-se no que couber, as regras de suspeição e impedimentos estabelecidas nos artigos 134 e 135 do Código de Processo Civil.

VII) Os auditores contratados pela AC para realizar auditoria em seu âmbito devem firmar declaração, sob as penas da lei, de que não se enquadram em quaisquer das causas de impedimento.

VIII) As auditorias de conformidade vinculadas à AC tem por objeto todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo os processos de solicitação até a revogação de certificados.

IX) Os documentos, registros históricos e demais elementos materiais que deram subsídios à elaboração dos relatórios de auditoria devem ficar sob guarda da AC responsável, em local seguro, pelo prazo mínimo de 5 (cinco) anos.

X) Os serviços de auditoria devem ser executados diretamente pela empresa de auditoria contratada ou pelo órgão de auditoria independente sendo vedada a subcontratação total ou parcial de serviços.

b) Observar procedimentos de extinção de PSC

I) As ACs devem comunicar à AC RAIZ, por intermédio da cadeia de hierarquia, a desvinculação de AC, AR ou PSS credenciado sob sua responsabilidade.

II) As ACs devem manter os registros dos procedimentos de extinção de instalação técnica de AR descritos no item 3.2.2.2 da DOC-ICP-03.

III) Caso a AR possua um único endereço de instalação técnica, a extinção deste, sem a abertura concomitante de um novo endereço de instalação técnica deve ser tratado pela AC como extinção de AR.

IV) As AR devem encaminhar por intermédio da AC à qual está vinculada relatório de extinção de posto provisório conforme disposto no item 3.2.4 do DOC-ICP-03.

V) As AR devem encaminhar por intermédio da AC à qual está vinculada relatório de extinção de posto provisório conforme disposto no item 3.2.4 do DOC-ICP-03.

VI) Caso ocorra uma ou mais das hipóteses previstas no item 4 da DOC-ICP-03, para encerramento de AC, AR ou PSS vinculada, as AC devem proceder o descredenciamento, conforme o caso, da AC ou AR vinculada.

VII) Nos descredenciamentos de AC, AR e PSS as AC ao qual se vinculam devem executar os procedimentos previstos no item 4 da DOC-ICP-03.

VIII) As AC devem executar os procedimentos descrito em suas DPC em relação ao disposto no item 4.9.1, que trata da notificação aos usuários, transferência de guarda de seus dados e registros de arquivos quando da extinção de AC, AR e PSS vinculada.

e) Observar procedimentos de credenciamento de PSC

As AC devem observar os critérios a serem atendidos pelos candidatos a

credenciamento na ICP-Brasil sob sua vinculação.

II) Todas as comunicações e requerimentos devem ser encaminhados por intermédio da cadeia de AC ou candidato à AC.

III) Nos credenciamentos de AC, AR e PSS, as AC ao qual se candidatam a vinculação devem executar os procedimentos previstos no item 2.2 da DOC-ICP-03.

d) Manter credenciamento de PSC

I) Nas aberturas de novos endereços de instalações técnicas, postos provisórios, contrato com serviços notariais e na celebração de acordos operacionais com outras ARs, as AC ao qual se candidatam a vinculação devem executar os procedimentos previstos no item 3.2 da DOC-ICP-03.

II) As alterações de endereço de instalação técnica de AR previamente reportadas às ACs responsáveis devem ser enviadas ao ITI (formulário de credenciamento ADE-ICP-03.E com os dados atualizados e com a solicitação de nova autorização de funcionamento, acompanhada dos documentos previstos no DOC-ICP-03.

III) A alteração de endereço de posto provisório de AR após a autorização de funcionamento dada pelo ITI, mediante intimação da solicitante, é vedada.

IV) Qualquer alteração em atos constitutivos, estatuto, contrato social ou administradores seus ou de seus vinculados; desvinculação de AC, AR ou PSS credenciados sob sua responsabilidade; ou ainda violação das diretrizes e normas técnicas da ICP-Brasil cometidas pela própria ou pelas AC, AR ou PSS que lhe sejam operacionalmente vinculados devem ser comunicadas ao ITI.

1.10. Manter segurança da informação, composto pelos sub-processos:

a) Manter inventário de ativos

I) Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado.

II) O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento deve estar registrado e mantido atualizado em intervalos de tempo definidos pelas entidades participantes da ICP-Brasil.

O inventário de todo o conjunto de ativos de processamento deve ser registrado e mantido atualizado, no mínimo, mensalmente.

b) Manter análise de risco e PCN

I) Todas as ACs integrantes da ICP-Brasil deverão apresentar um PCN que estabelecerá, no mínimo, o tratamento adequado dos seguintes eventos de segurança: a) comprometimento da chave privada das entidades; b)

invasão do sistema e da rede interna da entidade; c) incidentes de segurança física e lógica; d) indisponibilidade da Infra-estrutura; e, e) fraudes ocorridas no registro do usuário, na emissão, expedição, distribuição, revogação e no gerenciamento de certificados.

JJ) Um Plano de Continuidade do Negócio – PCN deve ser implementado e testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio.

III) Todas as AC devem apresentar plano de gerenciamento de incidentes e de ação de resposta a incidentes a serem aprovados pela AC Raiz ou AC de nível imediatamente superior. Este plano deve prever, no mínimo, o tratamento adequado dos seguintes eventos: a) comprometimento de controle de segurança em qualquer evento referenciado no PCN; b) notificação à comunidade de usuários, se for o caso; c) revogação dos certificados afetados, se for o caso; d) procedimentos para interrupção ou suspensão de serviços e investigação; e) análise e monitoramento de trilhas de auditoria; e) relacionamento com o público e com meios de comunicação, se for o caso.

IV) Todos os incidentes devem ser reportados à AC Raiz imediatamente, a partir do momento em que for verificada a ocorrência. Estes incidentes devem ser reportados de modo sigiloso a pessoas especialmente designadas para isso.

V) Todos os ativos de processamento das entidades devem estar relacionados no PCN.

VI) Todo pessoal envolvido com o PCN deve receber um treinamento específico para poder enfrentar estes incidentes.

VII) A AC responsável deve descrever os procedimentos de notificação e recuperação a serem utilizados nos seguintes casos: a) quando os recursos computacionais, software ou dados estiverem corrompidos ou houver suspeita de corrupção; b) na circunstância de revogação de certificados; c) na circunstância de comprometimento da chave privada da AC Responsável; d) após a ocorrência de um desastre natural ou de outra natureza, antes do restabelecimento de um ambiente seguro.

VIII) Em um processo de gerenciamento de riscos, que visa a proteção dos serviços das entidades integrantes da ICP-Brasil, os seguintes pontos principais devem ser identificados: a) o que deve ser protegido; b) a análise de riscos (contra quem ou contra o quê deve ser protegido); c) avaliação de riscos (análise da relação custo/benefício).

IX) A localização dos serviços baseados em sistemas de proteção de acesso (firewall) deve ser resultante de uma análise de riscos. No mínimo, os seguintes aspectos devem ser considerados: a) requisitos de segurança definidos pelo serviço; b) objetivo do serviço, público alvo; c) classificação da informação; d) forma de acesso; e) frequência de atualização do conteúdo; f) forma de administração do serviço e volume de tráfego.

X) O processo de gerenciamento de riscos deve ser revisto, no máximo a cada 18 (dezoito) meses, pela própria entidade, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados.

c) Manter documentos armazenados e classificados

I) Toda a documentação fornecida ao pessoal deve estar classificada segundo a política de classificação de informação definida pela AC e deve ser mantida atualizada.

II) A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, deve ser elaborado um sistema de classificação da informação.

III) Os registros devem ser protegidos e armazenados de acordo com a sua classificação.

IV) As cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 30 (trinta) anos a contar da data de expiração ou revogação do certificado.

2. Os processos nas AR – Autoridades de Registro estão assim distribuídos:

2.1. Atender solicitação e revogação de certificados, composto pelos sub-processos:

a) Identificar solicitante (presencial), que possui os seguintes controles:

I) A solicitação feita pelo titular/candidato deve ser presencial. Base legal: DOC-ICP-05 item 3.1.9.

II) Documentos obrigatórios de identificação, em suas versões originais, do solicitante devem ser apresentados durante/anteriormente a identificação presencial. Base legal: DOC-ICP-05 item 3.1.9 - 3.1.10 e 3.1.11.

III) A identidade do indivíduo deve ser confirmada pelo agente de registro. Base legal: DOC-ICP-05 item 3.1.1.1.a.i

IV) A identidade da organização deve ser confirmada pelo agente de registro. Base legal: DOC-ICP-05 item 3.1.1.1.a.ii.

V) O processo de validação realizado por agente de registro fora do ambiente de AR deve ser feito utilizando ambiente computacional auditável e devidamente registrado no inventário de hardware e software da AR. Base legal: DOC-ICP-05 item 3.1.1.2.

b) Avaliar documentos originais e cópias, que possui os seguintes controles:

I) O termo de titularidade deve ser assinado pelo candidato a titular. Base legal: DOC-ICP-05 item 3.1.10.1.3.d e 3.1.9.1.

II) O termo de responsabilidade deve ser assinado pelo responsável indicado pela organização. Base legal: DOC-ICP-05 item 3.1.10.1.2.

c) Confrontar dados de solicitação com documentos originais, que possui os seguintes controles:

I) Os dados da solicitação de certificado devem ser conferidos com os documentos originais apresentados. Base legal: DOC-ICP-05 item 3.1.1.1.a.iii.

d) Confrontar dados de solicitação com as cópias dos documentos, que possui os seguintes controles:

I) A validação dos dados dos certificados deve ser confirmada pelo agente de registro. Base legal: DOC-ICP-05 item 3.1.1.1.b.

II) A verificação da solicitação de certificado deve ser efetuada por agente de registro distinto do que executou a etapa de validação. Base legal: DOC-ICP-05 item 3.1.1.1.b.i.

III) A verificação da solicitação de certificado deve ser realizada em uma das instalações técnicas da AR. Base legal: DOC-ICP-05 item 3.1.1.1.b.ii.

IV) A verificação da solicitação de certificado deve ser realizada somente após o recebimento das cópias dos documentos pela instalação técnica de AR. Base legal: DOC-ICP-05 item 3.1.1.1.b.iii.

V) O certificado emitido com início de validade futura cuja verificação não ocorra antes do início de validade deve ser revogado automaticamente. Base legal: DOC-ICP-05 item 3.1.1.1.b.iv.

VI) Os processos de validação e verificação de solicitação de certificados devem ser registrado e assinados na solução de certificação disponibilizada pela AC. Base legal: DOC-ICP-05 item 3.1.1.3.

e) Revogar certificados, que possui os seguintes controles:

I) A revogação de certificado será solicitação pelo titular, que será identificado. Base legal: DOC-ICP-05 item 3.4 e DPC da AC, item 3.4.

II) A identidade do indivíduo deve ser confirmada pelo agente de registro. Base legal: DOC-ICP-05 item 3.4, DPC da AC, item 3.4.

III) A identidade da organização deve ser confirmada pelo agente de registro. Base legal: DOC-ICP-05 item 3.4, DPC da AC, item 3.4.

f) Armazenar documentos, que possui os seguintes controles:

I) Os documentos que compõem o dossiê dos titulares de certificado devem ser mantidos em arquivo chaveado num ponto de centralização pré-estabelecido. Base legal: DOC-ICP-05 item 3.1.1.4 e DOC-ICP-03.01 item 6.2.3.

II) Os documentos digitalizados cujas cópias devam constar no dossiê do titular do certificado devem ser assinados digitalmente com uso de

certificado ICP-Brasil e arquivados no ponto de centralização. Base legal: DOC-ICP-03.01 item 6.2.2.a.

III) Todos os arquivos que compõem um dossiê do titular do certificado devem ser organizados de forma a permitir sua recuperação conjunta, para fins de fiscalização e auditoria. Base legal: DOC-ICP-03.01 item 6.2.2.c.

IV) O diretório ou sistema onde são armazenados os documentos digitalizados do dossiê do titular do certificado deve ser protegido contra leitura e gravação, dando permissão de acesso somente aos agentes de registro ou responsáveis designados formalmente para trabalhar com os documentos. Base legal: DOC-ICP-03.01 item 6.2.2.d.

V) Procedimentos de cópias e recuperação dos documentos digitalizados em caso de sinistro devem ser especificados. Base legal: DOC-ICP-03.01 item 6.2.2.e.

VI) A AR deve ser capaz de determinar facilmente e a qualquer momento o local onde se encontra cada dossiê de titular de certificado que se encontra sob sua guarda. Base legal: DOC-ICP-03.01 item 6.2.6.

VII) Os pontos de centralização dos dossiês de titulares de certificados devem atender aos requisitos de segurança da instalação técnica. Base legal: DOC-ICP-03.01 item 6.2.7.

g) Transportar documentos, que possui os seguintes controles:

I) A remessa ou transmissão do dossiê para o local de armazenamento definitivo deve ser feita por meio seguro, no prazo máximo de 30 dias corridos, a partir da geração do dossiê. Base legal: DOC-ICP-03.01 item 6.2.5.

2.2. Manter Recursos Humanos, composto pelos sub-processos:

a) Avaliar desempenho, que possui os seguintes controles:

I) O acompanhamento de desempenho das funções e avaliação anual dos agentes de registro devem ser realizados. Base legal: DOC-ICP-03.01, item 2.4.1 DOC-ICP-02, item 7.3.5.1 e item 7.3.8.

b) Manter capacitação de pessoas, que possui os seguintes controles:

I) Todo agente de registro, na ocasião de sua admissão, deve receber treinamento documentado, em princípios e mecanismos de segurança da informação. Base legal: DOC-ICP-03.01, item 2.3, DOC-ICP-02, item 6.1.2.

II) Todo agente de registro deve manter-se atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC ou da AR. Base legal: DOC-ICP-05, item 5.3.4

III) Todo agente de registro, na ocasião de sua admissão, deve receber

treinamento documentado, em reconhecimento de assinaturas (grafotecnia) e validade dos documentos apresentados. Base legal: DOC-ICP-03.01, item 2.3.d.

IV) Todo agente de registro, na ocasião de sua admissão, deve receber treinamento documentado, referente ao sistema de certificação em uso na AC. Base legal: DOC-ICP-03.01, item 2.3.b.

c) Manter habilitação de Agentes de Registro, que possui os seguintes controles:

I) Antecedentes criminais dos agentes de registro devem ser verificados no processo de admissão. Base legal: DOC-ICP-03.01, item 2.2.1.b, DOC-ICP-05, item 5.3.2.1.a.

II) Situação de crédito dos agentes de registro devem ser verificados no processo de admissão. Base legal: DOC-ICP-03.01, item 2.2.1.c, DOC-ICP-05, item 5.3.2.1.b.

III) A habilitação e desabilitação (se for o caso) do agente de registro no sistema de certificação da AC deve ser formalizada e confirmada. Base legal: DOC-ICP-03.01, item 2.2.1.j.

IV) Os documentos de cada agente de registro que esteja atuando ou que já atuou em AR deve ser armazenados em um dossiê. Base legal: DOC-ICP-03.01, item 2.2.

V) Na eventualidade de ação não autorizada por agente de registro, real ou suspeita, deve-se suspender o acesso dessa pessoa ao sistema de certificação, e instaurar processo administrativo. Base legal: DOC-ICP-05, item 5.3.6.

d) Admitir Agentes de Registro, que possui os seguintes controles:

I) Os agentes de registro devem ser funcionários ou servidores da própria organização credenciada ou candidata ao credenciamento como AR junto à ICP-Brasil. Base legal: DOC-ICP-03.01, item 2.1.2, DOC-ICP-02, item 7.3.1.2.

II) Entrevista de Admissão dos agentes de registro deve ser realizada e formalizada documentalmente por profissional qualificado. Base legal: DOC-ICP-02, item 7.3.4.

III) Pesquisa do histórico de empregos anteriores deve ser realizado para os candidatos a agente de registro. Base legal: DOC-ICP-02, item 7.3.3, DOC-ICP-03.01, item 2.2.1.d.

IV) Termos de compromisso e das condições do perfil que ocuparão devem ser registrados em contrato ou termo de responsabilidade dos agentes de registro. Base legal: DOC-ICP-05, item 5.3.

V) Nível de escolaridade do agente de registro. Base legal: DOC-ICP-03.01, item 2.2.1.e, DOC-ICP-05, item 5.3.2.1.d.

VI) Comprovante de residência deve ser apresentado no processo de

admissão de agentes de registro. Base legal: DOC-ICP-03.01, item 2.2.1.e, DOC-ICP-05, item 5.3.2.1.d.

e) Suspender, movimentar e desligar pessoas, que possui os seguintes controles:

I) Declaração, antes do desligamento, de que não possui qualquer tipo de pendência junto às diversas unidades que compõem a entidade deve ser firmada pelo empregado ou servidor . Base legal: DOC-ICP-02, item 7.3.10.

II) Credenciais, identificações e acessos físicos e lógicos de agentes de registro desligados ou suspensos devem ser revogados. Base legal: DOC-ICP-02, item 7.3.9.

III) Entrevista de desligamento de agente de registro deve ser realizada. Base legal: DOC-ICP-02, item 7.3.11.

f) Manter dossiê de Agentes de Registro, que possui os seguintes controles:

I) Os dossiês de agentes de registro devem ficar armazenados em um mesmo ponto de centralização da AR. Base legal: DOC-ICP-03.01, item 6.2.

II) Antecedentes criminais dos agentes de registro devem ser renovados por período (anual ou bianual) definido na DPC. Base legal: DOC-ICP-03.01, item 2.4.2, DOC-ICP-05, item 5.3.2.1.a.

III) Situação de crédito dos agentes de registro devem ser renovados por período (anual ou bianual) definido nas normas da ICP-Brasil. Base legal: DOC-ICP-03.01, item 2.4.2, DOC-ICP-05, item 5.3.2.1.b.

2.3. Manter segurança física, lógica e da informação, composto pelos sub-processos:

a) Manter inventário de ativos, que possui os seguintes controles:

I) O inventário de todos os ativos da AR deve ser mensalmente atualizado. Base legal: DOC-ICP-02, item 6.3 e item 8.2.12, DOC-ICP-03.01, item 6.1.6 e item 6.1.7.

II) O inventário de ativos deve manter histórico das alterações e ser assinado pelo responsável pela instalação técnica ou posto provisório. Base legal: DOC-ICP-03.01, item 6.1.6.

b) Manter análise de risco e PCN, que possui os seguintes controles:

I) Plano de Continuidade de Negócios (PCN) deve ser implementado e testado anualmente. Base legal: DOC-ICP-02, item 6.4.1, item 13, DOC-ICP-03.01, item 6.1.3, item 6.1.4, DOC-ICP-05, item 4.8.5.

II) O processo de gerenciamento de risco deve ser realizado e revisto no máximo a cada 18 (dezoito) meses. Base legal: DOC-ICP-02, item 6.2 e 12, DOC-ICP-03.01, item 6.1.3.

c) Manter documentos armazenados e classificados, que possui os seguintes

controles:

I) Sistema de classificação da informação deve ser elaborado para proteger as informações de acordo com o seu valor, sensibilidade e criticidade. Base legal: DOC-ICP-02, item 9.2.1, DOC-ICP-03.01, item 6.1.1.

II) Cópias atualizadas dos documentos de cada Instalação Técnica ou Posto Provisório de AR relacionados no item 6.1.2 do DOC-ICP-03-01 devem estar armazenados em um dossiê. Base legal: DOC-ICP-03.01, item 6.1.2.

III) Uma cópia do PCN deve estar armazenada em local seguro, fora da sala da AR. Base legal: DOC-ICP-03.01, item 5.1.

IV) Dossiês dos titulares de certificados e da instalação técnica ou posto provisório devem ser guardados, obrigatoriamente, em armário chaveado, com acesso permitido somente aos agentes de registro. Base legal: DOC-ICP-03.01, item 6.2.1.

V) Caso a AR opte pela substituição da guarda física dos dossiês de agente de registro e de titulares de certificados por digitalização dos mesmos, os documentos cujas cópias devam constar nos dossiês devem ser digitalizados e assinados digitalmente com certificado ICP-Brasil. Base legal: DOC-ICP-03.01, item 6.2.2.

VI) Todos os arquivos digitais que compõem os dossiês devem ser organizados de forma a permitir sua recuperação conjunta e devem ter proteção contra leitura e gravação, com permissão de acesso somente aos agentes de registro ou responsáveis formalmente designados. Base legal: DOC-ICP-03.01, item 6.2.2.

VII) Os dossiês de titulares de certificados, em papel ou digitalizados, devem ser armazenados na própria instalação técnica de AR, quando houver apenas uma instalação técnica; em um dos pontos de centralização da AR, para aquelas que possuam mais de uma instalação técnica; ou no ponto de centralização da AC à qual a AR estiver vinculada. Base legal: DOC-ICP-03.01, item 6.2.3.

VIII) A remessa ou transmissão do dossiê para o local de armazenamento definitivo deve ser feita por meio seguro no prazo máximo de 30 dias corridos, da data de geração do dossiê. Base legal: DOC-ICP-03.01, item 6.2.5.

IX) A AR deve utilizar sistema que permita determinar, facilmente e a qualquer momento, o local onde se encontra cada dossiê de titular de certificados que se encontra sob sua guarda. Base legal: DOC-ICP-03.01, item 6.2.6.

X) O ponto de centralização da AR para armazenamento de dossiês de agentes de registro e dossiês de titulares de certificados deve atender as especificações de localização. Base legal: DOC-ICP-03.01, item 6.2.7 e item 6.2.8.

d) Manter equipamentos protegidos contra ameaças, que possui os seguintes controles:

I) Os usuários que necessitam de acesso aos equipamentos e recursos da AR devem ser identificados e autenticados. Base legal: DOC-ICP-02, item 9.3.4.1 e item 9.3.4.3, DOC-ICP-03-01 item 4.1.2.a.

II) O sistema de controle de acesso aos equipamentos e recursos da AR devem manter as habilitações atualizadas. Base legal: DOC-ICP-02, item 9.3.4.2.

III) Autorizações de acesso de cada usuário aos equipamentos e recursos da AR devem ser definidas de acordo com a função exercida e protegido contra modificações não autorizadas. Base legal: DOC-ICP-02, item 9.3.4.4 e item 9.3.4.6.

IV) As senhas devem ser protegidas com grau de segurança compatível com a informação associada. Base legal: DOC-ICP-02, item 9.3.4.7 a 9.3.4.14, DOC-ICP-03-01, item 4.1.2.b, item 4.1.2.c.

V) As mídias, quando não forem mais necessárias, devem ser eliminadas de forma segura e os procedimentos para eliminação segura devem estar formalizados. Base legal: DOC-ICP-02, item 9.3.4.4 e item 9.3.5.12.

VI) Os procedimentos de combate a processos destrutivos (antivírus, *antitrojan* e *antispyware*) devem estar sistematizados e abranger todos os equipamentos de computação. Base legal: DOC-ICP-02, item 9.3.5.3; item 9.3.6, DOC-ICP-03-01, item 4.1.1 e item 4.1.2.e.

VII) Todas as estações de trabalho da AR devem possuir *firewall* ativado, com permissões de acesso mínimo às atividades. Base legal: DOC-ICP-03-01, item 4.1.2.f.

VIII) Estações de trabalho devem possuir proteção de tela acionada no em conformidade com a análise de risco, com exigência de senha do usuário para desbloqueio. Base legal: DOC-ICP-02, item 9.3.4.13, DOC-ICP-03-01, item 4.1.2.g.

IX) O sistema operacional deve ser mantido atualizado com aplicação de correções necessárias (*patches*, *hotfix*, etc). Base legal: DOC-ICP-03-01, item 4.1.2.h.

X) A entidade deve utilizar apenas softwares licenciados e necessários para a realização das atividades do usuário. Base legal: DOC-ICP-03-01, item 4.1.2.i.

XI) Estações de trabalho devem impedir *login* remoto, via outro equipamento ligado à rede de computadores utilizadas pela AR, exceto para as atividades de suporte remoto. Base legal: DOC-ICP-03-01, item 4.1.2.j.

XII) Estações de trabalho devem utilizar a Data e Hora Legal Brasileira. Base legal: DOC-ICP-03-01, item 4.1.2.k.

XIII) Módulo criptográfico utilizado para geração e armazenamento de chaves

assimétricas de usuário final deve ser certificado com padrão FIPS 140-1.

e) Manter *logs* e trilhas de auditoria, que possui os seguintes controles:

I) Os *logs* de auditoria do sistema operacional devem registrar os acessos aos equipamentos e devem ficar armazenados localmente por um período mínimo de 60 dias. Base legal: DOC-ICP-02, item 9.2.3 e item 9.3.4.15, DOC-ICP-03-01, item 4.1.3.

II) Os *logs* de auditoria do sistema operacional devem ser analisados em caso de suspeitas quanto a acessos não autorizados ou para dirimir dúvidas que possam surgir sobre a utilização dos equipamentos. Base legal: DOC-ICP-03-01, item 4.1.4.

f) Manter segurança física, que possui os seguintes controles:

I) As Instalações Técnicas e os Postos Provisórios de uma AR devem possuir equipamentos de prevenção de incêndio. Base legal: DOC-ICP-03.01, item 3.2.a.

II) Os documentos mantidos na AR devem ser armazenados em armários ou gabinetes com chave, de uso exclusivo da AR. Base legal: DOC-ICP-03.01, item 3.2.b.

III) Os circuitos elétricos de alimentação dos equipamentos de processamento de dados devem ser protegidos por *no-break* ou estabilizadores de tensão. Base legal: DOC-ICP-03.01, item 3.2.c.

IV) Os circuitos elétricos e lógicos devem ser protegidos por tubulação e/ou canaletas adequadas. Base legal: DOC-ICP-03.01, item 3.2.d.

V) Instalação Técnica de AR em ambiente dedicado deve possuir controle de acesso permitindo apenas ingresso de agentes de registro e titulares de certificados. Base legal: DOC-ICP-03.01, item 3.3.a.

VI) Instalação Técnica de AR em ambiente dedicado deve possuir porta única de entrada, com fechadura que agregue mecanismo de segurança mais sofisticado que modelos simples de fechaduras. Base legal: DOC-ICP-03.01, item 3.3.b.

VII) Instalação Técnica de AR em ambiente dedicado deve possuir paredes de alvenaria de tijolos ou semelhante que minimizem o risco de acesso não autorizado. Base legal: DOC-ICP-03.01, item 3.3.c.

VIII) Instalação Técnica de AR em ambiente dedicado deve possuir iluminação de emergência. Base legal: DOC-ICP-03.01, item 3.3.d.

IX) Instalação Técnica de AR em ambiente compartilhado deve possuir vigilância ostensiva ou monitoramento por CFTV, este último com imagens mantidas por 60 dias em ambiente seguro. Base legal: DOC-ICP-03.01, item 3.4.a.

X) Instalação Técnica de AR em ambiente compartilhado deve possuir controle de acesso ao prédio ou ao ambiente onde se encontra a

instalação técnica de AR. Base legal: DOC-ICP-03.01, item 3.4.b.

XI) Modalidade de validação externa é permitida somente após adaptação dos computadores móveis (a serem utilizados) ao disposto no item 4.1.2 do DOC-ICP-03-01. Base legal: DOC-ICP-03.01, item 3.8.

XII) O ponto de centralização da AC e o ponto de centralização da AR devem possuir requisitos de segurança física e/ou lógica no mínimo equivalentes ao de uma instalação técnica de AR. Base legal: DOC-ICP-03.01, item 6.2.9.

g) Cumprir PS de AC, que possui os seguintes controles:

I) Empregados ou servidores devem cumprir com os deveres estabelecidos na Política de Segurança da AC ao qual está vinculado. Base legal: DOC-ICP-02, item 7.4.1.

II) A chefia ou responsável pela AR devem cumprir com os deveres estabelecidos na Política de Segurança da AC ao qual está vinculado. Base legal: DOC-ICP-02, item 7.4.2 e item 7.4.3.

III) A gerência de segurança da AR devem cumprir com os deveres estabelecidos na Política de Segurança da AC ao qual está vinculado. Base legal: DOC-ICP-02, item 7.4.4.

IV) Contrato com prestadores de serviço deve contemplar cláusula que responsabilize a prestadora quanto ao cumprimento da PS, normas e procedimentos. Base legal: DOC-ICP-02, item 7.4.5.

h) Manter sistemas básicos, que possui os seguintes controles:

I) Os agentes de registro devem utilizar apenas softwares licenciados pelo fabricante nos equipamentos das entidades, observadas as normas da ICP-Brasil e legislação de software. Base legal: DOC-ICP-02, item 9.3.5.7 e item 9.3.5.8.

2.4. Manter credenciamento de AR, composto pelos sub-processos:

a) Comunicar alterações operacionais e violação de normas, que possui os seguintes controles:

I) Acordos Operacionais previsto no item 3.2.5 do DOC-ICP-03 devem possuir no mínimo as cláusulas descritas no item 8.2 do DOC-ICP-03-01. Base legal: DOC-ICP-03-01, item 8.

II) Os acordos operacionais entre AR devem ser cientificados à AC RAIZ. Base legal: DOC-ICP-03, item 3.2.5.

III) Violações de diretrizes e normas técnicas da ICP-Brasil por parte de PSS operacionalmente vinculada devem ser comunicadas à AC o qual está vinculada. Base legal: DOC-ICP-03, item 3.2.a.iii.

b) Regularizar não-conformidades identificadas, que possui os seguintes controles:

I) A entidade auditada deve cumprir, no prazo estipulado, as recomendações para corrigir os casos de não-conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas. Base legal: DOC-ICP-08, item 9.1.

c) Observar procedimentos para abertura de instalações técnicas e posto provisório, que possui os seguintes controles:

I) Instalações Técnicas de AR somente poderão emitir certificados da ICP-Brasil após o devido credenciamento junto ao ITI. Base legal: DOC-ICP-03, item 2.2.3 e item 3.2.1, DOC-ICP-03-01, item 1.5, DOC-ICP-03-01, item 1.6.

II) Posto Provisório de Instalações Técnicas de AR somente poderão emitir certificados da ICP-Brasil no período que se inicia da autorização de funcionamento até a data de encerramento. Base legal: DOC-ICP-03, item 3.2.1, DOC-ICP-03-01, item 1.5.

d) Observar procedimentos para encerramento de instalações técnicas e posto provisório, que possui os seguintes controles:

I) Instalações Técnicas de AR em extinção devem realizar os procedimentos descritos no item 3.2.2 da DOC-ICP-03. Base legal: DOC-ICP-03, item 3.2.2.

II) Postos Provisórios de Instalações Técnicas de AR encerradas devem realizar os procedimentos descritos no item 3.2.4 da DOC-ICP-03. Base legal: DOC-ICP-03, item 3.2.4.

III) As AR em processo de descredenciamento devem adotar os procedimentos descritos no item 4.2 do DOC-ICP-03. Base legal: DOC-ICP-03, item 4.2.

e) Manter requisitos de credenciamento, que possui os seguintes controles:

I) Qualquer alteração nos atos constitutivos, estatuto, contrato social ou administradores nas AR devem ser comunicados à AC a que está operacionalmente vinculada. Base legal: DOC-ICP-03, item 3.2.a.i.

II) Candidatos ao credenciamento e entidades credenciadas na ICP-Brasil devem atender e manter os critérios definidos no item 2.1 da DOC-ICP-03. Base legal: DOC-ICP-03, item 2.1, e DOC-ICP-03, item 3.3.

f) Credenciar PSS, que possui os seguintes controles:

I) A atividade de identificação e autenticação de titulares e responsáveis pelos certificados não pode ser executado por PSS. Base legal: DOC-ICP-03, item 2.2.4.4.

g) Descredenciar PSS, que possui os seguintes controles:

I) Requerer à AC-Raiz o descredenciamento de PSS vinculado, informando os motivos e a data prevista para encerramento das atividades do PSS. Base legal: DOC-ICP-03, item 4.3.2.1.

II) Cumprir determinação da AC-Raiz para descredenciar PSS. Base legal: DOC-ICP-03, item 4.3.2.2

III) Atualizar a página *WEB* informando o descredenciamento de PSS e o credenciamento de novo PSS. Base legal: DOC-ICP-03, item 4.2.1.3.

IV) Elaborar relatório descrevendo os procedimentos efetuados no processo de descredenciamento de PSS, no prazo de 60 dias, encaminhando-o à AC-Raiz. Base legal: DOC-ICP-03, item 4.3.2.3.

h) Manter procedimentos para extinção de AR, que possui os seguintes controles:

I) Elaborar relatório de encerramento de atividades que será encaminhado à AC Raiz. Base Legal: DOC-ICP-03, item 4.2.3.”b”.v.

ANEXO H - CRITÉRIOS PARA EMISSÃO DE PARECER DE AUDITORIA

CRITÉRIOS PARA EMISSÃO DE PARECER DE AUDITORIA

n) O presente documento não esgota os processos e subprocessos existentes na cadeia da ICP-Brasil, devendo ser entendido apenas como um balizador ou ponto de partida para cada trabalho de auditoria. Sempre caberá ao Auditor a responsabilidade pela escolha dos processos a serem auditados em cada PSC, individualmente, assim como a classificação dos riscos observados em cada processo/subprocesso a ser avaliado.

o) No Relatório de Auditoria será utilizada a tabela a seguir, para emissão de parecer de auditoria sobre o PSC auditado.

Conceito	***Parecer***	***Situação****
1	Adequado	Ausência de não-conformidades
2	Aceitável	Média da avaliação dos riscos considerada baixa
3	Deficiente	Média da avaliação dos riscos considerada média
4	Inadequado	Média da avaliação dos riscos considerada alta
5	Inaceitável	Média da avaliação dos riscos considerada crítica

(*) A média aritmética é o somatório dos riscos encontrados nos controles que apresentaram inconformidade, dividido pela respectiva quantidade de controles que apresentaram não-conformidade.

2.1. Havendo dúvida quanto ao enquadramento, pelo princípio do conservadorismo, será adotado o conceito de maior valor numérico (mais crítico).

3. CRITÉRIOS PARA APLICAÇÃO DOS CONCEITOS

s) A atribuição do conceito geral do PSC, que constará do relatório de auditoria, refletirá a opinião do auditor sobre o nível de risco a que o PSC estiver exposto. Para auxiliar nesta atribuição de conceito, o auditor poderá se valer do valor médio das inconformidades encontradas, que não poderá prevalecer sobre a opinião do auditor.

t) A atribuição da criticidade de cada não-conformidade é de responsabilidade do auditor que deve se basear na metodologia adotada, confrontada com as condições identificadas, dentro do contexto auditado. Apenas a título de exemplo meramente ilustrativo., a criticidade das não-conformidades podem ser classificadas como:

Risco Crítico:

Certificado emitido com tamanho de chave inferior ao mínimo estabelecido;

II) LCR – Lista de certificados revogados:

a) inexistência de LCR.

b) intervalo de tempo sem LCR.

c) LCR sem conteúdo.

d) LCR com campo errado ou incorreto.

JJJ) Ausência de cobertura de seguro de responsabilidade civil.

IV) Ausência de realização de auditoria operacional anual.

Qualquer ato intencional de omissão ou manipulação de dados, alteração de documentos ou registros eletrônicos, ou qualquer ato que possa ser enquadrado como fraude.

VI) Vulnerabilidade em ambiente lógico de segurança de rede.

VII) Ausência de sincronismo de tempo entre os servidores e o Observatório Nacional (hora oficial brasileira).

VIII) Uso de algoritmo de criptografia diferente do estabelecido nas normas.

IX) Ausência de testes de restauração de cópia de segurança de base de dados, de logs, de LCR e de certificados digitais.

c Falhas nos sistemas de controle de acesso físico e lógico aos recursos de AC.

XI) Ausência de sincronismo dos aplicativos de AC entre os sítios principal e de contingência da AC.

XII) Falha de integridade das aplicações e bases de dados da AC.

b) Risco alto:

d) Falha no dossiê de certificado emitido, quanto a documentação, poderes e assinatura.

II) Erros ou falhas em campos de certificados emitidos.

III) Erros ou falhas em campos de LCR emitidas.

IV) Falha na apresentação de certidões de pessoal vinculado ao PSC.

V) Falha na manutenção de sistemas de ar-condicionado, sistema elétrico e de combate a incêndio que comprometa as atividades do sítio principal e de contingência da AC.

VI) Falha na identificação de equipamentos que se conectam à solução de certificação digital da AC.

VII) Ausência de testes de funcionamento do sítio de contingência.

VIII) Ausência de testes de recuperação de cópia de segurança de LCR, *logs* de aplicativos e bases de dados.

IX) Ausência ou deficiências nos procedimentos de testes de vulnerabilidade de rede.

X) Ausência ou falhas na monitoração de ocorrências registradas em *logs.*

XI) Ausência de licença de software proprietário de terceiros.

2.2.1.7 Risco médio:

Falha na apresentação de documentação fisco-tributária do PSC.

II) Falha no processo de treinamento de pessoal do PSC.
2.2.2.2.6 Falha no processo de avaliação do pessoal

do PSC. IV) Falha no sistema de gravação de imagens

de CFTV.

Falha nos procedimentos de desligamento de empregados do PSC, mesmo que sem desligamento da empresa responsável pelo PSC.

Risco baixo:
Falha na manutenção, sistema elétrico e de combate a incêndio nas AR.

Falha na atualização de informações de instalações técnicas disponíveis nos repositórios.

Falha em inventário de ativos.

3.3. Toda vez que os conceitos forem modificados em decorrência da convicção do auditor, o relatório de auditoria destacará a situação de forma fundamentada, cujas

evidências deverão ser anexadas à cópia destinada ao ITI.

3.4. Para estabelecimento do nível do risco de uma não-conformidade, será utilizada ferramenta de avaliação do risco, pelo menos com a utilização da matriz impacto versus probabilidade, onde:

Impacto			
	Médio	Alto	Crítico
	Baixo	Médio	Alto
	Baixo	Baixo	Médio
			Probabilidade

Y) Os valores a serem atribuídos aos eixos X e Y serão sempre em múltiplos de 3 (0 a 3; 0 a 6; 0 a 9; etc.); sempre em ordem crescente de exposição. Por exemplo, se adotada a escala de 0 a 9 teríamos a gradação de zero = sem qualquer impacto, até nove = impacto máximo possível.

Z) Poderá ser utilizada outra metodologia para atribuição do nível do risco, desde que faça parte da documentação aprovada no credenciamento, ou seja evidenciada sua aplicação de forma sistematizada pela entidade de auditoria.

AA) No relatório de auditoria, constará em parágrafo destacado, o conceito geral do PSC atribuído pelo auditor ao auditado e os motivos que levaram à referida conceituação. A opinião do Auditor será registrada no Parecer de Auditoria, que poderá ser: Adequado; Aceitável; Deficiente; Inadequado ou Inaceitável.

ANEXO I - CRITÉRIOS PARA APLICAÇÃO DE PENALIDADES A ENTIDADES CREDENCIADAS NA ICP-BRASIL

Infra-Estrutura de Chaves Públicas Brasileira

ADE ICP-08.G

CRITÉRIOS PARA APLICAÇÃO DE PENALIDADES POR NÃO-CONFORMIDADES EM AUDITORIAS OPERACIONAIS

1. As penalidades a serem aplicadas aos PSC serão:

p) Advertência: penalidade que não impede o normal prosseguimento das atividades e operações do PSC. Será aplicada, à critério do Diretor da DAFN, mediante parecer fundamentado, quando:

se tratar de fato já consumado e que não possa ser ou já esteja regularizado, independentemente da criticidade da inconformidade, como por exemplo, intervalo de tempo sem publicação de LCR;

houver uma ou mais ocorrências classificadas como de baixa criticidade e que não estejam regularizadas.

q) Restrição: cerceamento ao normal desenvolvimento de uma operação ou atividade exercida pelo PSC. Será aplicada quando:

o PSC incorrer em não-conformidades de risco médio ou maior, não regularizada ou com prazo de regularização vencido.

r) Suspensão: cerceamento na emissão de novos certificados para titulares ou autoridades certificadoras subseqüentes. Será aplicada quando:

houver risco iminente de dano irreparável à cadeia de confiança da ICP-Brasil.

s) Descredenciamento: penalidade que impede o PSC de continuar atuando na cadeia de confiança da ICP-Brasil. Será aplicada quando:

houver conceituação cinco (5) do PSC, em auditoria operacional, em duas auditorias subseqüentes;

houver comprometimento da cadeia de confiança da ICP-Brasil, por ação ou omissão do PSC, evidenciada em relatório de auditoria operacional.

2. As penalidades a serem aplicadas às entidades de auditoria serão:

JJ) Advertência: penalidade que não impede o normal prosseguimento das atividades da entidade de auditoria. Será aplicada quando:

houver falha na emissão do relatório de auditoria, que não comprometa a atribuição de conceito do PSC auditado, mas esteja em desacordo com a

documentação apresentada quando do credenciamento;

JJ) Suspensão: penalidade que impede, temporariamente a entidade de auditoria de iniciar novos trabalhos de auditoria, pelo prazo determinado, que poderá ser de 90 dias a um ano da data da publicação da penalidade. Será aplicada quando:

A for identificada inconsistência no relatório de auditoria que fira quaisquer dos princípios de auditoria mas não comprometa a cadeia de confiança da ICP-Brasil.

KK) Descredenciamento: penalidade que impede a entidade de auditoria de continuar atuando na cadeia de confiança da ICP-Brasil. Será aplicada:

A for identificada inconsistência no relatório de auditoria que fira quaisquer dos princípios de auditoria e que comprometa a cadeia de confiança da ICP-Brasil.

B por decisão do Diretor da DAFN, mediante parecer fundamentado, nos casos em que houver descumprimento de normas da ICP-Brasil ou do código de ética do auditor estabelecido por órgãos reguladores ou de classe.

ANEXO J - PROCEDIMENTOS PARA TROCA DE CORRESPONDÊNCIAS ENTRE AS ENTIDADES DE AUDITORIA E O ITI

PROCEDIMENTOS PARA TROCA DE CORRESPONDÊNCIAS ENTRE AS ENTIDADES DE AUDITORIA E O ITI

t) Na troca de correspondências, será adotado, preferencialmente, o correio eletrônico com assinatura digital da ICP-Brasil do representante legal da entidade de auditoria ou da autoridade competente.

u) Quanto aos anexos, serão observados os seguintes procedimentos:

para credenciamento de entidade de auditoria (interna ou independente):

gravados em CD ou DVD, no formato PDF, contendo a documentação exigida para credenciamento. Os arquivos em meio eletrônico terão calculados os respectivos *hashes*, com o algoritmo SHA1, cujos valores serão relacionados em arquivo no formato texto puro (extensão TXT), contendo o nome do arquivo e o respectivo *hash*, separados por ponto-e-vírgula (;).

Relatórios de Auditoria:

I) em arquivos eletrônicos, no formato PDF, anexados à correspondência protocolada no ITI, ou anexado a correio eletrônico assinado digitalmente com certificado da cadeia da ICP-Brasil.

iii) Os arquivos em meio eletrônico terão calculados os respectivos *hashes*, com o algoritmo SHA1, cujos valores serão listados em arquivo no formato texto puro (extensão TXT), contendo o nome do arquivo e o respectivo *hash*, separados por ponto e vírgula (;).

c) Recomendação de auditoria.

I) informando inclusive os *hashes* (SHA1) dos arquivos anexados, que poderão estar consolidados em arquivo único compactado nos formatos TAR ou ZIP

ANEXO K – REQUISIÇÃO DE TERMOS COMPLEMENTARES

REQUISIÇÃO DE INFORMAÇÕES COMPLEMENTARES (RIC)

Nº ___ – _____._____/____-__

PRESTADOR DE SERVIÇO DE CERTIFICAÇÃO – PSC

CNPJ:

RAZÃO SOCIAL: CNPJ:

ENDEREÇO: TEL: ( )

MUNICÍPIO: UF:

NOME DO REPRESENTANTE LEGAL:

TERMO DE FISCALIZAÇÃO A QUE SE REFERE:

CONTEÚDO DA REQUISIÇÃO:

Para a continuidade dos exames sob minha responsabilidade, solicito no prazo abaixo estabelecido os seguintes documentos e/ou informação:

_____
_____
_____
_____
_____
_____
_____.

PRAZO DE ENTREGA:

_____
_____.

FISCAL (IS) RESPONSÁVEL(IS)

LOCAL E DATA:

NOME: **ASSINATURA:**

NOME: **ASSINATURA:**

ANEXO L – AUTO DE INFRAÇÃO

	CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA **INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO** **DIRETORIA DE AUDITORIA FISCALIZAÇÃO E NORMALIZAÇÃO**

AUTO DE INFRAÇÃO Nº – NNNNN.XXXXX/AAAA - DV - V

PRESTADOR DE SERVIÇ O DE CERTIFICAÇ Ã O – PSC

RAZÃ O SOCIAL:

CNPJ:

ENDEREÇ O: TEL: ( )

MUNICÍPIO: UF:

NOME DO REPRESENTANTE LEGAL:

TERMO DE FISCALIZAÇ Ã O A QUE SE REFERE: NNNNN.XXXXXX/AAAA-DV

AUTO DE INFRAÇ Ã O

O Fiscal do ITI, com a responsabilidade dos procedimentos de fiscalizaç ã o, de acordo com o estabelecido pelo item 3.8 do anexo à Resoluç ã o nº 45, de 18 de abril de 2006, acostado nos autos do PAF nº NNNNN.XXXXXX/AAAA-DV notifica as nã o-conformidades descritas abaixo:

_____
_____
_____
_____
_____
_____
_____

FISCAL RESPONSÁ VEL	
NOME: **LOCAL E DATA:**	**ASSINATURA**

Instruç õ es de Preenchimento

Auto de Infraç ã o Nº NNNNN.XXXXXX/AAAA-DV - V
Obtido do Termo Fiscalizaç ã o Inicial (TFI), onde:

NNNNN – Tipo de Processo conforme estrutura de Numeraç ã o da Administraç ã o Federal XXXXXX – Núm ero seqüe ncial de PAF
AAAA – Ano a que se refere o PAF
V – Letra (no escopo A – Z) que dá a possibilidade de vá rios autos de infraç ã o vinculados a um TFI

Dados do Prestador de Serviç o de Certificaç ã o

Informaç õ es obtidas a partir do Termo de Fiscalizaç ã o Inicial - TFI

Termo de Fiscalizaç ã o a que se refere:
Obtido no Nú mero do Termo de Fiscalizaç ã o Inicial - TFI
É indicado repetidamente no Auto de Infraç ã o pela possibilidade deste nã o estar sempre acompanhado do PAF.

Auto de Infraç ã o
Espaç o destinado a especificaç ã o e enquadramento da Infraç ã o e demais consideraç õ es e anotaç õ es a serem feitas pelo FISCAL.

Fiscal Responsá vel
Nome: deve ser preenchido de forma legível e indica o FISCAL responsá vel pelo AIC.
Local e Data: devem mostrar o local onde o fiscal preencheu o AIC e a data do preenchimento.
Assinatura: deve conter a assinatura do fiscal responsá vel pelo preenchimento da AIC.

Auto de Infraç ã o de Certificaç ã o (meios digitais).
O Nome do Fiscal deve ser o mesmo de seu Certificado Digital.
Local e Data devem ser utilizados a partir dos mecanismos de carimbo de tempo da ICP-Brasil.
A Assinatura Eletrô nica do fiscal deverá ter seu *HASH* associado a toda AIC e nã o ao PAF.

ANEXO M – TERMO DE FISCALIZAÇÃO

CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA
INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO
DIRETORIA DE AUDITORIA FISCALIZAÇÃO E NORMALIZAÇÃO

TERMO DE FISCALIZAÇÃO Nº _____._____ /____-__

◯ INICIAL

◯ COMPLEMENTAR

◯ EXTENSIVO

◯ FINAL

PRESTADOR DE SERVIÇ O DE CERTIFICAÇ Ã O (PSC)

RAZÃ O SOCIAL: _____ CNPJ: _____

ENDEREÇ O:_____

MUNICÍPIO:_____ UF: _____

URL: _____

NOME DO REPRESENTANTE LEGAL: _____

E-MAIL:_____ TELEFONE: _____

AC RESPONSÁ VEL PELA SOLICITAÇ Ã O DE CREDENCIAMENTO: _____

NOME DO REPRESENTANTE LEGAL: _____

E-MAIL:_____ TELEFONE: _____

ENDEREÇ O:_____

OBJETO DO PROCEDIMENTO DE FISCALIZAÇ Ã O (PFC)

_____

_____

PRAZO PARA REALIZAÇ Ã O DA AFC: _____ dias

FISCAL RESPONSÁ VEL

NOME: _____ MATRÍCULA: _____

COORDENADOR DE FISCALIZAÇ Ã O

NOME: _____ TELEFONE: _____

AUTORIDADE OUTORGANTE

NOME: _____ MATRÍCULA: _____

E-MAIL: _____ TELEFONE: _____

ENCAMINHAMENTO

Determino, nos termos da Resoluç ã o CG ICP-Brasil nº 45, de 18 de abril de 2006, a execuç ã o da Aç ã o de Fiscalizaç ã o definida pelo presente Termo, que será responsabilidade do fiscal acima identificado, que está autorizado a praticar, isolada ou conjuntamente, todos os atos necessá rios a sua realizaç ã o.

Este instrumento poderá ser prorrogado a crité rio da autoridade outorgante.

_____ , _____ de _____ de _____

_____

Autoridade Outorgante

CIÊ NCIA

Declaro-me ciente deste Termo, do qual recebi cópi a.

Nome:_____ CPF: _____

Funç ã o: _____ Data da ciê ncia _____ /_____ /_____

_____

Assinatura

O fiscal deverá identificar-se, mediante apresentaç ã o de sua identidade funcional, no ato da entrega do presente Termo ao Prestador de Serviç o de Certificaç ã o, no caso de Aç ã o de Fiscalizaç ã o presencial.

ANEXO N - NOTIFICAÇÃO

CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA
INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO
DIRETORIA DE AUDITORIA FISCALIZAÇÃO E NORMALIZAÇÃO

NOTIFICAÇÃO Nº ____._____ /____-__

PRESTADOR DE SERVIÇ O DE CERTIFICAÇ Ã O – PSC

CNPJ:

RAZÃ O SOCIAL: CNPJ:

ENDEREÇ O: TEL: ( )

MUNICÍPIO: UF:

NOME DO REPRESENTANTE LEGAL:

TERMO DE FISCALIZAÇ Ã O A QUE SE REFERE:

CONTEÚ DO DA NOTIFICAÇ Ã O:

O Diretor de Auditoria, Fiscalizaç ã o e Normalizaç ã o do ITI, de acordo com o estabelecido pelo item 5.8 do anexo a Resoluç ã o nº 45, de 18 de abril de 2006, com base no Relatór io de Fiscalizaç ã o**,** acostado nos autos do processo administrativo nº _____ intima V.Sª. a, no prazo de 15 dias consecutivos, contados a partir da data do recebimento desta, apresentar justificativa ou defesa para as nã o-conformidades descritas abaixo:

_____
_____
_____
_____
_____
_____
_____

AUTORIDADE COMPETENTE

LOCAL E DATA

NOME: **ASSINATURA**

ANEXO O – RELATÓRIO DE FISCALIZAÇÃO

CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA
INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO
DIRETORIA DE AUDITORIA FISCALIZAÇÃO E NORMALIZAÇÃO

RELATÓRIO DE FISCALIZAÇÃO Nº _____._____ /____-__

PRESTADOR DE SERVIÇ O DE CERTIFICAÇ Ã O - PSC

RAZÃ O SOCIAL: CNPJ:

ENDEREÇ O: TEL: ( )

MUNICÍPIO: UF:

DESCRIÇ Ã O DO OBJETO DA FISCALIZAÇ Ã O:

RESULTADO DA FISCALIZAÇ Ã O

DESCRIÇ Ã O DOS EXAMES:

DESCRIÇ Ã O DOS EXAMES COMPLEMENTARES:

NÃ O-CONFORMIDADES IDENTIFICADAS E CORRIGIDAS DURANTE A FISCALIZAÇ Ã O:

NÃ O-CONFORMIDADES IDENTIFICADAS:

OUTRAS INFORMAÇ Õ ES

LEGISLAÇ Ã O APLICÁ VEL:

AÇ Ã O CORRETIVA APLICÁ VEL:

OUTROS PRAZOS PARA CORREÇ Ã O:

COMENTÁ RIOS ADICIONAIS:

LOCAL DE GUARDA DAS EVIDÊ NCIAS EM MEIO ELETRÔ NICO:

CONCLUSÃ O:

FISCAL (IS) RESPONSÁ VEL(IS)

LOCAL E DATA:

NOME: **ASSINATURA:**

APROVAÇ Ã O

COORDENADOR DE FISCALIZAÇ Ã O

LOCAL E DATA

NOME: **ASSINATURA:**

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo