SICAP - MÓDULO CARDUG

CARDUG – Cadastro de Responsáveis das Unidades Gestoras

Apresentação

Caro Aluno,

Confeccionamos este material para servir de apoio a você, aos gestores e responsáveis das unidades gestoras, usuárias do SICAP – Sistema Integrado de Controle e Auditoria Pública.

Esta apostila contempla orientações para melhor entendimento sobre assinatura digital, bem como sobre o Cadastro de Responsáveis das Unidades Gestoras – CARDUG. Esse cadastro é a porta de entrada para todos os módulos do SICAP. Através do CARDUG, o gestor gerenciará seu rol de responsáveis, incluindo, excluindo, alterando e solicitando permissões para acesso aos módulos do SICAP diretamente pela internet.

Aprenderemos todos os passos para acessar o sistema, desde a aquisição do certificado digital, o pré-cadastro do gestor, seu primeiro acesso, inclusão e exclusão do rol de responsáveis.

Conheceremos também informações relevantes como a legislação pertinente ao sistema e a importância do CARDUG, pois, somente a partir desse cadastro, é possível acessar e alimentar os demais módulos do SICAP.

Objetivos

Esperamos que, ao final deste capítulo, você seja capaz de:

- Conhecer os mecanismos de funcionamento da Certificação Digital;
- Entender a importância e a integração do módulo CARDUG com os demais módulos integrantes do SICAP;
- Conhecer a legislação pertinente ao CARDUG e o Rol de Responsável;
- Compreender todos os procedimentos para cadastramento, inserção de permissão, exclusão de permissão e finalização de servidor.

Pré-requisitos

Para a compreensão satisfatória do conteúdo desta apostila será necessário que você conheça o SICAP - Sistema Integrado de Controle e Auditoria Pública. Necessitará também de conhecimentos básicos de informática, para melhor operacionalização e entendimento do sistema. Você poderá, também, consultar o *site* do TCE-TO – Tribunal de Contas do Estado do Tocantins <http://www.tce.to.gov.br/sicap> para acompanhar um pouco mais sobre o sistema e sobre nossa história.

Introdução

Estudaremos, conceitos, objetivos, importância e segurança da assinatura digital, conheceremos também algumas empresas certificadoras, a mídia para armazenamento da assinatura e o passo a passo para instalação e acesso ao sistema através dessa assinatura.

Estudaremos também conceitos e objetivos do CARDUG - Cadastro de Responsáveis das Unidades Gestoras, que é o módulo componente do SICAP, que foi instituído através da Instrução Normativa nº 07/2008, a qual substituiu a nº IN 07/2003, e trata sobre o Rol de Responsáveis.

Para acessar o CARDUG e efetuar o lançamento dos responsáveis por dinheiro, bens e valores públicos das Unidades Gestoras e responsáveis pelo envio de dados ao TCE via *web*, é necessária a utilização da assinatura digital.

Iniciaremos este estudo aprendendo os caminhos para adquirir a assinatura digital e também como se dá o acesso ao sistema via internet tanto ao CARDUG como em todos os módulos do SICAP.

1. Entendendo o que é assinatura digital

Certificado digital é um documento eletrônico emitido por uma Autoridade Certificadora credenciada pela Autoridade Certificadora Raiz da ICP Brasil, ou seja, uma entidade habilitada pela Autoridade Certificadora da Receita Federal do Brasil. Essa entidade certifica a autenticidade dos emissores e dos destinatários dos documentos e dos dados eletrônicos ou digitais, bem como assegura a privacidade e a inviolabilidade desses dados.

Entendamos, então, que um certificado digital é um arquivo eletrônico que identifica seu titular, pessoa física ou jurídica, ou seja, é um Documento Eletrônico de Identidade, do qual o titular poderá fazer uso em qualquer transação através da *web*. Já a assinatura digital é como nossa carteira de identidade só que eletrônica, digital, uma identidade virtual.

O objetivo principal da assinatura digital é atribuir um nível maior de segurança nas transações eletrônicas, permitindo a identificação inequívoca das partes envolvidas, tendo ainda como garantia a autenticidade do emissor e do receptor, a integridade dos dados transmitidos, a confidencialidade entre as partes e principalmente o não-repúdio das transações efetuadas, ou seja, a **prova inegável** de que o usuário realizou essa ação. Tendo ainda como benefício uma maior agilidade na comunicação com o TCE, como a redução no custo de mão de obra e transporte de documentos e, com isso, a redução do risco de extravio desses documentos.

A nossa assinatura manual á passível de perícia, de um exame grafotécnico para a comprovação da veracidade da mesma, no entanto com a assinatura digital isso não é possível, mesmo que tenha provas de que sua mídia foi subtraída de seu poder, quem a utilizou indevidamente possuía sua senha. Por isso a imperiosa necessidade de manter sigilo de sua senha e não dar posse a outros de sua assinatura, ou seja, seu *token* ou *smart card.*

Vejamos, a seguir, como adquirir a assinatura digital.

1.1 Como adquirir a assinatura digital

Para obtermos uma assinatura digital, é necessário procurarmos uma entidade habilitada para esse serviço, ou seja, uma Autoridade Certificadora a qual tem a função de verificar a identidade do usuário e associar a ele uma chave privada. Essas informações são inseridas no documento chamado certificado digital.

Para sua utilização no TCE, é necessário assinatura E-CPF, ou seja, **pessoa física**. Existe também assinatura E-CNPJ, ou seja, pessoa jurídica, porém não atende ao nosso sistema.

Você poderá solicitar sua assinatura via internet, através dos *sites* das Autoridades Certificadoras, escolhida previamente. No estado do Tocantins, estão habilitadas a CAIXA ECONOMICA FEDERAL, a SERPRO e a SERASA. Deverá também escolher qual a validade e a segurança da assinatura. Existe, no mercado, assinatura com validade de um ano e três anos, ou seja, nos modelos A1 ou A3, respectivamente. No *site* da empresa certificadora escolhida, você deverá preencher a solicitação do certificado E-CPF e agendar o momento da apresentação da documentação com o original e cópia conforme relação específica da certificadora.

Depois de concretizado esse processo e já de posse da mídia para armazenar a assinatura, adquirida em lojas próprias, procurar a empresa certificadora para gravação da assinatura na mídia.

1.2 Adquirindo a mídia

Ao adquirir assinatura digital E-CPF modelo A-1, com validade apenas de um ano, ela será armazenada diretamente no computador, através de um disquete, CD ou mesmo *pendrive.* Esse tipo de armazenamento não nos assegura a inviolabilidade, pois sua segurança é frágil.

Já para armazenar a assinatura E-CPF modelo A-3, com validade de três anos, devemos adquirir o *smart card* (cartão magnético) (Fig. 1), ou *token,* equipamento semelhante ao *pendrive*, conforme (Fig. 2). Ao adquirir o *smart card*, é necessário adquirir também a leitora, equipamento que faz a conexão entre o cartão magnético e o computador, a ser instalada na máquina em que será utilizada.

A assinatura digital, através da identidade digital, poderá ser efetuada em qualquer local com acesso à internet, porém deverá ter instalado no computador de uso o *software* do *token.* Lembrando que, sendo cartão, deve estar de posse da leitora e instalada na maquina de uso. Percebemos, desse modo, que o *token* é mais prático.

Vejamos, a seguir, mais informações sobre as mídias utilizadas:

1.2.1 Smart card

Fig. 1 *Smart Card* e Leitora

É um cartão magnético capaz de gerar e armazenar as chaves que comporão os certificados digitais. Uma vez geradas, estarão totalmente protegidas, não sendo possível exportá-las para outra mídia ou retirá-las do *smart card*. Mesmo que o computador seja atacado por um vírus ou até mesmo *hacker*, as chaves estarão seguras e protegidas, não sendo expostas a risco de roubo ou violação.

A leitora é um dispositivo projetado para conectar um cartão inteligente a um computador, ela se encarregará de fazer a interface com o cartão. Instalar uma leitora é um procedimento simples, dispensa conhecimentos técnicos. Uma vez instalada, permitirá acesso seguro aos serviços na internet já preparados para a certificação digital e disponível para leitura de diversos cartões.

1.2.2 *Token*

Fig. 2 *Token*

O *token* é um *hardware* (semelhante a um *pendrive*) capaz de gerar e armazenar as chaves que comporão os certificados digitais. Depois de geradas, as assinaturas estarão protegidas, não sendo possível exportá-las ou retirá-las do *token,* além de protegê-las de risco como roubo ou violação. É de instalação simples também, você deverá conectar a um computador através de uma porta USB e instalar um gerenciador criptográfico (*software*) que é parte integrante da mídia, ou seja, é um instalador que recebemos junto com o *pendrive*. Dessa forma, tão logo instalado, será reconhecido pelo sistema operacional.

Para que o sistema operacional identifique a assinatura, é necessário ter instalado em seu computador o **Java** e também as **cadeias de certificados** de acordo com a empresa certificadora utilizada. Vejamos a seguir como fazer *donwload* desses aplicativos.

1.3 Como instalar o Java e as cadeias de certificados

Para você instalar o Java e as cadeias de certificados correspondentes à Autoridade Certificadora utilizada, é necessário seguir alguns passos. Em nossa página na internet <www.tce.to.gov.br/sicap>, localizamos, em Donwload Certificado (Fig. 3), existe os *links* para baixar o Java, as cadeias de certificados e tambem o conversor PDF, quando necessario, bastando apenas clicar, instalar e executar em seu computador.

Fig. 3 Donwload Certificado

Caso você adquiria assinatura da CEF – Caixa Econômica Federal, necessitará baixar as cadeias de certificados correspondentes a essa certificadora. Para isso, clique em cadeia certificados Caixa e localize os certificados conforme a figura 4.

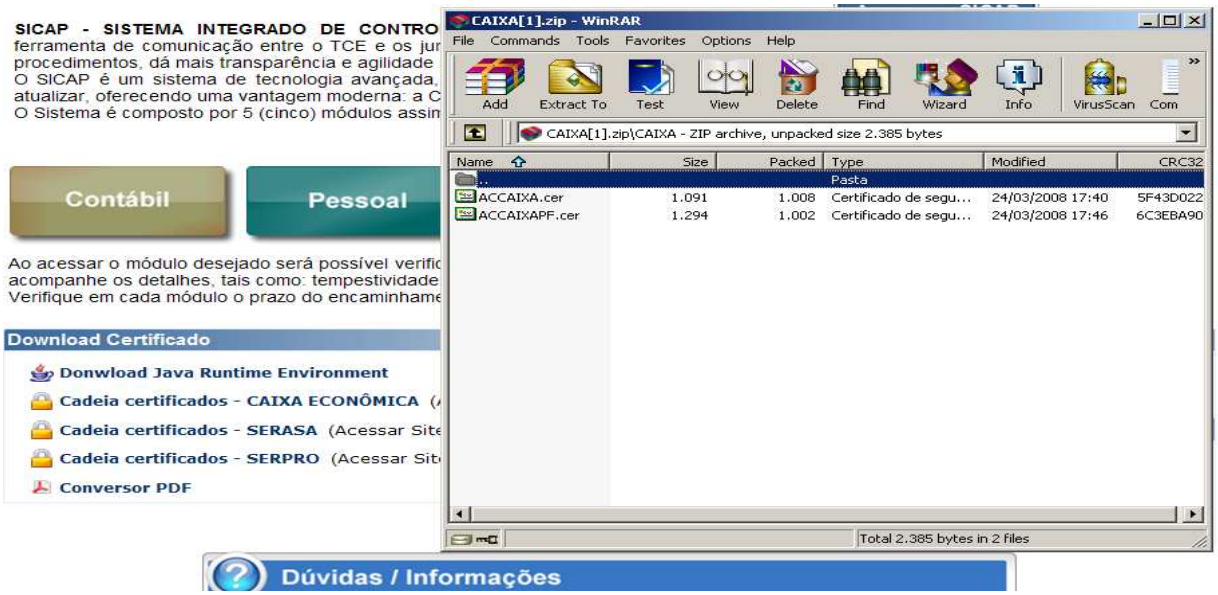

Fig. 4 Cadeias Certificados CEF

A cadeia de certificados da Caixa é composta de dois arquivos, ACCAIXA.cer e ACCAIXAPF.cer. Todos os arquivos que aparecerem na pasta, seja de qualquer certificadora, devem ser instalados no computador. Para fazermos a instalação, escolhemos a opção “Colocar todos os certificados no armazenamento a seguir” e selecionamos a pasta “Autoridades de Certificação Raiz Confiáveis”, conforme os passos apresentados na Figura 5.

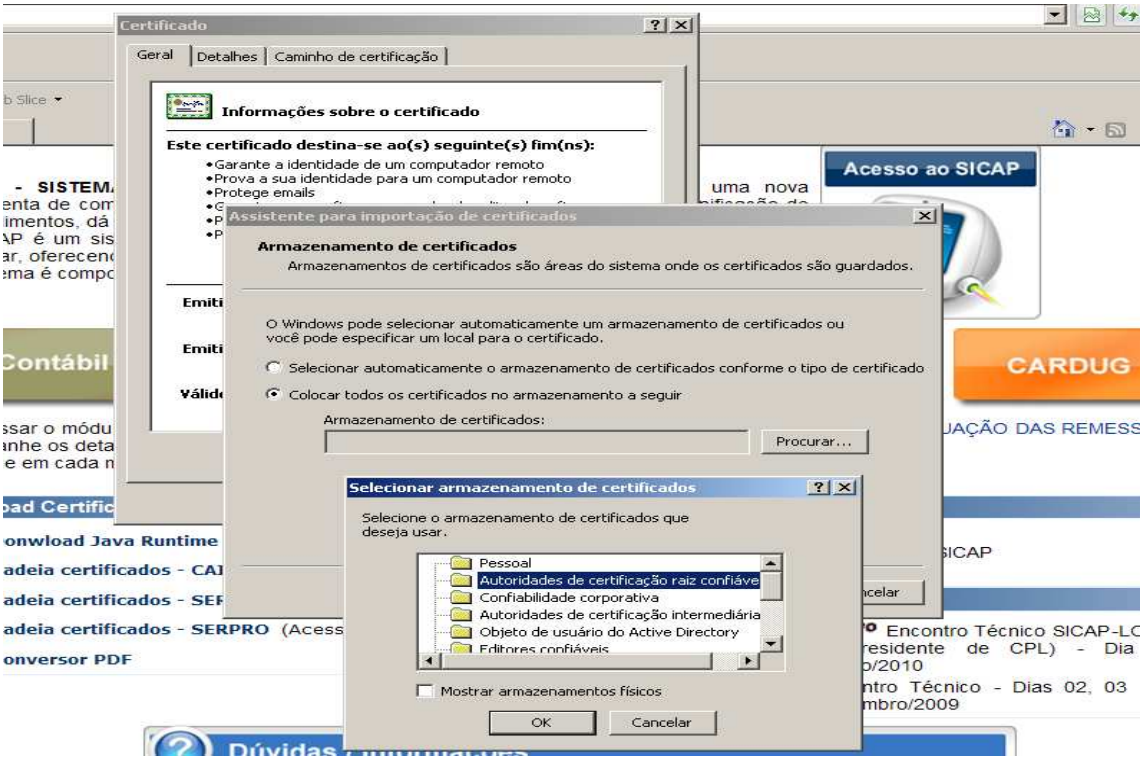

Fig. 5 Instalando as Cadeias

Concluída a instalação das cadeias, do Java e também do *software* da assinatura em seu computador, você está apto para acessar o sistema via assinatura digital através da internet.

Para que o SICAP identifique a assinatura, você deverá estar devidamente cadastrado no CARDUG, que é o cadastro do Rol de Responsáveis, o qual efetua a ligação entre os diversos módulos do SICAP.

Saiba mais

Acessando o *site* das empresas, você obterá maiores informações sobre certificação digital:

Identidade digital Caixa <http://icp.caixa.gov.br>

Serviço de Certificação SERPRO <https://ccd.serpro.gov.br/acserprospb>

Serasa – Certificados Digitais <http://www.serasaexperian.com.br/certificados>.

Alertamos que não poderão ser titulares de certificados e-CPF as pessoas físicas cuja situação cadastral perante o CPF esteja enquadrada na condição de cancelado.

No próximo item, conversaremos sobre funcionamento, importância e metodologia do cadastro o CARDUG.

2. CARDUG – Conceito

O CARDUG - Cadastro de Responsáveis da Unidade Gestora foi instituído com a finalidade precípua de atender ao cadastramento dos responsáveis por dinheiro, bens e valores públicos das Unidades Gestoras, o conhecido ROL DE RESPONSÁVEIS, eletronicamente. Sua instutuição

ocorreu através da Instrução Normativa nº 07/2008, regulamentada pelo seu Art. 1º que deteminou que

> Fica instituído o módulo do "Cadastro de Responsáveis das Unidades Gestoras" – CARDUG, componente do Sistema Integrado de Controle e Auditoria Pública a ser adotado pelos órgãos jurisdicionados destinados à qualificação dos responsáveis.

Cumpre, assim, o que determina os art. 165, 166, 167 e 168 do Regimento Interno TCE-TO, com nova redação através da Resolução Normativa 001/2010, também atende ao art. 5º da Lei 1284/2001 e ainda tem como objetivo manter um cadastro atualizado para a efetivação da assinatura digital, dando celeridade ao envio de documentos por meio eletrônico.

O art. 165 do Regimento Interno do TCE-TO determina que, em até 30 dias após o início do mandato, o novo gestor deve providenciar o envio do Rol de Responsáveis, ou seja, **atualizar** eletronicamente o cadastro, via assinatura digital.

O parágrafo único do art. 167 do Regimento Interno determina que

> A atualização dos dados constantes do rol de responsáveis será eletrônica e ficará a cargo de cada órgão ou entidade, que deverá efetuar as alterações necessárias, no prazo máximo de **quinze dias**, a contar da publicação dos respectivos atos de nomeação, designação ou exoneração (grifo nosso).

O acesso ao CARDUG é restrito ao Gestor da Entidade, ou seja, Gestor de Prefeituras, Presidente de Câmara, aos Gestores de Fundos, de Secretarias, às Autarquias e outras, através da web.

Para o primeiro acesso é necessário que o gestor assim que for eleito ou assumir o órgão deve **informar imediatamente este Tribunal**, através de documento de posse e o numero de seu CPF, para que seja efetuado seu pré-cadastro, liberando as permissões para que ao primeiro acesso já possa informar seus dados e cadastrar ou atualizar o seu Rol de Responsáveis.

Esse módulo é o responsavel pela interligação entre todos os módulos componentes do SICAP, ou seja, só terão acesso aos demais módulos, o Contábil, o Atos de Pessoal, o Controle Interno, Licitações e Obras, quando estiverem devidamente cadastrados no CARDUG e com as devidas permissões.

Resumindo: o CARDUG tem como finalidade informar servidores responsáveis por dinheiro, bens e valores da Unidade Gestora e informar servidores responsáveis por transmissão de dados via certificação digital.

Vejamos, a seguir, como acessar o cadastro.

2.1 Como acessar o CARDUG

No item 1.1, aprendemos como adquirir a assinatura digital e como instalar as cadeias de certificados. Preparamos o computador para receber a informação. Agora já com o equipamento pronto, vamos acessar através do assinador digital. Com a assinatura no computador, acessamos o *site* <www.tce.to.gov.br/sicap> e escolhemos o módulo CARDUG, ou diretamente através do *ícone* "Acesso ao SICAP" (Fig. 6).

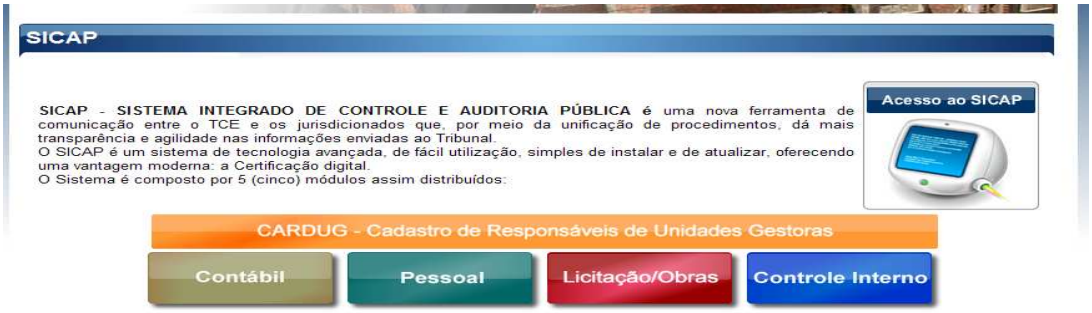

Fig. 6 Acesso ao SICAP

A clicar em “Acesso ao SICAP” entramos na página Sistema de Autenticação, conforme Fig. 7.

Fig. 7 Sistema de Autenticação

Nessa tela, com as assinaturas instaladas na máquina, você escolhe a esfera municipal ou estadual e seleciona a unidade gestora em questão. Digita seu CPF, seleciona sua assinatura, e informa sua senha para efetuar o *login*, conforme a figura 8. Quando aparecer a mensagem “Nenhum certificado válido foi encontrado no repositório” é porque não foi instalado o *software* do dispositivo, por exemplo, o CD do *token* deve ser corretamente instalado nesta maquina.

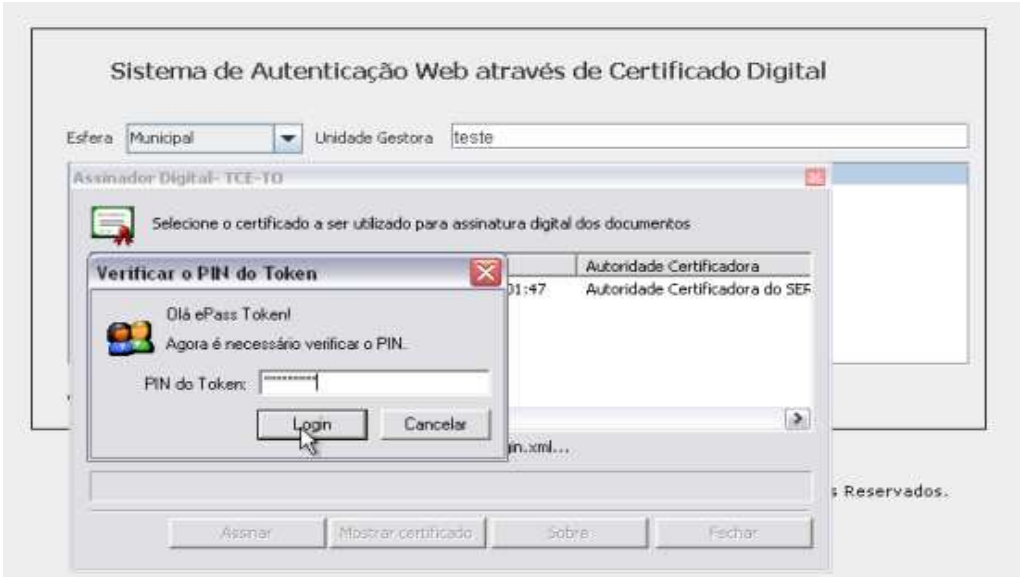

Fig. 8 Efetuando o Login

Você deve observar a instalação das cadeias de certificados, pois, não estando corretamente instaladas, aparecerá a mensagem conforme apresenta a figura 9. Assim você deve retornar ao item 1.3 e baixar novamente as cadeias de certificados para resolver esse problema.

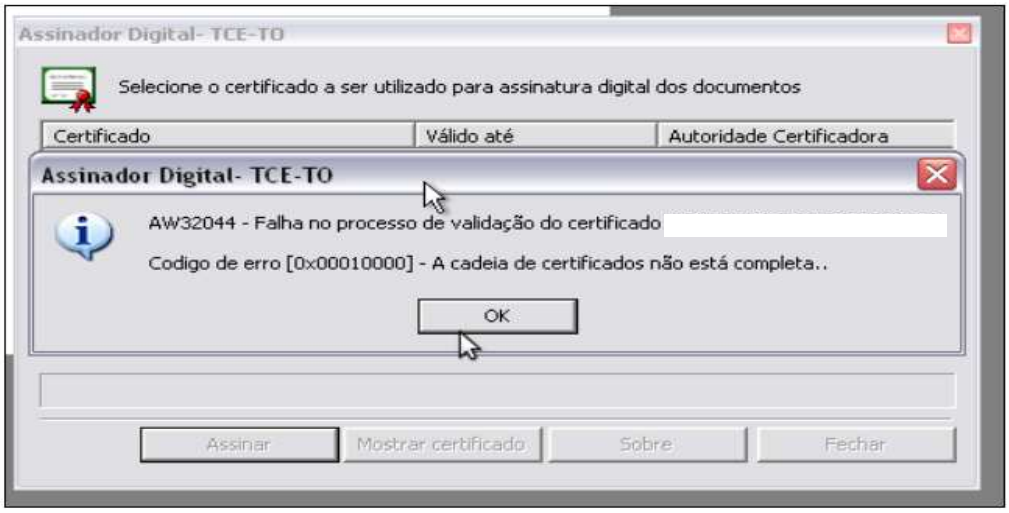

Fig. 9 Cadeia incompleta

Após digitar o PIN (senha pessoal), aparecerá a informação "Total de documentos assinados 1" (Fig. 10). Feche essa tela e aguarde o acesso aos "Sistemas permitidos para o usuário".

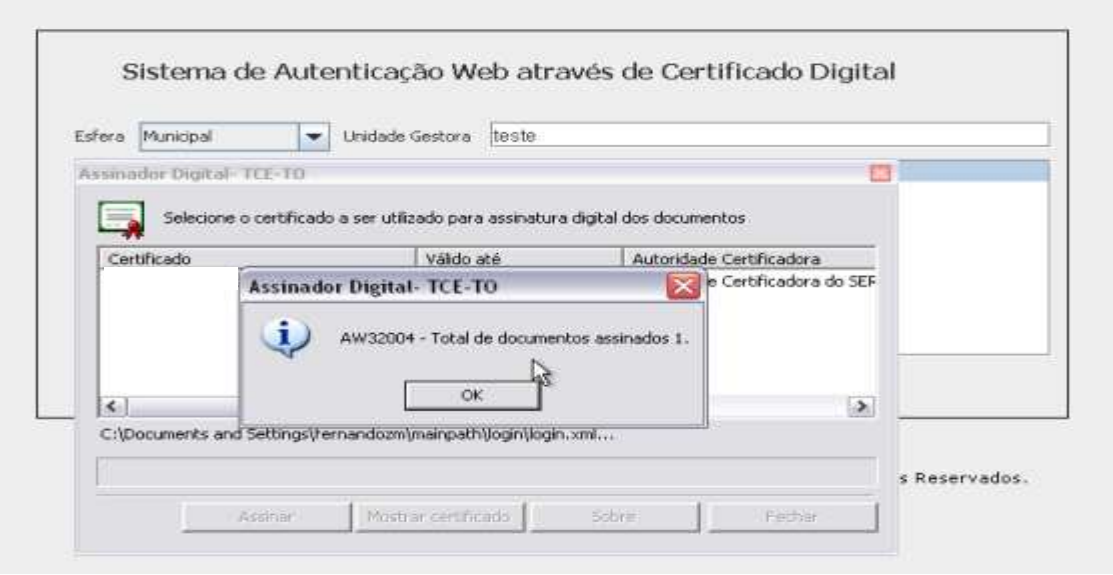

Fig. 10 Total de documentos assinados

Na tela a seguir (Fig.11), temos todos os sistemas, ou seja, todos os módulos do SICAP aos quais a assinatura conectada tem acesso. Sempre observe no cabeçalho a Unidade Gestora e o **usuário autenticado**. Caso não seja o interessado, você deve clicar em desconectar e conectar novamente com o usuário correto. Agindo assim você já está apto a operacionalizar o sistema escolhido.

Fig. 11 Sistemas permitidos para o usuário

Entendendo melhor a Tela “Sistemas permitidos para o Usuário”:

O SICAP Assinador de Remessas Contábeis, é a entrada para concretização das demais assinaturas do Módulo Contábil, já que a primeira foi efetuada através do envio pelo SICAP SUITE.

Existe os *links* SICAP MODULO ATOS DE PESSOAL e o SICAP ASSINADOR DE REMESSAS ATOS DE PESSOAL, no primeiro link o usuário informa os dados de atos de pessoal, no segundo link efetua as demais assinaturas.

O mesmo acontece com os Módulos LICITAÇÕES e OBRAS, onde existe um *link* para o envio e outro para a assinatura.

Quanto ao Módulo CARDUG e ACCI só existe uma entrada, pois somente uma pessoa assina e grava os dados no banco de dados do TCE-TO.

Uma breve explanação sobre nomes utilizados neste material:

- SICAP – Sistema Integrado de Controle e Auditoria Publica.
- MÓDULOS - são os sistemas que estão integrados ao SICAP, sendo:

- SICAP Contábil, SICAP ACCI, SICAP Atos de Pessoal, SICAP Licitação, SICAP Obras e CARDUG – Cadastro de Responsáveis das Unidades Gestoras.
- O CARDUG é um módulo do SICAP onde deve ser cadastrado todos os servidores pertencentes ao **Rol de Responsáveis** conforme art. 166 do RITCE-TO e os **responsáveis por módulos** do SICAP, conforme IN 07/2008,

O Único responsável pela alimentação do CARDUG é o Gestor, cuja informação e permissão são efetuadas pelo TCE-TO, que o habilita para o acesso.

- ABAS – são "fichas" onde constam as informações. Ex. abrindo o CARDUG encontramos as seguintes abas ou fichas:

GESTOR – CADASTRO DE RESPONSÁVEIS – UNIDADE GESTORA – PERMISSÃO

As abas Gestor e cadastro de responsáveis – são fichas com dados de pessoas físicas.

A aba Unidade Gestora são os dados da pessoa jurídica, a unidade gestora.

A aba Permissão, possui sub-abas que são a identificação dos módulos, por isso aqui as chamaremos de módulos listados abaixo e com as funções responsáveis pelos mesmos:

ACCI – Controle Interno,
SICAP Contábil - Gestor, Controle Interno e Contador
SICAP Atos de Pessoal – Gestor, Controle Interno e Responsável RH
SICAP Licitação – Gestor, Presidente CPL, ou Pregoeiro e/ou Servidor Autorizado
SICAP Obras - Gestor e Servidor Autorizado.

- Caixas – são fichas que se abrem ao clicar em determinados *ícones*. Alguns *ícones* apenas confirmam a informação, como por exemplo: inserir, adicionar, salvar. Os *ícones* "Deletar", "Visualizar Permissão de Acesso" e "Atualizar", ao serem clicados abrirá uma outra caixa de dialogo para completar a informação.

Vejamos, agora, como alimentar o cadastro.

2.2 Alimentando o CARDUG

Para a inclusão de **novo gestor**, deverá ser repassada informação contendo nome, CPF e documento de posse ao TCE via protocolo. Através dessa informação, o TCE efetua o **pré-cadastro** desse novo Gestor, incluindo apenas seu nome e CPF. Assim libera o acesso para que este gestor possa acessar e completar todo seu cadastro e, ainda, efetuar ou atualizar o cadastro de sua equipe, seu Rol de Responsáveis, através de abas específicas que veremos a seguir.

2.2.1 ABA GESTOR

Após acessar o CARDUG, temos a Aba GESTOR (Fig. 12), em que o gestor, já previamente cadastrado, deverá atualizar, ou seja, completar todos os seus dados pessoais, endereço, telefone, *e-mail* e demais informações solicitados nas telas auto-explicativas e conforme as descrições abaixo:

Ao identificar o estado civil 1 automaticamente abrirá uma caixa de texto para inclusão do nome do cônjuge. Ao inserir endereço, 2 o usuário poderá cadastrar quantos endereços desejar, bastando apenas informar todos os dados e **sempre** clicar em **Adicionar** **.** Ao necessitar visualizar um endereço clicar em **Editar** assim poderá com clareza visualizar o endereço completo tal como foi informado.

Havendo a necessidade de cancelar este endereço, clicar em **Deletar** que será excluída esta informação.

Para cadastrar o telefone é necessário rolar a pagina conforme item 3 na barra de rolagem lateral, para visualizar os campos e informar o telefone, utilizando o mesmo procedimento anterior, descrito para endereço, ou seja, para incluir (Adicionar), visualizar (Editar) e excluir (Deletar).

Lembramos que o GESTOR **somente** será informado pelo TCE-TO, sendo necessário enviar ao Tribunal, documento de finalização do Gestor anterior, (afastamento judicial, atestado de óbito, afastamento por doença, decreto exoneração etc.) e documento de posse ou Decreto de nomeação do novo Gestor, acompanhado de oficio e copia do CPF.

Quando de Eleições gerais não é necessário enviar informação do gestor anterior ou do eleito, pois estas informações são fornecidas pelo TSE.

Conheçamos a seguir a “Aba Gestor” identificada na fig. 12:

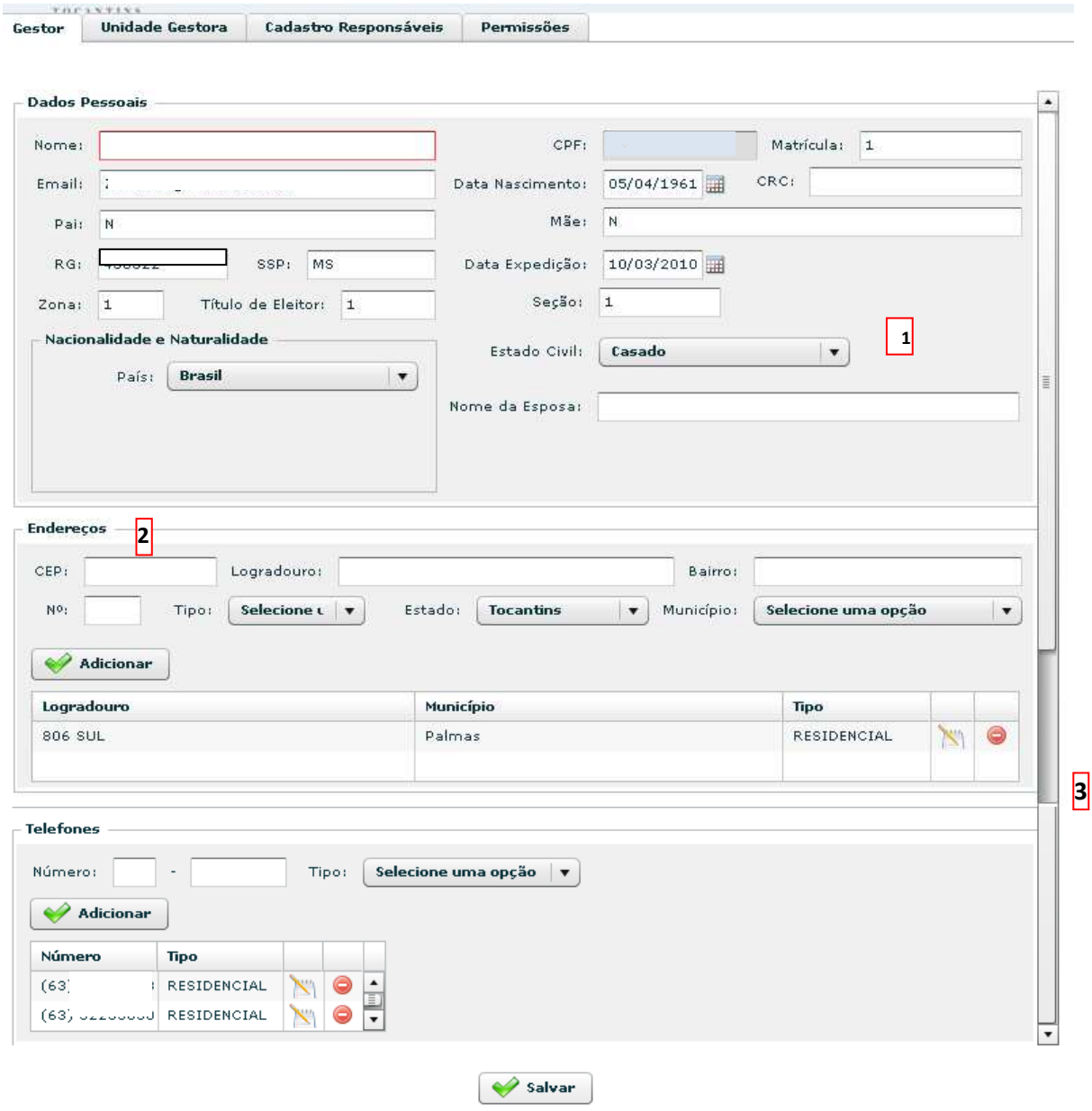

Fig. 12 Aba Gestor

É **muito importante** o gestor completar **todo** o seu cadastro, principalmente o endereço eletrônico, visto que o TCE ao fazer o pré-cadastro, informa apenas nome e CPF.

Após conclusão de todas as informações, sempre salvar o registro.

2.2.2 ABA CADASTRO DE RESPONSÁVEIS

Após completar o seu próprio cadastro, o gestor tem a Aba CADASTRO DE RESPONSÁVEIS (Fig. 13), na qual cadastra todos os servidores pertencentes ao **Rol de Responsáveis** e **responsáveis pelos módulos** do SICAP. Para isso, deve preencher todos os campos, pois existem campos obrigatórios e impeditivos para a conclusão do cadastro, sendo necessário colocar todos dados pessoais, documentos, endereço e telefone conforme foi descrito no item 2.2.1, Aba Gestor. Em seguida rolar a pagina para vincular um cargo para o servidor cadastrado, informando corretamente os dados solicitados, cargo, tipo de documento, número e data do documento desta nomeação.

Sempre ao informar um **contador** será obrigatória a informação do CRC em campo próprio, item 4 conforme identificado.

Em **Vínculos**, no item, **Cargos,** 5 encontra-se uma tabela de cargos, caso não encontre o cargo procurado, deverá fazer uma escolha aproximada e no campo "Especificação do Cargo" completar a especificação correta. Ex. Cargo Secretario, Especificação do Cargo: de Juventude e Esportes. .

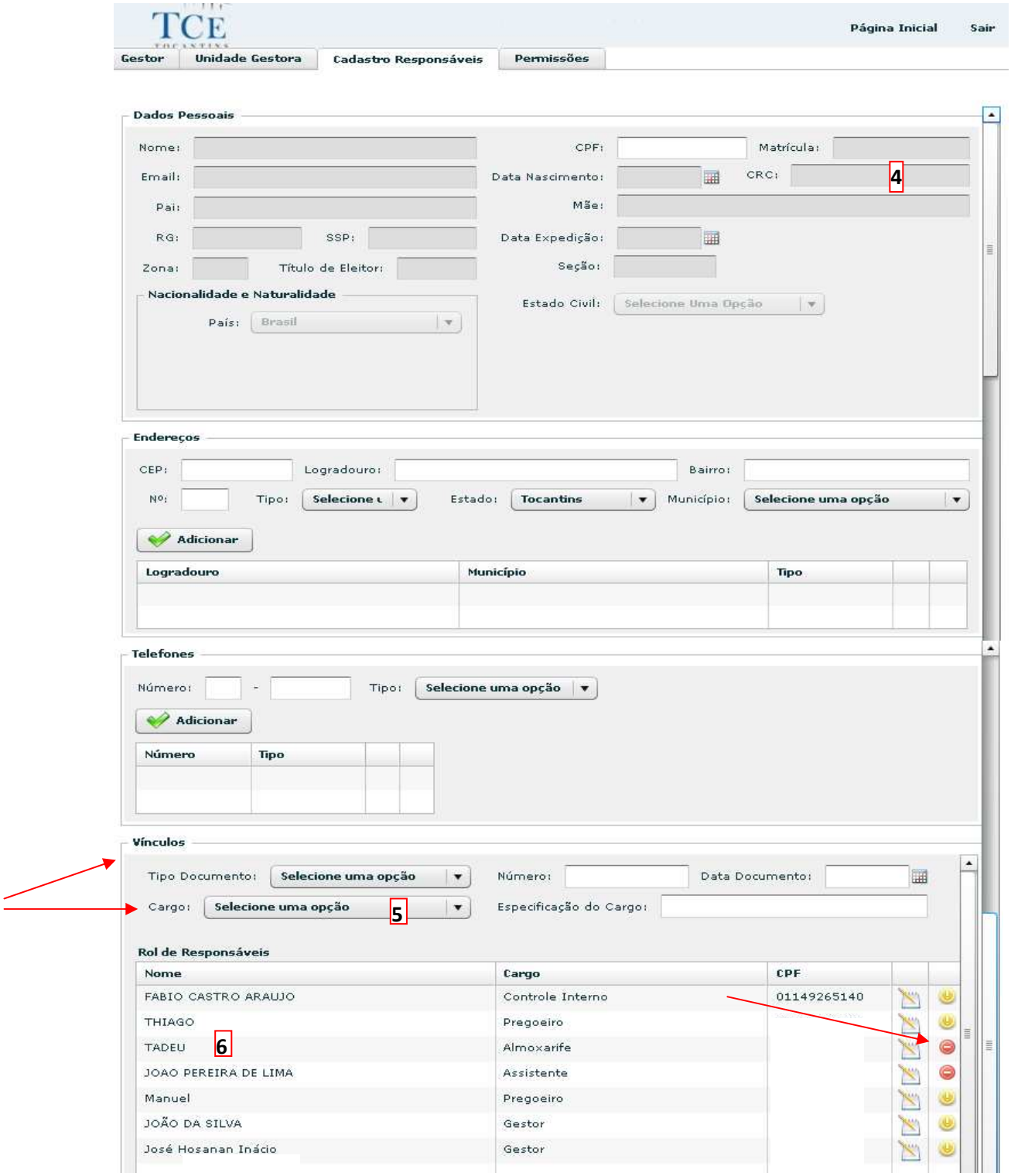

Fig. 13 Aba Cadastro Responsáveis

Logo abaixo de **Vínculos**, aparece o **Rol de Responsáveis**, onde constam todos os servidores ativos cadastrados, pertencentes ao Rol de Responsáveis conforme art. 166 do RITCE e dos responsáveis por Módulos, conforme IN 07/2008.

Depois de efetuado o cadastro, se o servidor for **responsável por módulos** do SICAP, o gestor necessita fazer a **vinculação** e liberar a **permissão,** conforme verificaremos no item 2.2.3 abaixo**,** para que esse servidor tenha acesso aos módulos do SICAP.

Quando o servidor pertencer apenas ao Rol de Responsáveis, ou seja, não está vinculado a Módulos do SICAP, aparecerá o ícone **Deletar** (sinal menos vermelho) conforme a linha do item 6 da Fig. 13 acima.

Caso esteja vinculado a módulos, e já liberado permissão, aparecerá um ícone (exclamação amarelo) apenas para identificar no momento da finalização deste servidor.

Para finalizar servidor pertencente apenas ao **Rol de Responsáveis,** o gestor deverá clicar em **Excluir** na frente do nome do referido servidor, item 6 citado, onde aparecerá a caixa, Fig. 14, "Dados de Finalização" ao lado, quando deve preencher conforme solicitação, tipo, número e a data do documento que gerou o afastamento deste servidor. Muita atenção com a informação desta data! Feito isto, **salvar** a informação.

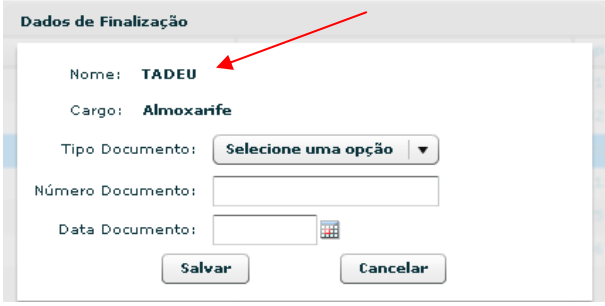

Fig. 14 - Finalizando Servidor do Rol

Quando se tratar de **responsáveis por módulos**, a finalização deve ser feita na aba Permissão, conforme a seguir.

2.2.3 ABA PERMISSÃO

Essa aba PERMISSÃO é utilizada para **vincular** servidor ao módulo, **liberar** permissão e para **finalizar** o vinculo.

Fig. 15 - Aba Permissão

Ao cadastrar um Controle Interno, automaticamente ele será vinculado nos Módulos ACCI, Atos de Pessoal e Contábil e no Rol já aparecerá o icone pois ainda não foi liberado permissão para os módulos, conforme especificado anteriormente.

a) Vinculando servidor

Para que o gestor possa informar os responsáveis por módulos SICAP, após concluir o cadastro, deverá ir para a Aba PERMISSÃO (Fig. 15), vincular este servidor ao módulo e liberar a permissão do mesmo para que possa efetuar as assinaturas digitais de acordo com o cargo determinado e aos módulos em que ele é o responsável.

Como já vimos, ao cadastrar um Controle Interno ele será automaticamente inserido no módulo SICAP **ACCI, Contábil e Atos de Pessoal**, lembrando que ACCI é semestral, com duas remessas, Contábil é bimestral sendo oito remessas anuais e Atos Pessoal é quadrimestral, com tres remessas anuais, portanto sendo necessário acessar a Aba Permissão e no módulo em questão, preenhcer a **Data Início**, em seguida clicar em **Atualizar,** assim aparecerá uma caixa **Inserir Permissão**, conforme Fig. 16 Permissão SICAP Contábil abaixo, onde estamos inserindo permissão para Controle Interno no Módulo Contábil.

Ao inserir a data inicio em qualquer um destes tres módulos citados para o cargo controle interno, automaticamente estes módulos terão esta mesma data iníco, sendo necessario neste caso, acessar o módulo ACCI e tambem Atos de Pessoal clicar em **Visuaslizar Permissões de Acesso** para **liberar as permissões** devidas para estes outros módulos.

Após a liberação da primeira permissão para este servidor, aparecerá no Rol o icone , informando que já existe permissão. Para finalizar este servidor somente a partir da tela **Permissões** conforme explicado no item "b" Finalizando Servidor pagina 20 a seguir.

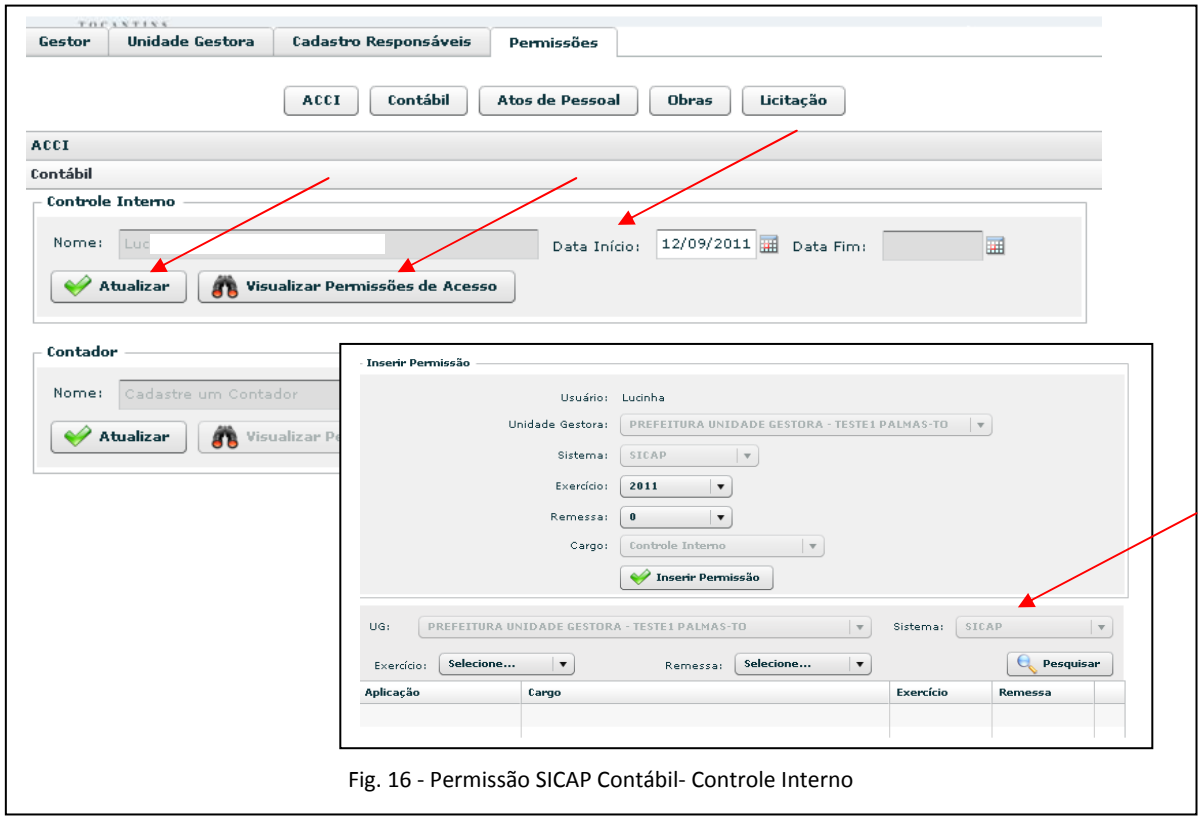

Fig. 16 - Permissão SICAP Contábil- Controle Interno

Analisamos agora um exemplo de um servidor do Rol, de nome João, cargo Assistente, que será vinculado ao Módulo **Atos de Pessoal** com Responsavel de RH e liberado permissões, conforme abaixo (Fig. 17).

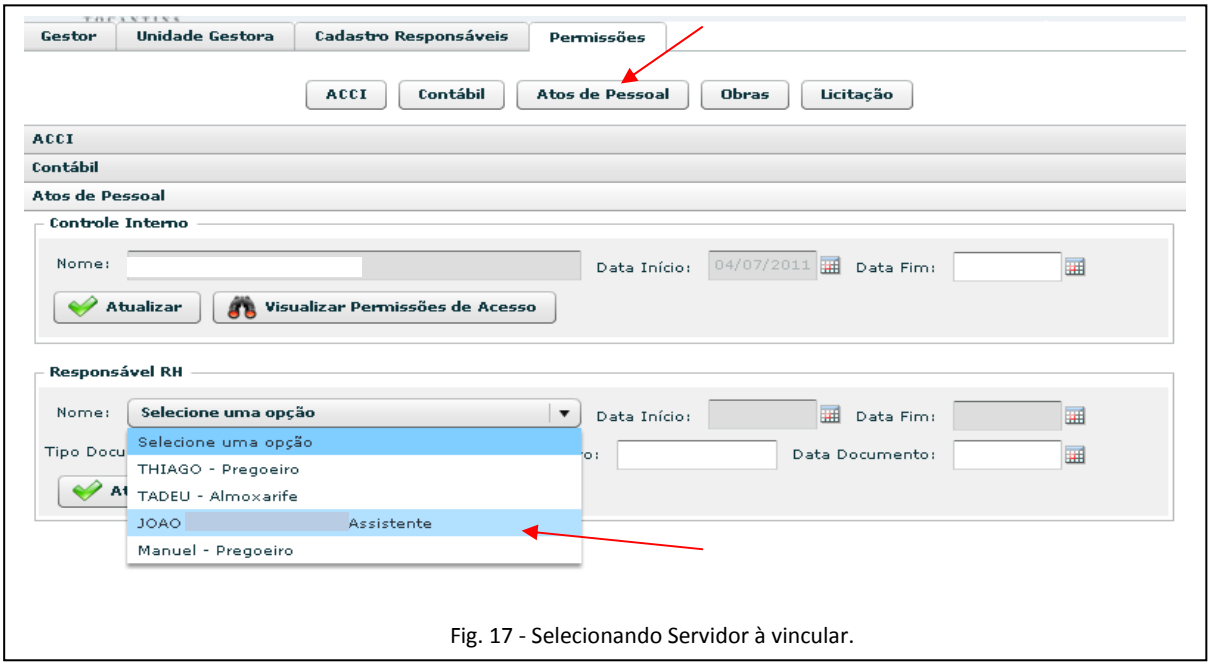

Fig. 17 - Selecionando Servidor à vincular.

Para vincular este servidor é simples, neste exemplo, o servidor João, que no Rol de Responsáveis tem o cargo de Assistente, porem em 03/10/2011 tornou-se responsável pelo setor de recursos humanos, conforme Fig. 18. Assim sendo, deverá ser preenchido conforme a documentação solicitada nos campos correspondentes, e muita atenção quanto a data de início. **NÃO** deve ser preenchida a **DATA FIM**, em hipótese nenhuma, mesmo que seja pré-determinada, ou seja, data futura.

Fig. 18 - Vinculando servidor ao Módulo AP

Após vincular o servidor no Módulo, **Atos de Pessoal**, clicar em **Atualizar**, assim procedendo abrirá uma nova tela, **Inserir Permissão** - Fig. 19, para liberar as permissões. Nesta tela, aparece o nome do servidor, a unidade gestora, o sistema e o cargo neste módulo, ou seja, Responsável RH, todos desabilitados, ou seja, estes campos não têm alteração, apenas deve ser escolhido o exercício e a remessa para qual este servidor tem autorização, e clicar em **Inserir Permissão.**

Fig. 19- Liberando Permissão para o servidor

Após esta liberação, o nome do servidor aparecerá na parte inferior da tela, conforme visualizado na FIg. 19, onde também é possível fazer filtros, por remessa e por exercício, e clicando em **Pesquisar**, assim, visualizando todas as permissões deste servidor neste módulo. Desta forma está liberada a permissão, podendo o mesmo assinar as remessas a qual recebeu permissão.

Para o Modulo **Obras e Licitação** que não possuem remessa, a liberação é um pouco diferente, é única, não tendo limite de pessoas vinculadas em Licitação, como Presidente CPL, Pregoeiro ou como Servidor Autorizado, sendo este último utilizado também para Obras.

Ao cadastrar um servidor como Presidente de CPL ou como Pregoeiro, automaticamente será inserido na tela de permissões, de acordo com o cargo cadastrado, sendo necessário apenas habilitar a permissão. Observando a (Fig. 20) abaixo, verificamos o nome da servidora Maria Teste a qual foi cadastrada como Presidente CPL, e automaticamente é inserida em Licitação, na caixa Presidente CPL. Assim sendo, aparece o sinal (verde), sendo necessário um clique para que fique (exclamação amarelo), desta forma, está inserida a permissão para assinar o módulo como Presidente CPL.

Caso esta mesma servidora deva assinar também com o cargo de Pregoeiro, deverá selecionar logo abaixo em Pregoeiro, na caixa **Nome**, escolher a servidora, preencher a documentação como pede, Data Início e **Adicionar,** desta forma já estará com permissão também como Pregoeiro, pois aparecerá o ícone , indicando com permissão.

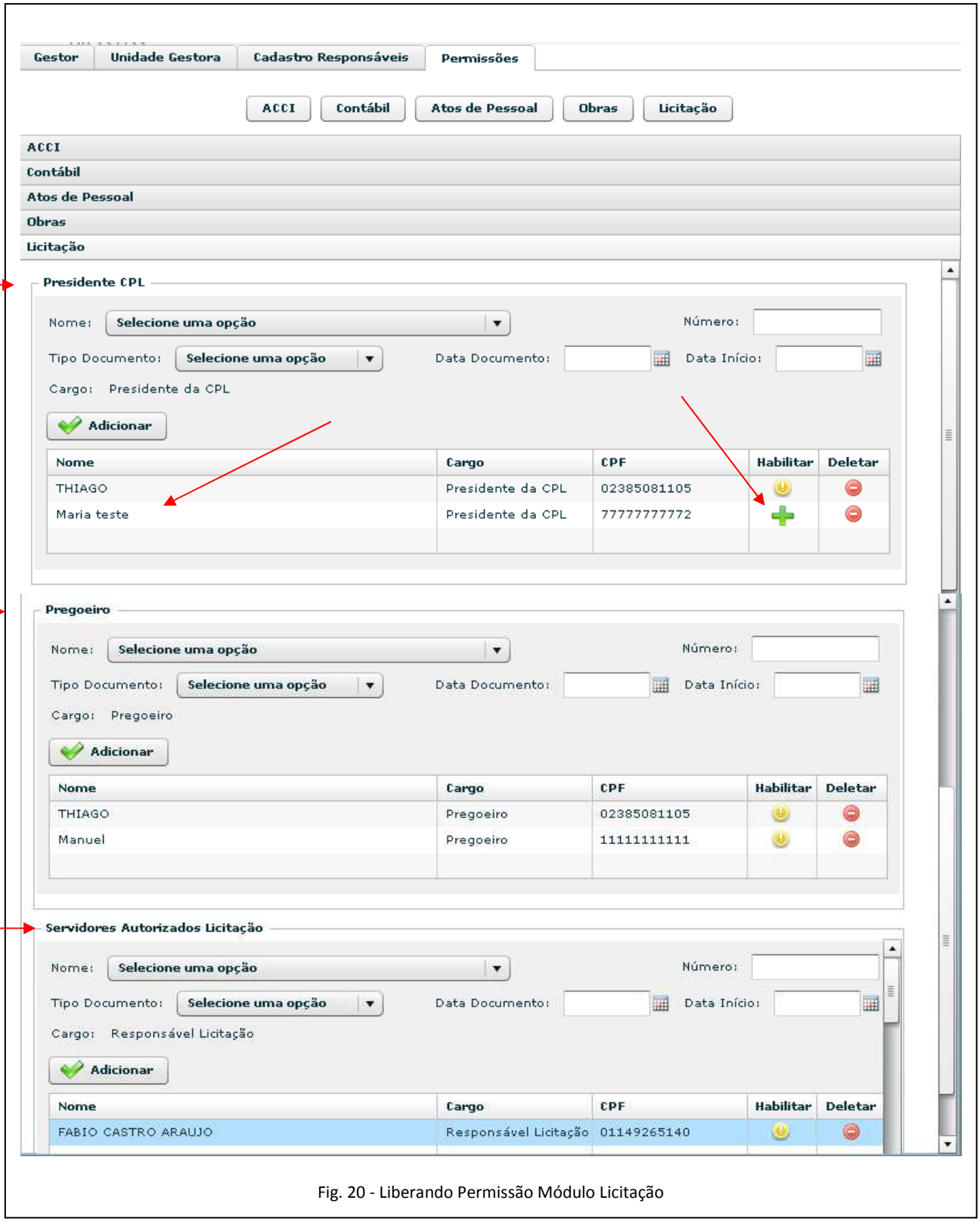

Fig. 20 - Liberando Permissão Módulo Licitação

Qualquer servidor cadastrado no Rol poderá ser vinculado em Licitação como Servidor Autorizado, preenchendo a documentação conforme a solicitada, a Data inicio e Adicionar , quando aparecerá relacionado em seguida.

A seguir estudaremos a finalização de servidor em módulos ou no Rol.

b) Finalização de servidor

Finalizando no Rol de Responsáveis

Quando se tratar de exoneração de servidor do **Rol de Responsáveis**, esta ação deve ser efetuada na Aba Cadastro de Responsável, conforme o item 2.2.2, Fig. 13 Rol de Responsáveis e Fig. 14 Dados de Finalização, já comentada.

Sempre que for finalizar um servidor que esteja vinculado à módulos SICAP, deverá antes de informar a data fim, **Deletar** todas as permissões "em ser", ou seja, ainda não assinadas.

Finalizando Licitação e Obras

Seguindo o exemplo da servidora Maria Teste cujo cadastro no Rol, foi Presidente CPL e posteriormente podendo ser vinculada como Pregoeiro, e Responsável Licitação, sua permissão deverá ser deletada primeiramente na aba Permissão, em todos os vínculos, preenchendo a caixa "Dados de Finalização", assim quando deletar do vinculo Presidente CPL, que é o mesmo cargo do Rol, este nome desaparece automaticamente do Rol.

Caso tenha um servidor no cargo de diretor, por exemplo, e este é eleito Presidente da CPL, deverá ser vinculado a partir da data da eleição, na Aba Permissão em Licitação, vinculando-o como Presidente CPL.

Neste exemplo, caso ele tenha apenas deixado de exercer funções em licitação, deve-se retirar as permissões na aba permissão, em nos módulos onde estava vinculado, inserindo as informações solicitadas em Dados de Finalização, continuando ainda assim no Rol como Diretor.

Caso este servidor tenha sido realmente exonerado, após deletar todas as permissões, retornar ao rol e excluir diretamente no próprio nome deste servidor em **Deletar** para finalizar definitivamente este servidor, assim, aparecerá a caixa conforme FIg. 14 Dados de Finalização, a ser preenchida.

Finalizando ACCI, Contábil e Atos de Pessoal – (controle interno)

Quando se tratar de módulos **SICAP ACCI, Contábil e Atos de Pessoal,** o gestor deverá acessar Permissões escolher o modulo, conforme exemplo da FIg. 21, onde temos o exemplo do módulo ACCI, encontrando o nome do servidor, clicar em **Visualizar Permissões de Acesso**, quando aparecerá a caixa "Inserir Permissão", clicar em **Pesquisar** para visualizar as permissões "em ser" e clicar em **Deletar** conforme a Fig. 21, Excluindo Permissão ACCI, quando então, aparecerá os dizeres "Permissão deletada com sucesso".

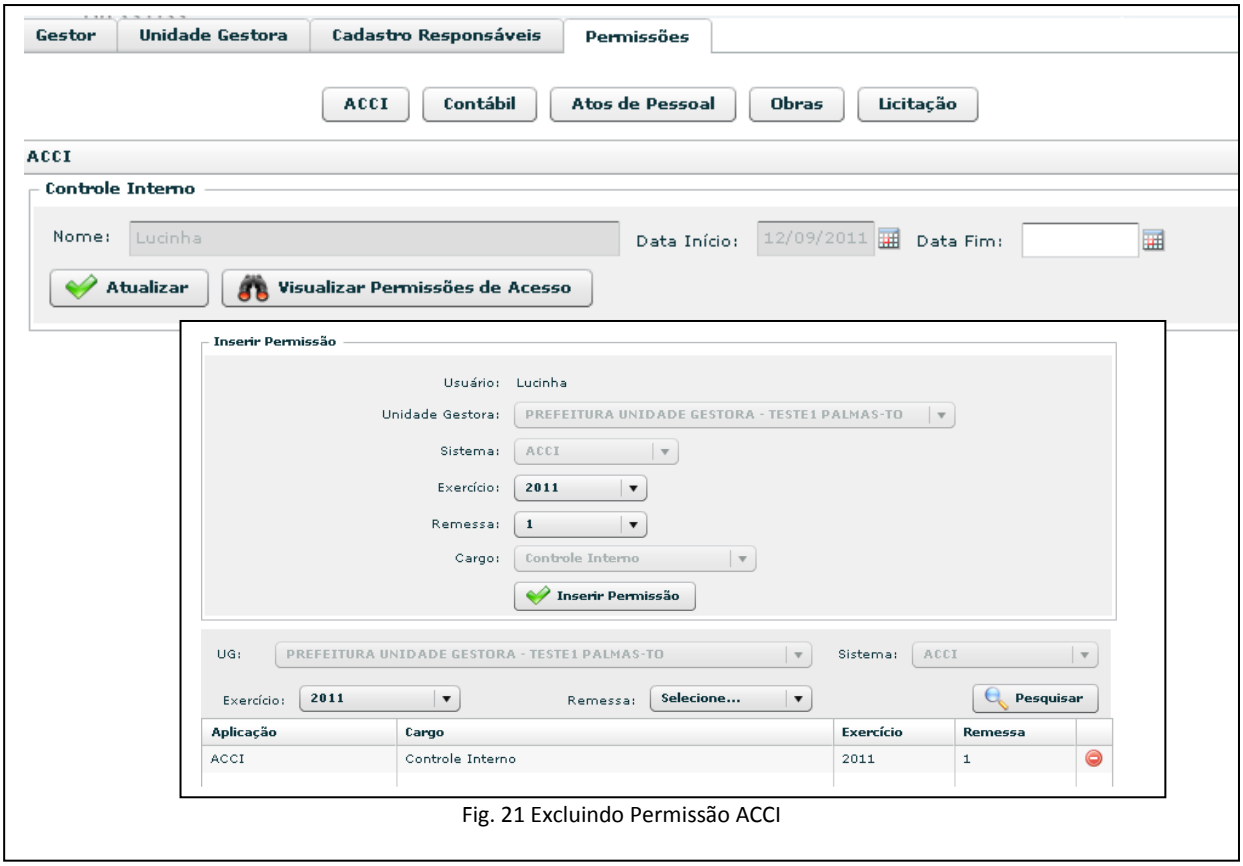

Fig. 21 Excluindo Permissão ACCI

Excluindo Controle Interno:

Como neste exemplo é um cargo de controle interno, deverá entrar também no módulo **Contábil** e em **Atos de Pessoal**, e verificar se este servidor possui permissão "em ser", ou seja, ainda não assinadas, e também se não será mais responsabilidade dele a assinatura, deletando as mesmas conforme a Fig. 21 do ACCI. Somente após estas providencias tratando-se de Controle Interno, é que deverá inserir data fim para este servidor, conforme FIg. 22, Finalizando Controle Interno, exemplo este do modulo Atos de Pessoal.

A partir da inserção da **Data Fim** para o Controle Interno **em um módulo** e preenchendo os Dados de Finalização, será finalizado **em todos os módulos** e também no Rol de Responsáveis, não sendo mais possível visualizar este servidor. Por isto a **imperiosa atenção** quanto a colocar a **data fim** para servidores, mesmo que seja data futura, **não será mais possível visualizar** o servidor, bem como excluir permissões que ainda não havia assinado.

Fig. 22 Finalizando Controle Interno

Para finalizar um Contador, deve acessar na Aba Permissões, em Contábil, em Visualizar Permissões de Acesso conforme Fig. 21, e deletar as permissões em ser. Feito isto inserir a data fim e preencher o campo “Dados de Finalização” conforme o exemplo do Controle Interno FIg. 22.

Tratando-se de **Controle Interno** e também de **Contador,** que são responsaveis solidários junto ao Gestor do órgão, mesmo encerrando o periodo em 31/12 por exemplo, poderão continuar com permissão para assinar a 6ª, 7ª e 8ª remessa, as quais ocorrerão no proximo exercicio, liberando assim o cadastro para um novo servidor nestes cargos para iniciar o novo exercício.

Vamos utilizar o exemplo abaixo, finalizando o servidor João, no módulo, **Atos de Pessoal**, com data de 20/09/2011, conforme visualizamos na tela Fig. 23, onde preenchemos os campos conforme pede, tipo de documento, número de data do documento. Após esta ação, caso este servidor caso tenha sido cadastrado no Rol como Responsável de RH, não será mais possível visualizá-lo no Rol de Responsáveis.

Caso tenha sido cadastrado no Rol com cargo diferente de Responsável RH, ele continuará no Rol, devendo ser finalizado conforme indica a Fig. 14, inserindo as informações solicitadas, caso tenha sido exonerado.

Lembramos mais uma vês, da **imperiosa atenção** quanto a colocar a **data fim** para servidores, mesmo que seja data futura, pois a partir desta informação, **não sendo mais possível visualizar** este servidor.

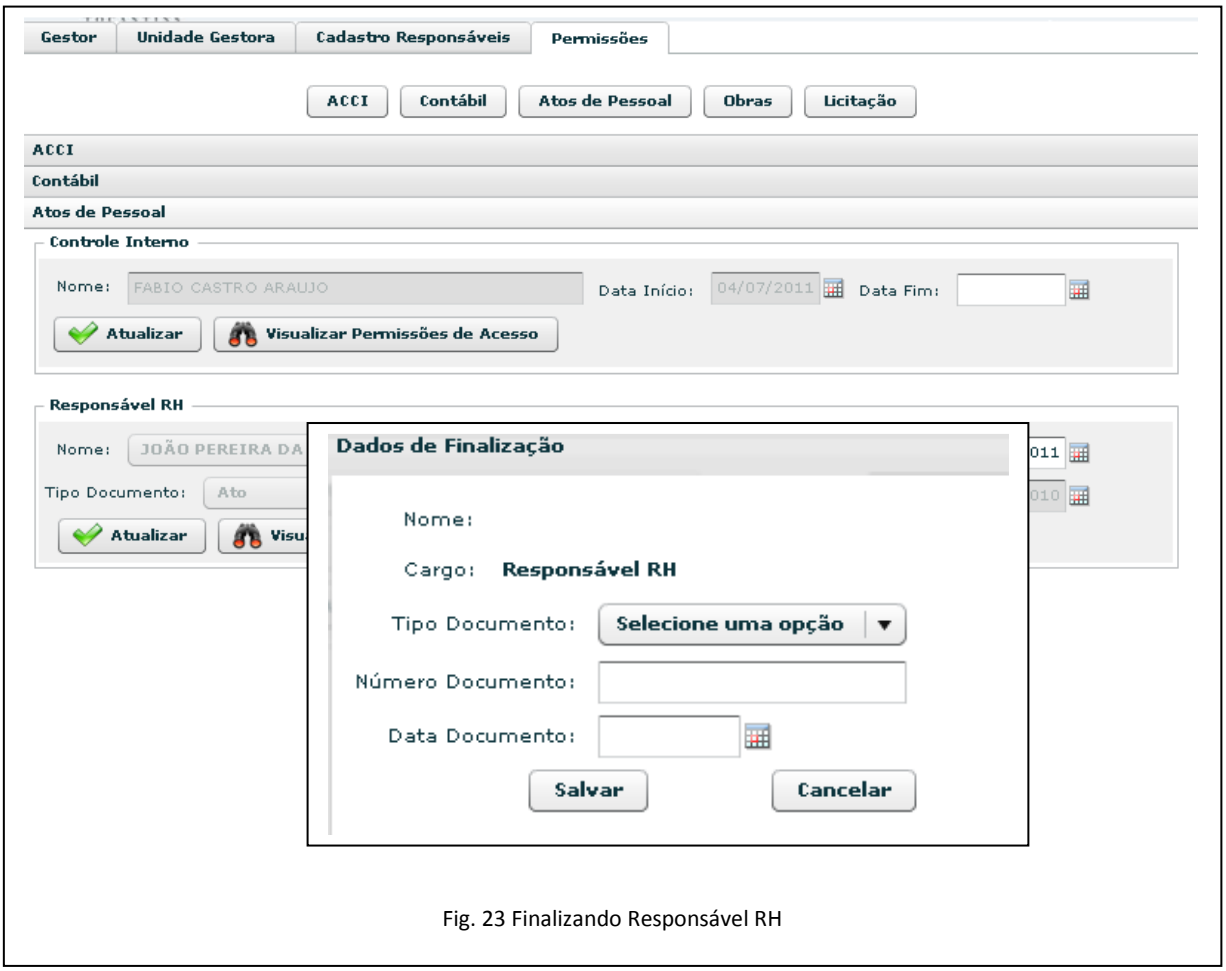

Fig. 23 Finalizando Responsável RH

2.2.4 ABA UNIDADE GESTORA

No CARDUG, temos também a Aba UNIDADE GESTORA (Fig. 24), espaço onde o Gestor deve atualizar os dados referentes à sua unidade gestora, quanto a endereço, telefone, horário de funcionamento, *e-mai*l, *site,* e outros dados necessários.

É de grande importância que esses dados sejam rigorosamente atualizados para agilizar a comunicação do TCE com os demais órgãos, tanto via telefone como correio e agora eletronicamente.

Caso a unidade não tenha um *site,* deve ser inserido um ***e-mail*** **institucional** para contatos com maior agilidade.

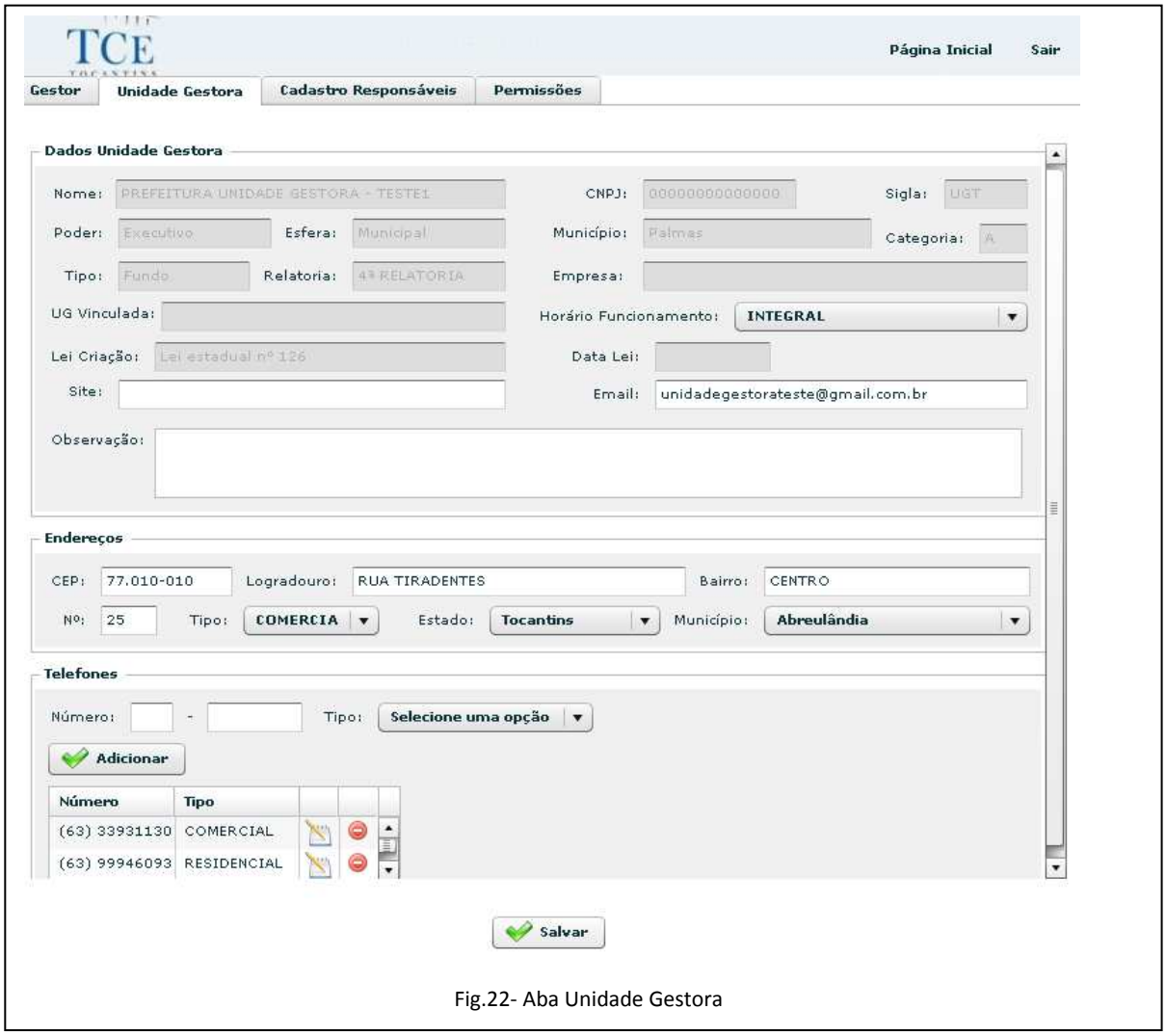

Fig.22- Aba Unidade Gestora

Diante do exposto cremos que você já conhece tanto sobre certificação digital como o sobre o cadastro, onde devem ser alocados o **Rol de Responsavel** bem como os **responsaveis por módulos,** o CARDUG é o módulo que efetua a ligação entre todos os módulos do SICAP.

Lembramos que este **módulo é dinâmico,** sendo constamente alterado e aperfeiçoado, sendo necesario **observar sempre as versões** deste material.