UNIVERSIDADE DE TAUBATÉ

Gabriel Pitágoras Silva e Brenner

INTEGRAÇÃO DE RECURSOS DAS IDENTIFICAÇÕES POR RADIOFREQUÊNCIA E BIOMETRIA DA IMPRESSÃO DIGITAL EM APLICAÇÃO DIRECIONADA PARA O CONTROLE DE ACESSOS DE PESSOAS A ÁREAS INDUSTRIAIS

Taubaté - SP
2012

UNIVERSIDADE DE TAUBATÉ

Gabriel Pitágoras Silva e Brenner

INTEGRAÇÃO DE RECURSOS DAS IDENTIFICAÇÕES POR RADIOFREQUÊNCIA E BIOMETRIA DA IMPRESSÃO DIGITAL EM APLICAÇÃO DIRECIONADA PARA O CONTROLE DE ACESSOS DE PESSOAS A ÁREAS INDUSTRIAIS

Dissertação apresentada para obtenção do Título de Mestre pelo Curso de Mestrado Profissional em Engenharia Mecânica do Departamento de Engenharia Mecânica da Universidade de Taubaté.
Área de concentração: Automação.
Orientador: Prof. Dr. José Walter Parquet Bizarria.
Co-orientador: Prof. Dr. Francisco Carlos Parquet Bizarria.

Taubaté - SP
2012

GABRIEL PITÁGORAS SILVA E BRENNER

INTEGRAÇÃO DE RECURSOS DAS IDENTIFICAÇÕES POR RADIOFREQUÊNCIA E BIOMETRIA DA IMPRESSÃO DIGITAL EM APLICAÇÃO DIRECIONADA PARA O CONTROLE DE ACESSOS DE PESSOAS A ÁREAS INDUSTRIAIS

Dissertação apresentada para obtenção do Título de Mestre pelo Curso de Mestrado Profissional em Engenharia Mecânica do Departamento de Engenharia Mecânica da Universidade de Taubaté.
Área de concentração: Automação**.**

Data:_____

Resultado:_____

BANCA EXAMINADORA

Prof. Dr. José Walter Parquet Bizarria — Universidade de Taubaté

Assinatura_____

Prof. Dr. Luis Fernando de Almeida — Universidade de Taubaté

Assinatura_____

Profa. Dra. Silvana Aparecida Barbosa — Instituto de Aeronáutica e Espaço

Assinatura_____

Dedico esse trabalho a minha primeira namorada, esposa, amiga e fiel companheira, Marília, que sempre me acompanhou e me fortaleceu na estrada da vida e ao nosso maior presente, Ana Clara, que com seu sorriso ilumina nosso dia e faz com que tudo pareça mais simples e fácil.

AGRADECIMENTOS

Ao orientador Prof. Dr. José Walter Parquet Bizarria, por sua paciência, constante direcionamento e compromisso total na elaboração desse trabalho.

Ao Co-orientador Prof. Dr. Francisco Carlos Parquet Bizarria, pelo apoio.

À Indústrias Nucleares do Brasil S/A pelo financiamento e apoio.

À Gilda Bastos Menezes e André Rafael Barboza, pelo precioso auxílio na revisão do abstract.

Ao amigo Marcelo Alleo pela ajuda nas disciplinas do mestrado e companheirismo durante as inúmeras viagens de Resende a Taubaté.

Ao Gerente da área de Tecnologia da Informação, Valmir Fernando da Silva e ao Coordenador da área de desenvolvimento, Carlos Alberto de Oliveira, pelo total apoio interno e confiança.

À Unitau por possibilitar realizar um sonho.

Ao Gerente de Segurança da INB, Jorge Eduardo Jean Tranjan, por esclarecer as dúvidas sobre segurança patrimonial.

À minha esposa Marília de Castro Viana Brenner, pela paciência, tolerância e apoio em todos os momentos.

À luz de minha vida, Ana Clara Viana Brenner, minha filha, por me alegrar diariamente com o seu sorriso e me ajudar a manter o foco e não desistir.

Dizem que uma critica destrói 10 elogios.
Porém, não se cresce com elogios.
O elogio alimenta o ego.
O ego não aceita mudanças.
A crítica é sempre dolorida.
Mas nos obriga a pensar.
O sábio aprende a lidar com a crítica e cresce.
O dependente torna-se escravo do elogio e perece.
Para vencer, você não precisa ser aceito.
Basta aprender a aceitar.
Não que se deva aceitar todas as críticas.
Existem aquelas que buscam derrubar.
Necessário é discernir.
A que derruba, daquelas que buscam edificar.

Desconhecido

RESUMO

INTEGRAÇÃO DE RECURSOS DAS IDENTIFICAÇÕES POR RADIOFREQUÊNCIA E BIOMETRIA DA IMPRESSÃO DIGITAL EM APLICAÇÃO DIRECIONADA PARA O CONTROLE DE ACESSOS DE PESSOAS A ÁREAS INDUSTRIAIS

No presente trabalho são abordados estudos sobre elementos do projeto conceitual de um sistema de controle de acessos de pessoas a áreas industriais, voltado para o propósito de oferecer contribuição para o segmento particular daqueles tipos que exigem a utilização de automatização para atender a respectiva viabilização operacional relativa às atividades pertinentes ao controle de acessos em questão. Os testes práticos realizados com protótipos apresentaram resultados satisfatórios, validando os princípios de funcionamento dos elementos envolvidos, haja vista que foram verificadas as realizações das operações previstas pelo sistema que possui as características de: identificação por radiofrequência fundamentada em tecnologia voltada para aplicações de identificação à curta distância com leitor fixo e transponder *read-only*, identificação por biometria da impressão digital fundamentada em tecnologia de captura de imagem com utilização de leitura óptica; utilização de equipamentos para controle físico do acesso de pessoas, cujas previsões de instalação permitam atender fluxos nos sentidos unidirecional e bidirecional com relação a área controlada; aplicação de recursos disponíveis por *Web Services* para atendimento das necessidades afins exigidas para o desenvolvimento do sistema; segurança no transporte de dados fundamentada na utilização do protocolo SSL; estações de trabalho e servidores constituídos por computadores pessoais com arquitetura Intel® ou compatível; utilização de elementos de integração de sistemas direcionados para a abrangência de sistemas computacionais empresariais empregados em indústrias. O objetivo proposto foi atingido, sendo que os testes práticos validaram os princípios de funcionamento dos elementos abordados, oferecendo contribuição para o mencionado segmento de sistemas de controle de acessos de pessoas.

Palavras-Chave: Controle de Acessos. Biometria. RFID. Automatização

ABSTRACT

RADIO FREQUENCY IDENTIFICATION (RFID) INTEGRATION WITH FINGERPRINTS BIOMETRIC SENSORS AS APPLIED TO CONTROL ACCESS IN INDUSTRIAL AREAS

The present work discusses studies about conceptual design elements to personal access control system to industrial areas. It aims at offering a contribution to enhance people control to areas with the use of automation resources. Practical template tests undertaken presented satisfactory results, thus validating their working principles and technological achievements of the operations previews of the system characteristics: radiofrequency identification based on the technology of short distance identification with fixed reader and "read-only" transponder; biometric identification based on image capture using optical reading; equipment for controlling personal physical access , whose installation would permit unidirectional and bidirectional flows to the controlled area; use of resources available by Web Services to meet the needs to system development; data transport safety based on SSL protocol; work station and servers of the Intel® type personal computers, or compatible; systems integration with corporate computer systems.

The proposed goal has been achieved, and the practical tests confirmed the operational principles of the elements in question, offering contributions to the automated control systems of personal access in industrial areas.

Keywords: Access Control. Biometrics. RFID. Automation.

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AA_PCAP_S - Ativação de Alarme de PCAP_S.

AP - Área Protegida.

ArVig - Área Vigiada.

ASCII - *American Standard Code for Information Interchange*.

AV - Área Vital.

BD_SICAP - Banco de Dados do SiCAP.

BEF - Bem Físico.

CFTV - Circuito Fechado de Televisão.

CI - Circuito Integrado.

CI_ARU - Código de Identificação da Associação da Rota R_USR.

CI_CId_S - Código de Identificação do Cartão CId_S.

CI_CON - Código de Identificação do Contratado.

CI_DU - Código de Identificação do Dedo do Usuário USR.

CI_EPP_S - Código de Identificação do Equipamento EPP_S.

CI_EPP_S_USR - Código de Identificação da Associação do Equipamento EPP_S ao Usuário USR.

CI_EST - Código de Identificação do Estagiário.

CI_MAT - Código de Identificação de Matrícula do Funcionário.

CI_MU - Código de Identificação da Mão do Usuário USR.

CI_PB - Código de Identificação do Perfil Biométrico.

CI_PCAP_S - Código de Identificação do PCAP_S.

CI_ROTA - Código de Identificação da Rota R_USR.

CI_T_EPP_S - Código de Identificação do Tipo de Equipamento EPP_S.

CI_USR - Código de Identificação de Usuário USR.

CI_VIS - Código de Identificação do Visitante.

CId - Cartão de Identificação.

CId_S - Cartão de Identificação-SiCAP.

CIRTA_USR - Código de Identificação do Registro de Tentativa de Acesso RTA_USR.

CNEM - Comissão Nacional de Energia Nuclear.

Col - Colaboradores.

CoRePBID_S - Componentes Referentes ao Perfil Biométrico da Impressão Digital-SiCAP.

CPF - Cadastro de Pessoas Físicas.

CT_CID_S - Código do Transponder no Cartão CId_S.

CT_EPP_S - Código do Transponder no Equipamento EPP_S.

DAdm - Diretor Administrativo.

DE_T_EPP_S - Descrição do Tipo de Equipamento EPP_S.

DESC_ROTA - Descrição da Rota R_USR.

DiAdm – Diretoria Administrativa.

DT_ACESSO - Data e Hora da Tentativa de Acesso.

DT_IAL - Data e Hora de Interrupção do Alarme de PCAP_S.

E_SICAP. PONTOCONTRO LE - Estação de Trabalho SICAP.PONTOCONTROLE.

E_SICAP.ADMINISTRA TIVO - Estação de Trabalho SICAP.ADMINISTRATIVO.

E_SICAP.AUDITORIA - Estação de Trabalho SICAP.AUDITORIA.

ECAP - Equipamento para Controle de Acessos de Pessoas.

ECAP_S - Equipamento para Controle de Acessos de Pessoas-SiCAP.

ECoFAP - Equipamentos para Controle Físico de Acessos de Pessoas.

ED_ALARME - Estado de Disparo do Alarme de PCAP_S.

EH_CId_S - Estado de Habilitação do Cartão CId_S.

EH_ROTA - Estado de Habilitação da Rota R_USR.

EH_USR - Estado de Habilitação do Usuário USR.

EHU_ROTA - Estado de Habilitação do Usuário USR para a Rota R_USR.

EIP - Etiqueta de Identificação Patrimonial.

ELAF - Estado de Liberação de Acesso Forçado.

EPC - *Electronic Product Code*™.

EPP - Equipamento de Proteção Pessoal.

EPP_S - Equipamento de Proteção Pessoal-SiCAP.

FA - *False Accept*.

FAR - *False Acceptance Rate*.

FOSSP - Funcionários Operacionais do Setor de Segurança Patrimonial.

FR - *False Reject*.

FRR - *False Rejection Rate*.

GeSIn - Gerência de Segurança da Informação.

GeSPa - Gerência de Segurança Patrimonial.

GeSPe - Gerência de Segurança de Pessoal.

GeSSE - Gerências da Subárea de Segurança Empresarial.

GOSeP - Gerente Operacional de Segurança Patrimonial.

GSIn - Gerente de Segurança da Informação.

GSPa - Gerente de Segurança Patrimonial.

GSPe - Gerente de Segurança de Pessoal.

HTTP - *Hypertext Transfer Protocol.*

IArch - Intel® *Architecture*.

IHM - Interface Homem-Máquina.

ISO - *International Organization for Standardization*.

LDA_PCAP_S - Limite para Disparo de Alarme de PCAP_S.

Le_BID_R - Leitor Biométrico da Impressão Digital por Reflexão.

Le_RFID - Leitor RFID.

LED - *Light Emitting Diode*.

LF - *Low Frequency*.

LF_EPP_S - Limite Final de Permissão para Utilização do EPP_S pelo Usuário USR.

LF_ROTA - Limite Final de Permissão para o Usuário USR Trafegar pela Rota R_USR.

LI_EPP_S - Limite Inicial de Permissão para Utilização do EPP_S pelo Usuário USR.

LI_ROTA - Limite Inicial de Permissão para o Usuário USR Trafegar pela Rota R_USR.

MB_CId_S - Motivo de Bloqueio do Cartão CId_S.

MB_ROTA - Motivo de Bloqueio da Rota R_USR.

MB_USR - Motivo de Bloqueio do Usuário USR.

MBU_ROTA - Motivo de Bloqueio do Usuário USR para a Rota R_USR.

MESiCAP - Modelo dos Elementos do Sistema de Controle de Acessos de Pessoas a Áreas.

Industriais Integrados em Estrutura Empresarial Industrial.

MIT - *Massachusetts Institute of Technology.*

MLAF - Motivo de Liberação de Acesso Forçado.

MoREOSCE - Modelo de Representação da Estrutura Organizacional e dos Sistemas Computacionais da Empresa.

MoROSCE - Modelo de Representação da Organização dos Sistemas Computacionais Empresariais.

MoSiCAP - Modelo de Representação da Estrutura Organizacional e dos Sistemas Computacionais da Empresa com Elementos de Controle de Acessos de Pessoas a Áreas Industriais.

N_CON - Nome do Contratado.

N_EST - Nome do Estagiário.

N_FUN - Nome do Funcionário.

N_VIS - Nome do Visitante.

NMAX_PCAP_S - Número Máximo de Usuários a Serem Inspecionados no PCAP_S.

No_PCAP_S - Nomenclatura do PCAP_S.

No_ROTA - Nomenclatura da Rota R_USR.

NURE - Nome de Usuário de Rede.

OA_SDR - Obrigatoriedade de Autenticação por Senha de Domínio de Rede.

OBID_IA - Obrigatoriedade de Biometria da Impressão Digital com Relação à Identificação e Autenticação.

OBS_IA - Observação ao Interromper o Alarme de PCAP_S.

OI_CId_S - Obrigatoriedade de Identificação por Cartão CId_S.

OpS - Operador de Segurança.

P_CId_S - Protótipo do Cartão de Identificação-SiCAP.

P_ECAP_S - Protótipos dos Equipamentos para Controle de Acessos de Pessoas-SiCAP.

P_ECoFAP - Protótipo do Equipamento para Controle Físico de Acessos de Pessoas.

P_EPP_S - Protótipo de Equipamento de Proteção Pessoal-SiCAP.

P_Le_BID_R - Protótipo do Leitor Biométrico da Impressão Digital por Reflexão.

P_Le_RFID - Protótipo do Leitor RFID.

P_SCNINO - Protótipo dos Sistemas Computacionais Não Industriais do Nível Operacional.

P_SCNT - Protótipo dos Sistemas Computacionais do Nível Tático.

P_SIReNIE – Protótipo do Sistema de Redes Não Industriais Empresarial.

P_SSOA - Protótipo do Subsistema SiCAP-Operacional-Administrativo.

P_SSOP - Protótipo do Subsistema SiCAP-Operacional-PCAP.

P_SSTA - Protótipo do Subsistema SICAP-Tático-Administrativo.

PAPArI - Permissão de Acessos de Pessoas a Áreas Industriais.

PBID_USR - Perfil Biométrico da Impressão Digital do Usuário USR.

PC_SCNINO - Protótipo dos Componentes do SCNINO.

PC_SCNT - Protótipo dos Componentes do SCNT.

PCAP - Ponto de Controle de Acessos de Pessoas.

PCAP_S - Ponto de Controle de Acessos de Pessoas-SiCAP.

PCMSO - Programa de Controle Médico de Saúde Ocupacional.

PCReLoNI - Protocolos de Comunicação das Redes Locais Não Industriais.

PCRInd - Protocolo de Comunicação das Redes Industriais.

PCRRNI - Protocolos de Comunicação das Redes Remotas Industriais.

PCSiReNIE - Protocolos de Comunicação do Sistema de Redes Não Industriais Empresarial.

Pixel - *Picture element*.

PLAF_PCAP_S - Permissão de Liberação de Acesso Forçado no PCAP_S.

PSCA - Pessoas Sujeitas a Controle de Acessos.

QTDI_PCAP_S - Quantidade de Usuários a Serem Inspecionados no PCAP_S.

R_USR - Rota de Usuário USR.

RC_PBID_USR - Referência Cronológica de Cadastro do Perfil Biométrico da Impressão Digital do Usuário USR.

ReLoNI - Redes Locais Não Industriais.

RFID - *Radio Frequency IDentification*.

RHDSP - Recursos Humanos do Departamento de Segurança Patrimonial.

RInd - Redes Industriais.

RRNI - Redes Remotas Não Industriais.

RS232 - *Recommended Standard* 232.

RT_ACESSO - Resultado da Tentativa de Acesso.

RTA_USR - Registro de Tentativa de Acesso de Usuário USR.

SCAPAI - Sistema de Controle de Acessos de Pessoas a Áreas Industriais.

SCCont - Sistema de Controle de Contratados.

SCInNO - Sistemas Computacionais Industriais do Nível Operacional.

SCNE - Sistemas Computacionais do Nível Estratégico.

SCNINO - Sistemas Computacionais Não Industriais do Nível Operacional.

SCNO - Sistemas Computacionais do Nível Operacional.

SCNO_CAPI - Sistemas Computacionais do Nível Operacional Aplicados ao Controle de Acessos de Pessoas a Áreas Industriais.

SCNT - Sistemas Computacionais do Nível Tático.

SCNT_CAPI - Sistemas Computacionais do Nível Tático Aplicados ao Controle de Acessos de Pessoas a Áreas Industriais.

SCVis - Sistema de Controle de Visitas.

SDK - *Software Development Kit*.

SE - Sistemas Especialistas.

SeP - Segurança Patrimonial.

SERV_SGBD_C - Servidor do Sistema Gerenciador de Banco de Dados Central.

SERV_SWSID - Servidor do Sistema de *Web Services* e Importação de Dados.

SGBD - Sistema Gerenciador de Banco de Dados.

SGBD_C - Sistema Gerenciador de Banco de Dados Central.

SIBiCaFi - Sistema com Identificação Biométrica por Características Físicas.

SIBID - Sistema com Identificação por Biometria da Impressão Digital.

SiCAP - Sistema de Controle de Acessos de Pessoas a Áreas Industriais por RFID e Biometria da Impressão Digital.

SIE - Sistemas de Informação Executiva.

SIG - Sistemas de Informações Gerenciais.

SiReNIE - Sistema de Redes Não Industriais Empresarial.

SO_CLIENTE - Sistema Operacional de Cliente.

SO_SERV - Sistema Operacional de Servidor.

SRH - Sistema de Controle de Recursos Humanos.

SSL - *Security Socket Layer.*

SSOA - Subsistema SiCAP-Operacional-Administrativo.

SSOP - Subsistema SiCAP-Operacional-PCAP.

SSTA - Subsistema SiCAP-Tático-Administrativo.

SW_HTTP - Servidor Web HTTP.

SWSID - Sistema de *Web Services* e Importação de Dados.

TCP/IP - *Transfer Control Protocol/Internet Protocol.*

TI_USR - Tipo de Usuário USR.

TOA_EPP_S - Tipo de Obrigatoriedade de Apresentação de Equipamento EPP_S no PCAP_S.

TSF_PCAP_S - Tipo de Sentido de Fluxo no PCAP_S.

UHF - *Ultra High Frequency*.

UML - *Unified Modeling Language*.

USB - *Universal Serial Bus*.

USR – Usuário.

V_PBID_USR - Vencimento do Perfil Biométrico da Impressão Digital do Usuário USR.

Vst – Visitantes.

WORM - *Write Once Read Many*.

SUMÁRIO

1 INTRODUÇÃO

Esta seção é dedicada à apresentação da justificativa, metodologia, objetivos e organização do texto.

1.1 JUSTIFICATIVA E METODOLOGIA

Atualmente, em muitas situações, o controle de acessos de pessoas à áreas restritas em instalações prediais industriais exige a utilização de sistemas automatizados para atender a viabilização operacional relativa às atividades pertinentes ao controle em questão. Esses tipos de sistemas estabelecem um segmento particular cujo mercado está em evolução, havendo uma grande variedade de produtos para as mais diversas aplicações. Como partes dessa evolução estão inclusões de sistemas de identificações por radiofrequência (RFID - *Radio Frequency IDentification*) e biometria, com especial destaque para a biometria da impressão digital, que dispõe de diversos produtos no mercado, com diferentes tecnologias voltadas para esse tipo de identificação (PINHEIRO, 2008; SANTINI, 2008). De forma pertinente a esse contexto, a pesquisa e o desenvolvimento aplicados à integração de recursos de identificações por radiofrequência e biometria da impressão digital, direcionados para o controle de acessos de pessoas a áreas industriais, permite estabelecer um legado que pode oferecer contribuição para o mencionado segmento desses sistemas de controle.

Tendo em vista o exposto e com o intuito de oferecer contribuição para o segmento particular em questão, doravante designado por "segmento de controle de acessos de pessoas a áreas industriais"; desenvolveu-se o presente trabalho cujo escopo da abordagem explora elementos conceituais pertinentes à integração de recursos de identificações por radiofrequência e biometria da impressão digital, em aplicação direcionada para controle de acessos de pessoas a áreas industriais. Essa abordagem tem por base o desenvolvimento do projeto conceitual de um sistema afim, intitulado "Sistema de Controle de Acessos de Pessoas a Áreas Industriais por RFID e Biometria da Impressão Digital" (SiCAP), o qual possui especificidades e finalidades dedicadas aos propósitos deste trabalho.

Para atender o presente trabalho utilizou-se metodologia estabelecida pelas seguintes atividades: obtenção de recursos computacionais necessários para o desenvolvimento do

trabalho; pesquisa bibliográfica realizada em bibliotecas e na *Internet*; desenvolvimento do texto da dissertação por meio de editoração eletrônica; elaboração de programas aplicativos afins; obtenção de protótipos a serem utilizados para a realização de testes práticos.

1.2 OBJETIVOS

Este trabalho tem por principal objetivo abordar elementos conceituais pertinentes à integração de recursos das identificações por radiofrequência e biometria da impressão digital, em aplicação direcionada para o controle de acessos de pessoas a áreas industriais, tendo por base o desenvolvimento do projeto conceitual de um sistema para essa aplicação, sendo a abordagem voltada para o propósito de oferecer contribuição para o segmento particular desses tipos de sistemas, no âmbito daqueles que exigem a utilização de automatização para atender a respectiva viabilização operacional relativa às atividades pertinentes ao controle de acessos em questão.

De forma cooperativa com o exposto estão as especificidades de objetivos, que propõem para o desenvolvimento do projeto conceitual do sistema, um modelo de aplicação que atenda as seguintes diretrizes:

- Identificação por radiofrequência fundamentada em tecnologia com as seguintes características: baixa frequência (LF- *Low Frequency*), voltada para aplicações de identificação a curta distância; leitor fixo; Transponder (Tag) *read-only*, somente de leitura (HID, 2012).
- Identificação por biometria da impressão digital, fundamentada em tecnologia de captura de imagem com utilização de leitura óptica (NITGEN, 2012).
- Utilização de equipamentos para controle físico do acesso de pessoas, cujas previsões de instalação permitam atender fluxos nos sentidos: unidirecional para entrada na área controlada; unidirecional para saída da área controlada; bidirecional para entrada e saída, da área controlada (WOLPAC, 2012; DIMEP, 2012).
- Aplicação de recursos disponíveis por *Web Services* para atendimento das necessidades afins, exigidas para o desenvolvimento do sistema de controle de acessos abordado (ERL, 2005; WCF, 2012).

- Segurança no transporte de dados em redes de comunicação, fundamentada na utilização do protocolo SSL (*Security Socket Layer*), como recurso voltado para a inviolabilidade de dados (RAMOS et al., 2008).
- Estações de trabalho e servidores, constituídos por computadores pessoais do tipo IArch (Intel® *Architecture*, Arquitetura Intel®) ou compatível (TORRES, 2001).
- Utilização de elementos de integração de sistemas direcionados para a abrangência de sistemas computacionais empresariais empregados em indústrias (ROSÁRIO, 2009; SOARES, 1995; SQLSERVER, 2012; TITTEL, 2003).

1.3 ORGANIZAÇÃO DO TEXTO

O texto do presente trabalho possui organização formada por cinco seções. A primeira é dedicada aos seguintes assuntos: justificativa da temática; metodologia para a realização da pesquisa e do desenvolvimento pertinentes; objetivos do trabalho; organização do texto da dissertação. Na segunda apresenta-se a pesquisa bibliográfica referente ao trabalho. A terceira se destina à abordagem do desenvolvimento do projeto conceitual do sistema SiCAP. Na quarta estão descritos os protótipos e os testes práticos referentes ao sistema SiCAP. A quinta trata das conclusões relativas ao trabalho, sendo acrescidas ao respectivo conteúdo as sugestões para trabalhos futuros.

2 PESQUISA BIBLIOGRÁFICA

Nesta seção é apresentada a pesquisa bibliográfica relativa ao desenvolvimento do trabalho, com subseções que envolvem os seguintes assuntos: segurança empresarial; elementos do controle de acessos de pessoas a áreas industriais; identificação por biometria da impressão digital; identificação por radiofrequência; equipamentos para controle físico de acessos de pessoas.

2.1 TÓPICOS REFERENTES À SEGURANÇA EMPRESARIAL

A abordagem desses tópicos tem seus princípios fundamentados em conceitos expostos por D'Angelo e Ferline (2012), explorando-se uma conjuntura na qual o controle de acessos está relacionado à Segurança Empresarial, que por sua vez possui três setores designados por Segurança Patrimonial, Segurança da Informação e Segurança Pessoal, cujas descrições são realizadas em subseções exclusivas, pertencentes a esta.

No âmbito da estrutura organizacional das empresas observou-se que os componentes dos setores da segurança empresarial, frequentemente, têm sua incorporação estabelecida por meio da área administrativa, em estruturas que podem incluir, isoladamente ou em conjunto, elementos como departamentos, divisões e subdivisões. Entretanto, conforme exposto por D'Angelo e Ferline (2012), a gestão da segurança empresarial requer a interação entre os componentes dos setores mencionados anteriormente, envolvendo todas as áreas da empresa relacionadas com a segurança, formando um todo que contém tanto os responsáveis pelos sistemas de segurança quanto os seus respectivos usuários.

2.1.1 Segurança Patrimonial

O setor da Segurança Patrimonial é direcionado à proteção do patrimônio material de uma empresa, visando evitar: acessos não autorizados as suas instalações, roubos, furtos, ameaças e outros tipos de sinistros. Os profissionais responsáveis pela Segurança Patrimonial deverão estudar a implantação de estratégias de defesa adequadas, de forma a atender as

necessidades da empresa (CARVALHO, 1982). Assim sendo, controlar o acesso das pessoas nas unidades industriais é uma das competências da segurança patrimonial, cujos recursos deverão permitir somente às pessoas autorizadas, acessar os perímetros sob esse tipo de segurança. Pertence ao âmbito da segurança patrimonial o provimento de recursos para bloqueios físicos (paredes, tetos, portas, cercas etc.) e de controle de acessos, adequados às respectivas funções.

De forma associada com o sistema de controle de acessos de pessoas, porém visando aumento da segurança patrimonial em instalações prediais, recomenda-se a existência de um "Serviço de Vigilância" cuja composição deverá dispor de recursos afins, dentre os quais estão vigilantes e os sistemas de monitoramento que permitem visualização, por meio de CFTV (Circuito Fechado de Televisão), de toda a área delimitada pelos perímetros controlados, bem como, a detecção de invasão por meio de sinalização de sensores adequados a essa finalidade. Como parte da infraestrutura predial relacionada a esses recursos está o centro de controle operacional de vigilância, que abrigará a central de monitoramento de imagens e alarmes, bem como, os profissionais responsáveis pelas respectivas operações relativas a esses sistemas.

No que se refere aos procedimentos para implementação do controle de acessos de pessoas e da vigilância de perímetros, foi observado na bibliografia pesquisada que há casos de empresas que podem adotar procedimentos próprios baseados em determinações internas e nas leis vigentes no país em que estão instaladas. Entretanto, há casos de empresas que devem seguir procedimentos estabelecidos por órgãos controladores, sendo exemplos dessas as que atuam no setor nuclear brasileiro, estando sujeitas às determinações da Comissão Nacional de Energia Nuclear (CNEN), que é o órgão fiscalizador de todas as atividades que envolvem material radioativo em solo nacional. Uma norma para esse tipo de empresa é a NE 2.01, que estabelece os princípios gerais e os requisitos básicos exigidos, enfatizando que proteção física é o conjunto de medidas destinadas a evitar atos de sabotagem contra materiais, instalações e equipamentos (NE2.01, 2011).

2.1.2 Segurança da Informação

Este setor visa garantir a segurança das informações de propriedade da empresa, abrangendo as físicas e as dispostas em meios computacionais, provendo os recursos

adequados para evitar ações criminosas e combater ameaças, como: acessos não permitidos as suas informações, cópias não autorizadas, espionagem, violações e fraudes (PINHEIRO, 2008). Com base na norma ISO/IEC 17799:2005 (ISO, 2005), observa-se que as informações em processos, sistemas e redes de comunicação de dados, são importantes ativos para os negócios de uma empresa, cuja relevância justifica a realização de ações para definir, alcançar, manter e melhorar a segurança da informação. Para exemplos de informações físicas podem ser citadas as seguintes: documentos impressos, plantas, esquemas, protótipos etc. No que diz respeito a exemplos das informações dispostas em meios computacionais citam-se: documentos eletrônicos, programas de computador, informações em sistemas de banco de dados, arquivos eletrônicos com códigos fonte de programas etc.

A segurança da informação, aplicada no caso das informações dispostas em meios computacionais, possui como característica a necessidade de manter os seguintes critérios para utilização, armazenamento, processamento e recuperação da informação (PINHEIRO, 2008):

- Confidencialidade: Garantir que a informação será acessada somente por pessoas e sistemas autorizados.
- Integridade: Garantir a preservação da informação.
- Disponibilidade: Garantir que os usuários autorizados tenham acesso à informação sempre que necessário.

O estabelecimento dos mencionados critérios está relacionado à existência de serviços de segurança, que podem ser abordados como características apresentadas por um sistema com o objetivo de atender a política de segurança adotada, em cujos preceitos podem estar documentos que incluem a apresentação das ações permitidas e não permitidas, para a operação do sistema. Nos itens a seguir, são expostos serviços que objetivam garantir a segurança da informação (SILVA et al., 2008):

1. Identificação: Declaração de identidade do usuário para com o sistema, apresentando os elementos requeridos para essa declaração.
2. Autenticação: Aplicação de recursos para a verificação da identidade do usuário, visando determinar se ele é quem declarou ser, por meio de análises nas evidências apresentadas para a determinação da sua identidade.
3. Autorização: Aplicação de recursos para estabelecimento das permissões definidas para o usuário, que garante acessar o que é lhe permitido, sendo impedido de acessar o que não lhe é permitido. Essa restrição de acessos pode incluir

informações, perímetros, utilização de programas de computador, arquivos digitais, periféricos de computador etc.

4. Privacidade: Aplicação de elementos visando garantir que a informação confidencial não seja acessada por quem não tem direito a esse acesso. A informação pode estar armazenada em uma base de dados, trafegar pela rede de comunicação de dados e ser exibida em interface de sistemas computacionais. O serviço de privacidade tem por obrigação resguardar as informações, sendo frequente a utilização de criptografia para atender essa obrigação. Os dados podem ser criptografados para armazenamento e transporte. No caso do armazenamento, há técnicas de criptografia baseadas em algoritmos proprietários ou com utilização de chaves criptográficas. No caso do transporte existem protocolos específicos como o SSL (*Security Socked Layer*), que utilizam o conceito de chave criptográfica pública e privada, para garantir que as informações não sejam indevidamente decifradas enquanto trafegam pelos meios de comunicação que as transportam.
5. Integridade: Aplicação de elementos visando garantir que a informação não será modificada, duplicada, inserida, reordenada e processada, de forma indevida.
6. Não Repúdio: Aplicação de recursos que visam garantir ao usuário o acesso às informações para as quais tem permissão, após liberação por meio da utilização de recursos de identificação, autenticação e autorização.
7. Disponibilidade: Aplicação de elementos visando garantir que o sistema, seus dados e recursos, estarão disponíveis para os usuários identificados, autenticados e autorizados, sempre que necessário, com o mínimo de interrupção possível, sendo que, a eventualidade dessa interrupção não traga prejuízos para as operações do sistema. Dentre exemplos desses recursos estão sistemas computacionais com suporte de tecnologia *hot standby* e equipamentos para suprimento ininterrupto de energia elétrica, que podem incluir *no-breaks*, grupos geradores etc.
8. Registros para Auditoria: É o armazenamento das informações sobre as utilizações dos recursos do sistema realizadas pelos usuários, para as finalidades de auditoria.

De forma relacionada com os serviços pertinentes aos itens “1” e “2”, estão os processos de identificação e autenticação. O “Processo de Identificação” pode ser abordado como aquele no qual o usuário se apresenta ao sistema declarando sua identidade por meio da entrada de informações que o discrimina dentre todos aqueles que compõem o universo de

usuários, como no caso de chaves primárias estabelecidas por: nome de usuário, código no Cadastro de Pessoas Físicas (CPF), código de matrícula na empresa, código em transponder de RFID etc. (SILVA et al., 2008). O "Processo de Autenticação" pode ser abordado como aquele que verifica a identidade do usuário que se apresentou no processo de identificação, sendo essa verificação realizada por meio de análises das credenciais (exemplo: senha, impressão digital etc.) dispostas por esse usuário, resultando em validação ou invalidação da identidade em questão (SILVA et al., 2008). Na hipótese de validação da identidade, será estabelecido o estado de "usuário identificado", entretanto, na hipótese contrária será estabelecido o estado de "usuário não identificado". Para um usuário, as credenciais autênticas são evidências apresentadas com o propósito de estabelecer o estado de usuário identificado (SILVA et al., 2008).

Os processos de identificação e autenticação estabelecem as etapas de uma sequência de identificação do indivíduo, que permite discriminar sobre a concessão ou negação de acessos para tudo aquilo previsto no respectivo serviço de autorização, que somente é levado a efeito após o estabelecimento do estado de usuário identificado. Nesse contexto, o processo de identificação permite ao individuo declarar sua identidade, tendo o processo de autenticação a finalidade de validar ou invalidar essa declaração, sendo concedidos ou negados os acessos previstos no respectivo serviço de autorização, somente após a finalização do processo de autenticação.

Sob um panorama geral, as tecnologias atualmente utilizadas nos processos pertencentes a sequência de identificação do indivíduo, têm por base três paradigmas (PINHEIRO, 2008; SILVA et al., 2008; SOUZA, 2010): "algo que você tem**"** (exemplo: cartão de acesso); "algo que você sabe**"** (exemplo: senha de acesso) e "algo que você é**"** (exemplo: impressão digital). Tendo em vista que as tecnologias pertinentes a um determinado paradigma, isoladamente, não permitem garantir a isenção de fraudes, recomenda-se a união de tecnologias relacionadas aos três diferentes paradigmas, para aplicação nos processos pertencentes à sequência de identificação do individuo, como forma de diminuir a probabilidade de ocorrência de fraudes e aumentar a segurança (PINHEIRO, 2008; SILVA et al., 2008; SOUZA, 2010).

2.1.3 Segurança de Pessoal

O setor da Segurança Pessoal implementa e mantém recursos com o objetivo de garantir a segurança no trabalho, por meio de medidas preventivas, treinamentos, fornecimento de equipamentos de proteção e cuidados para assegurar a utilização desses equipamentos. Esse setor também atua no Programa de Controle Médico de Saúde Ocupacional (PCMSO), que envolve exames periódicos e identificação de riscos relativos às atividades profissionais, preparando de forma adequada os indivíduos para exercerem suas funções e realizando acompanhamento para detecção de possíveis danos provocados pelas atividades em longo prazo (CARVALHO, 1982).

2.1.4 Exemplos de interações entre os setores de segurança

Relativamente às interações entre os setores das seguranças patrimonial, da informação e pessoal, citam-se os seguintes exemplos de situações:

- Os recursos do setor de segurança patrimonial contribuem com o setor de segurança da informação, evitando os acessos não autorizados às áreas de instalações prediais da empresa cujo ambiente contém informações físicas. Esses recursos atuam no sentido de impedir roubos, furtos e outras ações criminosas referentes a esse tipo de informação, sendo da mesma forma protegidos os equipamentos que as armazenam e os circuitos de comunicação pelos quais são transportadas. Os recursos em questão também contribuem com o setor de segurança pessoal, impedindo que pessoas não habilitadas e/ou não treinadas, adentrem em áreas que oferecem riscos ocupacionais, protegendo a vida e evitando perdas referentes a bens materiais. Ainda no que tange a segurança pessoal, evita-se que pessoas com restrições médicas acessem áreas não permitidas para as condições em que se encontram.
- Os recursos do setor de segurança da informação permitem manter e dispor informações confiáveis a serem utilizadas nos processos de identificação, autenticação e autorização de usuários, realizados pelo setor de segurança patrimonial no controle de acessos de pessoas as áreas de instalações da empresa. Esse controle de acessos também se reflete em benefícios para o setor de segurança

pessoal e para o próprio setor de segurança da informação, haja vista as contribuições descritas anteriormente.

- Os recursos do setor de segurança pessoal permitem definir se uma pessoa possui treinamento relativo à ações ocupacionais, para acessar áreas da empresa, sendo as informações decorrentes dessa definição utilizadas pelo setor de segurança patrimonial para impedir o acesso em questão. Esse impedimento evita os riscos ocupacionais descritos anteriormente, protegendo o patrimônio contra danos causados por procedimentos operacionais inadequados, bem como, proteger as pessoas de riscos à vida, sendo favorecidos os setores de segurança patrimonial, da informação e o próprio setor de segurança pessoal.

2.2 ABORDAGEM SOBRE ELEMENTOS DO CONTROLE DE ACESSOS DE PESSOAS A ÁREAS INDUSTRIAIS

2.2.1 Aspectos preliminares relacionados ao controle de acessos de pessoas no âmbito da indústria

Atualmente, as aplicações do controle de acessos de pessoas no âmbito da indústria, estão presentes em segmentos relacionados aos três setores da segurança empresarial descritos anteriormente, ou seja, patrimonial, da informação e pessoal. Nesses segmentos as aplicações, normalmente, são direcionadas a proporcionar administração, auditoria, registro, permissão ou impedimento, pertinentes aos acessos controlados pelos setores em questão, sendo buscadas a prevenção e a proteção contra riscos à vida e ao patrimônio (SOUZA, 2010). Em afinidade com o exposto, está o controle de acessos de pessoas a áreas industriais, em cujo tipo de controle podem ser destacadas duas características operacionais básicas: verificação de autenticidade das pessoas; verificação dos atributos de permissão de acessos que cada pessoa possui com relação a área que pretende acessar. Relativamente a essas características para o mencionado tipo de controle de acessos, podem ser citados como objetivos principais: verificar se a pessoa é realmente quem diz ser; negar acesso das pessoas as áreas em instalações prediais industriais, quando suas permissões decorrem em impedimento para esse acesso; permitir o acesso das pessoas as áreas em instalações prediais industriais, quando suas permissões não decorrem em impedimento para esse acesso (SOUZA, 2010).

No que se refere à permissão definida para cada pessoa, os respectivos atributos podem decorrer em restrições de acesso que combinam aos locais físicos outros fatores, como os relacionados a horários, afastamentos por ordem médica, ordens judiciais, tempo de exposição à substâncias específicas, número máximo de indivíduos, exigência de habilitação específica, exigência de treinamento específico etc.

Nessa conjuntura, as áreas sob controle de acessos pertencem aos chamados "perímetros controlados", que podem ser estabelecidos por meio de barreiras físicas ou virtuais, com condições para permitir os acessos as regiões que delimitam (SOUZA, 2010). De maneira geral, os perímetros controlados podem ser classificados como externos ou internos. Os externos delimitam o total da região a ser controlada, que por sua vez, internamente, pode possuir outros tipos de perímetros chamados de internos. Esses últimos podem possuir outros perímetros dentro dos limites de sua região, e assim, sucessivamente, podem ocorrer perímetros dentro de perímetros, entretanto, todos esses são designados por perímetros internos (SOUZA, 2010). No presente trabalho, a área sob os limites do perímetro externo será designada por "Área Industrial Vigiada", a qual inclui, além das áreas dos perímetros internos (que podem receber designações específicas), a chamada "Área Comum" existente entre perímetros internos e o externo. Entretanto, do ponto de vista conceitual, pode ser considerada "Área Industrial de Segurança" aquela que estiver sob os limites de um perímetro controlado qualquer, seja ele interno ou externo.

Os perímetros controlados delimitam regiões e podem possuir locais específicos para o controle de acessos de pessoas a essas regiões, com condições para entrada e saída. Esses locais específicos são designados, neste trabalho, por "Ponto de Controle de Acessos de Pessoas" (PCAP). Nos PCAP são instalados os equipamentos destinados ao controle de acessos de pessoas, dentre os quais podem ser citados: equipamentos para controle físico de acessos de pessoas (exemplos: catracas, portas giratórias e torniquetes); computadores; leitores RFID; leitores biométricos da impressão digital; vídeo porteiro eletrônico. Na Figura 2.1, apresentam-se exemplos dos mencionados equipamentos destinados ao controle de acessos de pessoas.

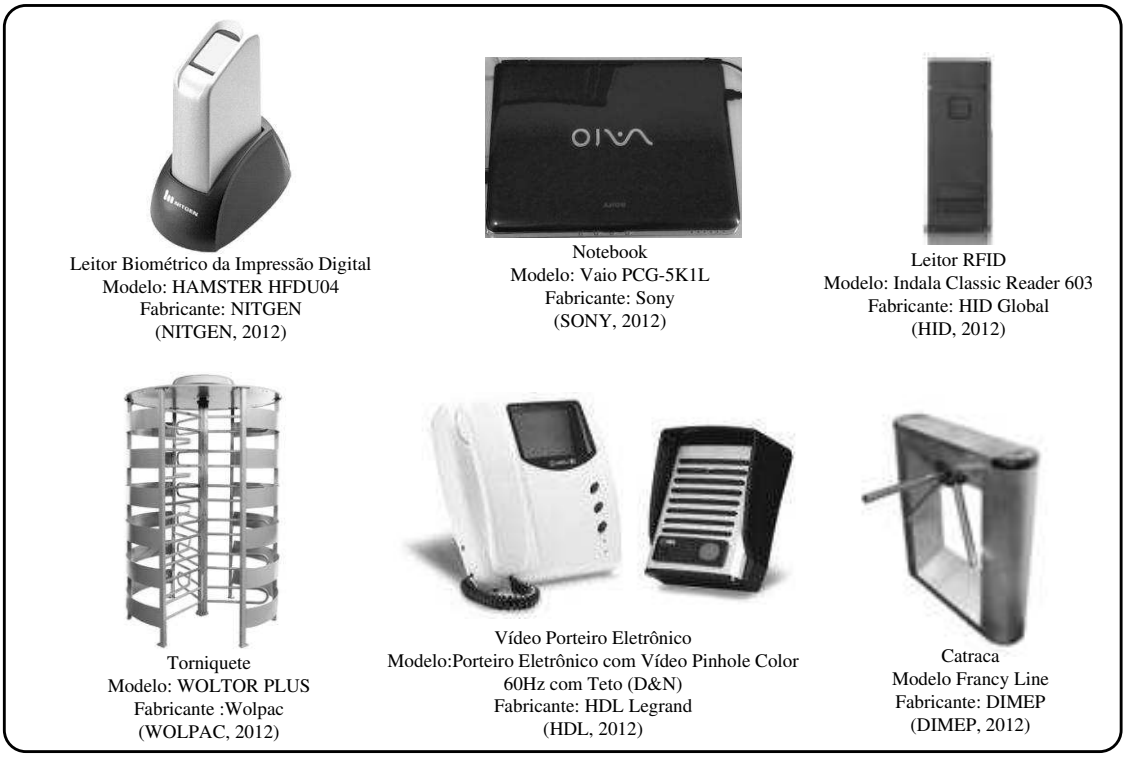

Figura 2.1 - Exemplos de equipamentos destinados para o controle de acessos de pessoas

Na Figura 2.2, apresenta-se esquemático representativo da organização de perímetros externo e internos, com respectivos PCAP, em unidade industrial confrontante com área pública, que possui áreas industriais de segurança referentes a instalações administrativas, da produção e a chamada área comum, existente entre perímetros internos e o externo. De forma a permitir o funcionamento dos equipamentos instalados no PCAP, observou-se que esses pontos de controle devem possuir infraestrutura na qual exista: pontos para fornecimento de energia elétrica; pontos para conexão as redes de comunicação de dados; equipamentos para fornecimento ininterrupto de energia elétrica. Pelo fato do controle de acessos de veículos ("veicular") não estar no escopo deste de trabalho, não se incluiu no esquemático que contém a unidade industrial, a representação referente às áreas de estacionamento de veículos.

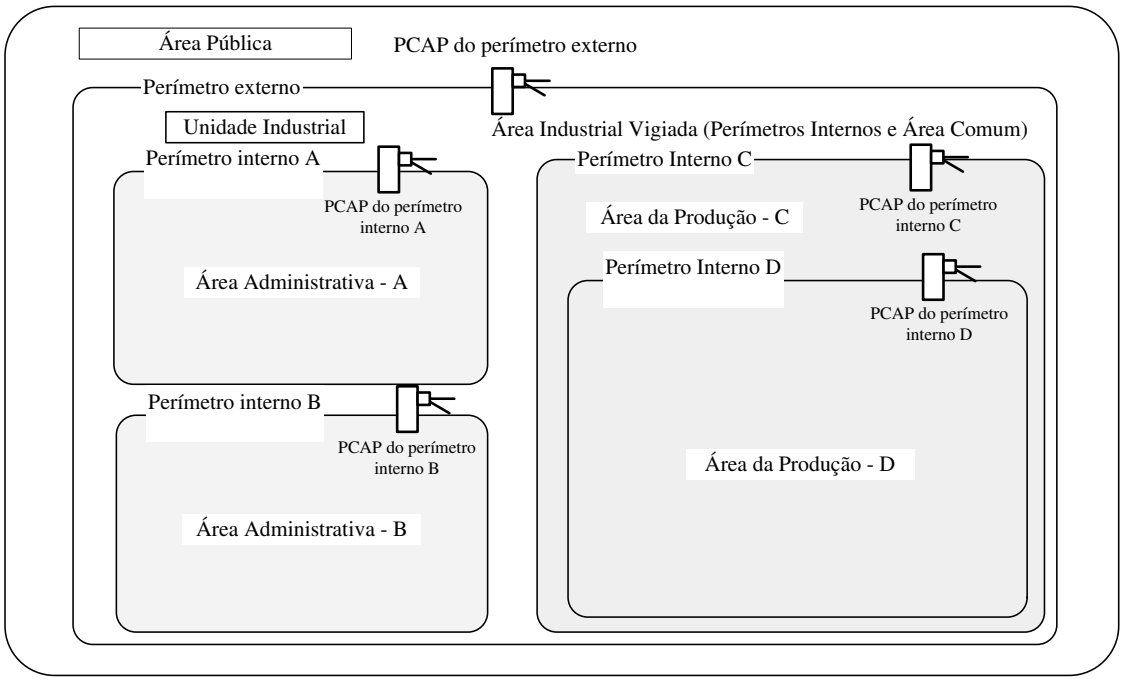

Figura 2.2 - Esquemático representativo da organização de perímetros internos e externo

Conforme informado na subseção "1.1", no segmento de controle de acessos de pessoas a áreas industriais, há a exigência de utilização de sistema automatizado para atender a viabilização operacional relativa às atividades pertinentes ao tipo de controle em questão. Relativamente ao exposto, porém, no que tange referência normativa pertinente a esse tipo de sistema, cita-se a norma ISO/IEC 15408:2005 (ISO, 2005), que trata de assuntos afins, incluindo-se abordagem sobre funcionalidades pertinentes ao ponto de controle de acessos de pessoas (PCAP). Na Figura 2.3 é apresentado esquemático fundamentado nessa norma, com adaptação para o setor empresarial industrial, que expõe a organização de elementos referentes ao PCAP e os respectivos sentidos de fluxo das informações entre esses elementos.

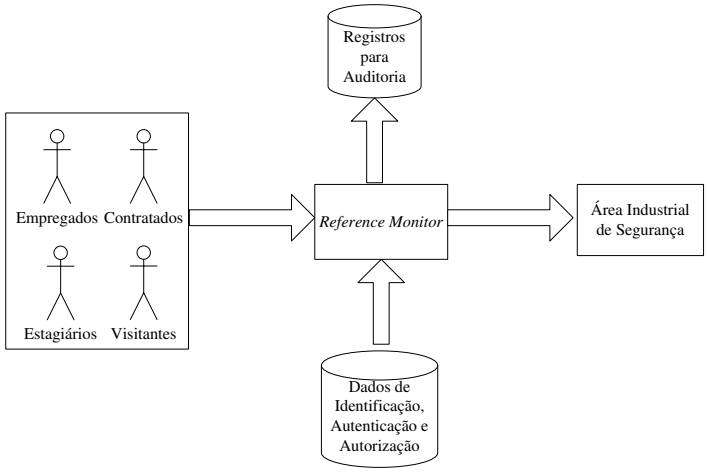

Figura 2.3 - Elementos referentes ao PCAP e sentidos de fluxos de informações (ISO, 2005)

Nessa organização pode ser observada a representação das pessoas sujeitas ao controle de acessos, que estão classificadas em: “Funcionários”, “Contratados”, “Estagiários” e “Visitantes”. Os “Dados de Identificação, Autenticação e Autorização”, estão em meios computacionais e serão utilizados nos processos de identificação, autenticação e autorização, das pessoas sujeitas ao controle de acessos, que deverão estar previamente cadastradas no sistema. Os “Registros para Auditoria” formam um conjunto de dados em meios computacionais que serão utilizados para fins de auditoria, envolvendo as tentativas de acessos realizadas. A “Área Industrial de Segurança” pertence a um perímetro controlado, com respectivos PCAP. O “*Reference Monitor”* é um recurso computacional central, que implementa as funcionalidades de interligação com os demais elementos, tendo por objetivo principal a execução de procedimentos que decorrerão na permissão ou impedimento do acesso da pessoa que pretende transitar pelo PCAP.

Em cada tentativa de acesso, o “*Reference Monitor*”, em suas funções centralizadoras, coleta as informações de identificação e autenticação da pessoa, busca os dados de autorização referentes à mesma, realiza os processos de identificação e autenticação, verificando se ela é quem diz ser e, se possui autorização para acessar a “Área Industrial de Segurança”, sendo definido se a tentativa de acesso finalizou em autorização ou impedimento. Caso a tentativa tenha finalizado em impedimento, o “*Reference Monitor*” atuará no PCAP impedindo o acesso em questão, porém, sendo os dados dessa tentativa armazenados em “Registros para Auditoria”. Caso a tentativa tenha finalizado em permissão, o “*Reference Monitor*” atuará no PCAP permitindo o acesso em questão e armazenando os dados dessa tentativa nos “Registros para Auditoria”.

2.2.2 Modelo de Representação da Estrutura Organizacional das Empresas e dos Sistemas Computacionais Associados

Para a representação da estrutura organizacional das empresas e dos sistemas computacionais associados, será utilizado um modelo proposto por Aguiar (2011), intitulado “Modelo de Representação da Estrutura Organizacional e dos Sistemas Computacionais da Empresa” (MoREOSCE), que visa abranger a empresas e os respectivos sistemas computacionais de uma maneira geral, sintetizando os elementos de interesse de forma a permitir adequações para se chegar a outros modelos de representação. A organização desse

modelo é apresentada na Figura 2.4, expondo os respectivos elementos pertencentes à sua constituição. O modelo em questão será aproveitado como base para o desenvolvimento de outro, que estende a aplicação do primeiro para atender as necessidades deste trabalho.

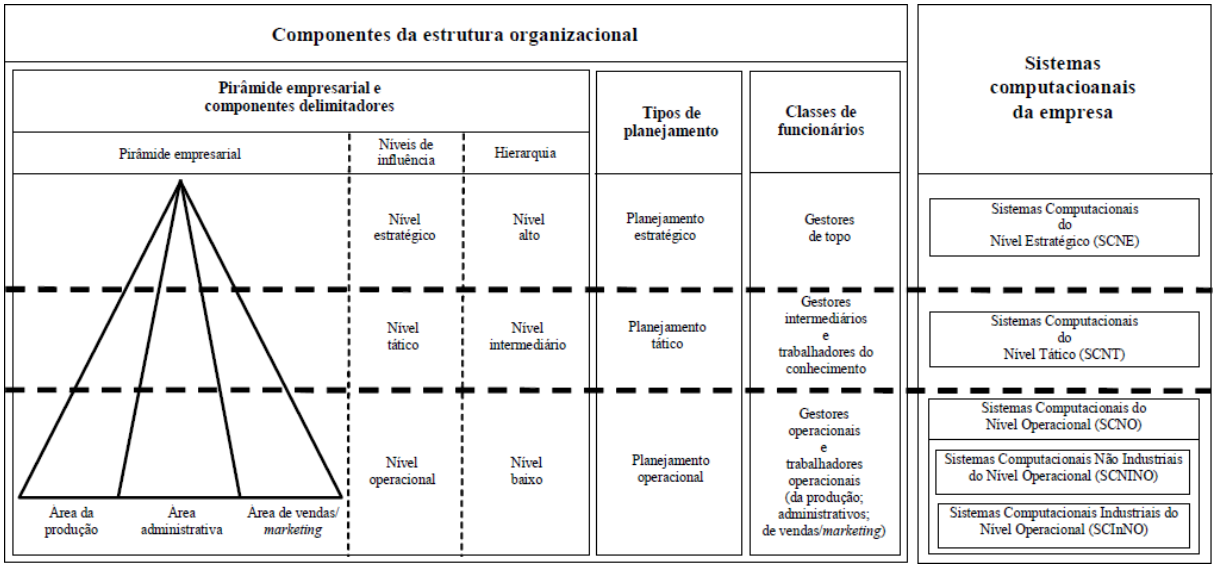

Figura 2.4 - Elementos do MoREOSCE (AGUIAR, 2011)

Na organização do MoREOSCE há duas regiões, sendo uma dedicada aos "Componentes da estrutura organizacional" e outra dedicada aos "Sistemas computacionais da empresa". Conforme abordagem sobre o MoREOSCE, os componentes da estrutura organizacional são fundamentados em conceitos de hierarquia de autoridades relacionada a níveis de influência, sendo que as delimitações existentes no modelo são caracterizadas por representação que associa componentes, condicionantes e níveis de influência. Ainda em conformidade com a mencionada abordagem, porém, no que diz respeito aos sistemas computacionais da empresa, o MoREOSCE inclui os tipos de sistemas de informação intraorganizacional com abrangência: à áreas funcionais específicas; a toda amplidão da empresa; à apoio de funcionários (AGUIAR, 2011).

Aguiar (2011), ao propor o MoREOSCE indicou que os sistemas computacionais de seu modelo representam todos os utilizados nas empresas e que esses devem possuir os recursos necessários para atender as demandas de aplicações no âmbito das empresas. Na Tabela 2.1 é apresentada descrição sucinta das classes e subclasses dos sistemas computacionais que constam dentre os elementos do MoREOSCE (AGUIAR, 2011).

Tabela 2.1 - Classificação dos sistemas computacionais do MoREOSCE (AGUIAR, 2011)

Classes e subclasses dos Sistemas Computacionais do MoREOSCE	
Designação	**Descrição**
Sistemas Computacionais do Nível Estratégico (SCNE)	Sistemas computacionais utilizados por gestores de topo em atividades que incluem o planejamento estratégico. Como exemplos dessa classe estão os Sistemas de Informação Executiva (SIE), cujos recursos permitem acessos a informações oportunas e estruturadas, voltadas para os citados gestores.
Sistemas Computacionais do Nível Tático (SCNT)	Sistemas computacionais utilizados por gestores intermediários e trabalhadores do conhecimento, em atividades que incluem o planejamento tático. Como exemplos dessa classe estão os Sistemas de Informações Gerenciais (SIG) e os Sistemas Especialistas (SE). Os SIG dispõem de recursos para a geração de relatórios específicos voltados para gestores intermediários. Os SE requerem habilidades de raciocínio e conhecimento num determinado domínio, sendo voltado para trabalhadores do conhecimento.
Sistemas Computacionais do Nível Operacional (SCNO)	Sistemas computacionais utilizados por gestores operacionais e trabalhadores operacionais da produção, administrativos e de vendas/*marketing*. Esta classe de sistemas computacionais divide-se em duas subclasses: Sistemas Computacionais Não Industriais do Nível Operacional (SCNINO) e Sistemas Computacionais Industriais do Nível Operacional (SCInNO). Essas subclasses são apresentadas nesta tabela.
Sistemas Computacionais Não Industriais do Nível Operacional (SCNINO)	Sistemas computacionais utilizados por gestores operacionais e trabalhadores operacionais, das áreas administrativas e de vendas/*marketing*, em atividades que incluem o planejamento operacional referente a essas áreas. Como exemplos dessa subclasse estão os sistemas de: folha de pagamento, controle de acessos (incluindo o de pessoas), finanças, contabilidade, vendas, *marketing* e recursos humanos.
Sistemas Computacionais Industriais do Nível Operacional (SCInNO).	Sistemas computacionais utilizados por gestores operacionais e trabalhadores operacionais, da área da produção, em atividades que incluem o planejamento operacional referente a essa área. Como exemplos dessa subclasse estão os sistemas de: controle de produção e automação industrial.

De forma relacionada ao MoREOSCE, Aguiar (2011) propôs um modelo geral para representação da organização dos sistemas computacionais empresariais, sendo esse designado por "Modelo de Representação da Organização dos Sistemas Computacionais Empresariais" (MoROSCE), cujos elementos estão expostos na Figura 2.5. Analogamente ao ocorrido com o MoREOSCE, o MoROSCE será aproveitado como base para o desenvolvimento de outro modelo, que estende a sua aplicação para atender as necessidades deste trabalho.

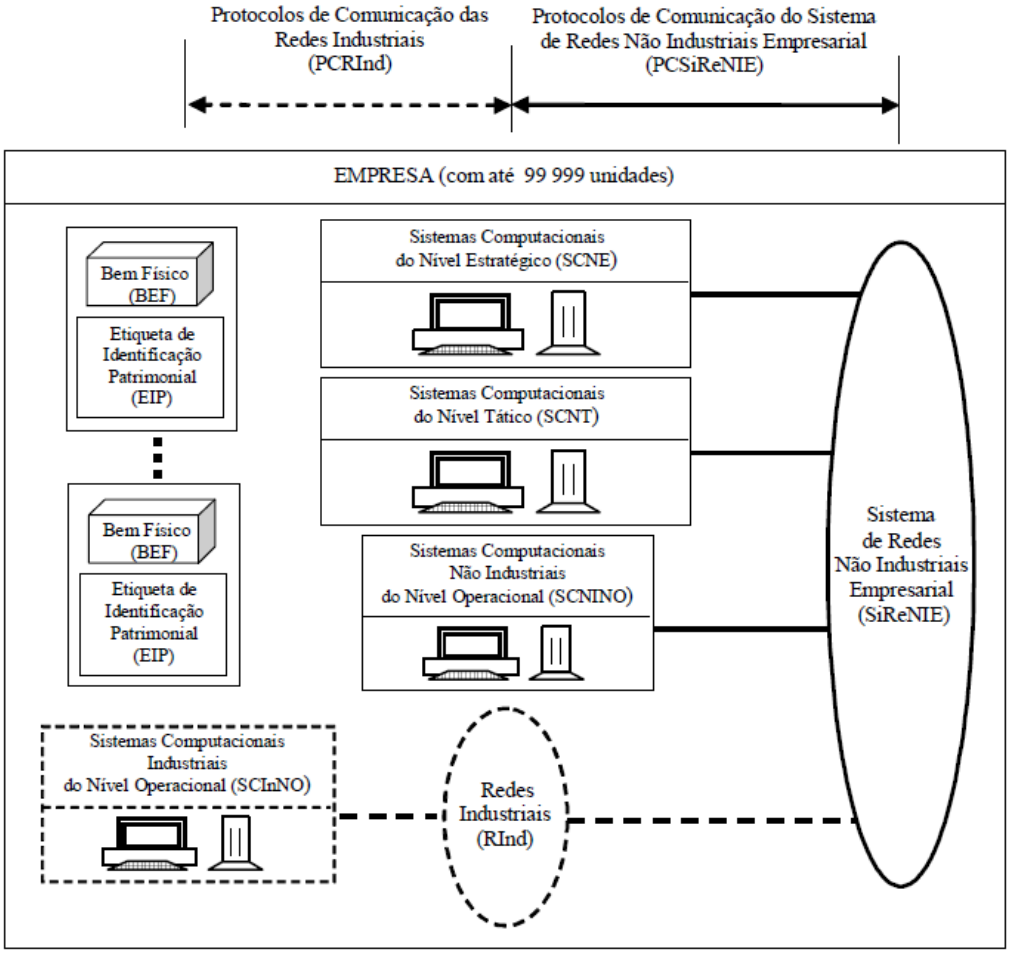

Figura 2.5 - Elementos do MoROSCE (AGUIAR, 2011)

O MoROSCE prevê empresas com até 99.999 unidades, que podem estar distribuídas pelo globo terrestre. Em seus elementos, além dos sistemas computacionais do MoREOSCE, são incluídos: Sistema de Redes Não Industriais Empresarial (SiReNIE); Protocolos de Comunicação do Sistema de Redes Não Industriais Empresarial (PCSiReNIE); Redes Industriais (RInd); Protocolo de Comunicação das Redes Industriais (PCRInd); Bem Físico (BEF); Etiqueta de Identificação Patrimonial (EIP).

O sistema de redes SiReNIE permite a comunicação de dados entre todos os sistemas computacionais da empresa (SCNE, SCNT, SCNINO e SCInNO), abrangendo redes de comunicação não industriais de curta e longa distância, sob as condições dos protocolos PCSiReNIE. Entretanto, o MoROSCE visa abranger as empresas de uma maneira geral sendo inclusas as redes industriais RInd e os protocolos PCRInd, que poderão não existir em empresas ou em unidades de empresas, que não necessitem ou não dispõem desses recursos, como é comum no caso daquelas que atuam exclusivamente no comércio varejista. Da mesma forma há empresas ou unidades de empresas que não necessitam dos sistemas computacionais industriais SCInNO, por suas atividades não exigirem esses tipos de sistemas computacionais.

Em função dessas considerações, as redes industriais RInd, os protocolos PCRInd e os sistemas computacionais industriais SCInNO, têm a ocorrência de sua representação no MoROSCE de forma tracejada, representado a possibilidade de suas inexistências em determinadas situações. O Bem Físico (BEF) e a Etiqueta de Identificação Patrimonial (EIP) são elementos envolvidos nos sistemas computacionais descritos anteriormente, sendo aplicados na dissertação apresentada por Aguiar (2011), porém, não utilizados neste trabalho.

Pelo fato do modelo MoROSCE prever empresas com até 99.999 unidades, Aguiar (2011) apresentou figura com detalhamentos desse modelo, relativos a empresas com mais de uma unidade, a qual é exposta na Figura 2.6.

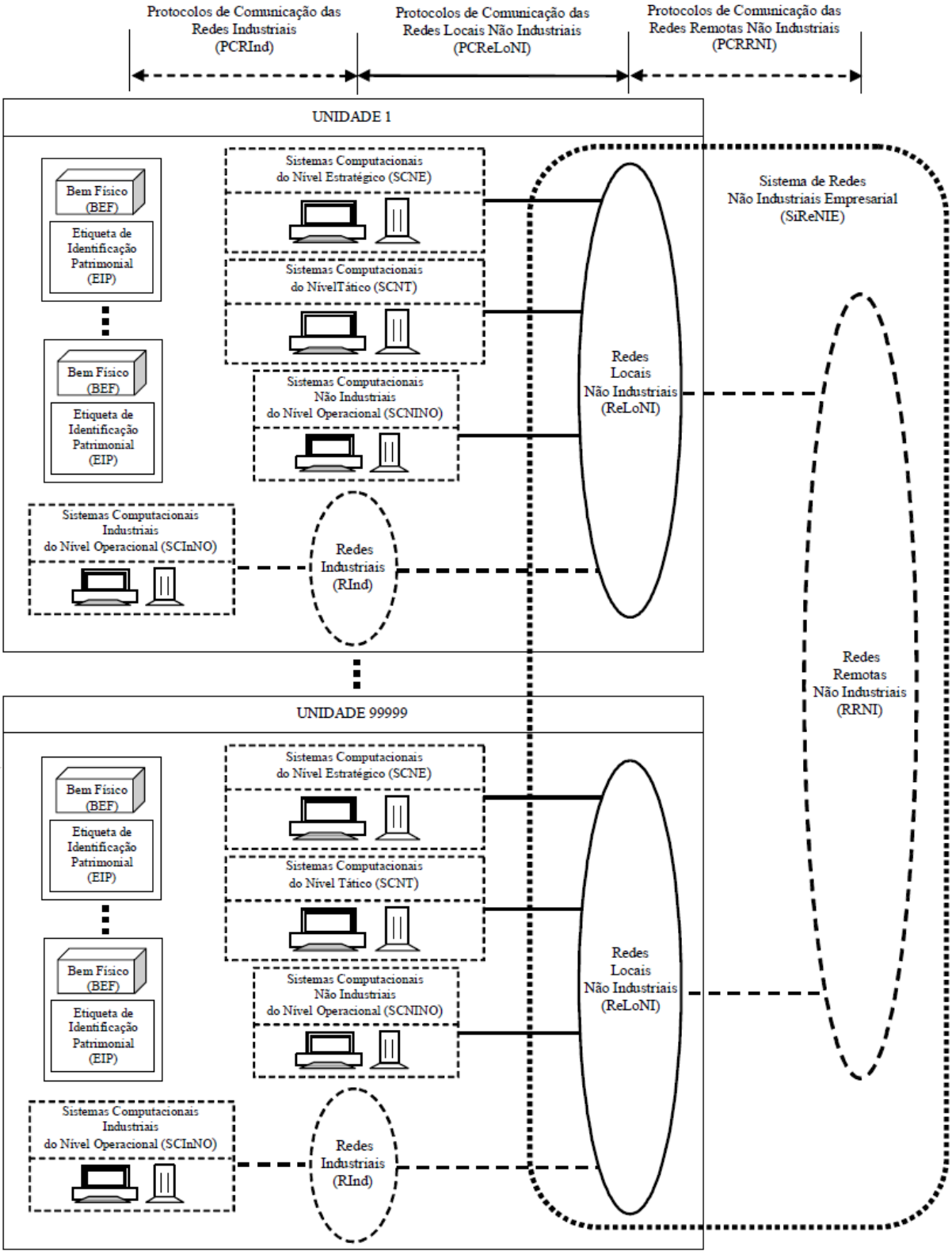

Figura 2.6 - Detalhamentos do MoROSCE para múltiplas unidades (AGUIAR, 2011)

Neste detalhamento pode ser observada a composição do sistema de redes SiReNIE, formada pelas Redes Locais Não Industriais (ReLoNI) e as Redes Remotas Não Industriais (RRNI), as quais estão, respectivamente, sob os protocolos PCReLoNI (Protocolos de Comunicação das Redes Locais Não Industriais) e PCRRNI (Protocolos de Comunicação das

Redes Remotas Não Industriais). Esses detalhamentos, juntamente com os demais apresentados, permitem observar os elementos da estrutura computacional que podem ser aplicados em cada unidade da empresa.

2.2.3 Elementos do controle de acessos de pessoas a áreas industriais em modelos de estruturas empresariais

2.2.3.1 Modelo de representação da estrutura organizacional e dos sistemas computacionais da empresa com elementos de controle de acessos de pessoas a áreas industriais

A partir do MoREOSCE desenvolveu-se um modelo para representação de elementos do controle de acessos de pessoas a áreas industriais em estrutura organizacional das empresas e sistemas computacionais associados, o qual foi denominado de "Modelo de Representação da Estrutura Organizacional e dos Sistemas Computacionais da Empresa com Elementos de Controle de Acessos de Pessoas a Áreas Industriais" (MoSiCAP). Esse modelo é voltado para o atendimento das necessidades deste trabalho, entretanto, poderá ser estendido para outros modelos, desde que, seja possível realizar as respectivas adequações. Na Figura 2.7, é apresentada a organização de seus elementos.

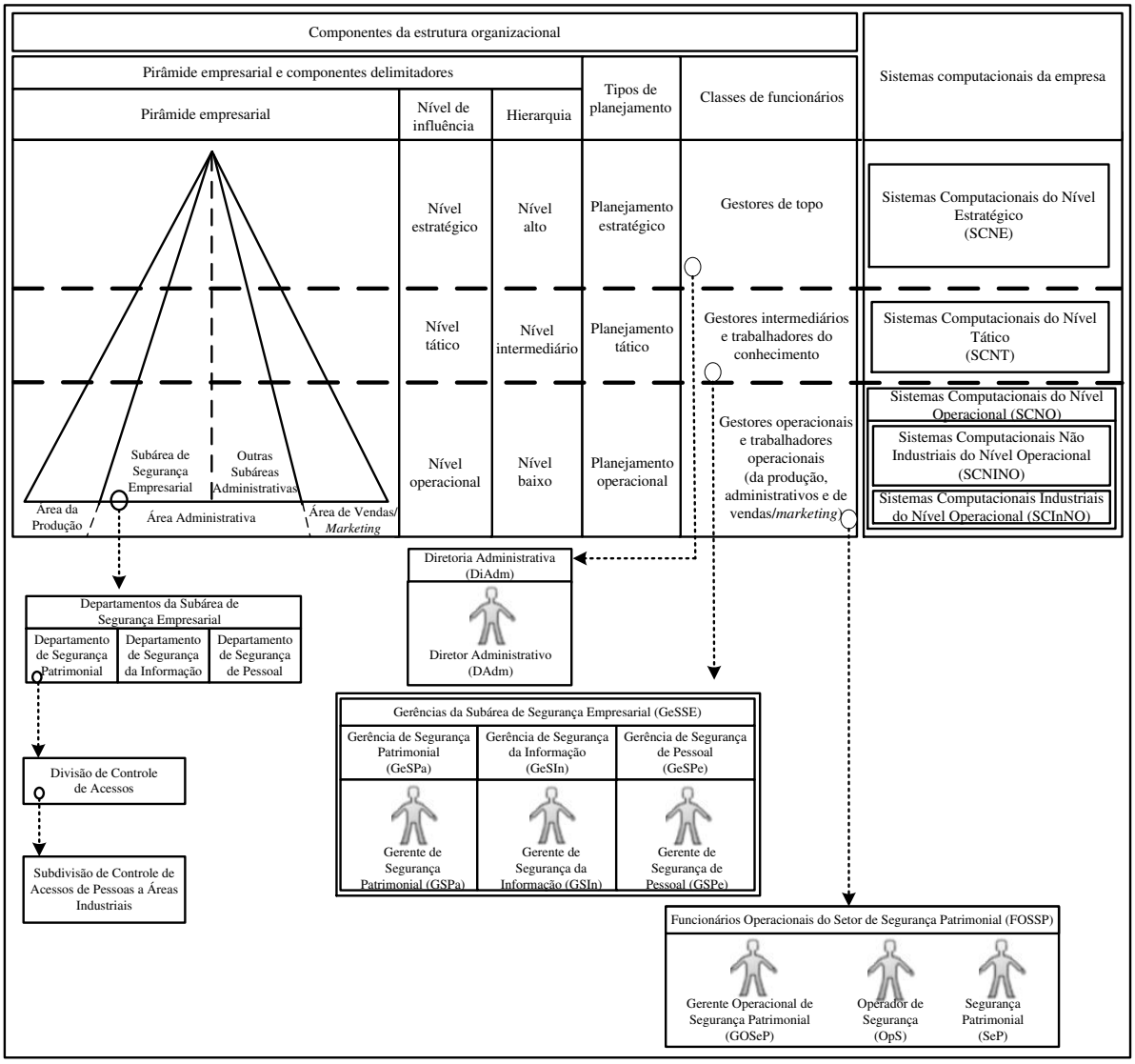

Figura 2.7 - Modelo de Representação MoSiCAP

Como resultado do desenvolvimento do MoSiCAP ocorreram modificações em relação ao MoREOSCE, havendo a inclusão de novos elementos. As modificações são comentadas nos itens a seguir, sendo os novos elementos apresentados em subseções pertencentes a esta.

- Na "Área Administrativa" existente na pirâmide empresarial, foi incluída a subárea de "Segurança Empresarial". Sob a abrangência dessa subárea indicou-se a inclusão dos seguintes departamentos: "Departamento de Segurança Patrimonial", "Departamento de Segurança da Informação" e "Departamento de Segurança de Pessoal". Sob a abrangência do departamento de segurança patrimonial indicou-se a inclusão da "Divisão de Controle de Acessos". Sob a abrangência dessa divisão incluiu-se a "Subdivisão de Controle de Acessos de Pessoas a Áreas Industriais".

- Nas “Classes de funcionários” indicou-se a inclusão de cargos referentes aos três níveis de influência. No nível dos “Gestores de topo” indicou-se a alocação da “Diretoria Administrativa” (DiAdm), com o cargo de “Diretor Administrativo” (DAdm). No nível dos “Gestores intermediários” indicou-se a alocação das “Gerências da Subárea de Segurança Empresarial” (GeSSE), compostas por: “Gerência de Segurança Patrimonial” (GeSPa), com o cargo de “Gerente de Segurança Patrimonial” (GSPa); “Gerência de Segurança da Informação” (GeSIn), com o cargo de “Gerente de Segurança da Informação” (GSIn); “Gerência de Segurança de Pessoal” (GeSPe), com o cargo de “Gerente de Segurança de Pessoal” (GSPe). No nível dos “Gestores operacionais e trabalhadores operacionais”, porém, referentes àqueles administrativos, indicou-se a alocação dos “Funcionários Operacionais do Setor de Segurança Patrimonial” (FOSSP), com os cargos de “Gerente Operacional de Segurança Patrimonial” (GOSeP), “Operador de Segurança” (OpS) e “Segurança Patrimonial” (SeP).

2.2.3.1.1 Descrição dos elementos indicados a partir da pirâmide empresarial

A descrição desses elementos é realizada nos itens a seguir, sendo utilizadas para a indexação as respectivas designações expostas na organização do modelo de representação MoSiCAP:

- Subárea de Segurança Empresarial: É a subárea da “Área Administrativa”, que abrange todos os departamentos, divisões e subdivisões, relacionadas aos setores das seguranças patrimonial, da informação e de pessoal, abordados na subseção “2.1”.
- Departamento de Segurança Patrimonial: É o departamento cujas divisões e subdivisões, estão relacionadas ao setor de segurança patrimonial abordado na subseção “2.1.1” anterior.
- Divisão de Controle de Acessos: Essa divisão pertence ao Departamento de Segurança Patrimonial descrito no item anterior, abrangendo todas as subdivisões relacionadas ao setor de controle de acessos, incluindo os de pessoas, veículos, materiais etc.

- Subdivisão de Controle de Acessos de Pessoas a Áreas Industriais: Essa subdivisão pertence à Divisão de Controle de Acessos descrita no item anterior, porém, dedicada ao controle de acessos de pessoas a áreas industriais, cujas características foram abordadas nas subseções “1.1” e “2.1”.

2.2.3.1.2 Descrição dos elementos indicados a partir da classe de funcionários

2.2.3.1.2.1 Referentes aos gestores de topo

De forma relativa aos “Gestores de topo” está o cargo de “Diretor Administrativo” (DAdm) que compõe a “Diretoria Administrativa” (DiAdm) da empresa. Sob a hierarquia do diretor DAdm está a Subárea de Segurança Empresarial, sendo exemplos de responsabilidades desse diretor, no tocante a essa subárea, o que segue (CARVALHO, 1982):

- Tomar conhecimento, por meio de várias fontes, dos riscos que a empresa está sujeita.
- Definir objetivos e planejamentos estratégicos referentes aos programas de segurança empresarial, incluindo-se um plano geral de segurança.
- Permitir que recursos adequados sejam destinados aos responsáveis pela segurança, com a finalidade de elaboração dos planos necessários.
- Decidir sobre a aplicação dos itens que compõem a proposta do plano geral de segurança, definindo as prioridades na execução.
- Determinar as diretrizes para a contratação, treinamento e capacitação dos recursos humanos que atuarão nas atividades de segurança.
- Avaliar os resultados da política de segurança empresarial.

2.2.3.1.2.2 Referentes aos gestores intermediários

De forma relativa aos “Gestores de intermediários” estão os cargos de gerentes que respondem à diretoria administrativa DiAdm e compõem as “Gerências da Subárea de

Segurança Empresarial" (GeSSE), sendo esses: "Gerente de Segurança Patrimonial" (GSPa), que irá compor a "Gerência de Segurança Patrimonial", sendo responsável pela gestão do "Departamento de Segurança Patrimonial"; "Gerente de Segurança da Informação" (GSIn), que irá compor a "Gerência de Segurança da Informação", sendo responsável pela gestão do "Departamento de Segurança da Informação"; "Gerente de Segurança de Pessoal" (GSPe), que irá compor a "Gerência de Segurança de Pessoal", sendo responsável pela gestão do "Departamento de Segurança de Pessoal". São exemplos de responsabilidades gerais desses gerentes, nos respectivos setores de segurança em que atuam, as seguintes (CARVALHO, 1982):

- Obter levantamentos com a finalidade de detectar riscos potenciais e avaliação das ameaças.
- Auxiliar a direção da empresa indicando treinamentos e designando os responsáveis pela segurança nos respectivos departamentos sob sua gestão.
- Investigar, visando detectar as causas que deram origem a incidentes ou qualquer acontecimento que possa ter ocasionado prejuízo à empresa.
- Assessorar a direção na avaliação dos problemas de segurança.
- Obter os planos de segurança.
- Obter as rotinas e procedimentos de segurança.
- Obter planos com medidas de anulação e/ou mitigação de riscos.
- Obter planos de contingência.
- Propor normas eficazes.

De forma complementar a esses exemplos de responsabilidades, destacam-se as seguintes características particulares de cada tipo de gerente (CARVALHO, 1982):

- Pertinentes ao Gerente de Segurança Patrimonial: Esse funcionário gerencia o departamento de segurança patrimonial e é responsável pela gestão de segurança patrimonial e proteção física da empresa, bem como, pela garantia na qual o controle de acessos (incluindo o de pessoas a áreas industriais) funcione de forma adequada, disponibilizando e organizando os recursos necessários. São exemplos de suas atribuições: propor as normas e regras de acessos; determinar quais informações estarão vinculadas ao controle de acessos de cada tipo de pessoa e as respectivas condições dessas vinculações; definir as rotas permitidas para cada tipo de pessoa sob o controle de acessos; definir os pontos de controle de acessos;

definir as tecnologias de identificação e autenticação a serem utilizadas no sistema de controle de acessos.

- Pertinentes ao Gerente de Segurança da Informação: Esse funcionário gerencia o departamento de segurança da informação e é responsável pela gestão da segurança da informação, tendo suas atribuições relacionadas com as atividades inerentes à segurança da informação no ambiente empresarial, sendo exemplo dessas atribuições a aplicação de recursos para garantir: a inviolabilidade dos dados armazenados em meios computacionais e daqueles que transitam pelos meios de comunicação; o controle de acessos de usuários aos programas de computador e respectivos dados digitais como os dispostos em servidores de arquivos pertencentes aos sistemas computacionais da empresa; os recursos para controle de acessos à informações físicas (desenhos, memoriais de cálculo, especificações de produtos).
- Pertinentes ao Gerente de Segurança de Pessoal: Esse funcionário gerencia o departamento de segurança de pessoal e é responsável pela gestão de segurança de pessoal e, suas atribuições estão relacionadas com a identificação das informações vinculadas às pessoas que irão acessar e/ou exercer atividades profissionais na empresa, visando garantir a segurança no trabalho e/ou nos acessos em questão. Como partes dessas informações incluem-se aquelas referentes ao programa de controle médico de saúde ocupacional (PCMSO).

2.2.3.1.2.3 Referentes aos gestores operacionais e trabalhadores operacionais

De forma relativa aos “gestores operacionais e trabalhadores operacionais” estão os cargos dos pertencentes ao grupo dos “Funcionários Operacionais do Setor de Segurança Patrimonial” (FOSSP), sendo esses: “Gerente Operacional de Segurança Patrimonial” (GOSeP), “Operador de Segurança” (OpS) e “Segurança Patrimonial” (SeP). O gerente operacional de segurança patrimonial GOSeP, responde ao gerente de segurança patrimonial GSPa, sendo exemplos de sua responsabilidade (CARVALHO, 1982):

- Gerir as operações cotidianas de setor de segurança patrimonial, tomando as decisões necessárias para o correto funcionamento dos elementos do sistema de

segurança sob a sua competência administrativa, como no caso da delegação de tarefas para os seus subordinados, do controle das escalas de trabalho etc.

- Analisar os pontos críticos e de vulnerabilidades que a empresa apresenta, buscando a adoção de medidas de segurança aplicáveis para cada caso.
- Providenciar treinamento e capacitação para as pessoas que atuarão na segurança patrimonial da empresa.
- Indicar os operadores de segurança e os seguranças patrimoniais, cuidando para que esses cumpram com suas obrigações no tocante ao sistema de controle de acessos.
- Orientar as eventuais empresas prestadoras de serviço de segurança contratadas, quanto aos requisitos de segurança exigidos.
- Acompanhar cuidadosamente a conduta dos profissionais de segurança, verificando se todos cumprem integralmente os seus deveres.
- Avaliar e tomar as providências administrativas cabíveis com relação às ocorrências e alterações.
- Acompanhar e fazer cumprir as ordens e/ou determinações em vigor.
- Conhecer as habilidades, virtudes e defeitos dos profissionais de segurança.

O "Operador de Segurança" (OpS), responde ao gerente operacional de segurança patrimonial GOSeP e atua em operações referentes ao sistema computacional pertencente ao sistema de controle de acessos de pessoas a áreas industriais, sendo exemplos da sua responsabilidade (CARVALHO, 1982):

- A inclusão e a manutenção dos dados utilizados no sistema de controle de acessos.
- O registro e o controle dos componentes de *hardware* utilizados para identificação, autenticação e autorização dos indivíduos (exemplo: cartões de identificação, leitores biométricos da impressão digital, equipamentos de segurança pessoal), no sistema de controle de acessos.
- A associação, no sistema de controle de acessos, dos indivíduos aos respectivos itens exigidos para identificação (exemplo: associação com o cartão de identificação), autenticação (exemplo: senha, biometria da impressão digital) e autorização (exemplo: perímetros autorizados com identificação dos PCAP que compreendem as rotas permitidas; equipamentos de segurança necessários).
- A configuração dos equipamentos utilizados nos pontos de controle de acessos de pessoas, PCAP, referentes ao sistema de controle de acessos.

O “Segurança Patrimonial” (SeP) responde ao gerente operacional de segurança patrimonial GOSeP e atua diretamente na operação do PCAP, sendo exemplos da sua responsabilidade (CARVALHO, 1982):

- Possuir competência para exercer sua atividade, observando as instruções técnicas e executando corretamente os procedimentos previstos, sendo fiel ao cumprimento de suas atividades.
- Registrar e informar as ocorrências e alterações à sua chefia imediata, executando os procedimentos previstos para tal, devendo ser comunicadas imediatamente, as ocorrências consideradas graves.
- Cumprir as ordens e/ou determinações em vigor.
- Possuir equilíbrio emocional e manter-se estável durante situações de emergência.
- Ser capaz de tomar decisões rápidas utilizando sempre a energia necessária, sem excessos, para resolver as situações de transgressão pertinentes à segurança patrimonial empresarial, observando sempre a ética e a boa conduta.
- Solicitar a intervenção da chefia imediata, sempre que necessário.
- Estar sempre atento e em condições de cumprir corretamente suas atividades.
- Evitar que os procedimentos de segurança da empresa sejam conhecidos por pessoas não autorizadas, sendo as tentativas para esse tipo de conhecimento, imediatamente informadas para a respectiva chefia.

2.2.3.2 Modelo de representação dos elementos do sistema de controle de acessos de pessoas a áreas industriais integrados em estrutura empresarial

A partir do MoROSCE, desenvolveu-se um modelo para representação dos elementos do sistema de controle de acessos de pessoas a áreas industriais integrados em estrutura empresarial, o qual foi denominado de “Modelo dos Elementos do Sistema de Controle de Acessos de Pessoas a Áreas Industriais Integrados em Estrutura Empresarial Industrial” (MESiCAP). Esse modelo é voltado para o atendimento das necessidades deste trabalho, sendo dedicado à abrangência de empresas que podem possuir unidades industriais. Entretanto, o MESiCAP poderá ser estendido para outros modelos, desde que, seja possível realizar as respectivas adequações. Embora o modelo tenha abrangência a unidades industriais, considerou-se a possibilidade da existência de instalações não industriais nessas

unidades, e, também, a possibilidade da existência de unidades totalmente não industriais. Na Figura 2.8 é apresentada a organização dos elementos do MESiCAP.

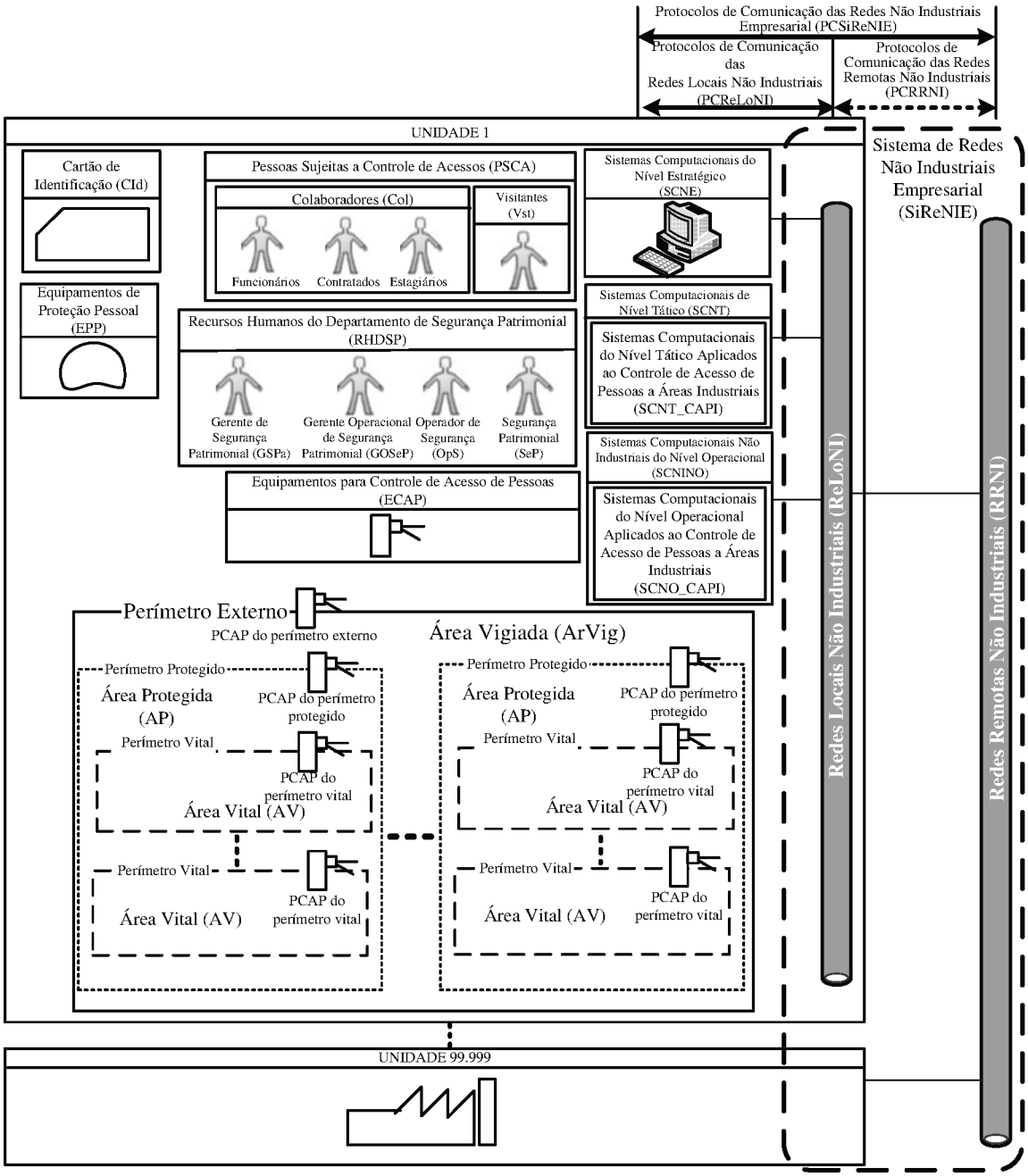

Figura 2.8 - Modelo de representação MESiCAP

O conceito utilizado no desenvolvimento do MESiCAP prevê que cada unidade da empresa possuirá seus próprios recursos para o controle de acessos de pessoas a áreas industriais, sendo esses adequados às respectivas necessidades particulares de segurança patrimonial de cada localidade, porém, dentro das condições determinadas para a empresa como um todo. Assim sendo, os elementos pertencentes ao modelo MESiCAP são gerais para todas as unidades, variando-se as suas configurações para a aplicação em cada unidade de

forma particular. A descrição dos elementos do MESiCAP é apresentada a seguir, em subseções pertencentes a esta, entretanto, informa-se que são considerados elementos do sistema de controle de acessos de pessoas a áreas industrias, os seguintes: “Sistemas Computacionais do Nível Tático Aplicados ao Controle de Acessos de Pessoas a Áreas Industriais” (SCNT_CAPI); “Sistemas Computacionais do Nível Operacional Aplicados ao Controle de Acessos de Pessoas a Áreas Industriais” (SCNO_CAPI); “Pessoas Sujeitas ao Controle de Acessos” (PSCA); “Equipamentos para Controle de Acessos de Pessoas” (ECAP); “Cartão de Identificação” (CId); “Equipamento de Proteção Pessoal” (EPP); “Recursos Humanos do Departamento de Segurança Patrimonial” (RHDSP); “Perímetro Externo”; “Perímetro Protegido”; “Perímetro Vital”; “PCAP do perímetro externo”; “PCAP do perímetro protegido”; “PCAP do perímetro vital”; “Área Vigiada” (ArVig); “Área Protegida” (AP); “Área Vital” (AV).

2.2.3.2.1 Sistemas computacionais dedicados ao controle de acessos de pessoas a áreas industriais e sistema de redes não industriais

Os sistemas computacionais dedicados ao controle de acessos de pessoas a áreas industriais são formados pelos: Sistemas Computacionais do Nível Tático Aplicados ao Controle de Acessos de Pessoas a Áreas Industriais, SCNT_CAPI; Sistemas Computacionais do Nível Operacional Aplicados ao Controle de Acessos de Pessoas a Áreas Industriais, SCNO_CAPI. O primeiro pertence aos sistemas computacionais do nível tático (SCNT) e o segundo aos sistemas computacionais não industriais do nível operacional (SCNINO). No nível estratégico não há partes dos sistemas computacionais dedicados ao controle de acessos de pessoas a áreas industriais, haja vista que no MESiCAP considerou-se que as informações a serem utilizadas no nível em questão deverão ser tratadas no nível tático para atender as demandas do nível estratégico, não sendo função desses sistemas computacionais esse tratamento.

Relativamente aos meios de comunicação, utilizou-se para o MESiCAP a composição do sistema de redes da empresa SiReNIE, formada pelas Redes Locais Não Industriais (ReLoNI) e as Redes Remotas Não Industriais (RRNI), as quais estão, respectivamente, sob os protocolos PCReLoNI (Protocolos de Comunicação das Redes Locais Não Industriais) e PCRRNI (Protocolos de Comunicação das Redes Remotas Não Industriais), conforme

exposto na subseção “2.2.2”. Entretanto, no caso do MESiCAP, há a necessidade das redes locais ReLoNI e das redes remotas RRNI, dispor de recursos aplicados a inviolabilidade dos dados transmitidos em seus meios de comunicação, sendo exemplo desses recursos o protocolo de criptografia SSL (*Security Socket Layer*), integrado ao protocolo TCP/IP (*Transfer Control Protocol/Internet Protocol*).

2.2.3.2.2 Pessoas sujeitas a controle de acessos

As Pessoas Sujeitas a Controle de Acessos (PSCA) estão classificadas em dois grupos, os Colaboradores (Col) e os Visitantes (Vst), sendo que o grupo dos colaboradores reúne Funcionários, Contratados e Estagiários. Nos itens a seguir apresenta-se a descrição das características dos componentes desses grupos:

- Funcionários: são pessoas que fazem parte do quadro de funcionários da empresa possuindo vínculo empregatício direto com a mesma, ou seja, um contrato de trabalho vigente.
- Contratados: são pessoas que não pertencem ao quadro de funcionários da empresa, porém, são contratadas para exercer atividades profissionais no seu âmbito. Podem ser profissionais contratados como pessoa física ou pertencer a outras empresas contratadas como pessoa jurídica.
- Estagiários: são pessoas que possuem contrato de estágio vigente com a empresa.
- Visitantes: pode ser qualquer pessoa que não pertença aos componentes descritos nos itens anteriores, que por motivos profissionais, de estudos ou familiares, precise acessar os perímetros controlados da empresa por períodos de tempos definidos.

2.2.3.2.3 Equipamentos para controle de acessos de pessoas

Os Equipamentos para Controle de Acessos de Pessoas (ECAP), reúnem todos àqueles que poderão ser utilizados nos pontos de controle PCAP, existentes nos perímetros controlados, cujos exemplos são mencionados na subseção “2.2.1” e compreendem: equipamentos para o controle físico de acessos de pessoas (detalhados na subseção “2.5”);

leitores RFID (detalhados na subseção “2.4”); leitores biométricos da impressão digital (detalhados na subseção “2.3”).

2.2.3.2.4 Cartão de identificação e equipamentos de proteção pessoal

O Cartão de Identificação (CId) é emitido pela empresa para identificação das pessoas sujeitas ao controle de acessos PSCA, entretanto, no caso dos Funcionários poderá juntar as funções de outros elementos de identificação pessoal, como no caso daquelas referentes aos crachás.

Os Equipamentos de Proteção Pessoal (EPP) são aqueles exigidos para o exercício das atividades profissionais e proteção nos acessos às áreas da empresa, sendo definidos a partir de membros pertencentes ao Departamento de Segurança de Pessoal. São exemplos desses equipamentos: capacete, luvas, máscaras, óculos, protetor auricular, dosímetros, botas com biqueira de aço etc.

2.2.3.2.5 Perímetros e seus componentes

No caso do MESiCAP o conceito de perímetro controlado é o mesmo descrito na subseção “2.2.1”, entretanto, os perímetros e as respectivas áreas que delimitam foram classificados em tipos fundamentados na norma CNEN (Comissão Nacional de Energia Nuclear) NE 2.01 (NE2.01, 2011), que trata da proteção física de unidades operacionais pertencentes ao segmento de energia nuclear, especificando as áreas contidas em unidades operacionais. Em decorrência do exposto, classificou-se os perímetros em “Perímetro Externo” (classe de perímetro externo), “Perímetro Protegido” (classe de perímetro interno) e “Perímetro Vital” (classe de perímetro interno), sendo as áreas delimitadas por esses perímetros respectivamente designadas por “Área Vigiada” (ArVig), “Área Protegida” (AP) e “Área Vital” (AV). O perímetro externo contém os perímetros protegidos, que por sua vez, contém os perímetros vitais. Assim sendo, a Área Vigiada contém as Áreas Protegidas, que por sua vez, contém as Áreas Vitais. O conceito de “Área Industrial de Segurança” é o mesmo

citado na subseção “2.2.1”. Na Tabela 2.2 é apresentada a classificação desses perímetros controlados, com as respectivas descrições e designações das áreas sob delimitações.

Tabela 2.2 - Classificação dos perímetros controlados e designação das respectivas áreas no MESiCAP

Tipos de Perímetros Controlados		
Designação	**Descrição**	**Designação da área sob delimitação**
Perímetro Externo	Esse perímetro delimita toda a área da propriedade na qual estão as instalações da unidade da empresa, sendo fronteira com a área pública. Sob suas delimitações pode conter um ou mais perímetros protegidos, além da considerada área comum existente entre esses perímetros.	Área Vigiada (ArVig) e área comum
Perímetro Protegido	Esse perímetro delimita uma área mantida sob constante proteção, cercada por uma barreira física (exemplo: muro, cerca, cerca virtual, grade etc) com número restrito de usuários, podendo conter um ou mais perímetros vitais.	Área Protegida (AP)
Perímetro Vital	Esse perímetro delimita uma área que contenha equipamentos vitais ou que apresente riscos à vida, estando essa área no interior de uma estrutura que necessariamente possua piso, paredes e teto, como itens específicos da barreira física.	Área Vital (AV)

Além da área, estão relacionados aos perímetros os seguintes elementos: ponto de controle de acessos de pessoas, PCAP; equipamentos para controle de acessos de pessoas, ECAP. O conceito de PCAP é o mesmo descrito na subseção “2.2.1”, ou seja, são locais específicos para controle de acessos de pessoas, pertencentes ao perímetro controlado, com condições para entrada e saída. Os equipamentos ECAP são os mesmos descritos na subseção “2.2.1”.

2.2.3.2.6 Tipos de informações associadas a definições do PCAP e permissão de acessos de pessoas a áreas industriais no MESiCAP

Para abordar os tipos de informações associadas a definições do ponto de controle PCAP e a “Permissão de Acessos de Pessoas a Áreas Industriais” (PAPArI), será utilizada a Figura 2.9, na qual podem ser observados exemplos de fluxos percorridos por esses tipos de informações entre setores da empresa e o “Sistema de Controle de Acessos de Pessoas a Áreas Industriais” (SCAPAI). Relativamente aos setores apresentados na figura em questão, informa-se que as diretorias e departamentos da produção, administração (que inclui a Diretoria Administrativa) e vendas/*marketing*, pertencem respectivamente às áreas da

produção, administrativa e de vendas/marketing, existentes na pirâmide empresarial apresentada na Figura 2.7, sendo pertencente à área administrativa o Departamento de Recursos Humanos e o Departamento de Segurança de Pessoal.

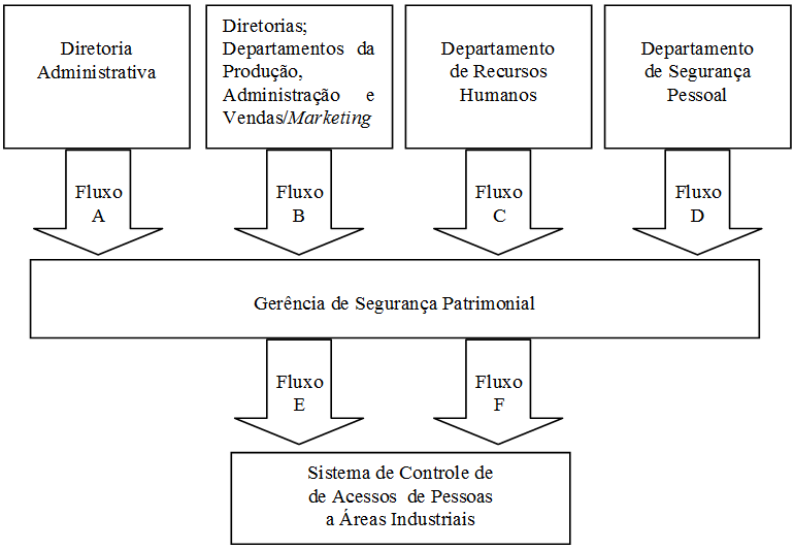

Figura 2.9 - Exemplo de fluxo de informações referentes a definições do PCAP e PAPArI

Os tipos de informações em questão são apresentados nos tens a seguir, cuja organização os agrupa em função do fluxo apresentado na Figura 2.9:

- Tipos pertinentes ao Fluxo A
  - Informações sobre o planejamento estratégico de segurança patrimonial.
- Tipos pertinentes ao Fluxo B
  - Informações pessoais dos contratados.
  - Informações dos horários permitidos para os acessos de contratados.
  - Comunicação dos direitos de acessos circunstanciais temporários de contratados.
  - Comunicação das restrições de acessos circunstanciais temporárias de contratados.
  - Informações sobre mudanças ocupacionais de contratados.
  - Informações dos visitantes.
  - Lista de treinamentos exigidos para os indivíduos pertencentes às PSCA.
  - Lista dos treinamentos realizados pelos indivíduos pertencentes às PSCA.
- Tipos pertinentes ao Fluxo C
  - Informações pessoais dos funcionários e estagiários.
  - Informações dos horários permitidos para os acessos de funcionários e estagiários.

- Comunicação dos direitos de acessos circunstanciais temporários de funcionários e estagiários.
- Comunicação das restrições de acessos circunstanciais temporárias de funcionários e estagiários.
- Informações sobre mudanças ocupacionais de funcionários e estagiários.

- Tipos pertinentes ao Fluxo D
  - Lista de riscos das áreas de segurança.
  - Equipamentos de proteção pessoal necessários para os acessos as áreas de segurança, considerando além do local, os cargos, as funções e as atividades.
  - Vigências dos atestados de saúde ocupacional.
- Tipos pertinentes ao Fluxo E
  - Informações de definições sobre o Ponto de Controle de Acessos de Pessoas, PCAP:
    - Recursos humanos necessários.
    - Locais nos perímetros.
    - Equipamentos utilizados no PCAP.
    - Conectividade exigida.
    - Pontos de conexão para suprimento de energia elétrica.
    - Requisitos exigidos para as instalações prediais.
    - Informação sobre a quantidade máxima de ocupantes permitida para o respectivo perímetro controlado.
- Tipos pertinentes ao Fluxo F
  - Informações de definição da permissão de acessos de pessoas a áreas industriais, PAPArI:
    - Exigências para identificação (exemplo: código de identificação).
    - Exigências para autenticação (exemplos: senha e biometria da impressão digital).
    - Exigências para autorização (exemplos: áreas industriais de segurança autorizadas, com identificação dos PCAP que compreendem as rotas permitidas; equipamentos de segurança pessoal necessários).

2.3 TÓPICOS PERTINENTES A IDENTIFICAÇÃO POR BIOMETRIA DA IMPRESSÃO DIGITAL

Biometria é uma palavra cuja etimologia indica origem no grego, na qual “bios” é referente à vida e “metros” a contagem ou medida. Essa palavra designa a ciência que trata da mensuração dos seres vivos, podendo ser estudadas características físicas, fisiológicas e comportamentais desses seres, entretanto, no âmbito dessa ciência inclui-se um segmento direcionado à identificação de seres humanos por meio das características em questão (LOURENÇO, 2009). As características físicas são traços no corpo do indivíduo, com pouca variação ao longo do tempo, sendo exemplos dessas características àquelas referentes a digitais, íris e retina. As fisiológicas estão relacionadas com as funções orgânicas e processos vitais do indivíduo, podendo variar em função das situações que o indivíduo está submetido, sendo exemplos dessas características aquelas referentes à respiração e frequência cardíaca. As comportamentais ou dinâmicas, estão relacionadas com a interação entre o indivíduo e o ambiente, sendo caracterizadas pela volatilidade em função de situações que o indivíduo está submetido e ao longo do tempo, sendo exemplo dessas características aquelas referentes a assinatura, forma de digitação e o modo de andar (LOURENÇO, 2009).

As evoluções no segmento da biometria direcionado à identificação de seres humanos e, nas tecnologias utilizadas nas aplicações desse segmento, estão relacionadas à disponibilização de recursos para o desenvolvimento de sistemas com identificação biométrica, nos quais a biometria tem a conotação de reconhecimento automatizado de indivíduos, fundamentado em características e/ou comportamentos mensuráveis dos respectivos corpos, cuja quantificação é pertinente à estatística que trata de atributos biológicos (BAZEN, 2006). Dentre esses tipos de sistemas, há aqueles fundamentados em características físicas dos indivíduos, doravante designados por “Sistema com Identificação Biométrica por Características Físicas” (SIBiCaFi). Nesse tipo de sistema a identificação do indivíduo está relacionada aos serviços de identificação e autenticação, descritos na subseção “2.1.2”. No primeiro o resultado da identificação biométrica pode ser utilizado como informação a ser aproveitada para declaração de identidade do indivíduo para com o sistema. No segundo o resultado da identificação biométrica pode ser utilizado como informação a ser aproveitada para verificação da identidade do indivíduo (PINHEIRO, 2008).

Um elemento utilizado nos sistemas do tipo SIBiCaFi é o chamado perfil biométrico, que pode ser entendido, sob o ponto de vista de sua utilização, como as informações

biométricas do indivíduo que serão armazenadas em meios computacionais, para serem utilizadas em processo de comparação realizado por *software*. Nesse processo, um universo de indivíduos é representado por seus perfis armazenados num sistema computacional, sendo função do *software* determinar a similaridade entre os atributos biométricos de um determinado indivíduo e aquele respectivo armazenado no sistema computacional. No processo em questão, o *software* realiza a captura das características biométricas do indivíduo, extrai os atributos e efetua a comparação, que definirá se o processo resultou em coincidência com perfil armazenado, ou não. De forma pertinente ao exposto, apresenta-se na Figura 2.10 um esquemático que representa as etapas típicas realizadas por sistemas do tipo SIBiCaFi, no que se refere a identificação biométrica. Nesse esquemático a formação do universo de indivíduos a ser utilizado no processo de comparação descrito anteriormente, ocorre em outro processo designado por "Cadastramento". Também nesse esquemático, o processo de comparação descrito anteriormente é abordado como uma etapa de outro processo, designado por "Verificação" (NEWMAN, 2009).

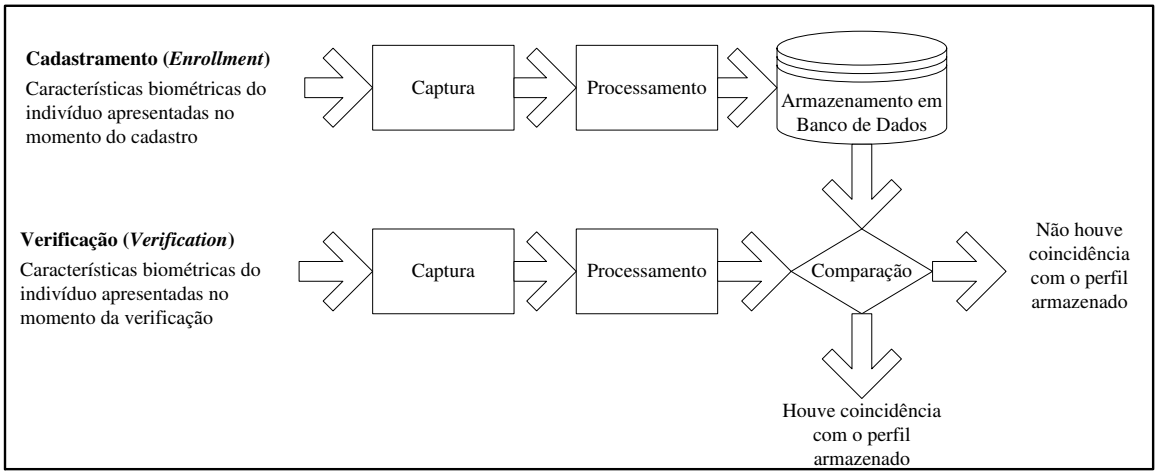

Figura 2.10 - Etapas típicas da identificação biométrica realizada em SIBiCaFi (NEWMAN, 2009)

O processo de "Cadastramento" (*enrollment*) é destinado ao armazenamento, em banco de dados, dos perfis biométricos dos indivíduos que irão compor o universo de comparação, sendo esse processo formado pelas etapas de "Captura", "Processamento" e "Armazenamento em Banco de Dados". Na etapa de Captura é realizada a aquisição de dados biométricos das características físicas do indivíduo, mediante sua apresentação presencial no SIBiCaFi. Na etapa de Processamento é realizada a extração dos atributos referentes às características físicas do indivíduo, cujos dados foram anteriormente obtidos na etapa de Captura. Na etapa de Armazenamento em Banco de Dados, ocorre o armazenamento do perfil biométrico do indivíduo, em banco de dados do SIBiCaFi.

O processo de "Verificação" (*Verification* ou *Match*) realiza a verificação de identidade do indivíduo, definindo um resultado que indica se houve coincidência com o perfil armazenado, ou não. Esse processo é formado pelas etapas de "Captura", "Processamento" e "Comparação", sendo as duas primeiras idênticas àquelas de mesma denominação aplicadas ao processo de Cadastramento. Na etapa de Comparação é obtida a medida de semelhança, que envolve técnicas de comparação de dados referentes a atributos biométricos do indivíduo sob verificação e, aqueles armazenados no banco de dados do SIBiCaFi, sendo utilizados os perfis biométricos. O resultado da etapa de Comparação ocorre por meio de comparação da medida de semelhança com um limiar, determinando a partir de fundamentações estatísticas e de parametrização referente à confiabilidade, se o perfil sob verificação coincide com o perfil armazenado, ou não. No serviço de autenticação pertinente ao SIBiCaFi, o processo de verificação normalmente ocorre uma vez. Entretanto, no serviço de identificação pode ocorrer por repetidas vezes até passar por todos os perfis armazenados, na busca que tem por função determinar se um determinado indivíduo pertence ao universo daqueles cadastrados no sistema.

Em que pese o atual estado de evolução dos tipos de sistemas SIBiCaFi, há a probabilidade da identificação do indivíduo ocorrer de forma incorreta, podendo existir variação no que se refere à confiança proporcionada pelas diferentes tecnologias empregadas para a identificação em questão. Assim sendo, para aplicações nas quais se busca maior segurança na identificação de indivíduos, se faz necessária a utilização de recursos adicionais, como aqueles fundamentados em cartões de identificação e senhas pessoais (PINHEIRO, 2008). De forma pertinente ao exposto, podem ocorrer dois tipos de erros relacionados ao processo de comparação, sendo que esses estão respectivamente relacionados a dois tipos de frequências, conforme exposto a seguir (PINHEIRO, 2008):

- *False Accept* (Falsa Aceitação), FA: Esse erro é aquele no qual o sistema decidiu que o perfil verificado coincide com o armazenado, entretanto, o individuo sob verificação não é aquele que gerou o perfil armazenado utilizado na comparação em questão. A frequência associada com este tipo de erro é designada por FAR (*False Acceptance Rate*, Taxa de Falsa Aceitação). Esse erro é também referenciado por erro do tipo I.
- *False Reject* (Falsa Rejeição), FR: Esse erro é aquele no qual o sistema decidiu que o perfil verificado não coincide com o armazenado, entretanto, o individuo sob verificação é aquele que gerou o perfil armazenado utilizado na comparação em questão. A frequência associada com este tipo de erro é designada por FRR (*False*

Rejection Rate, Taxa de Falsa Rejeitação). Esse erro é também referenciado por erro do tipo II.

Variando-se o limiar mencionado na etapa de comparação, a FAR e a FRR comportam-se de forma inversamente proporcional, ou seja, quando a FAR diminui a FRR aumenta e vice-versa (PINHEIRO, 2008). Dessa forma, os sistemas devem operar com valores de limiar adequados às aplicações que se destinam, haja vista que a diminuição da FAR aumenta a segurança (aumenta a confiança) e diminui a conveniência (relacionada a fatores como: conforto para os indivíduos; tempo demandado para a comparação) e a diminuição da FRR aumenta o conveniência e diminui a segurança (diminui a confiança).

Dentre os tipos de sistemas pertencentes ao SIBiCaFi estão aqueles dedicados à biometria da impressão digital, os quais doravante serão referenciados por "Sistema com Identificação por Biometria da Impressão Digital" (SIBID) e cujos elementos de interesse para este trabalho são abordados nas subseções a seguir, pertencentes a esta.

2.3.1 Elementos envolvidos na caracterização de uma impressão digital

A impressão digital pode ser abordada como a impressão resultante do contato das dobras cutâneas das polpas dos dedos com uma superfície lisa, que permita a aplicação de processos dactiloscópicos e possibilite a identificação de um indivíduo (FERREIRA, 1998). A imagem oriunda da impressão digital (dactilograma) possui regiões com formas designadas por minúcias, cujas obtenções da orientação e do posicionamento, estão envolvidas na caracterização de uma impressão digital, não sendo necessário aos sistemas SIBID armazenar toda a imagem da impressão digital. Na Figura 2.11, são apresentados desenhos que exemplificam as minúcias em questão, ressaltando-se que essas podem sofrer modificações provocadas por fatores biológicos como cicatrizes (oriundas de cortes ou queimaduras), desgaste decorrente de atividades manuais e, perda de elasticidade da pele em função da idade do indivíduo (BOECHAT, 2008; MALTONI et al., 2009).

Figura 2.11 - Principais tipos de minúcias da impressão digital (MALTONI et al., 2009)

Relativamente à indicação de utilização da biometria da impressão digital para o controle de acessos de pessoas, citam-se os parâmetros informados por Boechat (2008), nos quais a impressão digital possui: universalidade média (a grande maioria dos indivíduos possui esta característica); unicidade alta (dificilmente existem duas ou mais iguais); permanência alta (varia pouco no tempo); desempenho alto (possuem algoritmos rápidos e eficientes para a identificação); aceitação média (a população a aceita, de modo geral); proteção média (há certa dificuldade em fraudar um sistema que possua esse tipo de autenticação).

2.3.2 Sensoriamento óptico

O tipo de sensoriamento de interesse para este trabalho é aquele cujo sensor óptico utiliza para Pixel (Pixel - *Picture element*, Elemento de imagem) material semicondutor a estado sólido, de forma que um conjunto de Pixels irá compor uma matriz sobre a qual será projetada a imagem a ser capturada. Na Figura 2.12 é apresentado um esquemático com a arquitetura básica de um sistema de aquisição de imagem da impressão digital, que utiliza o tipo de sensoriamento em questão.

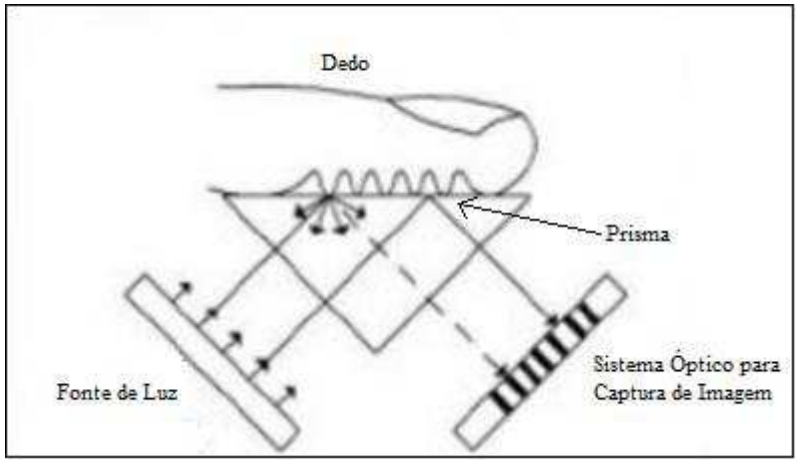

Figura 2.12 - Arquitetura básica de sistema com sensoriamento óptico (COELHO, 2009)

A arquitetura em questão é composta por: Fonte de Luz, normalmente LEDs (*Light Emitting Diode*, Diodo Emissor de Luz); Prisma, normalmente de vidro; Sistema Óptico para Captura de Imagem, normalmente uma câmera digital cujos pixels são fotodiodos.

Nesse sistema a Fonte de Luz é dirigida para o Prisma, que reflete sobre a área do Sistema Óptico para Captura de Imagem, a impressão digital formada por regiões escuras e claras. As cristas da impressão digital marcam o prisma como uma região mais escura (absorção de luz) e os sulcos (regiões entre cristas) como uma região mais clara (reflexão de luz), formando uma imagem que será capturada e processada para extração das características que irão compor o perfil biométrico, tendo por base as minúcias citadas anteriormente. Esse tipo de sensoriamento apresenta resoluções relativamente altas e baixo custo, favorecendo a disseminação nas aplicações que utilizam esse tipo de biometria (COELHO, 2009).

2.3.3 Leitor biométrico da impressão digital por reflexão (Le_BID_R) e recurso para desenvolvimento de aplicativos com esse tipo de biometria

O leitor biométrico da impressão digital, também conhecido por *Fingerprint Reader* ou *Fingkey*, é um equipamento destinado à aquisição dos dados biométricos da impressão digital (de forma presencial), para a extração das características a serem utilizadas na composição do respectivo perfil biométrico que será armazenado em meios computacionais ou empregado no processo de comparação descrito na subseção “2.3”. Dentre os tipos desses leitores biométricos é de interesse para este trabalho aquele que utiliza o sensoriamento óptico descrito na subseção “2.3.2”, sendo designado neste trabalho por “Leitor Biométrico da

Impressão Digital por Reflexão" (Le_BID_R), haja vista que a imagem utilizada para a leitura da impressão digital é refletida pelo sistema óptico para sua captura.

O leitor Le_BID_R se integra a equipamentos de um sistema computacional por meio de comunicação de dados, sendo as funções relativas a essa comunicação e a realização da biometria da impressão digital, implementadas em aplicativos por meio de bibliotecas específicas, fornecidas por empresas especializadas, que as desenvolvem para os diferentes tipos de Le_BID_R disponíveis no mercado. As bibliotecas em questão normalmente são disponibilizadas para as principais linguagens de programação como C#, C++, JAVA, VB.NET e J#, bem como, para os principais sistemas operacionais dos quais citam-se o Microsoft Windows XP e o Linux. Seus recursos podem incluir: aquisição de imagem da impressão digital; extração das características biométricas da impressão digital para comparação e armazenamento dos perfis biométricos; realização da etapa de "Comparação" do processo de "Verificação" (*Verification* ou *Match*), cujo resultado indica se houve coincidência com o perfil armazenado, ou não. Informa-se, relativamente às rotinas que executam a etapa de comparação, que normalmente é possível definir um valor correspondente ao nível de confiança desejado, de forma a diminuir ou aumentar a FAR.

Como exemplo de Le_BID_R cita-se o modelo HAMSTER HFDU04, fornecido pela empresa NITGEN (NITGEN, 2012), que também disponibiliza um conjunto de bibliotecas para desenvolvimento de aplicativos em linguagens de programação de grande utilização no mercado, como as citadas anteriormente. Na Figura 2.13 é apresentada imagem do modelo em questão.

Figura 2.13 - Le_BID_R modelo HAMSTER HFDU04 (NITGEN, 2012)

Na Tabela 2.3, são apresentadas características técnicas do leitor biométrico HAMSTER HFDU04.

Tabela 2.3 - Características técnicas do Le_BID_R modelo HAMSTER HFDU04 (NITGEN, 2012)

Tipo:	Óptico com prisma de vidro.
Modelo do leitor:	Torre com base removível.
Captura:	Qualquer ângulo (360º).
Interface:	USB 2.0.
Resolução:	500 DPI.
Temp. de Operação:	0 ~ 55ºC.
Voltagem:	5V.
Área de Captura:	16 x 18 mm.
Tempo de Captura:	~ 300 milissegundos.
Tamanho da Imagem:	248 x 292 pixels.
Padrões:	MIC, CE, FCC, WHQL.
SDK:	eNBSP SDK (Tecnologia própria Nitgen) Criptografia AES 256 bit.
Padrões:	ISO/IEC 19794-2:2005 ANSI/INCITS 378-2004.
Sistemas Operacionais:	Windows 98/2000/ME/2003/2008/XP/Vista/7 Linux kernel 2.6 ou superior.

2.3.4 Aspectos legais sobre a biometria da impressão digital

A Lei número 6.015, de 31 de dezembro de 1973, reconhece a impressão digital como forma de identificação irrefutável, permitindo a qualquer individuo ser identificado ou verificado por meio de suas impressões digitais, no entanto, não foi observada legislação específica que trate do uso desse recurso para aplicações como as pertinentes ao sistema SIBiCaFi (LEI, 1973). Sob outro ponto de vista, a Lei pétrea, no artigo 5º, inciso X, informa que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, tratando do direito à indenização pelo dano material ou moral decorrente de sua violação (CF, 1998).

2.4 TÓPICOS PERTINENTES À IDENTIFICAÇÃO POR RADIOFREQUÊNCIA

A identificação por radiofrequência (RFID - *Radio Frequency IDentification*) é uma tecnologia bastante disseminada em aplicações que envolvem a identificação de objetos e seres vivos, incluindo-se o controle de acessos (SANTINI, 2008). Apesar dessa forma de identificação ser utilizada desde antes da segunda guerra mundial (SEUFITELLI et al., 2009), a RFID como hoje se conhece foi desenvolvida na década de 1980, no MIT (*Massachusetts Institute of Technology*) juntamente com outros centros de pesquisas, com o objetivo de

utilizar a radiofrequência em desenvolvimento de aplicações para rastreamento e localização de objetos e seres vivos (BERNARDO, 2004).

Segundo Seufitelli et al. (2009) e Pinheiro (2008), o sistema de RFID funciona com o envio e recepção de dados através de sinal de radiofrequência, tendo por componentes preliminares: Leitor RFID; Transponder (ou Tag); Computador Hospedeiro. Em seu funcionamento básico, o Leitor RFID é conectado ao Computador Hospedeiro, para permitir que esse último receba as informações contidas no Transponder. Para essa recepção de informações o Leitor RFID realiza a leitura do Transponder, que compreende a seguinte sequência: 1) Leitor RFID emite sinal de radiofrequência que chega ao Transponder; 2) Transponder capta o sinal emitido pelo Leitor RFID e responde emitindo sinal de radiofrequência que chega ao Leitor de RFID, sendo nesse sinal enviadas as informações armazenadas (em memória não volátil) no seu circuito integrado (CI); 3) Leitor RFID capta o sinal emitido pelo Transponder, extrai as informações recebidas e as transmite para o Computador Hospedeiro. Nesse processo, tanto para as comunicações entre o Computador Hospedeiro e o Leitor RFID, quanto para as comunicações entre o Leitor RFID e o Transponder, são utilizados protocolos específicos. Esse processo básico é utilizado na identificação de objetos e seres vivos, associando a cada unidade ou indivíduo, um Transponder cujo conteúdo armazenado permita a discriminação que os identificará.

No que se refere a organizações que estabelecem padrões referentes à RFID cita-se a EPCGlobal e a ISO (*International Organization for Standardization*). A EPCglobal desenvolveu as normativas estabelecidas pelos códigos EPC-*Electronic Product Code*™ (EPC, 2012). Relativamente aos padrões ISO citam-se os seguintes (BHUPTANI e MORADPOUR, 2005):

- ISO 11784, 11785 e 14223: contém a estrutura do código para identificação de animais.
- ISO 10536, 14443 e 15693: abrange os aspectos físicos, aéreos e do protocolo de comunicação para os cartões que operam a curta distância.
- ISO 10374: especifica o padrão de etiquetas para identificação de containers.
- ISO 15961, 15962 e 15963: direcionado ao gerenciamento de itens, trata das técnicas para identificação automática, incluindo o protocolo de dados, interface, regras de codificação e funções lógicas de memória.

- Série ISO 18000: essas tratam os parâmetros de comunicações para as frequências aceitas globalmente, tais como a de 136 kHz, 15,56 MHz e a faixa de 2,45 GHz a 5,8 GHz.

A frequência do sinal de rádio utilizado na RFID está relacionada com a distância de alcance entre Leitor RFID e Transponder, sendo apresentada na Tabela 2.4 uma síntese de relação entre valores frequência, distâncias típicas e exemplos de aplicações (BHUPTANI e MORADPOUR, 2005).

Tabela 2.4 - Síntese de relação para frequências, distâncias e exemplos (BHUPTANI e MORADPOUR, 2005)

FREQUÊNCIA	DISTÂNCIA TÍPICA	EXEMPLOS DE APLICAÇÕES
Baixa Frequência; menos de 135 kHz.	Até 0,2 m	-Identificação de animais. -Automação industrial. -Controle de acessos de pessoas.
Alta frequência; 13,56 MHz.	Até 1,0 m	-Diversas aplicações de rastreamento para produtos, tais como livros, malas e vestuário. -Controle de acessos de pessoas. -Prateleiras inteligentes. -Identificação e monitoramento de pessoas.
Ultra alta frequência (UHF - *Ultra High Frequency*); 433 MHz e de 860 MHz à 930 MHz.	Até 6,0 m	-Cadeia de abastecimento e logística. -Controle de fluxo de pessoas.
Microondas; 2,45 GHz e 5,8 GHz.	Até 60 m	-Cobrança eletrônica de pedágio. -Automação industrial.

2.4.1 Transponder

O Transponder possui, como itens de sua constituição, circuito integrado (*microship*) e antena (que pode ser forma de bobina), tendo invólucro em vários formatos e tamanhos, sendo exemplos: cartões, chaveiros, pulseiras, crachás, etiquetas. Há também empresas que fornecem transponder para serem incorporados a produtos, permitindo que esses se tornem produtos com RFID. Existe uma classificação que os divide em dois tipos designados por: passivo e ativo. O Transponder passivo não utiliza bateria e possui uma bobina que sendo sensibilizada pelo sinal emitido pelo leitor, gera energia suficiente para suas operações, sendo enviado o sinal de resposta, que normalmente é de curto alcance. O Transponder ativo possui bateria interna e um transmissor cujo sinal de resposta pode chegar a alguns quilômetros, permitindo a captura de dados em movimento. Os transponders também podem ser dos tipos

read-only, *read-write* e *Write Once Read Many* (WORM). Nos *read-only*, somente de leitura, as informações armazenadas não podem ser alteradas. Nos *read-write*, leitura e escrita, há informações que podem ser modificadas e outras fixas. Nos WORM é possível realizar única gravação de dados, que não podem ser modificados posteriormente (HID, 2012; HUA, 2012).

Relativamente a exemplo de Trasponder do tipo cartão, pertinente as funções de crachá e controle de acessos de pessoas, cita-se o modelo Indala FlexISO, fornecido pela empresa HID Global (HID, 2012), que opera com frequência de 125kHz. Na Figura 2.14 é apresentada imagem do modelo de cartão RFID em questão.

Figura 2.14 - Cartão de identificação RFID modelo Indala FlexISO (HID, 2012)

Relativamente a exemplo de Trasponder (sem invólucro) que pode ser incorporado a produto, cita-se o modelo 1390 eProx Tag, fornecido pela empresa HID Global (HID, 2012), que opera com frequência de 125 kHz. Na Figura 2.15 é apresentada imagem do modelo de trasponder em questão.

Figura 2.15 - Transponder sem invólucro modelo 1390 eProx Tag (HID, 2012)

2.4.2 Leitor RFID

O Leitor RFID é destinado à leitura do Transponder, entretanto, em função do modelo, também pode ser aplicado à escrita, nos casos referentes aos transponders dos tipos *read-write* e WORM. Os leitores RFID podem ser classificados em Portátil e Fixo, sendo escolhidos em

função da aplicação que se destinam, entretanto, devem atender os padrões de RFID utilizados nos Transponders, de tal maneira que sejam compatíveis entre si.

Relativamente a exemplo de Leitor RFID do tipo portátil cita-se o modelo DS908-R, fornecido pela empresa Motorola (MOTOROLA, 2012), que opera na faixa de frequência de 865 MHz até 915 MHz. Na Figura 2.16, é apresentada imagem do modelo de leitor em questão.

Figura 2.16 - Leitor RFID do tipo portátil modelo DS908-R (MOTOROLA, 2012)

Relativamente a exemplo de Leitor RFID do tipo fixo, utilizado para a leitura de transponder com funções de crachá e controle de acessos de pessoas, cita-se o modelo Indala Classic Reader 603, fornecido pela empresa HID Global (HID, 2012), que opera com frequência de 125kHz. Na Figura 2.17, é apresentada imagem do modelo de leitor em questão.

Figura 2.17 - Leitor RFID do tipo fixo modelo Indala Classic Reader 603 (HID, 2012)

2.5 ABORDAGEM SOBRE EQUIPAMENTOS PARA CONTROLE FÍSICO DE ACESSOS DE PESSOAS

O “Equipamento para Controle Físico de Acessos de Pessoas” (ECoFAP), tem a função de fisicamente impedir ou permitir o trânsito de uma pessoa que pretende entrar ou sair de uma área industrial de segurança. O ECoFAP possui mecanismo que libera ou trava uma barreira física, sendo que a liberação permite a pessoa transitar pela trajetória na qual o ECoFAP exerce sua função, entretanto, o travamento não permite a pessoa transitar pela trajetória na qual o ECoFAP exerce sua função. Com relação ao sentido do fluxo de pessoas, há ECoFAP Unidirecional e Bidirecional. O Unidirecional permite fluxo num único sentido e o Bidirecional em dois sentidos, ocorrendo a transposição de única pessoa em único sentido por vez. Entretanto, é desejável (ou até necessário em função da aplicação) que uma vez iniciada a transposição pelo ECoFAP, num determinado sentido, seu mecanismo não permita retorno da pessoa no sentido contrário.

A integração dos ECoFAP com os sistemas computacionais é realizada através de conexão para envio de sinais elétricos ou para comunicação de dados. Assim sendo, neste trabalho, os tipos de conexão são respectivamente designados por: Conexão por sinais elétricos; Conexão por comunicação de dados. As conexões em questão permitem os acionamentos necessários e são especificadas por protocolos dedicados. Desta forma o sistema computacional comanda o ECoFAP, recebendo informações sobre o andamento dos comandos, que tipicamente são aqueles que permitem liberação e definição do sentido de fluxo. Na Figura 2.18, é apresentado exemplo de arquitetura básica de aplicação com ECoFAP.

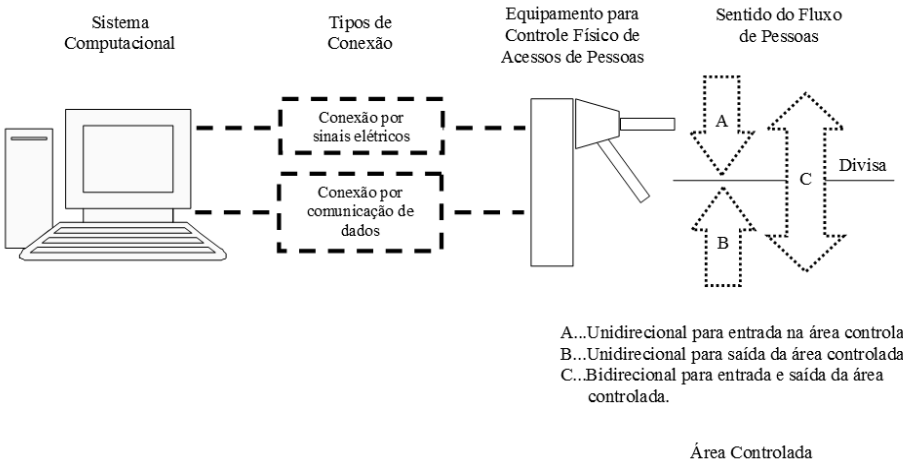

Figura 2.18 - Exemplo de arquitetura básica de aplicação com ECoFAP

2.5.1 Exemplos de ECoFAP

2.5.1.1 Catraca eletrônica

As catracas eletrônicas, em função do modelo, podem ser unidirecionais ou bidirecionais, no entanto, sua aplicação mais comum é como ECoFAP unidirecional. Relativamente a exemplo de catraca eletrônica cita-se o modelo Evoluation Pedestal, fornecido pela empresa APORTEC (APORTEC, 2012), cuja imagem é apresentada na Figura 2.19.

Figura 2.19 - Catraca eletrônica modelo Evoluation Pedestal (APORTEC, 2012)

Esse modelo de catraca apresenta as seguintes características: fluxo de pessoas bidirecional; acionamento por comunicação de dados.

2.5.1.2 Torniquetes e portas giratórias

Os torniquetes e as portas giratórias, em função do modelo, podem ser unidirecionais ou bidirecionais. Nas subseções pertinentes a esta, são apresentados exemplos de torniquetes e portas giratórias.

2.5.1.2.1 Torniquete modelo Simple Access

O torniquete modelo Simple Access é fornecido pela empresa IECO Top Security (IECO, 2012), sendo sua imagem apresentada na Figura 2.20. Esse modelo de torniquete

apresenta as seguintes características: fluxo de pessoas bidirecional; acionamento por sinais elétricos.

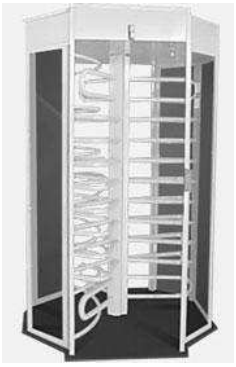

Figura 2.20 - Torniquete modelo Simple Access (IECO, 2012)

2.5.1.2.2 Porta giratória modelo Tourlock VIP

A porta giratória modelo Tourlock Vip é fornecida pela empresa IECO Top Security (IECO, 2012), sendo sua imagem apresentada na Figura 2.21. Esse modelo de porta giratória apresenta as seguintes características: fluxo de pessoas bidirecional; acionamento por sinais elétricos.

Figura 2.21 - Porta giratória modelo Tourlock Vip (IECO, 2012)

2.5.1.2.3 Torniquete modelo Double Access

O torniquete modelo Double Access é fornecido pela empresa IECO Top Security (IECO, 2012), sendo sua imagem apresentada na Figura 2.22. Esse modelo de torniquete

apresenta as seguintes características: fluxo de pessoas bidirecional; acionamento por sinais elétricos.

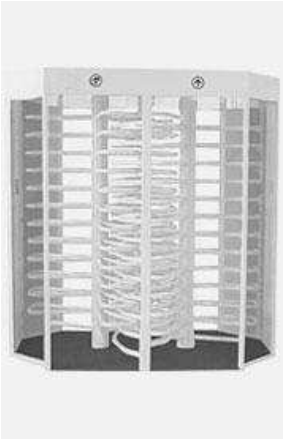

Figura 2.22 - Torniquete modelo Double Access (IECO, 2012)

2.5.1.2.4 Torniquete modelo Woltor Plus

O torniquete modelo Woltor Plus é fornecido pela empresa WOLPAC (WOLPAC, 2012), sendo sua imagem apresentada na Figura 2.23. Esse modelo de torniquete apresenta as seguintes características: fluxo de pessoas bidirecional; acionamento por comunicação de dados.

Figura 2.23 - Torniquete modelo Woltor Plus (WOLPAC, 2012)

3 PROJETO CONCEITUAL DO SiCAP

Nesta seção é apresentado o desenvolvimento do projeto conceitual do "Sistema de Controle de Acessos de Pessoas a Áreas Industriais por RFID e Biometria da Impressão Digital" (SiCAP).

3.1 ARQUITETURA DA APLICAÇÃO SiCAP-MESiCAP

O sistema de controle de acessos de pessoas a áreas industriais por RFID e biometria da impressão digital, SiCAP, é um projeto conceitual que trata da implementação do controle o acessos de pessoas a áreas industriais, com integração de recursos das identificações por radiofrequência (RFID) e biometria da impressão digital, tendo por base as diretrizes mencionadas na subseção "1.2". O SiCAP se aplica aos tipos de sistemas de controle de acessos de pessoas cuja automatização permite atender a viabilização operacional exigida para o tipo de controle em questão. Na Figura 3.1 apresenta-se a arquitetura da aplicação SiCAP-MESiCAP, na qual pode ser observada a organização para integração do SiCAP a uma variação do MESiCAP.

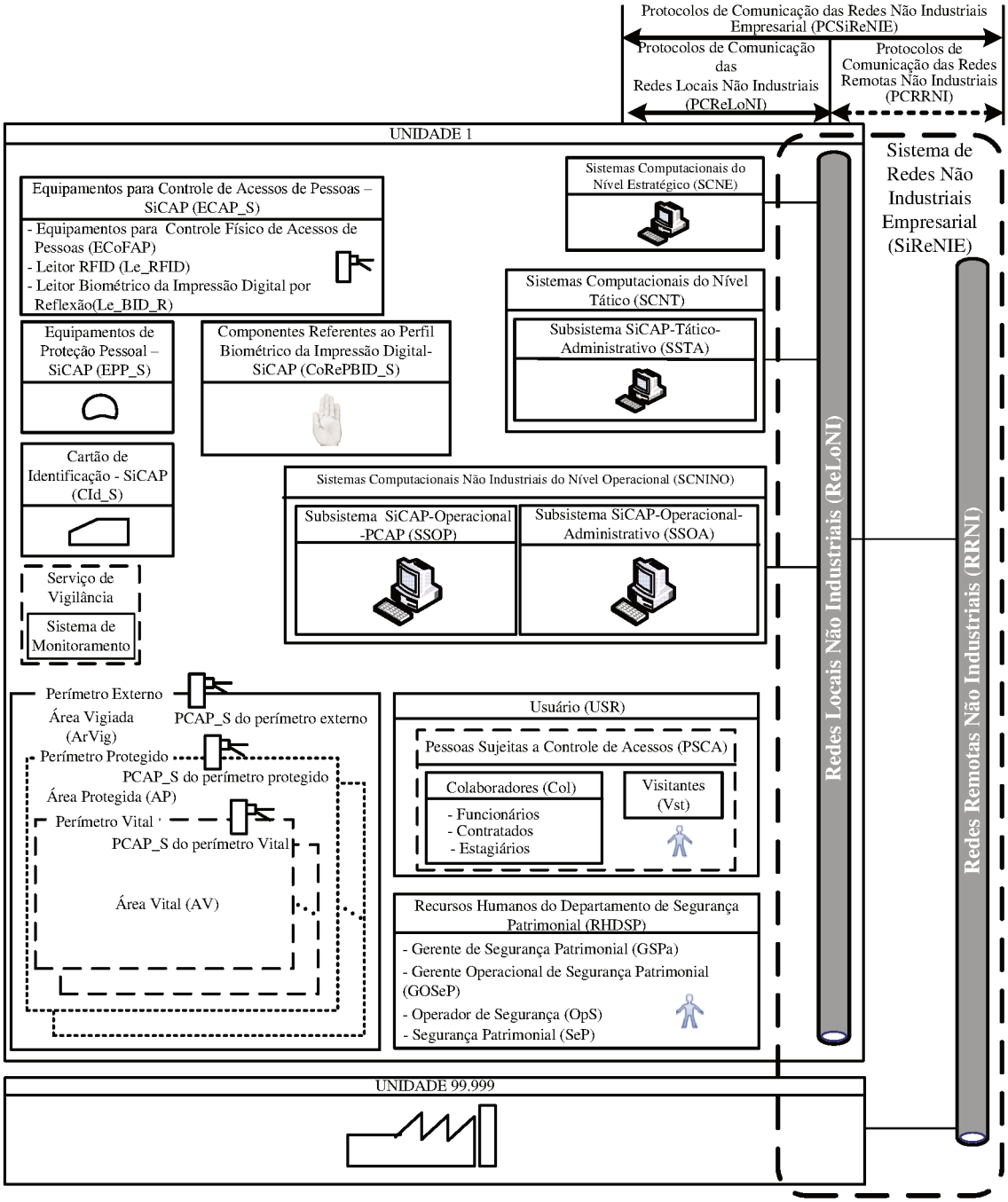

Figura 3.1 - Arquitetura da aplicação SiCAP-MESiCAP

Dos elementos existentes nessa arquitetura pertencem ao SiCAP os mencionados nos itens a seguir:

- Usuário (USR).
- Cartão de Identificação-SiCAP (CId_S).
- Componentes Referentes ao Perfil Biométrico da Impressão Digital-SiCAP (CoRePBID_S).
- Equipamentos de Proteção Pessoal-SiCAP (EPP_S).

- Equipamentos para Controle de Acessos de Pessoas-SiCAP (ECAP_S).
- Ponto de Controle de Acessos de Pessoas-SiCAP (PCAP_S).
- Subsistema SiCAP-Tático-Administrativo (SSTA).
- Subsistema SiCAP-Operacional-Administrativo (SSOA).
- Subsistema SiCAP-Operacional-PCAP (SSOP).

O subsistema tático-administrativo SSTA, possui os seguintes componentes não explicitados na Figura 3.1:

- "Sistema Gerenciador de Banco de Dados Central" (SGBD_C). Esse sistema possui os seguintes componentes: equipamento designado por "Servidor do Sistema Gerenciador de Banco de Dados Central" (SERV_SGBD_C); *softwares* designados por "Sistema Operacional de Servidor" (SO_SERV) e "Sistema Gerenciador de Banco de Dados" (SGBD); base única de dados designada por "Banco de Dados do SiCAP" (BD_SICAP).
- "Sistema de *Web Services* e Importação de Dados" (SWSID). Esse sistema possui os seguintes componentes: equipamento designado por "Servidor do Sistema de *Web Services* e Importação de Dados" (SERV_SWSID); *softwares* designados por "Sistema Operacional de Servidor" (SO_SERV), "Servidor Web HTTP" (SW_HTTP), "SICAP.MODEL", "SICAP.WEBSERVICES" e "SICAP.IMPORTAÇÃO".
- "Estação de Trabalho SICAP.AUDITORIA" (E_SICAP.AUDITORIA). Essa estação hospedará os *softwares* designados por "SICAP.AUDITORIA" e "Sistema Operacional de Cliente" (SO_CLIENTE).

O subsistema operacional-administrativo SSOA, possui os seguintes componentes não explicitados na Figura 3.1:

- "Estação de trabalho SICAP.ADMINISTRATIVO" (E_SICAP. ADMINISTRATIVO). Essa estação hospedará os *softwares* descritos no item imediatamente a seguir.
- *Softwares* designados por "SICAP.ADMINIDSTRATIVO" e "Sistema Operacional de Cliente" (SO_CLIENTE).
- "Leitor Biométrico da Impressão Digital por Reflexão" (Le_BID_R).

O subsistema operacional-PCAP SSOP, possui os seguintes componentes não explicitados na Figura 3.1:

- "Estação de trabalho SICAP.PONTOCONTROLE" (E_SICAP.PONTOCONTROLE). Essa estação hospedará os *softwares* descritos no item imediatamente a seguir.
- *Softwares* designados por "SICAP.PONTOCONTROLE" e "Sistema Operacional de Cliente" (SO_CLIENTE).

Os demais elementos que não constam nos itens anteriores, são os mesmos pertencentes ao MESiCAP, sendo acrescentado a esses o "Serviço de Vigilância", que aparece em tracejado por ser opcional nesta aplicação, entretanto, nos casos em que houver a necessidade de monitoração por imagens dos pontos de controle PCAP_S, esse sistema deverá ser empregado. Em função do exposto devem ser consideradas as descrições dos elementos em questão, realizadas nas respectivas subseções anteriores a esta.

Nas subseções a seguir, são apresentados todos os elementos do SiCAP incluindo aqueles que não constam de forma explícita na arquitetura de aplicação SiCAP-MESiCAP, tendo abrangência que chega aos elementos do MESiCAP utilizados na integração do SiCAP. Nessas subseções são definidas informações cujas variáveis possuem tipos representativos específicos, estabelecidos no âmbito do SiCAP conforme apresentado nos itens a seguir, indexados pela designação de cada tipo e seguidos da respectiva descrição:

- NR_01. É numérico e pertencente aos números inteiros, com intervalo definido pelo seguinte conjunto: $\{x \in \mathbb{Z} \mid 0 \leq x \leq 2.147.483.647\}$. Seus valores devem ser atribuídos de forma sequencial e não podem se repetir, discriminando um do outro.
- NR_02. É numérico e pertencente aos números inteiros, com intervalo definido pelo seguinte conjunto: $\{x \in \mathbb{Z} \mid 0 \leq x \leq 500\}$.
- AN_01. É alfanumérico, sendo os caracteres pertencentes ao código ASCII (*American Standard Code for Information Interchange*, Código do Padrão Americano para Troca de Informações).
- AB_01. É alfabético, sendo os caracteres pertencentes ao código ASCII.
- DI_01. É discreto, representado por Verdadeiro ou Falso.
- DT_01. É numérico para registrar data e horário, sendo utilizados 14 caracteres pertencentes ao código ASCII. Para a data são utilizados 8 caracteres como segue: dois para o dia, dois para o mês e quatro para o ano. O horário utiliza 6 caracteres

referentes ao padrão 24 horas, agrupados dois a dois, para representação de unidades de hora, minuto e segundo.

Também nessas subseções, porém, para apresentar os campos referentes às estruturas de dados do sistema em questão, serão utilizadas tabelas nas quais a definição de representação do conteúdo de cada campo é realizada por uma coluna intitulada “Tipo”, cujas descrições dos códigos lançados nas respectivas linhas é exposta no Anexo A, sendo adotado para esses códigos o padrão oriundo do Microsoft® SQL-Server™ (SQLSERVER, 2012). De forma relacionada à apresentação dessas estruturas de dados, são utilizados termos pertinentes a UML (*Unified Modeling Language*, LMU - Linguagem de Modelagem Unificada).

Tendo em vista que para funcionamento do SiCAP há a necessidade de fornecimento de energia elétrica para seus equipamentos, decorrendo nessa mesma necessidade para equipamentos do MESiCAP envolvidos com o SiCAP, serão exigidos recursos para fornecimento ininterrupto de energia elétrica para os equipamentos em questão. O tratamento para situações operacionais em caso de falta de energia elétrica, deverão ser previstos pela empresa considerando os recursos dos elementos do SiCAP envolvidos, cuja descrição é apresentada nas subseções a seguir.

3.2 ELEMENTOS DO MESiCAP UTILIZADOS PARA INTEGRAÇÃO COM O SiCAP

3.2.1 Sistemas de Redes Não Industriais Empresarial (SiReNIE)

O Sistema de Redes Não Industriais Empresarial (SiReNIE) é um recurso da empresa que será utilizado pelo SiCAP para comunicação de dados entre componentes de seus respectivos sistemas computacionais, sendo empregado, também, para integração do SiCAP aos sistemas computacionais da empresa representados no MESiCAP, por meio de comunicação de dados. Em função do exposto há a exigência de utilização de protocolo de criptografia SSL nos meios de comunicação a serem utilizados pelo SiCAP, devendo o sistema de redes SiReNIE dispor desse recurso.

3.2.2 Sistema de controle de contratados (SCCont)

Para integração do SiCAP ao MESiCAP, será considerado que a empresa possui um "Sistema de Controle de Contratados" (SCCont), ou outro assemelhado, que deverá dispor para o SiCAP, as informações sobre os recursos humanos contratados de outras empresas. Como exemplos de informações administradas por meio do sistema SCCont estão as referentes aos Fluxos B e F descritos na subseção "2.2.3.2.6". As informações requeridas para integração do SiCAP ao MESiCAP são descritas nos itens a seguir, devendo essas estar em banco de dados acessível pelo SiCAP, sendo utilizado padrão adequado. A título de exemplo de tecnologia referente a esse banco de dados, cita-se o padrão SQL-Server 2005 (SQLSERVER, 2012), que foi utilizado nos protótipos e testes práticos descritos neste trabalho.

- Código de Identificação do Contratado (CI_CON)

  O código de identificação do contratado CI_CON, é uma informação gerada pelo sistema SCCont, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária e referência cruzada de identificação do indivíduo contratado, na integração SiCAP-MESiCAP.

- Nome do Contratado (N_CON)

  O nome do contratado N_CON é uma informação adquirida por meio do sistema SCCont, que contém o nome completo individuo contratado, correspondente ao código de identificação CI_CON. A informação N_CON é representada por variável alfanumérica do tipo AN_01, sendo permitidos 50 caracteres.

3.2.3 Sistema de controle de recursos humanos (SRH)

Para integração do SiCAP ao MESiCAP, será considerado que a empresa possui um "Sistema de Controle de Recursos Humanos" (SRH), ou outro assemelhado, que deverá dispor para o SiCAP, as informações sobre os recursos humanos pertencentes a empresa, compreendidos por funcionários e estagiários. Como exemplos de informações administradas por meio do SRH estão as referentes aos Fluxos C e F descritos na subseção "2.2.3.2.6". As informações requeridas para integração do SiCAP ao MESiCAP são descritas nos itens a

seguir, devendo essas estar em banco de dados acessível pelo SiCAP, sendo utilizado padrão adequado. Como exemplo desse banco de dados cita-se o mesmo indicado na subseção "3.2.2" referente ao sistema SCCont.

- Código de Identificação do Estagiário (CI_EST)

  O código de identificação do estagiário CI_EST, é uma informação gerada pelo sistema SRH, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária e referência cruzada de identificação do indivíduo estagiário, na integração SiCAP-MESiCAP.

- Nome do Estagiário (N_EST)

  O nome do estagiário N_EST é uma informação adquirida por meio do sistema SRH, que contém o nome completo do indivíduo estagiário, correspondente ao código de identificação CI_EST. A informação N_EST é representada por variável alfanumérica do tipo AN_01, sendo permitidos 50 caracteres.

- Código de Identificação de Matrícula do Funcionário (CI_MAT)

  O código de identificação de matrícula do funcionário CI_MAT, é uma informação gerada pelo sistema SRH, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária e referência cruzada de identificação do indivíduo funcionário, na integração SiCAP-MESiCAP.

- Nome do Funcionário (N_FUN)

  O nome do funcionário N_FUN é uma informação adquirida por meio do sistema SRH, que contém o nome completo do indivíduo funcionário, correspondente ao código de identificação CI_MAT. A informação N_FUN é representada por variável alfanumérica do tipo AN_01, sendo permitidos 50 caracteres.

3.2.4 Sistema de controle de visitas (SCVis)

Para integração do SiCAP ao MESiCAP, será considerado que a empresa possui um "Sistema de Controle de Visitas" (SCVis), ou outro assemelhado, que deverá dispor para o SiCAP as informações sobre os visitantes. Como exemplos de informações administradas por meio do sistema SCVis estão as referentes aos Fluxos B e F descritos na subseção "2.2.3.2.6". As informações requeridas para integração do SiCAP ao MESiCAP são descritas nos itens a seguir, devendo essas estar em banco de dados acessível pelo SiCAP, sendo utilizado padrão

adequado. Como exemplo desse banco de dados cita-se o mesmo indicado na subseção "3.2.2" referente ao sistema SCCont.

- Código de Identificação do Visitante (CI_VIS)

  O código de identificação do visitante CI_VIS, é uma informação gerada pelo sistema SCVis, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária e referência cruzada de identificação do indivíduo visitante, na integração SiCAP-MESiCAP.

- Nome do Visitante (N_VIS)

  O nome do visitante N_VIS é uma informação adquirida por meio do sistema SCVis, que contém o nome completo do indivíduo visitante, correspondente ao código de identificação CI_VIS. A informação N_VIS é representada por variável alfanumérica do tipo AN_01, sendo permitidos 50 caracteres.

3.3 USUÁRIO (USR)

No âmbito do SiCAP definiu-se "Usuário" (USR), como qualquer indivíduo que pertença ao grupo de pessoas sujeitas ao controle de acessos PSCA, ou seja, os colaboradores (funcionários, contratados e estagiários) e os visitantes. Essa unificação é voltada para o desenvolvimento de *software*, sendo proposta uma organização na qual os dados referentes aos usuários USR sejam separados por tipo, mantendo-se a referência de sua origem, porém, relacionando-se com uma "entidade mãe", empregada para agrupá-los.

3.3.1 Informações referentes ao usuário USR

3.3.1.1 Código de identificação (CI_USR) e tipo (TI_USR) de usuário USR

O "Código de Identificação do Usuário USR" (CI_USR) é uma informação gerada automaticamente pelo SiCAP, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária de identificação do usuário USR no âmbito dos respectivos *softwares* do SiCAP.

O “Tipo de Usuário USR” (TI_USR) é uma informação definida no âmbito do SiCAP, utilizando-se um caractere para discriminar o tipo de usuário USR dentre aqueles existentes no grupo das pessoas PSCA, sendo que: F => FUNCIONÁRIO; E => ESTAGIÁRIO; C => CONTRATADO; V => VISITANTE. A informação TI_USR é representada por variável alfabética do tipo AB_01, sendo permitido 1 caractere.

3.3.1.2 Nome de usuário de rede (NURE)

O “Nome de Usuário de Rede” (NURE), *user name*, é uma informação definida pela gerência de segurança da informação GeSIn, para controle de acessos aos sistemas computacionais do MESiCAP, por meio do sistema de redes SiReNIE. No caso do SiCAP o NURE é utilizado no processo de autenticação integrado com a senha de domínio de rede existente no SiReNIE, aproveitando esse sistema de redes (definido pelo departamento de segurança da informação), que está conectado ao SiCAP. Dessa forma, o SiCAP aproveita o nome de usuário e a senha de domínio de rede, como elementos de autenticação do usuário USR. A informação NURE é representada por variável alfanumérica do tipo AN_01, sendo permitidos 50 caracteres.

3.3.1.3 Estado de habilitação (EH_USR) e motivo do bloqueio (MB_USR) do usuário USR

O “Estado de Habilitação do Usuário USR” (EH_USR) é uma informação definida no âmbito do SiCAP. O usuário USR em estado habilitado poderá utilizar o SiCAP e usufruir dos recursos proporcionados por esse sistema de controle de acessos, entretanto, o usuário USR em estado bloqueado não poderá utilizar o SiCAP, sendo impedido de usufruir dos recursos em questão. Os pedidos de habilitação ou bloqueio de usuário USR, devem ser enviados ao gerente operacional de segurança patrimonial GOSeP, que ordenará para o operador de segurança OpS a realização do estabelecimento dos respectivos estados EH_USR, entre habilitado ou bloqueado. No SiCAP esse estabelecimento é realizado por meio do *software* SICAP.ADMINISTRATIVO. A informação EH_USR é representada por variável discreta do

tipo DI_01, sendo que: Verdadeiro => Usuário USR habilitado; Falso => Usuário USR bloqueado.

O "Motivo de Bloqueio de Usuário USR" (MB_USR) é uma informação definida no âmbito do SiCAP para permitir o estabelecimento de estado de habilitação de usuário como bloqueado (EH_USR = Falso; Usuário USR bloqueado). Para esse estabelecimento de estado é necessário registrar um texto explicativo sobre o(s) motivo(s) do bloqueio, sendo esse registro realizado por informação definida para o MB_USR, inserida pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO. A informação MB_USR é representada por variável alfanumérica do tipo AN_01, sendo permitidos 255 caracteres.

3.3.2 Informações referentes à entidade USUARIO

De forma pertinente à propositura mencionada na subseção "3.3" e, seguindo o modelo de herança, definiu-se para o modelo de dados do SiCAP uma entidade designada por "USUARIO", cuja representatividade está associada a um ator que pode assumir o papel de qualquer indivíduo pertencente ao grupo de pessoas PSCA, conforme indica a organização ilustrada na Figura 3.2.

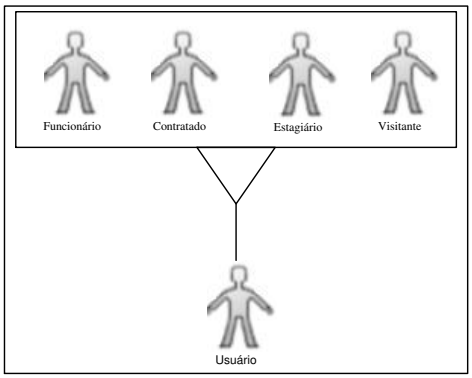

Figura 3.2 - Organização para a entidade USUARIO

Essa organização possibilitará ao SiCAP relacionar dados dos funcionários, contratados, estagiários e visitantes, com a entidade USUARIO. Para tanto, apresenta-se na Figura 3.3, sugestão de diagrama entidade relacionamento pertinente a essa organização.

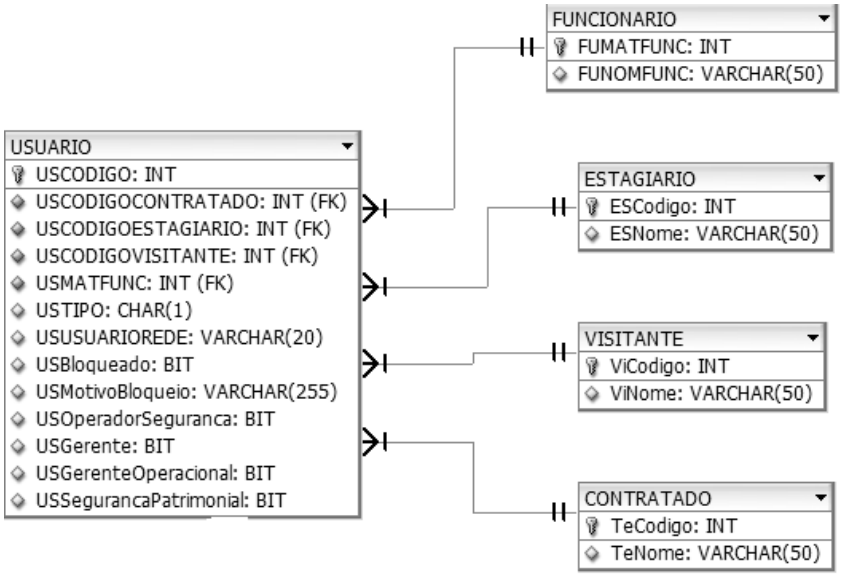

Figura 3.3 - Diagrama entidade relacionamento referente à USUARIO e PSCA

Na Tabela 3.1, são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada a entidade USUARIO.

Tabela 3.1 - Detalhes da estrutura de dados aplicada à entidade USUARIO

CAMPOS REFERENTES À ENTIDADE USUARIO		
Designação	**Tipo**	**Descrição**
USCODIGO	INT	Define o código de identificação do usuário USR, CI_USR, descrito na subseção "3.3.1.1".
USCODIGOCONTRATADO	INT	Armazena o código de identificação do contratado, CI_CON, oriundo da entidade de dados CONTRATADO (ver Tabela 3.2).
USCODIGOESTAGIARIO	INT	Armazena o código de identificação do estagiário, CI_EST, oriundo da entidade de dados ESTAGIARIO (ver Tabela 3.3).
USCODIGOVISITANTE	INT	Armazena o código de identificação do visitante, CI_VIS, oriundo da entidade de dados VISITANTE (ver Tabela 3.4).
USMATFUNC	INT	Armazena o código de identificação de matrícula do funcionário, CI_MAT, oriundo da entidade de dados FUNCIONA (ver Tabela 3.5).
USTIPO	CHAR(1)	Define o tipo de usuário USR, TI_USR (ver subseção "3.3.1.1").
USUSUARIOREDE	VARCHAR(50)	Armazena o nome de usuário de rede, NURE (ver subseção "3.3.1.2"), para autenticação integrada com a senha de domínio de rede utilizada no SiReNIE.
UsBloqueado	BIT	Define o estado de habilitação do usuário USR, EH_USR (ver subseção "3.3.1.3").
UsMotivoBloqueio	VARCHAR(255)	Armazena o motivo de bloqueio de Usuário USR, MB_USR, descrito na subseção "3.3.1.3".
USOperadorSegurança	BIT	Define "Usuário OpS". Indica que o usuário USR exerce o papel de Operador de Segurança OpS no SiCAP (ver subseção "2.2.3.1"), sendo que: Verdadeiro => Exerce papel de OpS; Falso => Não Exerce papel de OpS.
USGerente	BIT	Define "Usuário GSPa". Indica que o usuário USR exerce o papel de Gerente de Segurança Patrimonial GSPa (ver subseção "2.2.3.1") no SiCAP, sendo que: Verdadeiro => Exerce papel de GSPa; Falso => Não Exerce papel de GSPa.
USGerenteOperacional	BIT	Define "Usuário GOSeP". Indica que o usuário USR exerce o papel de Gerente Operacional de Segurança Patrimonial GOSeP (ver subseção "2.2.3.1") no SiCAP, sendo que: Verdadeiro => Exerce papel de GOSeP; Falso => Não Exerce papel de GOSeP.
USSegurancaPatrimonial	BIT	Define "Usuário SeP". Indica que o usuário USR exerce o papel de Segurança Patrimonial SeP (ver subseção "2.2.3.1") no SiCAP, sendo que: Verdadeiro => Exerce papel de SeP; Falso => Não Exerce papel de SeP.

Os campos USCODIGOCONTRATADO, USCODIGOESTAGIARIO, USCODIGOVISITANTE e USMATFUNC, são "ou exclusivos" e juntamente com o campo USTIPO, definem na entidade USUARIO a origem de cada usuário USR, que no âmbito do SiCAP será discriminado pelo código de identificação do usuário USR, CI_USR, armazenado no campo USCODIGO.

Na Tabela 3.2, são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada à entidade CONTRATADO, sendo o conteúdo desses campos importados do sistema

de controle de contratados SCCont (descrito na subseção “3.2.2”), por meio do *software* de importação descrito na subseção “3.9.3”.

Tabela 3.2 - Detalhes da estrutura de dados aplicada à entidade CONTRATADO

CAMPOS REFERENTES À ENTIDADE CONTRATADO		
Designação	**Tipo**	**Descrição**
TeCodigo	INT	Armazena o “Código de Identificação do Contratado”, CI_CON, descrito na subseção “3.2.2”.
TeNome	VARCHAR(50)	Armazena o “Nome do Contratado”, N_CON, descrito na subseção “3.2.2”.

Na Tabela 3.3, são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada à entidade ESTAGIARIO, sendo o conteúdo desses campos importados do sistema de controle de recursos humanos SRH (descrito na subseção “3.2.3”), por meio do *software* de importação descrito na subseção “3.9.3”.

Tabela 3.3 - Detalhes da estrutura de dados aplicada à entidade ESTAGIARIO

CAMPOS REFERENTES À ENTIDADE ESTAGIARIO		
Designação	**Tipo**	**Descrição**
ESCodigo	INT	Armazena o “Código de Identificação do Estagiário”, CI_EST, descrito na subseção “3.2.3”.
ESNome	VARCHAR(50)	Armazena o “Nome do Estagiário”, N_EST, descrito na subseção “3.2.3”.

Na Tabela 3.4, são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada a entidade VISITANTE, sendo o conteúdo desses campos importados do sistema de controle de visitas SCVis (descrito na subseção “3.2.4”), por meio do *software* de importação descrito na subseção “3.9.3”.

Tabela 3.4 - Detalhes da estrutura de dados aplicada à entidade VISITANTE

CAMPOS REFERENTES À ENTIDADE VISITANTE		
Designação	**Tipo**	**Descrição**
ViCodigo	INT	Armazena o “Código de Identificação do Visitante”, CI_VIS, descrito na subseção “3.2.4”.
ViNome	VARCHAR(50)	Armazena o “Nome do Visitante”, N_VIS, descrito na subseção “3.2.4”.

Na Tabela 3.5, são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada a entidade FUNCIONARIO, sendo o conteúdo desses campos importados do sistema de controle de recursos humanos SRH (descrito na subseção “3.2.3”), por meio do *software* de importação descrito na subseção “3.9.3”.

Tabela 3.5 - Detalhes da estrutura de dados aplicada à entidade FUNCIONARIO

CAMPOS REFERENTES À ENTIDADE FUNCIONARIO		
Designação	**Tipo**	**Descrição**
FUMATFUNC	INT	Armazena o "Código de Identificação de Matrícula do Funcionário", CI_MAT, descrito na subseção "3.2.3".
FUNOMFUNC	VARCHAR(50)	Armazena o "Nome do Funcionário", N_FUN, descrito na subseção "3.2.3".

3.4 CARTÃO DE IDENTIFICAÇÃO-SiCAP (CId_S)

Nas subseções pertencentes a esta, são realizadas descrições sobre o "Cartão de Identificação-SiCAP" (CId_S), para o qual é utilizada tecnologia RFID. As descrições envolvem aspectos da tecnologia empregada, de integração de sistemas, dos códigos utilizados e das estruturas relativas ao modelo de dados do SiCAP.

3.4.1 Informações referentes ao cartão de identificação CId_S

Para o cartão de identificação CId_S, será utilizado um transponder RFID do tipo cartão, *read-only*, descrito na subseção "2.4", que opera em baixa frequência e à curta distância, entretanto, limitado em até 50 *Bytes* de informações armazenadas nesse transponder, sendo utilizado o padrão ASCII para representação alfanumérica do código em seu conteúdo. No SiCAP o cartão CId_S será utilizado no processo de identificação do usuário USR, declarando sua identidade ao sistema em questão, por meio do código existente no transponder cuja entrada das respectivas informações será efetuada de forma automática no processo de leitura, aproximando-se o cartão do leitor Le_RFID, que disponibilizará as informações do transponder nos meios computacionais do SiCAP, utilizando transmissão de dados realizada através da interface de comunicação disponível no leitor.

3.4.1.1 Código do transponder no cartão CId_S (CT_CID_S)

O "Código do Transponder no Cartão CId_S" (CT_CID_S) é utilizado para registrar os *Bytes* de informação armazenadas no transponder do cartão CId_S, devendo esses *Bytes*

serem dados no padrão ASCII, para representação alfanumérica das informações no cartão CId_S. A informação CT_CID_S é representada por variável alfanumérica do tipo AN_01, sendo permitidos 50 caracteres. Essa representação possibilita utilização de cartões CId_S com até 50 *Bytes* de informação, armazenados no transponder.

Para aplicação no SiCAP, exigi-se cartões RFID com transponders cujos conteúdos armazenados sejam diferentes, estabelecendo um universo de cartões no qual não hajam transponders com dados iguais. Para impedir a utilização de cartões com os mesmos dados armazenados nos transponders, deve ser prevista no SiCAP uma sistemática que não permita o cadastramento de cartões de identificação CId_S cujos códigos armazenados nos transponders preexistam na base de dados do sistema em questão, sendo essa sistemática uma atribuição do *software* SiCAP.ADMINISTRIVO. Informa-se que para o cartão CId_S, poderão ser utilizados cartões de identificação funcional RFID preexistentes na empresa, não havendo a necessidade de cartões exclusivos para o SiCAP, desde que, atendam as especificações requeridas para funcionar nesse sistema de controle de acessos. Essa utilização permite o aproveitamento dos cartões preexistentes na empresa, contribuindo para a flexibilização da integração do SiCAP.

3.4.1.2 Código de identificação do cartão CId_S (CI_CId_S)

O "Código de Identificação do Cartão CId_S" (CI_CId_S) é uma informação gerada automaticamente pelo SiCAP, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária de identificação do cartão CId_S no âmbito dos respectivos *softwares* do SiCAP. Esse código é gerado no momento de cadastramento do cartão CId_S no SiCAP, sendo associado ao código do transponder CT_CID_S, descrito na subseção anterior. Esse cadastramento é realizado pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO.

3.4.1.3 Estado de habilitação (EH_CId_S) e motivo do bloqueio (MB_CId_S) do cartão CId_S

O "Estado de Habilitação do Cartão CId_S" (EH_CId_S) é uma informação definida no âmbito do SiCAP. O cartão CId_S em estado habilitado poderá ser utilizado no SiCAP como recurso de identificação do usuário USR, entretanto, o cartão CId_S em estado bloqueado não será aceito pelo SiCAP como recurso de identificação do usuário USR. Os pedidos de habilitação e bloqueio de cartão CId_S devem ser enviados ao gerente operacional de segurança patrimonial GOSeP, que ordenará para o operador de segurança OpS a realização do estabelecimento dos respectivos estados EH_CId_S, entre habilitado ou bloqueado. No SiCAP esse estabelecimento é realizado por meio do *software* SICAP.ADMINISTRATIVO. A informação EH_CId_S é representada por variável discreta do tipo DI_01, sendo que: Verdadeiro => cartão CId_S habilitado; Falso => cartão CId_S bloqueado.

O "Motivo de Bloqueio do Cartão CId_S" (MB_CId_S) é uma informação definida no âmbito do SiCAP para permitir o estabelecimento do estado de cartão CId_S como bloqueado (EH_CId_S = Falso). Para esse estabelecimento é necessário registrar um texto explicativo sobre o(s) motivo(s) do bloqueio, sendo o registro realizado com informação definida no MB_CId_S e inserida pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO. A informação MB_CId_S é representada por variável alfanumérica do tipo AN_01, sendo permitidos 255 caracteres.

3.4.2 Informações referentes à entidade CARTAO

Relativamente ao modelo de dados do SiCAP e de forma pertinente ao cartão CId_S, é proposta a definição de uma entidade designada por "CARTAO" cuja estrutura de dados sugerida é apresentada na Figura 3.4.

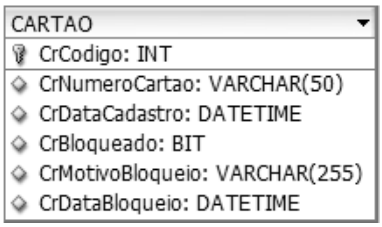

Figura 3.4 - Estrutura de dados relativa à entidade CARTAO

Na Tabela 3.6, são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada à entidade CARTAO, sendo que os conteúdos desses campos deverão ser inseridos pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO.

Tabela 3.6 - Detalhes da estrutura de dados aplicada à entidade CARTAO

CAMPOS REFERENTES À ENTIDADE CARTAO		
Designação	**Tipo**	**Descrição**
CrCodigo	INT	Define o código de identificação do cartão CId_S, CI_CId_S,descrito na subseção "3.4.1.2".
CrNumeroCartao	VARCHAR(50)	Armazena o código do transponder no cartão CId_S, CT_CID_S, descrito na subseção "3.4.1.1".
CrDataCadastro	DATETIME	Armazena a data e hora de cadastro do cartão CId_S, no SiCAP.
CrBloqueado	BIT	Define o estado de habilitação do cartão CId_S, EH_CId_S, descrito na subseção "3.4.1.3".
CrMotivoBloqueio	VARCHAR(255)	Armazena o motivo do bloqueio do cartão CId_S , MB_CId_S, descrito na subseção "3.4.1.3".
CrDataBloqueio	DATETIME	Armazena a data e hora de bloqueio do cartão CId_S, no SiCAP.

3.5 COMPONENTES REFERENTES AO PERFIL BIOMÉTRICO DA IMPRESSÃO DIGITAL-SiCAP (CoRePBID_S)

Nas subseções pertencentes a esta, são realizadas descrições sobre os "Componentes Referentes ao Perfil Biométrico da Impressão Digital-SiCAP" (CoRePBID_S), sendo que essas descrições envolvem aspectos da tecnologia empregada, de integração de sistemas, dos códigos utilizados e das estruturas relativas ao modelo de dados do SiCAP. Preliminarmente informa-se que os componentes CoRePBID_S são utilizados para integração, no SiCAP, de recursos da biometria da impressão digital, de maneira a atender as exigências desse sistema de controle de acessos, sendo inclusos nesses componentes o perfil biométrico da impressão digital disposto em meios computacionais. O perfil em questão consiste de informações biométricas da impressão digital do indivíduo, armazenadas em meios computacionais, para serem utilizadas em processo de comparação realizado por *software*. No âmbito do SiCAP

esse perfil é designado por “Perfil Biométrico da Impressão Digital do Usuário USR” (PBID_USR).

No mencionado processo de comparação, um universo de indivíduos é representado por seus perfis armazenados no sistema computacional, sendo função do *software* determinar a similaridade entre os atributos da impressão digital de um determinado indivíduo (extraídos a partir de leitura proporcionada pelo leitor biométrico da impressão digital) e aqueles armazenados no sistema computacional. No processo em questão, o indivíduo apresenta sua digital no leitor biométrico da impressão digital, sendo a extração dos atributos e a comparação realizada pelo *software*, que definirá se o processo resultou em coincidência com o perfil armazenado, ou não.

Tendo em vista que o presente trabalho inclui abordagem sobre integração de recursos da identificação por biometria da impressão digital em aplicação direcionada para sistema de controle de acessos a áreas industriais, os *softwares* do SiCAP devem ser concebidos de maneira a permitir a utilização de biblioteca específica para implementar os recursos da biometria em questão, sendo essa biblioteca fornecida por empresa que atua no segmento do mencionado tipo de biometria, dispondo de produtos com qualidade adequada às aplicações do SiCAP.

3.5.1 Descrição dos componentes referentes ao perfil biométrico da impressão digital-SiCAP

3.5.1.1 Código de identificação do perfil biométrico (CI_PB)

O “Código de Identificação do Perfil Biométrico” (CI_PB) é uma informação gerada automaticamente pelo SiCAP, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária de identificação associada ao perfil biométrico da impressão digital do usuário USR, PBID_USR (descrito na subseção “3.5.1.4”), no âmbito dos respectivos *softwares* do SiCAP. Esse código é gerado no momento de coleta do perfil biométrico do usuário USR, em seu cadastramento no SiCAP. Esse cadastramento é realizado pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO, sendo coletados três pefis PBID_USR de cada digital do usuário USR. Poderão ser incluídos no

cadastro perfis PBID_USR referentes à todas as digitais do usuário USR, entretanto, para cada perfil haverá um código CI_PB diferente.

3.5.1.2 Código de identificação da mão do usuário USR (CI_MU)

O "Código de Identificação da Mão do Usuário USR" (CI_MU), é uma informação definida no SiCAP para registrar o lado do corpo humano ao qual pertence a mão do usuário USR cujas digitais serão utilizadas no seu cadastramento. A informação CI_MU é representada por variável alfanumérica do tipo AN_01, sendo permitido 1 caractere. Para esse caractere: "D" => mão direita; "E" => mão esquerda. A definição do CI_MU é realizada pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO, no processo de cadastramento do usuário USR.

3.5.1.3 Código de identificação do dedo do usuário USR (CI_DU)

O "Código de Identificação do Dedo do Usuário USR" (CI_DU), é uma informação definida no SiCAP para registrar o dedo pertencente a mão definida pelo código CI_MU, cujas digitais serão utilizadas no respectivo cadastramento do usuário USR. A informação CI_DU é representada por variável alfanumérica do tipo AN_01, sendo permitido 1 caractere. Para esse caractere: A => Dedo Anelar; I => Dedo Indicador; M => Dedo Médio; N => Dedo Mínimo; P => Dedo Polegar. A definição do CI_DU é realizada pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO, no processo de cadastramento do usuário USR.

3.5.1.4 Perfil biométrico da impressão digital do usuário USR (PBID_USR)

O "Perfil Biométrico da Impressão Digital do Usuário USR" (PBID_USR) é uma informação que representa, no SiCAP, o *hash* gerado pela biblioteca de *software* específica utilizada para implementar os recursos da biometria da impressão digital exigidos pelo

sistema em questão. A informação PBID_USR é representada por variável alfanumérica do tipo AN_01, sendo permitidos 255 caracteres.

O perfil PBID_USR é armazenado na base de dados do SiCAP para finalidades de cadastramento referentes ao usuário USR e, também, utilizado em processo de comparação (pertinente ao descrito na subseção "3.5") realizado por *software* desse sistema. No SiCAP são armazenados três PBID_USR para cada digital do usuário USR, conforme descrito na subseção "3.5.1.1", visando diminuir a FRR. O armazenamento do perfil PBID_USR pode ocorrer nas seguintes situações: inicialmente, como exigência para cadastramento do usuário USR no SiCAP; periodicamente em função do vencimento do prazo de validade para o perfil em questão, obrigando o recadastramento do usuário USR; eventualmente, em função de deformidades ou perda das digitais.

Os perfis PBID_USR de todos os usuários USR representam o universo a ser utilizado no processo de comparação para determinação de similaridade entre os atributos da impressão digital de um indivíduo (extraídos a partir de leitura proporcionada pelo leitor Le_BID_R) e aqueles referentes ao universo em questão, armazenados no SiCAP. Nesse processo o usuário USR apresenta sua digital no leitor Le_BID_R, sendo a extração dos atributos e a comparação realizadas por *software* do SiCAP, que definirá se o processo resultou em coincidência com o perfil armazenado, ou não. No SiCAP, os *softwares* que incluem rotinas para essa comparação são os seguintes: SICAP.PONTOCONTROLE (pertencente ao subsistema SSOP); SICAP.ADMINISTRATIVO (pertencente ao subsistema SSOA).

3.5.1.5 Referência cronológica de cadastro do perfil biométrico da impressão digital do usuário USR (RC_PBID_USR)

A "Referência Cronológica de Cadastro do Perfil Biométrico da Impressão Digital do Usuário USR" (RC_PBID_USR), é um informação do SiCAP que permite registrar a data e o horário de cadastramento ou recadastramento do perfil PBID_USR, em função das situações descritas na subseção "3.5.1.4". Essa referência representa o início do prazo de validade do perfil PBID_USR, cujo tempo e o vencimento são abordados na subseção "3.5.1.6". A informação RC_PBID_USR é representada por variável numérica do tipo DT_01.

3.5.1.6 Vencimento do perfil biométrico da Impressão Digital do Usuário USR (V_PBID_USR)

O "Vencimento do Perfil Biométrico da Impressão Digital do Usuário USR" (V_PBID_USR), é uma informação do SiCAP que permite registrar a data e o horário de vencimento do prazo de validade do perfil PBID_USR, do respectivo usuário USR. O SiCAP deverá dispor de recurso para definir o tempo do prazo de validade do perfil PBID_USR, sendo o vencimento V_PBID_USR calculado automaticamente pelos *softwares* do SiCAP nas situações descritas na subseção "3.5.1.4". O tempo do prazo de validade do perfil PBID_USR deve ser definido pela gerência de segurança patrimonial GeSPa, entretanto, sugere-se que seja de 5 (cinco) anos. A informação V_PBID_USR é representada por variável numérica do tipo DT_01.

3.5.2 Informações referentes à entidade HASHDIGITAL

Relativamente ao modelo de dados do SiCAP e, de forma pertinente aos componentes referentes ao perfil biométrico da Impressão digital CoRePBID_S, é proposta a definição de uma entidade designada por "HASDIGITAL" cuja estrutura de dados sugerida é apresentada na Figura 3.5.

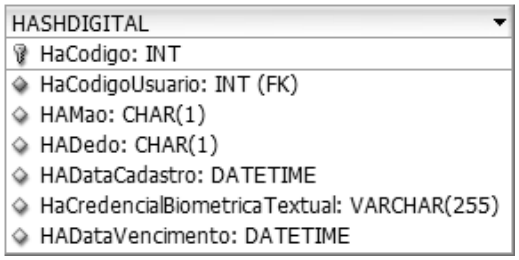

Figura 3.5 - Estrutura de dados relativa à entidade HASDIGITAL

Na Tabela 3.7, são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada a entidade HASHDIGITAL, sendo que os conteúdos desses campos utilizados pelos *softwares*: SICAP.ADMINISTRATIVO; SICAP.PONTOCONTROLE.

Tabela 3.7 - Detalhes da estrutura de dados aplicada à entidade HASHDIGITAL

CAMPOS REFERENTES À ENTIDADE HASHDIGITAL		
Designação	**Tipo**	**Descrição**
HACodigo	INT	Define o código de identificação do perfil biométrico, CI_PB, descrito na subseção "3.5.1.1".
HACodigoUsuario	INT	Armazena o código de identificação do usuário USR, CI_USR, oriundo da entidade USUARIO (ver Tabela 3.1).
HAMao	CHAR(1)	Define o código de identificação da mão do usuário USR, CI_MU, descrito na subseção "3.5.1.2".
HADedo	CHAR(1)	Define o código de identificação do dedo do usuário USR, CI_DU, descrito na subseção "3.5.1.3".
HADataCadastro	DATETIME	Define a data e o horário da referência cronológica de cadastro do perfil biométrico da impressão digital do usuário USR, RC_PBID_USR, descrito na subseção "3.5.1.5".
HACredencialBiometricaTextual	VARCHAR(255)	Armazena o perfil biométrico da impressão digital do usuário USR, PBID_USR, descrito na subseção "3.5.1.4".
HADataVencimento	DATETIME	Define a data e o horário do vencimento do perfil biométrico da impressão digital do usuário USR, V_PBID_USR, descrito na subseção "3.5.1.6".

3.6 EQUIPAMENTOS DE PROTEÇÃO PESSOAL–SiCAP (EPP_S)

Na concepção do SiCAP foi prevista a possibilidade dos equipamentos de proteção pessoal EPP possuírem transponder RFID integrado, de forma a individualizar cada unidade e associá-la ao respectivo usuário USR, permitindo exigir desse usuário a apresentação dos respectivos equipamentos de segurança nos pontos de controle PCAP_S, como condicionante para estabelecer a autorização de acessos as áreas industriais de segurança que têm direito. Em função dessa concepção os equipamentos de proteção pessoal EPP utilizados no SiCAP foram designados por "Equipamentos de Proteção Pessoal - SiCAP" (EPP_S).

O SiCAP permite que o mencionado condicionante seja programável por meio do *software* SICAP.ADMINISTRATIVO, dentre as opções de inspeção apresentadas nos itens a seguir:

- Inspeção 100% de EPP_S: Será exigida de todos os usuários USR a leitura dos transponders RFID de seus respectivos equipamentos de proteção pessoal EPP_S, requeridos para autorização de acessos às áreas industriais de segurança, nos respectivos PCAP_S.

- Inspeção Aleatória de EPP_S: Será exigida, de forma aleatória, para uma determinada quantidade de usuários USR, a leitura dos transponders RFID de seus respectivos equipamentos de proteção pessoal EPP_S, requeridos para autorização de acessos às áreas industriais de segurança, nos respectivos PCAP_S. Essa inspeção deverá ser realizada em função da ordem de chegada dos usuários USR previstos para transitar pelo PCAP_S, sendo escolhidos números ordinais de forma aleatória, para cada dia de expediente. Em função do exposto, para cada PCAP_S, deverá ser definido o número máximo de usuários USR previstos para trafegar, bem como, a quantidade desses usuários a serem inspecionados, sendo essas definições realizadas pelo gerente de segurança patrimonial GSPa, que ordenará ao operador de segurança OpS o estabelecimento por meio do *software* SICAP.ADMINISTRATIVO. Um algoritmo para definição da lista ordinal de inspeção aleatória de EPP_S é proposto a seguir, nesta subseção.
- Sem Inspeção de EPP_S: Não será exigida dos usuários USR a leitura dos transponders RFID de seus respectivos equipamentos de proteção pessoal EPP_S, requeridos para autorização de acessos às áreas industriais de segurança, nos respectivos PCAP_S, ocorrendo o processo de autorização sem a exigência de inspeção de EPP_S.

Para apresentar a proposição de algoritmo de definição da lista ordinal para inspeção aleatória de EPP_S, será utilizado o fluxograma analítico exposto na Figura 3.6. Esse algoritmo exige números randômicos entre 1 (um) e o máximo de usuários USR (variável "MAX_USR" no fluxograma) previsto para trânsito no PCAP_S e, também, a quantidade de usuários a serem inspecionados (variável "QTD_USR" no fluxograma). Na figura em questão pode ser observado como é definida a lista ordinal (variável "oLista" no fluxograma) dos usuários USR a serem inspecionados, por meio dos respectivos números entre um e o número máximo de usuários USR (inclusive), referentes à ordem de chegada no PCAP_S.

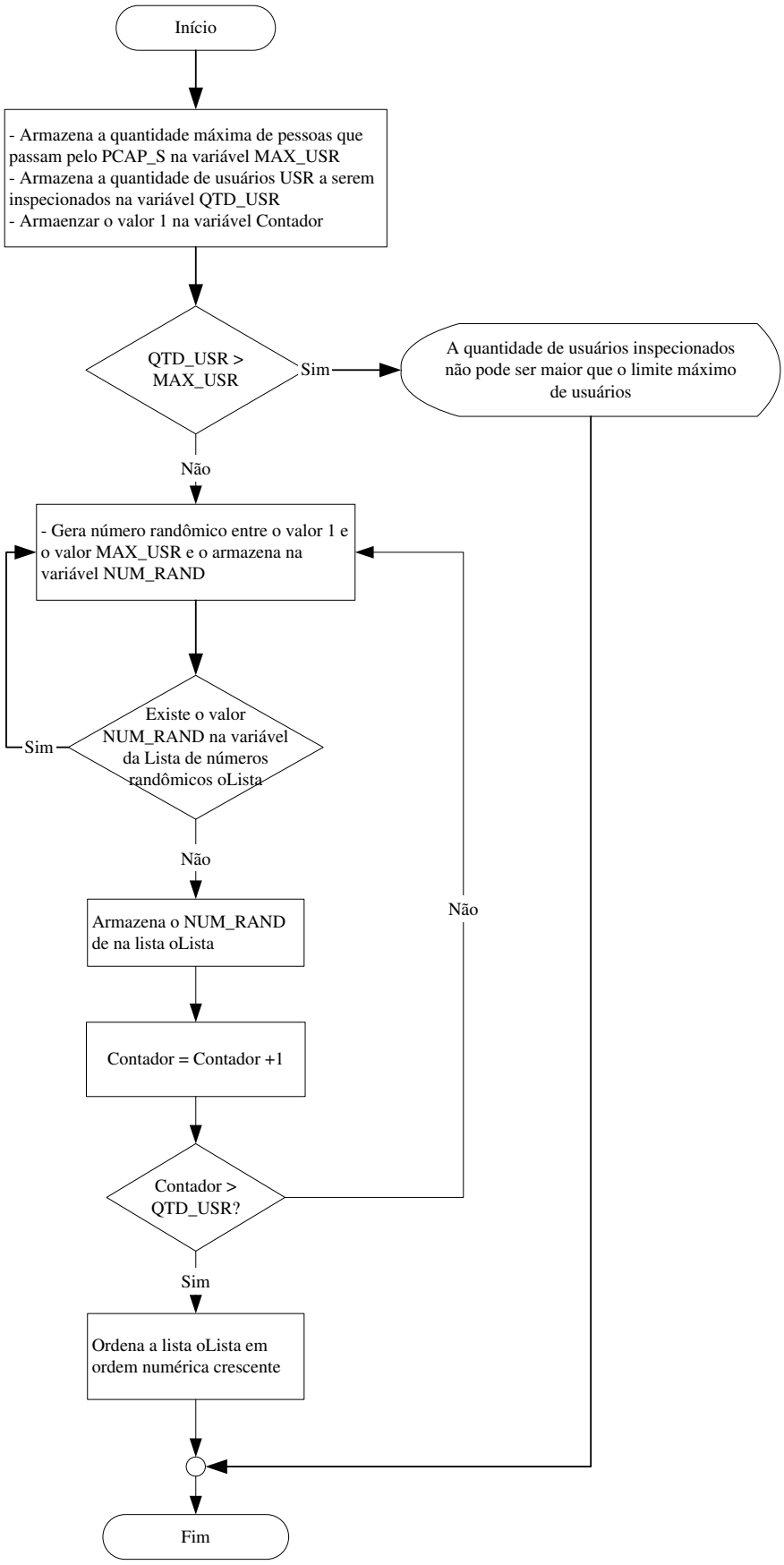

Figura 3.6 - Fluxograma analítico do algoritmo de definição da lista ordinal para inspeção aleatória de EPP_S

3.6.1 Informações referentes aos EPP_S

3.6.1.1 Código de identificação do tipo de equipamento EPP_S (CI_T_EPP_S)

O "Código de Identificação do Tipo de Equipamento EPP_S" (CI_T_EPP_S) é uma informação gerada automaticamente pelo SiCAP, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária de identificação do tipo de equipamento EPP_S no âmbito dos respectivos *softwares* do SiCAP que empregam o conjunto desses tipos para classificar todos os equipamentos de proteção pessoal EPP_S. Esse código é gerado no momento de cadastramento do tipo de equipamento EPP_S no SiCAP. O cadastramento em questão é realizado pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO.

3.6.1.2 Descrição do tipo de equipamento EPP_S (DE_T_EPP_S)

A "Descrição do Tipo de Equipamento EPP_S" (DE_T_EPP_S) é informação do SiCAP que corresponde a um texto associado ao respectivo código de identificação de EPP_S, CI_T_EPP_S, que designa o tipo de equipamento em questão (exemplos: capacete, protetor auricular, dosímetro etc.). Esse texto é definido pela gerência de segurança de pessoal GeSPe, e inserido no SiCAP pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO, como parte das exigências para cadastramento dos tipos de equipamento EPP_S. A informação DE_T_EPP_S é representada por variável alfanumérica do tipo AN_01, sendo permitidos 50 caracteres.

3.6.1.3 Código do transponder no equipamento EPP_S (CT_EPP_S)

O "Código do Transponder no Equipamento de Proteção Pessoal EPP_S" (CT_EPP_S) é informação do SiCAP que contém os valores dos *Bytes* armazenados no transponder integrado ao equipamento de proteção pessoal EPP_S, devendo esses *Bytes* serem

dados no padrão ASCII para representação alfanumérica das informações no EPP_S. A informação CT_EPP_S é representada por variável alfanumérica do tipo AN_01, sendo permitidos 50 caracteres. Essa representação de dados possibilita utilização de equipamentos de proteção pessoal EPP_S com até 50 *Bytes* de informação, armazenados no transponder.

3.6.1.4 Código de identificação do equipamento EPP_S (CI_EPP_S)

O "Código de Identificação do Equipamento EPP_S" (CI_EPP_S), é uma informação gerada automaticamente pelo SiCAP, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária de identificação e individualização de cada equipamento EPP_S no âmbito dos respectivos *softwares* do SiCAP. Esse código é gerado no momento de cadastramento da unidade de equipamento de proteção EPP_S no SiCAP, sendo associado ao código em questão o código do transponder CT_EPP_S, armazenado na respectiva unidade RFID integrada no EPP_S. Esse cadastramento é realizado pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO.

Para aplicação no SiCAP exigem-se unidades de RFID integradas ao EPP_S, com transponders cujos conteúdos armazenados sejam diferentes, estabelecendo um universo no qual não haja transponders com dados iguais. Para impedir a utilização de unidades de RFID integradas a EPP_S, com os mesmos dados armazenados nos transponders, deve ser prevista no SiCAP uma sistemática que não permita o cadastramento de equipamentos EPP_S cujos códigos armazenados nos transponders preexistam na base de dados do sistema em questão, sendo essa sistemática uma atribuição do *software* SICAP.ADMINISTRIVO.

3.6.1.5 Código de identificação da associação do equipamento EPP_S ao usuário USR (CI_EPP_S_USR)

O "Código de Identificação da Associação do Equipamento EPP_S ao Usuário USR" (CI_EPP_S_USR) é uma informação gerada automaticamente pelo SiCAP, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária de identificação da associação do equipamento EPP_S ao usuário USR, no âmbito dos respectivos *softwares* do SiCAP. Esse código é gerado no momento da associação do

equipamento EPP_S ao usuário USR, no SiCAP. Essa associação é realizada pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO, quando da entrega do equipamento EPP_S para o usuário USR.

3.6.1.6 Limite inicial (LI_EPP_S) e final (LF_EPP_S) de permissão para utilização do EPP_S pelo usuário USR

O "Limite Inicial de Permissão para Utilização do EPP_S pelo Usuário USR" (LI_EPP_S) e o "Limite Final de Permissão para Utilização do EPP_S pelo Usuário USR" (LF_EPP_S), são informações do SiCAP e têm por principal função registrar o prazo de validade associado ao equipamento de proteção pessoal EPP_S, proporcionando dados para impedir o uso fora do prazo em questão. Além dessa restrição de uso, os limites LI_EPP_S e LF_EPP_S, permitem atender outras situações de desuso do EPP_S, como aquelas referentes a: danificação; sinistro; perda; não atendimento a normativas. As informações LI_EPP_S e LF_EPP_S, são representadas por variável numérica do tipo DT_01.

O limite inicial LI_EPP_S permite registrar data e horário, sendo essas informações cronológicas correspondentes ao momento de entrega do equipamento EPP_S ao usuário USR, realizada pelo operador de segurança OpS. Esse operador registra as informações cronológicas no SiCAP por meio do *software* SICAP.ADMINISTRATIVO.

O limite final LF_EPP_S permite registrar data e horário, sendo essas informações lançadas pelo operador de segurança OpS em função das situações descritas anteriormente. Esse lançamento é realizado por meio do *software* SICAP.ADMINISTRATIVO.

3.6.2 Informações referentes às entidades pertinentes aos EPP_S

Relativamente ao modelo de dados do SiCAP e de forma pertinente aos equipamentos de proteção EPP_S, é proposta a definição das entidades designadas por "TIPOEQUIPAMENTO", "EQUIPAMENTO" e "EQUIPUSUARIO", cuja sugestão de diagrama entidade relacionamento é apresentada na Figura 3.7.

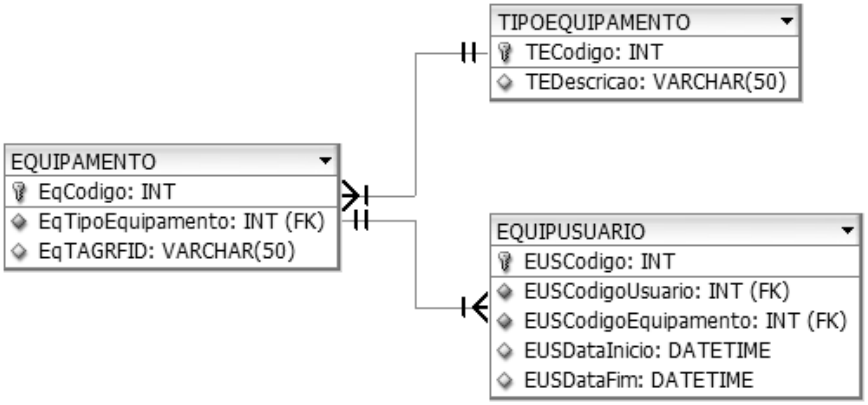

Figura 3.7 - Diagrama de entidade relacionamento referente aos EPP_S

Na Tabela 3.8, são apresentados detalhes dos campos pertencentes a estrutura de dados aplicada a entidade TIPOEQUIPAMENTO, utilizada para cadastramento do conjunto de tipos de equipamentos EPP_S.

Tabela 3.8 - Detalhes da estrutura de dados aplicada à entidade TIPOEQUIPAMENTO

CAMPOS REFERENTES À ENTIDADE TIPOEQUIPAMENTO		
Designação	**Tipo**	**Descrição**
TECodigo	INT	Define o código de identificação do tipo de equipamento EPP_S, CI_T_EPP_S, descrito na subseção “3.6.1.1”.
TEDescricao	VARCHAR(50)	Define a descrição do tipo de equipamento EPP_S , DE_T_EPP_S, abordada na subseção “3.6.1.2”.

Na Tabela 3.9, são apresentados detalhes dos campos existentes na estrutura de dados aplicada a entidade EQUIPAMENTO, que é destinada para cadastramento dos equipamentos EPP_S pertencentes à empresa e utilizados no SiCAP.

Tabela 3.9 - Detalhes da estrutura de dados aplicada à entidade EQUIPAMENTO

CAMPOS REFERENTES À ENTIDADE EQUIPAMENTO		
Designação	**Tipo**	**Descrição**
EqCodigo	INT	Define o código de identificação do equipamento EPP_S, CI_EPP_S, descrito na subseção “3.6.1.4”.
EqTipoEquipamento	INT	Armazena o código de identificação do tipo de equipamento EPP_S, CI_T_EPP_S, oriundo da entidade TIPOEQUIPAMENTO (ver Tabela 3.8).
EqTAGRFID	VARCHAR(50)	Armazena o código do transponder no equipamento EPP_S, CT_EPP_S, descrito na subseção “3.6.1.3”.

Na Tabela 3.10, são apresentados detalhes dos campos pertencentes a estrutura de dados aplicada à entidade EQUIPUSUARIO, utilizada para armazenar os dados que associam os equipamentos de proteção pessoal EPP_S aos usuários USR. Essa associação é realizada pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO.

Tabela 3.10 - Detalhes da estrutura de dados aplicada a entidade EQUIPUSUARIO

CAMPOS REFERENTES À ENTIDADE EQUIPUSUARIO		
Designação	**Tipo**	**Descrição**
EUSCodigo	INT	Define o código de identificação da associação do equipamento EPP_S ao usuário USR, CI_EPP_S_USR, descrito na subseção "3.6.1.5".
EUSCodigoUsuario	INT	Armazena o código de identificação do usuário USR, CI_USR, oriundo da entidade USUARIO (ver Tabela 3.1)
EUSCodigoEquipamento	INT	Armazena o código de identificação do equipamento EPP_S, CI_EPP_S, oriundo da entidade EQUIPAMENTO (ver Tabela 3.8).
EUSDataInicio	DATETIME	Armazena a data e hora do limite inicial de permissão para utilização do EPP_S pelo usuário USR, LI_EPP_S, descrito na subseção "3.6.1.6".
EUSDataFim	DATETIME	Armazena a data e hora do limite final de permissão para utilização do EPP_S pelo usuário USR, LF_EPP_S, descrito na subseção "3.6.1.6".

3.7 EQUIPAMENTOS PARA CONTROLE DE ACESSOS DE PESSOAS-SiCAP (ECAP_S)

3.7.1 Equipamentos para controle físico de acessos de pessoas (ECoFAP)

No SiCAP os "Equipamentos para Controle Físico de Acessos de Pessoas" (ECoFAP) são dos mesmos tipos descritos na subseção "2.5", entretanto, as definições de modelos e fabricantes devem ser realizadas pelo gerente de segurança patrimonial GSPa, em função das necessidades de aplicação pertinentes aos PCAP_S nos quais serão instalados, sendo previstas as compatibilidades para integração ao subsistema operacional-PCAP SSOP.

3.7.2 Leitor RFID (Le_RFID)

No SiCAP o Leitor RFID (Le_RFID) poderá ser dos mesmos tipos descritos na subseção "2.4.2", entretanto, a definição de modelo e fabricante deve ser realizada pelo gerente de segurança patrimonial GSPa, em função das necessidades de aplicação pertinentes ao PCAP_S no qual será instalado, sendo previstas as compatibilidades para integração com os subsistemas operacional-PCAP SSOP e operacional-administrativo SSOA. Recomenda-se a utilização de um modelo de Le_RFID do tipo portátil, porém, fixado a estrutura predial do

PCAP_S por meio de cordão, haja vista que poderá ser utilizado tanto para a leitura do cartão de identificação CId_S, quanto para a leitura do equipamento de proteção pessoal EPP_S, sendo possível a movimentação para aproximação de EPP_S que não pode chegar ao leitor.

3.7.3 Leitor biométrico da impressão digital por reflexão (Le_BID_R)

No SiCAP, o "Leitor Biométrico da Impressão Digital por Reflexão" (Le_BID_R) poderá ser do mesmo tipo descrito na subseção "2.3.3", entretanto, a definição de modelo e fabricante deve ser realizada pelo gerente de segurança patrimonial GSPa, em função das necessidades de aplicação pertinentes ao PCAP_S no qual será instalado, sendo previstas as compatibilidades para integração com os subsistemas operacional-PCAP SSOP e operacional-administrativo SSOA.

3.8 PONTO DE CONTROLE DE ACESSOS DE PESSOAS-SiCAP (PCAP_S)

O "Ponto de Controle de Acessos de Pessoas–SiCAP" (PCAP_S) é um tipo de PCAP restrito aos elementos expostos na arquitetura da aplicação SiCAP-MESiCAP (Figura 3.1), com especial destaque a peculiaridade do tipo de controle de acessos concebido para o SiCAP, que prevê, além dos requisitos de apresentação de elementos pessoais pertinentes à identificação das pessoas, outro, que requer a apresentação de equipamentos de segurança necessários para o exercício das atividades dessas pessoas. No PCAP_S são instalados os equipamentos para controle de acessos ECAP_S e aqueles referentes ao subsistema operacional-PCAP SSOP, que controlam os equipamentos ECAP_S. Embora o Sistema de Monitoramento não seja parte do SiCAP, seus componentes como câmeras de vídeo e sensores, podem ser instalados no PCAP_S para atender a opção de utilização do Serviço de Vigilância. Da mesma forma poderão ser instalados os equipamentos do tipo vídeo porteiro eletrônico, quando necessários para permitir operações no PCAP_S.

3.8.1 Informações referentes ao ponto de controle de acessos de pessoas PCAP_S

3.8.1.1 Nomenclatura do PCAP_S (No_PCAP_S)

Para a informação de "Nomenclatura do PCAP_S" (No_PCAP_S), definiu-se um padrão cuja estrutura é composta por duas regiões separadas por um traço curto, sendo uma denominada "Prefixo" e a outra "Designação", conforme organização exposta na Tabela 3.11. O "Prefixo" é formado por dois caracteres cuja codificação é apresentada na tabela em questão, tendo por propósito indicar a classificação da área industrial interna ao perímetro associada ao PCAP_S, sendo utilizadas as classes designadas por área vigiada, área protegida e área vital. A "Designação" é formada por 47 (quarenta e sete) caracteres, sendo esses de livre arbítrio para representação da nomenclatura da área interna associada ao PCAP_S, que deverá ser definida pelo gerente de segurança patrimonial GSPa, sob o condicionante de não haver nomenclaturas iguais.

Tabela 3.11 - Informações sobre a estrutura para nomenclatura dos PCAP_S

ESTRUTURA PARA NOMENCLATURA DOS PCAP_S		
"Prefixo" (2 caracteres)	**–**	**"Designação"** (47 caracteres)
CÓDIGIOS DA REGIÃO "Prefixo"		
Caracteres	**Descrição**	
AG	Prefixo de PCAP_S associado a uma área vigiada. Exemplo: AG–Empresa XYZ	
AP	Prefixo de PCAP_S associado a uma área protegida. Exemplo: AP–Unidade Fabril Principal.	
AV	Prefixo de PCAP_S associado a uma área vital. Exemplo: AV–Usinagem.	

A informação No_PCAP_S é representada por variável alfanumérica do tipo AN_01, sendo permitidos 50 caracteres.

3.8.1.2 Código de identificação do PCAP_S (CI_PCAP_S)

O "Código de Identificação do PCAP_S" (CI_PCAP_S) é uma informação gerada automaticamente pelo SiCAP, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária de identificação do PCAP_S no âmbito dos respectivos

softwares do SiCAP. Esse código é gerado no momento de cadastramento do PCAP_S no SiCAP. Esse cadastramento é realizado pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO.

3.8.1.3 Tipo de sentido de fluxo no PCAP_S (TSF_PCAP_S)

O "Tipo de Sentido de Fluxo no PCAP_S" (TSF_PCAP_S) é uma informação definida no âmbito do SiCAP, pelo gerente de segurança patrimonial GSPa, para identificar e estabelecer o tipo de sentido de fluxo permitido para o trânsito de pessoas no PCAP_S. Essa informação é decorrente do planejamento de configuração dos PCAP_S, realizado pelo gerente de segurança patrimonial GSPa, para atender as necessidades de controle de acessos de pessoas, requeridas pela empresa. Assim sendo, deve ser compatível com as instalações físicas do PCAP_S, que envolvem elementos prediais, de equipamentos e de recursos humanos.

O SiCAP prevê três tipos de sentido de fluxo permitidos para o trânsito de pessoas no PCAP_S, sendo dois unidirecionais e um bidirecional, com relação a área interna associada ao ponto de controle em questão. A representação desses tipos e suas descrições são expostas nos itens a seguir. Para representação dos tipos é utilizado um caractere, que indexa os itens em questão.

- E => fluxo somente no sentido de entrada para a área interna associada ao PCAP_S.
- S => fluxo somente no sentido de saída da área interna associada ao PCAP_S.
- A => fluxos nos sentidos de entrada e saída, para a área interna associada ao PCAP_S.

Tendo em vista o exposto, a informação TSF_PCAP_S é representada por variável alfabética do tipo AB_01, sendo permitido 1 caractere. Em função dos tipos de sentidos de fluxo TSF_PCAP_S e dos equipamentos para controle físico de acesso de pessoas ECoFAP, o SiCAP possui quatro possibilidades de organização do PCAP_S cuja apresentação é realizada nas respectivas subseções a seguir.

3.8.1.3.1 PCAP_S unidirecional com ECoFAP unidirecional de entrada

O PCAP_S unidirecional com ECoFAP unidirecional de entrada, permite fluxo somente no sentido de entrada para a área interna associada ao PCAP_S (TSF_PCAP_S = E), sendo sua organização apresentada na Figura 3.8.

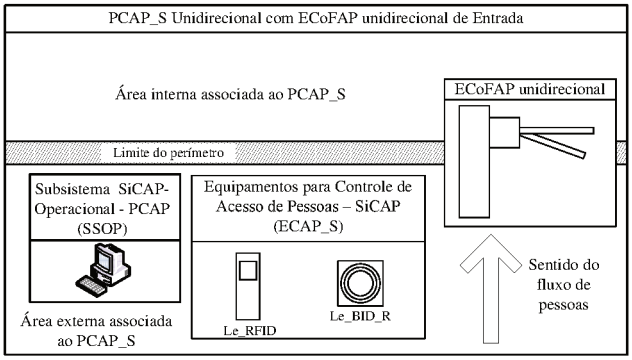

Figura 3.8 - PCAP_S unidirecional com ECoFAP unidirecional de entrada

3.8.1.3.2 PCAP_S unidirecional com ECoFAP unidirecional de saída

O PCAP_S unidirecional com ECoFAP unidirecional de saída, permite fluxo somente no sentido de saída da área interna associada ao PCAP_S (TSF_PCAP_S = S), sendo sua organização apresentada na Figura 3.9.

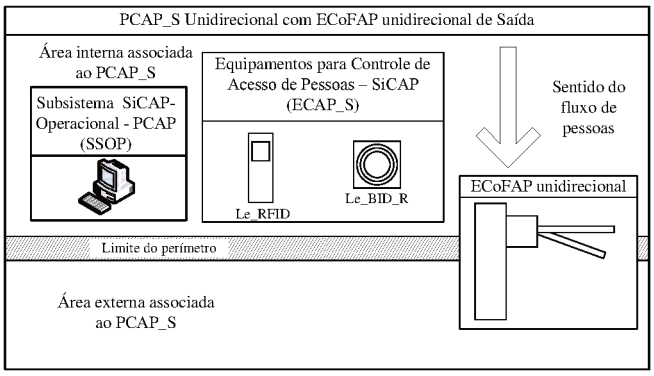

Figura 3.9 - PCAP_S unidirecional com ECoFAP unidirecional de saída

3.8.1.3.3 PCAP_S bidirecional com ECoFAP bidirecional

O PCAP_S bidirecional com ECoFAP bidirecional, permite fluxos nos sentidos de entrada e saída, para a área interna associada ao PCAP_S (TSF_PCAP_S = A), sendo sua organização apresentada na Figura 3.10.

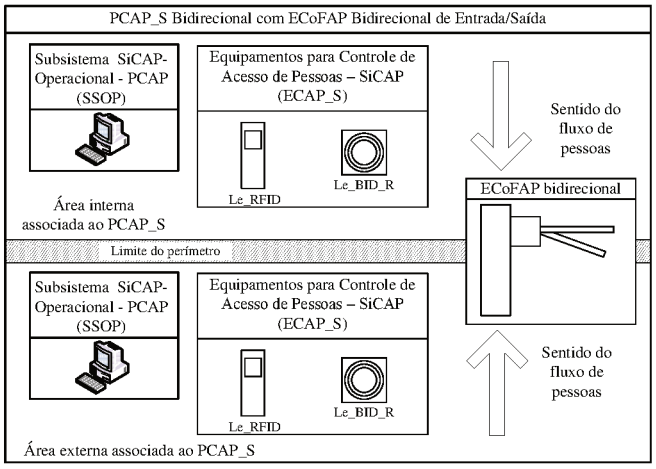

Figura 3.10 - PCAP_S bidirecional com ECoFAP bidirecional

3.8.1.3.4 PCAP_S bidirecional com ECoFAP unidirecional

O PCAP_S bidirecional com ECoFAP unidirecional, permite fluxos nos sentidos de entrada e saída, para a área interna associada ao PCAP_S (TSF_PCAP_S = A), sendo sua organização apresentada na Figura 3.11.

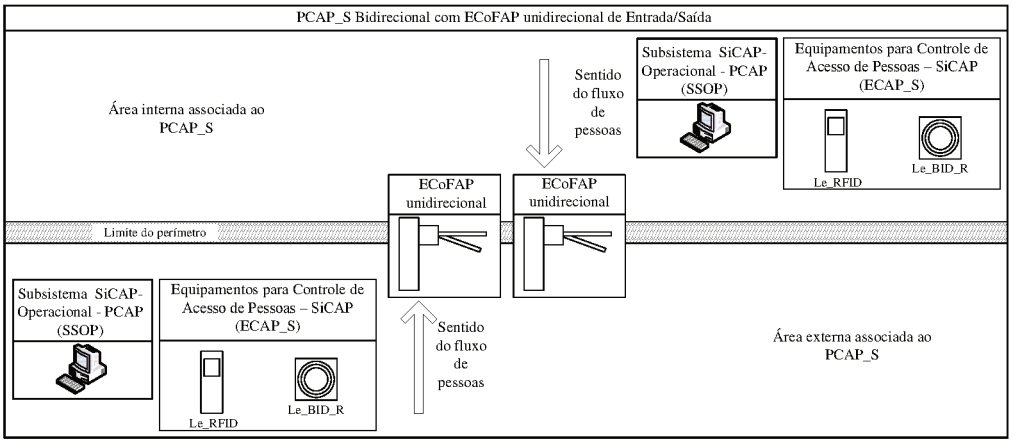

Figura 3.11 - PCAP_S bidirecional com ECoFAP unidirecional de entrada/saída

3.8.1.4 Obrigatoriedade de identificação por cartão CId_S (OI_CId_S)

A “Obrigatoriedade de Identificação por Cartão CId_S” (OI_CId_S) é uma informação definida no âmbito do SiCAP pelo gerente de segurança patrimonial GSPa e estabelecida pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO. A informação OI_CId_S é representada por variável discreta do tipo DI_01, sendo que: Verdadeiro => Obrigatória a identificação por Cartão CId_S; Falso => Não obrigatória a identificação por Cartão CId_S.

Se a variável referente a obrigatoriedade OI_CId_S for definida como Verdadeiro, será exigida a leitura do cartão CId_S, decorrendo na imposição do uso do leitor Le_RFID. Para essa condição, o processo de autenticação deverá ser realizado por biometria de impressão digital e/ou pela senha de domínio de rede. Se a variável referente à obrigatoriedade OI_CId_S for definida como Falso, decorrerá na dispensa de uso do leitor Le_RFID, sendo o processo de identificação realizado por meio do leitor biométrico Le_BID_R.

3.8.1.5 Obrigatoriedade de biometria da impressão digital com relação à identificação e autenticação (OBID_IA)

A “Obrigatoriedade de Biometria da Impressão Digital com Relação à Identificação e Autenticação” (OBID_IA) é uma informação definida no âmbito do SiCAP pelo gerente de segurança patrimonial GSPa e estabelecida pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO. A informação OBID_IA é representada por variável discreta do tipo DI_01, sendo que: Verdadeiro => Obrigatória biometria da impressão digital com relação à identificação e/ou autenticação; Falso => Não obrigatória biometria da impressão digital com relação à identificação e/ou autenticação. Se a variável referente à obrigatoriedade OBID_IA for definida como Verdadeiro, será exigida biometria da impressão digital para identificação e/ou autenticação, decorrendo na imposição do uso do leitor biométrico Le_BID_R.

A identificação por biometria da impressão digital somente poderá ser exigida quando a obrigatoriedade de identificação por cartão OI_CId_S for definida como Falso, sendo que nessa condição, necessariamente, a autenticação incluirá a biometria em questão (nesse caso tanto a identificação quanto a autenticação serão realizadas por meio da biometria da

impressão digital). De forma complementar ressalta-se que a identificação por biometria da impressão digital é um processo relativamente lento se comparado a identificação que utiliza o cartão CId_S, haja vista que é necessário comparar o perfil extraído, com todos aqueles armazenados na base de dados do SiCAP.

A autenticação por biometria da impressão digital deverá ocorrer quando: a obrigatoriedade de identificação por cartão OI_CId_S for definida como Verdadeiro e a obrigatoriedade por biometria OBID_IA for definida como Verdadeiro; a obrigatoriedade de identificação por cartão OI_CId_S for definida como Falso e a obrigatoriedade por biometria OBID_IA for definida como Verdadeiro. Informa-se que esse tipo de autenticação poderá ocorrer de forma combinada com a autenticação que utiliza senha de domínio de rede, sendo utilizados ambos os recursos no processo de autenticação.

Se a variável referente à obrigatoriedade OBID_IA for definida como Falso, não será exigida biometria da impressão digital para identificação e/ou autenticação, decorrendo na dispensa de uso do leitor biométrico Le_BID_R. A não exigência de identificação por biometria da impressão digital, somente poderá ocorrer quando a obrigatoriedade de identificação por cartão OI_CId_S for definida como Verdadeiro. A não exigência de autenticação por biometria da impressão digital, poderá ocorrer quando: o processo de autenticação for dispensado (exemplo: acesso a refeitório); a autenticação for realizada por senha de domínio de rede descrita na subseção “3.8.1.6”.

3.8.1.6 Obrigatoriedade de autenticação por senha de domínio de rede (OA_SDR)

A “Obrigatoriedade de Autenticação por Senha de Domínio de Rede” (OA_SDR) é uma informação definida no âmbito do SiCAP pelo gerente de segurança patrimonial GSPa e estabelecida pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO. A informação OA_SDR é representada por variável discreta do tipo DI_01, sendo que: Verdadeiro => Obrigatória a autenticação por senha de domínio de rede; Falso => Não obrigatória a autenticação senha de domínio de rede.

Se a variável referente à obrigatoriedade OA_SDR for definida como Verdadeiro, será exigida a entrada de senha de domínio de rede no processo de autenticação, decorrendo na imposição do uso de um terminal interligado ao sistema de redes não industriais empresarial SiReNIE, para digitação de dados. Essa condição poderá ocorrer de forma combinada com a

autenticação por biometria da impressão digital (OBID_IA = Verdadeiro e OA_SDR = Verdadeiro) ou isoladamente, quando a autenticação for realizada somente por senha de domínio de rede (OBID_IA = Falso e OA_SDR = Verdadeiro).

Se a variável referente à obrigatoriedade OA_SDR for definida como Falso, não será exigida a entrada de senha de domínio de rede no processo de autenticação, decorrendo na dispensa do uso de um terminal interligado ao sistema de redes não industriais empresarial SiReNIE, para digitação de dados. Essa condição poderá ocorrer quando não for necessária a autenticação por senha de domínio de rede (OA_SDR = Falso).

3.8.1.7 Ativação (AA_PCAP_S) e limite para disparo (LDA_PCAP_S) de Alarme de PCAP_S

O "Alarme de PCAP_S" é um recurso utilizado para sinalizar por meio de dispositivo sonoro, no ambiente do PCAP_S, que houve uma quantidade consecutiva de tentativas de acessos negadas, para um usuário USR em interação com o subsistema SSOP, no PCAP_S. De forma pertinente a esse recurso estão as informações descritas nos respectivos parágrafos a seguir.

A informação de "Ativação de Alarme de PCAP_S" (AA_PCAP_S) é definida no âmbito do SiCAP pelo gerente de segurança patrimonial GSPa e estabelecida pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO. A informação AA_PCAP_S é representada por variável discreta do tipo DI_01, sendo que: Verdadeiro => Alarme de PCAP_S ativado; Falso => Alarme de PCAP_S desativado. Se a variável referente a ativação AA_PCAP_S for definida como Verdadeiro, então as funções do Alarme de PCAP_S serão levadas a efeito, havendo a sinalização em função do limite de disparo descrito a seguir, nesta subseção. Se a variável referente a ativação AA_PCAP_S for definida como Falso, então as funções do Alarme de PCAP_S serão inibidas, não havendo a sinalização em função do limite de disparo.

A informação de "Limite para Disparo de Alarme de PCAP_S" (LDA_PCAP_S) é definida no âmbito do SiCAP pelo gerente de segurança patrimonial GSPa e estabelecida pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO. A informação LDA_PCAP_S estabelece o número de tentativas consecutivas de acessos negados, que irá disparar o Alarme de PCAP_S. Para essa informação será utilizado um

número inteiro, positivo maior que 1 e menor ou igual a 10 (dez), sendo representada por variável numérica do tipo NR_02.

3.8.1.8 Permissão de liberação de acesso forçado no PCAP_S (PLAF_PCAP_S)

A "Permissão de Liberação de Acesso Forçado no PCAP_S" (PLAF_PCAP_S) é uma informação definida no âmbito do SiCAP pelo gerente de segurança patrimonial GSPa e estabelecida pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO. A informação PLAF_PCAP_S é representada por variável discreta do tipo DI_01, sendo que: Verdadeiro => Permissão de liberação de acesso forçado concedida; Falso => Permissão de liberação de acesso forçado não concedida.

Se a variável referente à permissão PLAF_PCAP_S for definida como Verdadeiro, será permitido ao segurança patrimonial SeP, liberar o acesso à área de segurança sem a necessidade dos processos de identificação, autenticação e autorização, realizados pelo SiCAP. Nesse caso há procedimento específico descrito na subseção "3.11.2", Figura 3.39, que permite liberar o equipamento para controle físico de acessos de pessoas e registrar a ocorrência.

3.8.1.9 Tipo de obrigatoriedade de apresentação de equipamento EPP_S no PCAP_S (TOA_EPP_S)

O "Tipo de Obrigatoriedade de Apresentação de Equipamento EPP_S no PCAP_S" (TOA_EPP_S) é uma informação definida no âmbito do SiCAP pelo gerente de segurança patrimonial GSPa e estabelecida pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO. A informação TOA_EPP_S é representada por variável discreta do tipo DI_01, sendo que: Verdadeiro => Obrigatória a apresentação de equipamento EPP_S por inspeção 100%; Falso => Obrigatória a apresentação de equipamento EPP_S por inspeção aleatória.

Para que o tipo de obrigatoriedade TOA_EPP_S seja levado a efeito (ativando as opções de inspeção descritas na subseção "3.6" e designadas por: Inspeção 100% de EPP_S; Inspeção Aleatória de EPP_S) é necessário associar ao PCAP_S os tipos de equipamentos de

segurança pessoal EPP_S (informação CI_T_EPP_S descrita na subseção "3.6.1.1") que deverão ser apresentados como condicionante para estabelecer a autorização de acessos às áreas industriais de segurança que o usurário USR têm direito. Essa associação é prevista pelo gerente de segurança patrimonial GSPa e estabelecida pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO. Se nenhum tipo de EEP_S for associado ao PCAP_S, as funções relativas ao tipo de obrigatoriedade TOA_EPP_S serão inibidas, sendo estabelecida a opção de inspeção de EPP_S como "Sem Inspeção de EPP_S".

Se um ou mais tipos de EEP_S for associado ao PCAP_S e a variável referente ao tipo de obrigatoriedade TOA_EPP_S for definida como Verdadeiro, será estabelecida a opção de inspeção de EPP_S como "Inspeção 100% de EPP_S". Se um ou mais tipos de EEP_S for associado ao PCAP_S e a variável referente ao tipo de obrigatoriedade TOA_EPP_S for definida como Falso, será estabelecida a opção de inspeção de EPP_S como "Inspeção Aleatória de EPP_S", sendo os parâmetros desse tipo de inspeção definidos conforme exposto na subseção "3.8.1.10" a seguir.

3.8.1.10 Quantidade (QTDI_PCAP_S) e número máximo (NMAX_PCAP_S) de usuários a serem inspecionados no PCAP_S

A "Quantidade de Usuários a Serem Inspecionados no PCAP_S" (QTDI_PCAP_S) é uma informação definida no SiCAP, sendo um número inteiro, positivo, maior que 1 e menor ou igual a 1.000.000. Esse número será utilizado para determinar a quantidade de usuários a serem inspecionados no PCAP_S, referente a opção de inspeção "Inspeção Aleatória de EPP_S". Essa definição é realizada pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO. A informação QTDI_PCAP_S é representada por variável numérica do tipo NR_01.

O "Número Máximo de Usuários a Serem Inspecionados no PCAP_S" (NMAX_PCAP_S) é uma informação definida no SiCAP, sendo um número inteiro, positivo, maior que 1 e menor ou igual a 1.000.000, e, também, maior ou igual a quantidade QTDI_PCAP_S. É utilizado para determinar a quantidade máxima de usuários a serem inspecionados no PCAP_S, referente a opção de inspeção "Inspeção Aleatória de EPP_S". Essa definição é realizada pelo operador de segurança OpS por meio do *software*

SICAP.ADMINISTRATIVO. A informação NMAX_PCAP_S é representada por variável numérica do tipo NR_01.

3.8.2 Informações referentes a entidades pertinentes ao PCAP_S

Relativamente ao modelo de dados do SiCAP e de forma pertinente aos pontos de controle de acesso de pessoas PCAP_S, é proposta a definição das entidades designadas por "PONTOCONTROLE" e "EQUIPAMENTOPONTO", cuja sugestão de diagrama entidade relacionamento é apresentada na Figura 3.12.

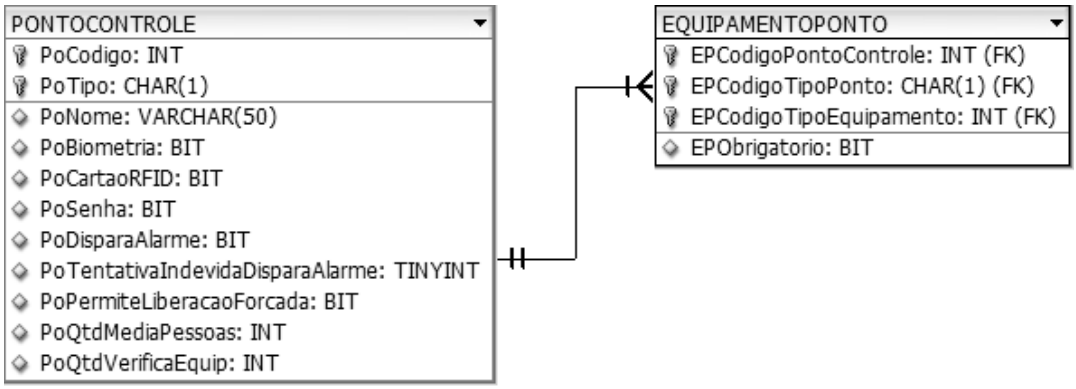

Figura 3.12 - Diagrama entidade relacionamento referente ao PCAP_S

Na Tabela 3.12, são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada a entidade PONTOCONTROLE, utilizada para armazenar os dados de configuração do funcionamento do *software* SICAP.PONTOCONTROLE. Essa configuração é realizada a partir de definições do gerente de segurança patrimonial GSPa e estabelecida no SiCAP pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO.

Tabela 3.12 - Detalhes da estrutura de dados aplicada à entidade PONTOCONTROLE

CAMPOS REFERENTES À ENTIDADE PONTOCONTROLE		
Designação	**Tipo**	**Descrição**
PoCodigo	INT	Define o código de identificação do PCAP_S, CI_PCAP_S, descrito na subseção “3.8.1.2”.
PoTipo	CHAR(1)	Define o tipo de sentido de fluxo no PCAP_S, TSF_PCAP_S, descrito na subseção “3.8.1.3”.
PoNome	VARCHAR(50)	Define a nomenclatura do PCAP_S, No_PCAP_S, descrita na subseção “3.8.1.1”.
PoBiometria	BIT	Define a obrigatoriedade de biometria da impressão digital com relação a identificação e autenticação, OBID_IA, descrita na subseção “3.8.1.5”.
PoCartaoRFID	BIT	Define a obrigatoriedade identificação por cartão CId_S, OI_CId_S, descrito na subseção “3.8.1.4”.
PoSenha	BIT	Define a obrigatoriedade de autenticação por senha de domínio de rede, OA_SDR, descrita na subseção “3.8.1.6”.
PoDisparaAlarme	BIT	Define ativação de Alarme de PCAP_S, AA_PCAP_S, descrita na subseção “3.8.1.7”.
PoTentativaIndevidaDisparaAlarme	TINYINT	Define o limite para disparo de Alarme de PCAP_S, LDA_PCAP_S, descrito na subseção “3.8.1.7”.
PoPermiteLiberacaoForcada	BIT	Define permissão de liberação de acesso forçado no PCAP_S, PLAF_PCAP_S, descrita na subseção “3.8.1.8”.
PoQtdMediaPessoas	INT	Define o número máximo de usuários a serem inspecionados no PCAP_S, NMAX_PCAP_S, descrito na subseção “3.8.1.10”.
PoQtdVerificaEquip	INT	Define a quantidade de usuários a serem inspecionados no PCAP_S, QTDI_PCPA_S, descrita na subseção “3.8.1.10”.

Na Tabela 3.13, são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada a entidade EQUIPAMENTOPONTO, utilizada para armazenar os dados que associam os tipos de equipamentos de proteção pessoal EPP_S (exigidos como condicionantes para estabelecer a autorização de acessos a área industrial de segurança) ao ponto de controle PCAP_S. Essa associação é realizada a partir de definições do gerente de segurança patrimonial GSPa e estabelecido no SiCAP pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO.

Tabela 3.13 - Detalhes da estrutura de dados aplicada a entidade EQUIPAMENTOPONTO

CAMPOS REFERENTES À ENTIDADE EQUIPAMENTOPONTO		
Designação	**Tipo**	**Descrição**
EPCodigoPontoControle	INT	Armazena o código de identificação do PCAP_S, CI_PCAP_S, oriundo da entidade PONTOCONTROLE (ver campo "PoCodigo" na Tabela 3.12).
EPCodigoTipoPonto	CHAR(1)	Armazena o tipo de sentido de fluxo no PCAP_S, TSF_PCAP_S, oriundo da entidade PONTOCONTROLE (ver campo "PoTipo" na Tabela 3.12).
EPCodigoTipoEquipamento	INT	Armazena o código de identificação do tipo de equipamento EPP_S, CI_T_EPP_S, oriundo da entidade TIPOEQUIPAMENTO (ver campo "TECodigo" na Tabela 3.8).
EPObrigatorio	BIT	Define o tipo de obrigatoriedade de apresentação de equipamentos EPP_S no PCAP_S, TOA_EPP_S, descrita na subseção "3.8.1.9".

3.8.3 Rota de usuário USR (R_USR)

Na concepção do SiCAP, definiu-se o conceito de "Rota de Usuário USR" (R_USR), como sendo o conjunto de pontos de controle PCAP_S pertencentes a um percurso cujas áreas industriais de segurança poderão ser acessadas por usuários USR, em função das respectivas permissões de acessos. Em função do exposto, os usuários USR deverão ser associados às rotas R_USR, para transitar pela empresa e atingir as áreas industriais de segurança cujos acessos lhes são permitidos. A definição das rotas R_USR é realizada pelo gerente de segurança patrimonial GSPa e estabelecida no SiCAP pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO. O *software* em questão permite associar a cada rota R_USR os respectivos pontos de controle PCAP_S envolvidos no percurso.

Para essa definição o gerente GSPa não pode proporcionar condições que levem a ocasionar infringência das normativas de controle de acessos estabelecidas pela empresa, devendo, também, buscar os caminhos mais curtos que atendam a necessidade de cada usuário USR, sendo incluídas análises sobre os seguintes pontos: não permitir o tráfego de usuários USR por áreas que não têm direito de acessar; observância quanto ao sentido de fluxo de cada PCAP_S (TSF_PCAP_S), de maneira que a rota proporcione o percurso desejado; observância quanto às obrigatoriedades referentes a identificação por cartão CId_S (OI_CId_S), biometria da impressão digital (OBID_IA) e autenticação por senha de domínio de rede (OA_SDR); observância quanto a permissão de liberação de acesso forçado (PLAF_PCAP_S); observância quanto ao tipo de obrigatoriedade de apresentação de equipamento EPP_S (TOA_EPP_S).

A associação das rotas aos usuários USR é definida pelo gerente GSPa e realizada pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO. Cada usuário USR deverá possuir um conjunto limitado de rotas R_USR, que definirá as áreas industriais de segurança que poderá acessar.

3.8.3.1 Informações referentes a rota de usuário USR

3.8.3.1.1 Código de identificação da rota R_USR (CI_ROTA)

O "Código de Identificação da Rota R_USR" (CI_ROTA) é uma informação gerada automaticamente pelo SiCAP, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária de identificação das rotas de acessos no âmbito dos respectivos *softwares* do SiCAP. Esse código é gerado no momento de cadastramento da rota no SiCAP. O cadastramento é realizado pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO.

3.8.3.1.2 Nomenclatura da rota R_USR (No_ROTA)

A "Nomenclatura da Rota" (No_ROTA) é um texto com até 50 caracteres, associado ao respectivo código de identificação da rota CI_ROTA, que designa a rota R_USR. Para esse texto devem ser utilizados termos que indiquem a semântica de aplicação da rota, sendo sua definição realizada pelo gerente de segurança patrimonial (GSPa) e tendo sua inserção no SiCAP efetuada pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO, como parte das exigências para cadastramento da rota R_USR. A informação No_ROTA é representada por variável alfanumérica do tipo AN_01, sendo permitidos 50 caracteres.

3.8.3.1.3 Descrição da rota R_USR (DESC_ROTA)

A “Descrição da Rota R_USR” (DESC_ROTA) é um texto com até 500 caracteres, associado ao respectivo código de identificação da rota CI_ROTA, utilizado para descrever, com detalhamentos, a rota R_USR. Esses detalhamentos devem incluir itens como: objetivo, a nomenclatura dos PCAP_S (No_PCAP_S) envolvidos e uma designação das respectivas áreas internas. A definição do texto em questão é realizada pelo gerente de segurança patrimonial (GSPa), tendo sua inserção no SiCAP, efetuada pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO, como parte das exigências para cadastramento da rota R_USR. A informação DESC_ROTA é representada por variável alfanumérica do tipo AN_01, sendo permitidos 500 caracteres.

3.8.3.1.4 Estado de habilitação (EH_ROTA) e motivo de bloqueio (MB_ROTA) da rota R_USR

O “Estado de Habilitação da Rota R_USR” (EH_ROTA) é uma informação definida no âmbito do SiCAP. A rota R_USR em estado habilitada permite a realização do respectivo percurso pelos usuários USR a ela vinculados, não havendo nos PCAP_S pertinentes, impedimento referente a este estado de habilitação. A rota R_USR em estado bloqueada não permite a realização do respectivo percurso pelos usuários USR a ela vinculados, havendo nos PCAP_S pertinentes, impedimento referente a este estado de habilitação.

O gerente operacional de segurança patrimonial GOSeP, poderá habilitar ou bloquear uma rota R_USR, ordenando ao operador de segurança OpS a realização do estabelecimento dos respectivos estados entre habilitada ou bloqueada. No SiCAP esse estabelecimento é realizado meio do *software* SICAP.ADMINISTRATIVO. A informação EH_ROTA é representada por variável discreta do tipo DI_01, sendo que: Verdadeiro => rota R_USR habilitada; Falso => rota R_USR bloqueada.

O “Motivo de Bloqueio da Rota R_USR” (MB_ROTA) é uma informação definida no âmbito do SiCAP para estabelecimento de estado de habilitação da rota R_USR como bloqueada (EH_ROTA = Falso; rota R_USR bloqueada). Para esse estabelecimento de estado é necessário registrar um texto explicativo sobre o(s) motivo(s) do bloqueio, sendo esse registro realizado por meio da informação definida para o MB_ROTA, inserida pelo operador

de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO. A informação MB_ROTA é representada por variável alfanumérica do tipo AN_01, sendo permitidos 255 caracteres.

3.8.3.1.5 Código de identificação da associação da rota R_USR (CI_ARU)

O "Código de Identificação da Associação da Rota R_USR" (CI_ARU) é uma informação gerada automaticamente pelo SiCAP, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária de identificação da associação da rota R_USR ao usuário USR, no âmbito dos respectivos *softwares* do SiCAP. Esse código é gerado no momento de associação da rota R_USR ao usuário USR no SiCAP, que é realizada pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO.

3.8.3.1.6 Limite inicial (LI_ROTA) e final (LF_ROTA) de permissão para o usuário USR trafegar pela rota R_USR

O "Limite Inicial de Permissão para o Usuário USR Trafegar pela rota R_USR" (LI_ROTA) e o "Limite Final de Permissão para o Usuário USR Trafegar pela rota R_USR" (LF_ROTA), são informações do SiCAP e têm por principal função registrar o prazo de vigência que o usuário USR terá direito de utilizar a rota R_USR, de forma a impedir que esse acesse as áreas industriais de segurança que têm direito, fora do prazo em questão. Esse prazo de vigência permite que contratados e estagiários, sejam automaticamente impedidos de acessar áreas industriais de segurança fora do prazo de seus respectivos contratos. Também, pode restringir os acessos de determinados usuários USR, para permitir a realização de atividades nas áreas controladas, das quais esses estão impedidos de participar.

O limite inicial LI_ROTA e o final LF_ROTA, devem permitir o registro de data e horário, sendo essas informações cronológicas definidas pelo gerente operacional de segurança patrimonial GOSeP, que ordenará para o operador de segurança OpS o respectivo estabelecimento, por meio do *software* SICAP.ADMINISTRATIVO. As informações LI_ROTA e LF_ROTA, são representadas por variável numérica do tipo DT_01.

3.8.3.1.7 Estado de habilitação (EHU_ROTA) e motivo de bloqueio (MBU_ROTA) do usuário USR para a rota R_USR

O “Estado de Habilitação do Usuário USR para a Rota R_USR” (EHU_ROTA) é uma informação definida no âmbito do SiCAP, que pode permitir ou impedir a utilização de uma determinada rota R_USR, por um usuário USR específico, vinculado à rota em questão. Quando o estado EHU_ROTA de um usuário USR para com a rota R_USR, for definido como habilitado, será permitida a realização do respectivo percurso pelo usuário USR, não havendo nos PCAP_S pertinentes, impedimento referente a este estado de habilitação. Quando o estado EHU_ROTA de um usuário USR para com a rota R_USR, for definido como bloqueado, não será permitida a realização do respectivo percurso pelo usuário USR, havendo nos PCAP_S pertinentes, impedimento referente a este estado de habilitação.

O gerente operacional de segurança patrimonial GOSeP, poderá habilitar ou bloquear um usuário USR com relação a uma rota R_USR, ordenando ao operador de segurança OpS a realização do estabelecimento dos respectivos estados entre habilitado ou bloqueado. No SiCAP esse estabelecimento é realizado meio do *software* SICAP.ADMINISTRATIVO. A informação EHU_ROTA é representada por variável discreta do tipo DI_01, sendo que: Verdadeiro => Habilitado o usuário USR para com a rota R_USR; Falso => Bloqueado o usuário USR para com a rota R_USR.

O “Motivo de Bloqueio do Usuário USR para a Rota R_USR” (MBU_ROTA) é uma informação definida no âmbito do SiCAP para estabelecimento do estado de habilitação do usuário USR para a rota R_USR, como bloqueado (EHU_ROTA = Falso). Para esse estabelecimento de estado é necessário registrar um texto explicativo sobre o(s) motivo(s) do bloqueio, sendo esse registro realizado por meio da informação definida para o MBU_ROTA, inserida pelo operador de segurança OpS por meio do *software* SICAP.ADMINISTRATIVO. A informação MBU_ROTA é representada por variável alfanumérica do tipo AN_01, sendo permitidos 255 caracteres.

3.8.3.2 Informações referentes a entidades pertinentes a rota de usuário USR

Relativamente ao modelo de dados do SiCAP e de forma pertinente às rotas de usuários USR, R_USR, é proposta a definição das entidades designadas por “PONTOROTA”, “ROTA” e “ROTAUSUARIO”, cuja sugestão de diagrama entidade relacionamento é apresentada na Figura 3.13.

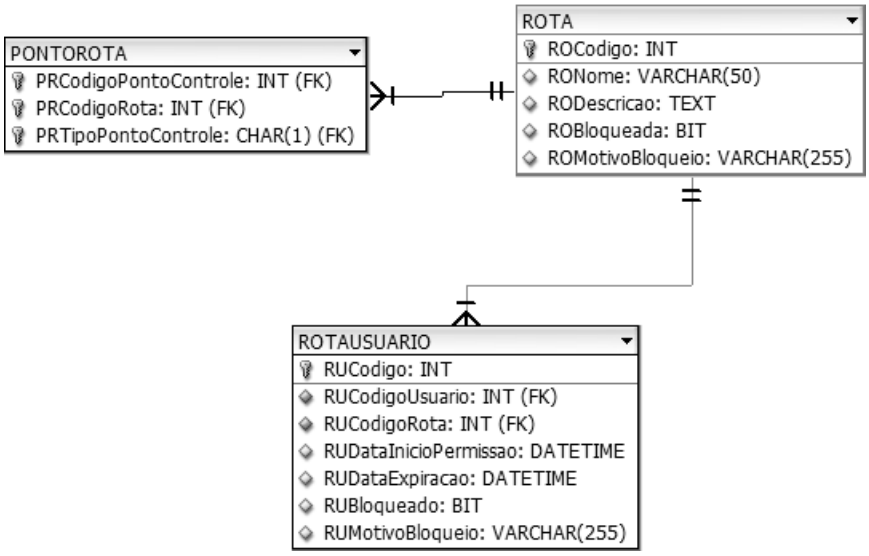

Figura 3.13 - Diagrama entidade relacionamento referente as rotas R_USR

Na Tabela 3.14 são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada a entidade ROTA, utilizada para armazenar os dados referentes ao cadastramento das rotas R_USR. Esse cadastramento é realizado a partir de definições do gerente de segurança patrimonial GSPa e estabelecida no SiCAP pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO.

Tabela 3.14 - Detalhes da estrutura de dados aplicado à entidade ROTA

CAMPOS REFERENTES À ENTIDADE ROTA		
Designação	**Tipo de dados**	**Descrição**
ROCodigo	INT	Define o código de identificação da rota R_USR, CI_ROTA, descrito na subseção “3.8.3.1.1”.
RONome	VARCHAR(50)	Define a nomenclatura da rota R_USR, No_ROTA, descrito na subseção “3.8.3.1.2”.
RODescricao	TEXT	Define a descrição da rota R_USR, DESC_ROTA, exposta na subseção “3.8.3.1.3”.
ROBloqueada	BIT	Define o estado de habilitação da rota R_USR, EH_ROTA, descrito na subseção “3.8.3.1.4”.
RoMotivoBloqueio	VARCHAR(255)	Define o motivo de bloqueio da rota R_USR, MB_ROTA, descrito na subseção “3.8.3.1.4”.

Na Tabela 3.15, são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada a entidade PONTOROTA, utilizada para armazenar os dados referentes associação dos pontos de controle PCAP_S às rotas R_USR. Essa associação é realizada a partir de definições do gerente de segurança patrimonial GSPa e estabelecida no SiCAP pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO.

Tabela 3.15 - Detalhes da estrutura de dados aplicada à entidade PONTOROTA

CAMPOS REFERENTES À ENTIDADE PONTOROTA		
Designação	**Tipo**	**Descrição**
PRCodigoPontoControle	INT	Armazena o código de identificação do PCAP_S, CI_PCAP_S, oriundo da entidade PONTOCONTROLE. (ver Tabela 3.12).
PRCodigoRota	INT	Armazena o código de identificação da rota R_USR, CI_ROTA, oriundo da entidade ROTA (ver Tabela 3.14).
PRTipoPontoControle	CHAR(1)	Armazena o tipo de sentido de fluxo no PCAP_S, TSF_PCAP_S, oriundo da entidade ponto controle (ver Tabela 3.12).

Na Tabela 3.16, são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada a entidade ROTAUSUARIO, utilizada para armazenar os dados referentes associação dos usuários USR às rotas R_USR. Essa associação é realizada a partir de definições do gerente de segurança patrimonial GSPa e estabelecida no SiCAP pelo operador de segurança OpS, por meio do *software* SICAP.ADMINISTRATIVO.

Tabela 3.16 - Detalhes da estrutura de dados aplicada à entidade ROTAUSUARIO

CAMPOS REFERENTES À ENTIDADE ROTAUSUARIO		
Designação	**Tipo**	**Descrição**
RUCodigo	INT	Define o código de identificação da associação da rota R_USR, CI_ARU, descrito na subseção “3.8.3.1.5”.
RUCodigoUsuario	INT	Armazena o código de identificação do usuário USR, CI_USR, oriundo a da entidade USUARIO (ver Tabela 3.1).
RUCodigoRota	INT	Armazena o código de identificação da rota R_USR, CI_ROTA, oriundo da entidade ROTA (ver Tabela 3.14).
RUDataInicioPermissao	DATETIME	Define a data e hora do limite inicial de permissão para o usuário USR trafegar pela rota R_USR, LI_ROTA, descrito na subseção “3.8.3.2”.
RUDataExpiracao	DATETIME	Define a data e hora do limite final de permissão para o usuário USR trafegar pela rota R_USR, LF_ROTA, descrito na subseção “3.8.3.2”.
RUBloqueado	BIT	Define o estado de habilitação do usuário USR para a rota R_USR, EHU_ROTA, descrito na subseção “3.8.3.3”.
RUMotivoBloqueio	VARCHAR (255)	Define o motivo de bloqueio do usuário USR para a rota R_USR, MBU_ROTA, descrito na subseção “3.8.3.3”.

3.8.4 Controle de acesso de pessoas com deficiência física

Os deficientes acessarão os PCAP_S com auxílio de um segurança patrimonial SeP, sendo responsabilidade da empresa possuir portas laterais para cadeirantes ou um conjunto de ECAP_S preparados para esse trânsito. O segurança patrimonial SeP deve auxiliar o deficiente na interação com o SiCAP, seja na situação de permissão do acesso ou na de impedimento.

3.8.5 Registro de tentativa de acesso de usuário USR (RTA_USR)

Na concepção do SiCAP, definiu-se o conceito de "Registro de Tentativa de Acesso de Usuário USR" (RTA_USR), como sendo o conjunto de informações referentes à tentativa de acesso realizada pelo usuário USR (quer essa termine em permissão ou em impedimento) ou de tentativa de acesso forçado, a serem armazenas nos meios computacionais do SiCAP para a finalidade principal de auditoria. Assim sendo, o *software* SICAP.PONTOCONTROLE (utilizado nas operações do PCAP_S) deve realizar o controle de acessos dos usuários USR e, também, registrar os dados pertinentes aos registros RTA_USR. Nesse contexto, os dados pertencentes aos registros RTA_USR deverão ser acessados pelo *software* SICAP.AUDITORIA pertencente ao subsistema tático-administrativo SSTA, para atender as finalidades de auditorias que envolvem o controle de acessos de pessoas.

O conjunto de informações referentes ao registro RTA_USR é formado por algumas descritas anteriormente e outras, abordadas nas subseções pertinentes a esta. As informações descritas anteriormente são as seguintes:

- Código de identificação do usuário USR, CI_USR (ver subseção "3.3.1.1"). Essa informação tem por finalidade identificar qual usuário está envolvido na tentativa de acesso registrada pelo RTA_USR.
- Código de identificação do cartão CId_S, CI_CId_S (ver subseção "3.4.1.2"). Essa informação tem por finalidade identificar qual cartão CId_S foi utilizado na tentativa de acesso registrada pelo RTA_USR.

- Código de identificação do PCAP_S, CI_PCAP_S (ver subseção “3.8.1.2”). Essa informação tem por finalidade identificar em qual PCAP_S ocorreu a tentativa de acesso registrada pelo RTA_USR.
- Tipo do sentido de fluxo no PCAP_S, TSF_PCAP_S (ver subseção“3.8.1.3”). Essa informação tem por finalidade identificar o sentido de fluxo no PCAP_S, referente a tentativa de acesso registrada pelo RTA_USR.
- A identificação do segurança patrimonial SeP (descrita na subseção “3.3.1.1”), que atendeu o disparo de Alarme de PCAP_S ocorrido na tentativa de acesso registrada pelo RTA_USR. Para a identificação em questão deverá ser utilizado código de identificação do usuário USR, CI_USR, associado segurança patrimonial SeP.
- A identificação do segurança patrimonial SeP (descrita na subseção “3.3.1.1”), que realizou acesso forçado pelo PCAP_S, ocorrido na tentativa de acesso registrada pelo RTA_USR. Para a identificação em questão deverá ser utilizado código de identificação do usuário USR, CI_USR, associado segurança patrimonial SeP.

3.8.5.1 Informações complementares referentes ao registro de tentativa de acesso de usuário USR

3.8.5.1.1 Código de identificação do registro de tentativa de acesso RTA_USR (CIRTA_USR)

O “Código Identificação do Registro de Tentativa de Acesso RTA_USR” (CIRTA_USR) é uma informação gerada de forma automática pelo SiCAP, sendo representada por variável numérica do tipo NR_01, para utilização como chave primária de identificação do registro de tentativa de acesso RTA_USR no âmbito dos respectivos *softwares* do SiCAP. A geração automática desse código é realizada pelo *software* SICAP.PONTOCONTROLE, no momento da tentativa de acesso realizada pelo usuário USR ou de tentativa de acesso forçado.

3.8.5.1.2 Data e hora da tentativa de acesso (DT_ACESSO)

A “Data e Hora da Tentativa de Acesso” (DT_ACESSO) é uma informação do SiCAP utilizada para informar a data e o horário da tentativa de acesso, registrada pelo RTA_USR. No SiCAP essas informações são providas automaticamente por meio do *software* SICAP.PONTOCONTROLE. A informação DT_ACESSO é representada por variável numérica do tipo DT_01.

3.8.5.1.3 Resultado da tentativa de acesso (RT_ACESSO)

O “Resultado da Tentativa de Acesso” (RT_ACESSO) é informação do SiCAP utilizada para informar o resultado da tentativa de acesso registrada pelo RTA_USR. A informação RT_ACESSO é representada por variável discreta do tipo DI_01, sendo que: Verdadeiro => acesso permitido; Falso => acesso impedido. No SiCAP essas informações são providas automaticamente por meio do *software* SICAP.PONTOCONTROLE.

3.8.5.1.4 Estado de Disparo do Alarme de PCAP_S (ED_ALARME)

O “Estado de Disparo do Alarme de PCAP_S” (ED_ALARME) é informação do SiCAP utilizada para indicar se na tentativa de acesso registrada pelo RTA_USR o Alarme de PCAP_S disparou. A informação ED_ALARME é representada por variável discreta do tipo DI_01, sendo que: Verdadeiro => Alarme de PCAP_S disparou; Falso => Alarme de PCAP_S não disparou. No SiCAP essas informações são providas automaticamente por meio do *software* SICAP.PONTOCONTROLE.

3.8.5.1.5 Data e hora de interrupção do Alarme de PCAP_S (DT_IAL)

A “Data e Hora de Interrupção do Alarme de PCAP_S” (DT_IAL) é informação do SiCAP utilizada para indicar a data e o horário de interrupção do Alarme de PCAP_S disparado na tentativa de acesso registrada pelo RTA_USR. No SiCAP essas informações são providas automaticamente por meio do *software* SICAP.PONTOCONTROLE, conforme descrito na subseção “3.11.2”, Figura 3.40. Entretanto, nessa situação, o *software* em questão impediu o uso do PCAP_S a partir do momento de disparo do alarme, aguardando a desativação desse alarme a ser realizada pelo segurança patrimonial SeP, sendo nessa desativação registradas as informações referentes ao DT_IAL. A desativação em questão ocorre a partir da operação de reiniciação do alarme de PCAP_S indicada na Figura 3.37. A informação DT_IAL é representada por variável numérica do tipo DT_01.

3.8.5.1.6 Observação ao interromper o alarme de PCAP_S (OBS_IA)

A “Observação ao Interromper o Alarme de PCAP_S” (OBS_IA) é informação do SiCAP e possui texto com até 255 caracteres utilizados para descrever as observações do segurança patrimonial SeP, com relação a sua percepção da ocorrência de disparo de Alarme de PCAP_S. Essa informação é relacionada com a data e hora de interrupção do alarme de PCAP_S, DT_IAL. A informação OBS_IA é representada por variável alfanumérica do tipo AN_01, sendo permitidos 255 caracteres. As observações OBS_IA são digitadas pelo segurança patrimonial SeP por meio do *software* SICAP.PONTOCONTROLE.

3.8.5.1.7 Estado de liberação de acesso forçado (ELAF)

O “Estado de Liberação de Acesso Forçado” (ELAF) é uma informação definida no âmbito do SiCAP que identifica se o ocorreu a liberação forçada, ou não. No SiCAP essa informação é gerada no momento em que o segurança patrimonial SeP definir que o acesso a ser realizado é do tipo forçado. A informação ELAF é estabelecida por meio do *software* SICAP.PONTOCONTROLE, pertencente ao subsistema operacional–PCAP SSOP. A

informação ELAF é representada por variável discreta do tipo DI_01 sendo que: Verdadeiro => houve acesso de forma forçada; Falso => não houve acesso de forma forçada.

3.8.5.1.8 Motivo de liberação de acesso forçado (MLAF)

O "Motivo de Liberação de Acesso Forçado" (MLAF) é uma informação do SiCAP que possui texto com até 255 caracteres, associado a data e hora da tentativa de acesso DT_ACESSO, utilizado para descrever os motivos que levaram o segurança patrimonial SeP a realizar o acesso forçado. A informação MLAF é representada por variável alfanumérica do tipo AN_01, sendo permitidos 255 caracteres. Os motivos, MLAF, serão digitados pelo segurança patrimonial SeP por meio do *software* SICAP.PONTOCONTROLE, pertencente ao subsistema operacional–PCAP SSOP.

3.8.5.2 Estrutura de dados aplicada à entidade ACESSOPONTOCONTROLE

Relativamente ao modelo de dados do SiCAP e de forma pertinente ao registro de tentativa de acesso de usuário USR RTA_USR, é proposta a definição da entidade designada por "ACESSOPONTOCONTROLE", cuja estrutura de dados sugerida é apresentada Figura 3.14.

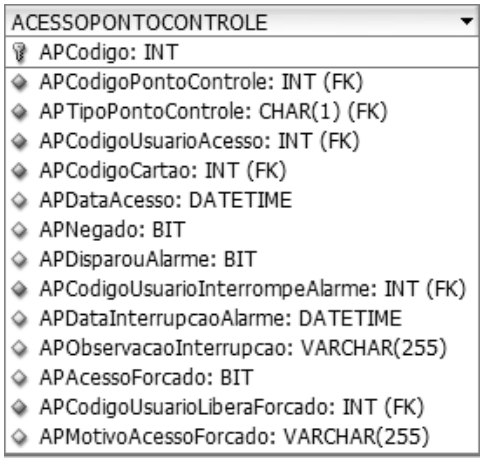

Figura 3.14 - Estrutura de dados aplicada à entidade ACESSOPONTOCONTROLE

Na Tabela 3.17, são apresentados detalhes dos campos pertencentes à estrutura de dados aplicada à entidade ACESSOPONTOCONTROLE.

Tabela 3.17 - Detalhes da estrutura de dados aplicada à entidade ACESSOPONTOCONTROLE

CAMPOS REFERENTES À ESTRUTURA DE DADOS ACESSOPONTOCONTROLE		
Designação	**Tipo**	**Descrição**
APCodigo	INT	Define o código identificação do registro de tentativa de acesso RTA_USR, CIRTA_USR, descrito na subseção “3.8.5.1.1”.
APCodigoPontoControle	INT	Armazena o código de identificação do PCAP_S, CI_PCAP_S, oriundo da entidade PONTOCONTROLE (ver Tabela 3.12).
APTipoPontoControle	CHAR(1)	Armazena o tipo de sentido de fluxo no PCAP_S, TSF_PCAP_S, oriundo da entidade PONTOCONTROLE (ver Tabela 3.12).
APCodigoUsuarioAcesso	INT	Armazena o código de identificação do usuário USR, CI_USR, oriundo da entidade USUARIO (ver Tabela 3.1).
APCodigoCartao	INT	Armazena o código de identificação do cartão CId_S, CI_CId_S, oriundo da entidade CARTAO (ver Tabela 3.6).
APDataAcesso	DATETIME	Define a data e hora da tentativa de acesso DT_ACESSO, descrita na subseção “3.8.5.1.2”.
APNegado	BIT	Define o resultado da tentativa de acesso RT_ACESSO, descrito na subseção “3.8.5.1.3”.
APDisparouAlarme	BIT	Define o estado de disparo do alarme de PCAP_S, ED_ALARME, descrito na subseção “3.8.5.1.4”.
APCodigoUsuarioInterrompeAlarme	INT	Armazena o código de identificação do usuário USR, CI_USR, oriundo da entidade USUARIO (ver Tabela 3.1), porém, referente ao segurança patrimonial SeP que atendeu o disparo de Alarme de PCAP_S.
APDataInterrupcaoAlarme	DATETIME	Define a data e hora de interrupção do Alarme de PCAP_S, DT_IAL, descrita na subseção “3.8.5.1.5”.
APObservacaoInterrupcao	VARCHAR(255)	Define a observação ao interromper o Alarme de PCAP_S, OBS_IA, descrita na subseção “3.8.5.1.6”.
APAcessoForcado	BIT	Define o estado de liberação de acesso forçado ELAF, descrito na subseção “3.8.5.1.7”.
APCodigoUsuarioLiberaForcado	INT	Armazena o código de identificação do usuário USR, CI_USR, oriundo da entidade USUARIO (ver Tabela 3.1), porém, referente ao segurança patrimonial SeP que realizou acesso forçado pelo PCAP_S.
APMotivoAcessoForcado	VARCHAR(255)	Define o motivo de liberação de acesso forçado MLAF, descrito na subseção “3.8.5.1.8”.

3.9 SUBSISTEMA SiCAP-TÁTICO-ADMINISTRATIVO (SSTA)

3.9.1 Arquitetura do SSTA

O "Subsistema SiCAP-Tático-Administrativo" (SSTA) está alocado junto aos sistemas computacionais do nível tático SCNT e provê a infraestrutura de banco de dados e servidor *Web*, necessária para as operações do SiCAP. Também contém o *software* dedicado a acessar as informações de auditoria, sendo esse utilizado pelo gerente de segurança patrimonial GSPa e o operador de segurança OpS. Na Figura 3.15, é apresentada a arquitetura do subsistema SSTA, sendo a descrição de seus elementos expostas nas subseções a seguir, pertinentes a esta.

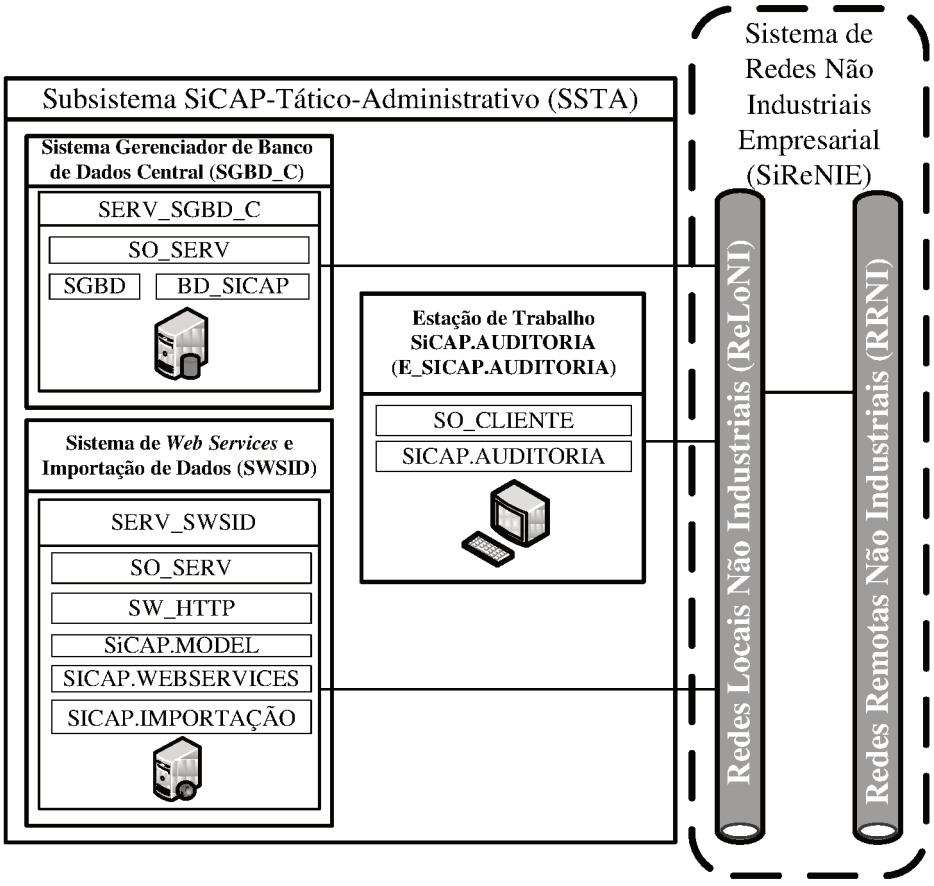

Figura 3.15 - Arquitetura do SSTA

3.9.2 Sistema Gerenciador de Banco de Dados Central (SGBD_C)

O "Sistema Gerenciador de Banco de Dados Central" (SGBD_C) contém, de forma centralizada, a base única de dados utilizada pelo SiCAP e os recursos necessários para permitir o acesso a essa base, pelas demais partes do sistema de controle de acessos em questão. Para tanto, o sistema SGBD_C está interligado às redes locais não industriais ReLoNI por meio do equipamento designado por "Servidor do Sistema Gerenciador de Banco de Dados Central" (SERV_SGBD_C), que hospedará os *softwares* denominados "Sistema Operacional de Servidor" (SO_SERV) e "Sistema Gerenciador de Banco de Dados" (SGBD), além da base única de dados designada por "Banco de Dados do SICAP" (BD_SICAP).

O sistema gerenciador de banco de dados SGBD permite armazenamento e acesso aos dados da base única BD_SICAP, sendo esse sistema gerenciador executado sobre o sistema operacional SO_SERV.

Como exemplo do sistema operacional SO_SERV, podem ser citados os seguintes: Microsoft Windows 2003 (MICROSOFT, 2012) e o Linux (LINUX, 2012). Como exemplo do sistema gerenciador de banco de dados SGBD, podem ser citados os seguintes: Microsoft SQL-Server 2005 (SQLSERVER, 2012); MySQL (MYSQL, 2012); Oracle (ORACLE, 2012). Como exemplo do equipamento utilizado para o servidor do sistema gerenciador de banco de dados central SERV_SGBD_C, pode ser citado o computador modelo PowerEdge R910, fornecido pela empresa Dell Inc. (DELL, 2012).

3.9.3 Sistema de *Web Services* e Importação de dados (SWSID)

O "Sistema de *Web Services* e Importação de Dados" (SWSID) é destinado ao interfaceamento entre os demais componentes computacionais do SiCAP e o sistema gerenciador de banco de dados central SGBD_C, sendo também aplicado às importações de dados dos seguintes sistemas para com o SiCAP: sistema de controle de contratados SCCont; sistema de controle de recursos humanos SRH; sistema de controle de visitas SCVis. Para tanto, o sistema SWSID está interligado às redes locais não industriais ReLoNI por meio do equipamento designado por "Servidor do Sistema de *Web Services* e Importação de Dados"

(SERV_SWSID), que hospedará os *softwares* denominados "Sistema Operacional de Servidor" (SO_SERV), "Servidor Web HTTP" (SW_HTTP), "SICAP.MODEL"; "SICAP.WEBSERVICES"; "SICAP.IMPORTAÇÃO". Neste servidor, os quatro últimos *softwares* são executados sobre o sistema operacional SO_SERV. Esse sistema operacional é do mesmo tipo aplicado sistema gerenciador SGBD_C exposto na subseção "3.9.2", sendo válidos os mesmos exemplos.

No interfaceamento mencionado anteriormente, os demais componentes computacionais do SiCAP acessam o servidor SERV_SWSID (pertencente ao sistema SWSID) e este acessa o servidor SERV_SGBD_C (pertencente ao sistema SGBD_C), entretanto, na concepção do SiCAP, os servidores SERV_SWSID e SERV_SGBD_C deverão estar no mesmo ambiente predial, protegidos fisicamente e logicamente de acessos indevidos. Para as comunicações referentes ao primeiro interfaceamento (demais componentes do SiCAP para com o servidor SERV_SWSID) são utilizados recursos de criptografia pertencentes ao protocolo SSL, permitindo a implementação pertinente à inviolabilidade de dados que trafegam nos respectivos meios de comunicação. Entretanto, para as comunicações referentes ao segundo interfaceamento (servidor SERV_SWSID para com o servidor SERV_SGBD_C), deverá ser empregada uma rede de alta velocidade, sem a necessidade de utilização de recursos do protocolo SSL, haja vista as condições de segurança descritas anteriormente, relativas aos servidores SERV_SWSID e SERV_SGBD_C.

O Servidor Web HTTP, SW_HTTP, tem por função publicar os serviços do *software* SICAP.WEBSERVICES por meio de protocolo HTTP (*Hypertext Transfer Protocol*). São exemplos do SW_HTTP os servidores de páginas HTTP: Internet Information Server (IIS7, 2009); Apache TomCat (APACHE, 2012).

O *software* SICAP.MODEL representa a implementação do modelo de classes do SiCAP e tem a finalidade de disponibilizar os dados personificados em forma de objetos e, as funcionalidades por meio de métodos, para permitir ao sistema realizar suas funções. Essa técnica possibilita que a informação dos objetos do sistema seja persistida em suas respectivas estruturas de objetos, sendo também cooperativa para facilitação da manutenção do próprio sistema.

O *software* SICAP.WEBSERVICES realiza o interfaceamento descrito anteriormente, interconectando o subsistema tático-administrativo SSTA (por meio do servidor SERV_SWSID) aos subsistemas operacional-administrativo SSOP e operacional-PCAP SSOA. Entre os benefícios mais evidentes, agregados com a criação de uma camada controladora de *Web Services*, está o isolamento das regras de negócios de *softwares* e a

independência de plataforma para desenvolvimento dos *softwares* SICAP.MODEL e SICAP.WEBSERVICES, além de possibilitar a criptografia de informações por meio do protocolo SSL. Na Figura 3.16 são apresentadas as subdivisões do SICAP.WEBSERVICES, indicadas para uso no SiCAP.

Figura 3.16 - Subdivisões do SICAP.WEBSERVICES

Essas subdivisões organizam e facilitam a manutenção do *software* SICAP.WEBSERVICES, separando os *Web Services* de acordo com o subsistema que irá atender, formando assim as três divisões designadas por *Web Services* do SSTA, *Web Services* do SSOP e *Web Services* do SSOA.

O *software* SICAP.IMPORTAÇÃO é dedicado à realização das importações de dados descritas anteriormente. Permite integração com as bases de dados pertencentes aos sistemas externos ao SiCAP, dos quais os dados serão importados. Essa integração isola do SiCAP as regras para acessos as bases em questão, utilizadas pelos respectivos sistemas externos. De forma pertinente ao exposto informa-se que deve ser prevista a atualização dos dados importados, de forma periódica, sendo atualizadas somente as diferenças entre o SiCAP e os sistemas externos. Na Figura 3.17, é exibido o fluxo das informações importadas pelo SICAP.IMPORTAÇÃO.

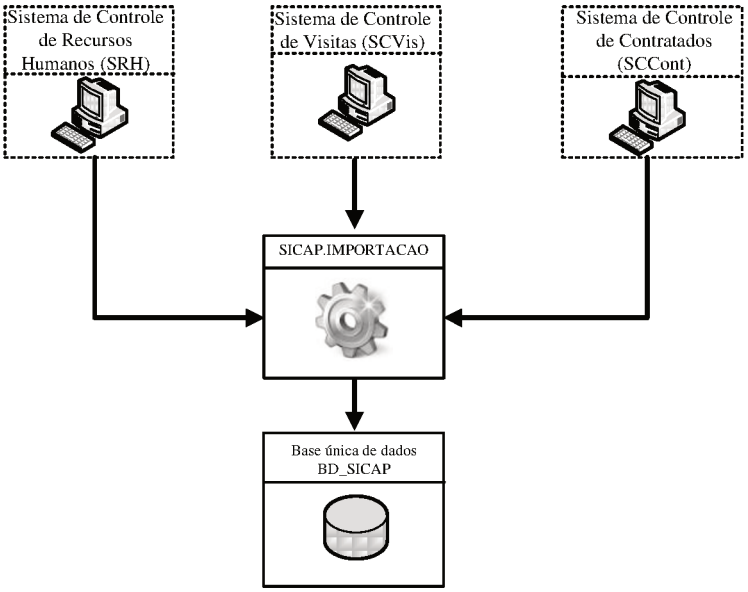

Figura 3.17 - Fluxo das informações importadas pelo SICAP.IMPORTAÇÃO

Para expor as operações do *software* SICAP.IMPORTAÇÃO, será utilizado o fluxograma analítico contido na Figura 3.18.

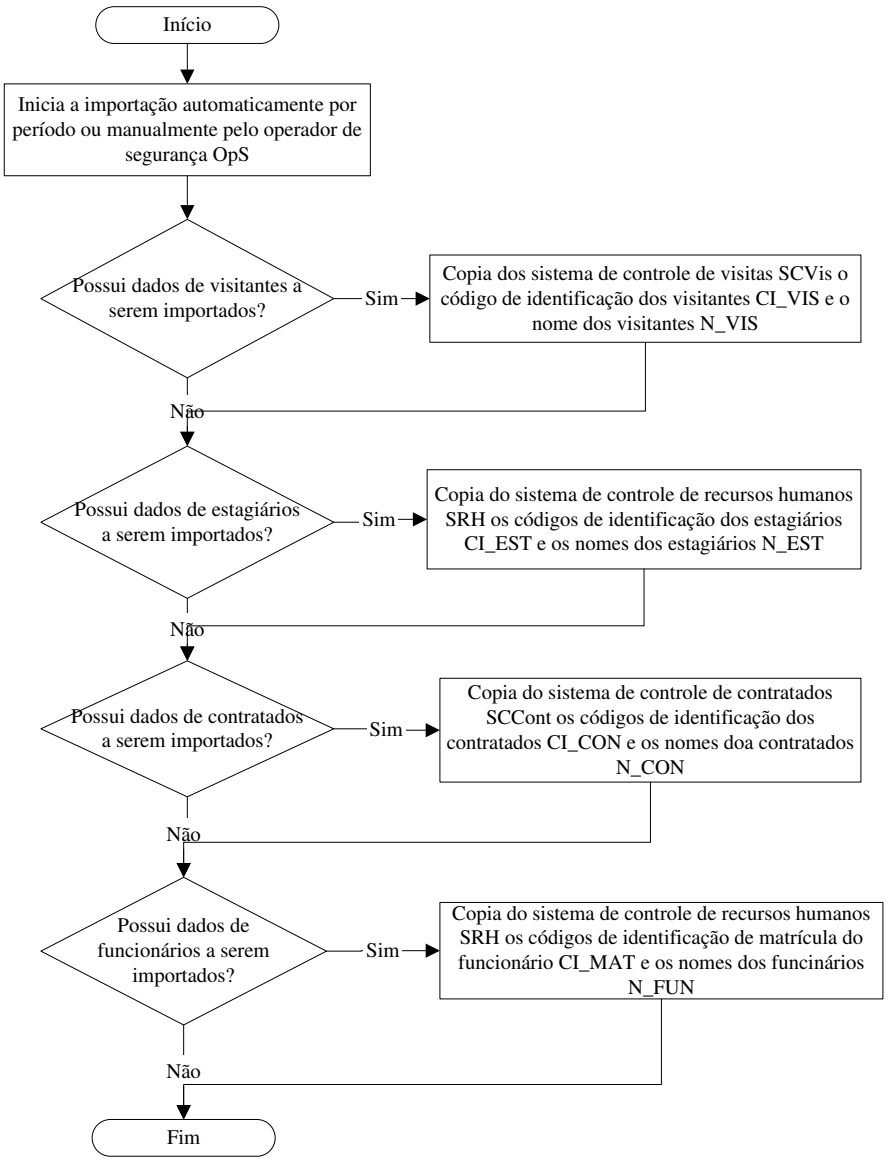

Figura 3.18 - Fluxograma analítico das operações do SICAP.IMPORTAÇÃO

3.9.4 Estação de trabalho SICAP.AUDITORIA (E_SICAP.AUDITORIA)

A "Estação de Trabalho SICAP.AUDITORIA" (E_SICAP.AUDITORIA) é o equipamento que hospedará os *softwares* "SICAP.AUDITORIA" e "Sistema Operacional de Cliente" (SO_CLIENTE). Além de hospedar esses *softwares*, a E_SICAP.AUDITORIA deverá permitir a comunicação de dados com os respectivos equipamentos utilizados nos demais elementos do SiCAP, por conexão com as redes locais ReLoNI. O *software* SICAP.AUDITORIA permite acessar as informações referentes aos registros de tentativas de acessos de usuários USR, RTA_USR, que são destinadas às finalidades de auditoria, sendo

sua operação pertinente ao gerente de segurança patrimonial GSPa e operador de segurança OpS. O SICAP.AUDITORIA é executado sobre o sistema operacional de cliente SO_CLIENTE, e suas operações permitem visualizar ou imprimir as informações em questão, além de exteriorizá-las ou interiorizá-las, proporcionando cópias de segurança e liberação de espaço de memória secundária no SiCAP. Entretanto, os dados referentes a essas informações poderão ser acessados, para leitura e cópia, pelos demais sistemas computacionais da empresa, devidamente autorizados, acessando os respectivos campos da base de dados BD_SICAP, por meio das redes locais ReLoNI.

Como exemplo do sistema operacional SO_CLIENTE, podem ser citados os seguintes: Microsoft Windows XP, Vista, Seven (MICROSOFT, 2012); Linux (LINUX, 2012). Na concepção do SiCAP estações de trabalho utilizadas na empresa poderão exercer as funções da estação de trabalho E_SICAP.AUDITORIA, desde que, sejam adequadas e permitam a execução dos *softwares* hospedados por essa última. Como tipo de equipamento que permite a implementação de estações de trabalho E_SICAP.AUDITORIA são indicados os computadores pessoais do padrão IArch ou compatíveis, sendo exemplo desses o *notebook* modelo Vaio PCG-5K1L, fornecido pela Empresa Sony Inc (SONY, 2012).

Para expor as operações do *software* SICAP.AUDITORIA serão utilizados fluxogramas analíticos, sendo um principal e outros referentes a subprocessos específicos existentes nesse principal. Na Figura 3.19 é exposto o fluxograma analítico principal, referente às operações do *software* SICAP.AUDITORIA.

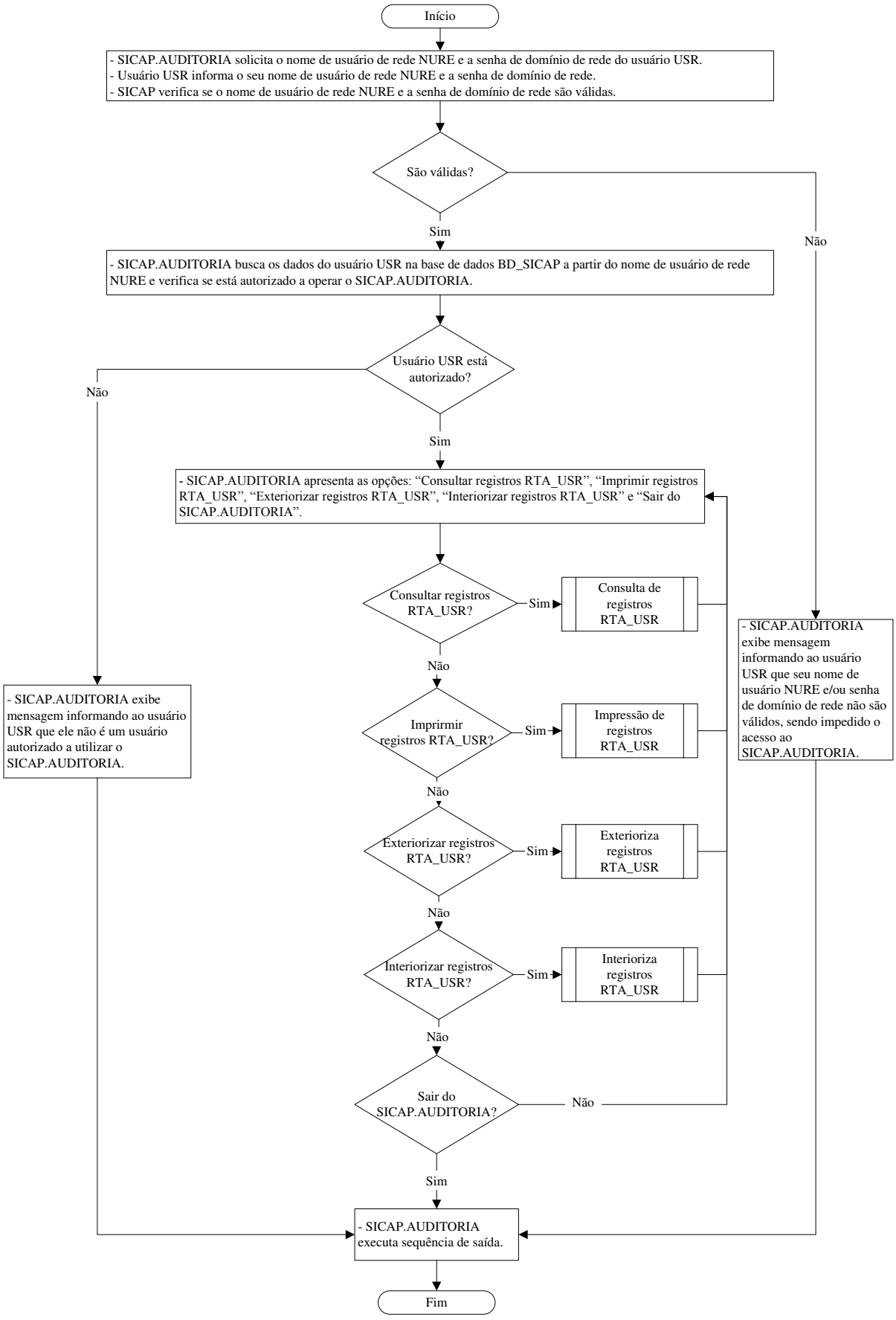

Figura 3.19 - Fluxograma analítico principal do *software* SICAP.AUDITORIA

Na Figura 3.20, é exposto o fluxograma analítico referente ao subprocesso “Consulta de registros RTA_USR”.

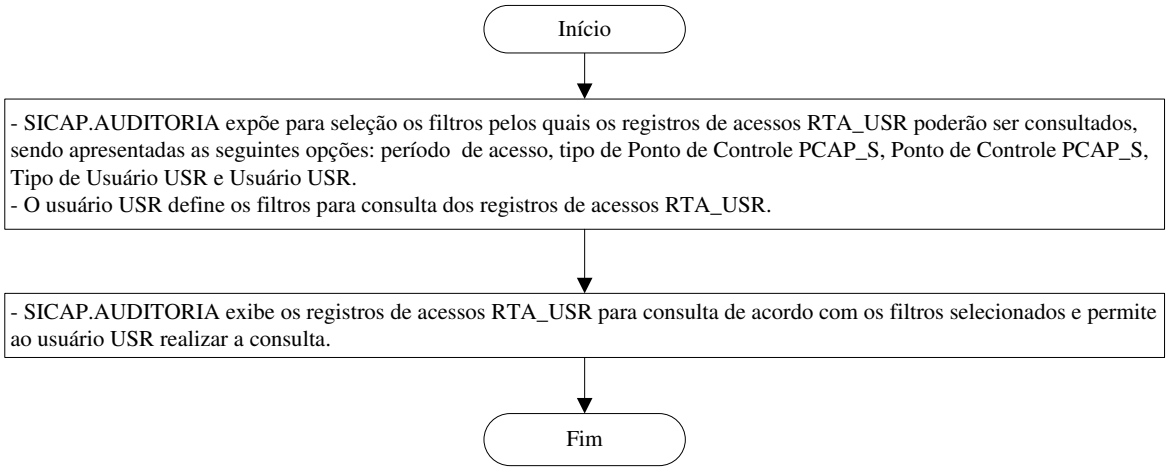

Figura 3.20 - Fluxograma analítico do subprocesso “Consulta de registros RTA_USR”

Na Figura 3.21, é exposto o fluxograma analítico referente ao subprocesso “Impressão de registros RTA_USR”.

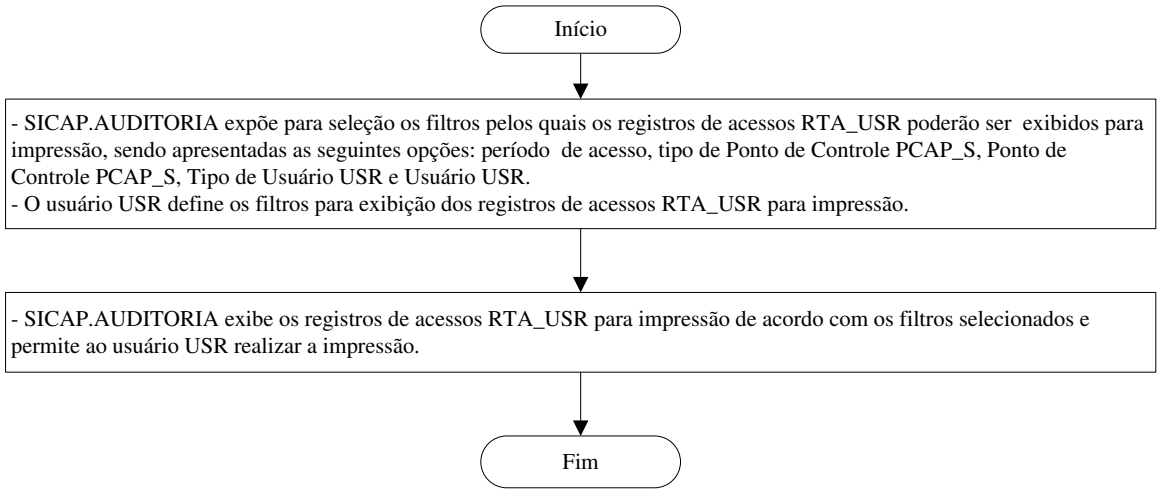

Figura 3.21 - Fluxograma analítico do subprocesso “Impressão de registros RTA_USR”

Na Figura 3.22, é exposto o fluxograma analítico referente ao subprocesso “Exterioriza registros RTA_USR”.

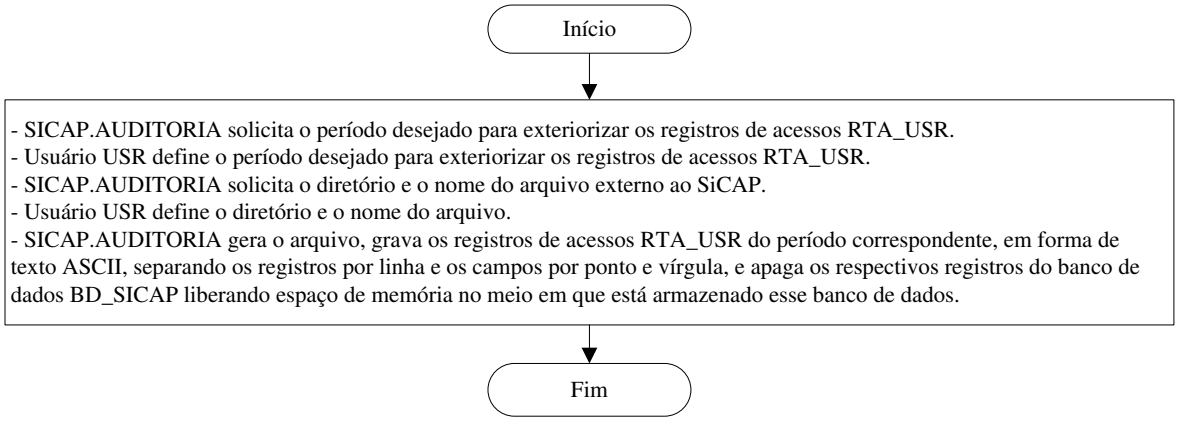

Figura 3.22 - Exterioriza registros RTA_USR

Na Figura 3.23, é exposto o fluxograma analítico referente ao subprocesso “Interioriza registros RTA_USR”.

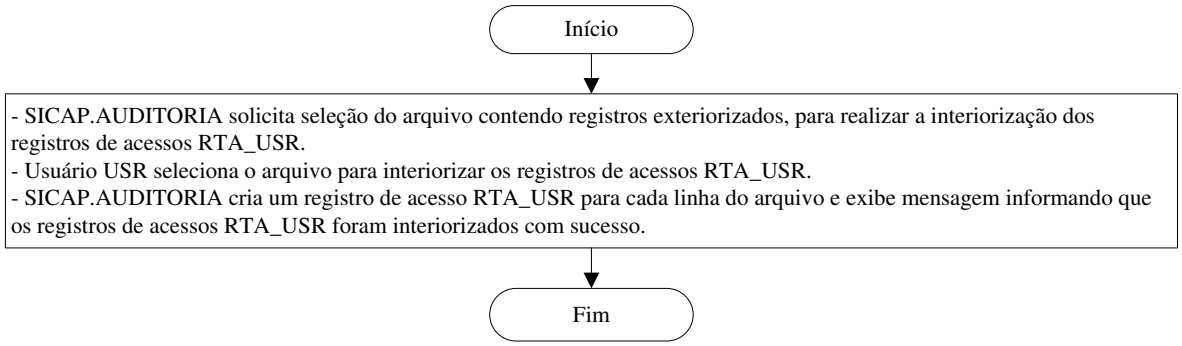

Figura 3.23 - Interioriza registros RTA_USR

3.10 SUBSISTEMA SiCAP-OPERACIONAL-ADMINISTRATIVO (SSOA)

3.10.1 Arquitetura do SSOA

O “Subsistema SiCAP-Operacional-Administrativo” (SSOA) está alocado junto aos sistemas computacionais não industriais do nível operacional SCNINO e se aplica a realização das operações destinadas ao operador de segurança OpS, descritas anteriormente e referentes aos seguintes elementos do SiCAP: usuário USR; cartão de identificação CId_S; componentes referentes ao perfil biométrico da impressão digital CoRePBID_S; equipamentos de proteção pessoal EPP_S; ponto de controle de acessos de pessoas PCAP_S. Na Figura 3.24, é apresentada a arquitetura do subsistema SSOA, sendo a descrição de seus elementos expostas nas subseções a seguir, pertinentes a esta.

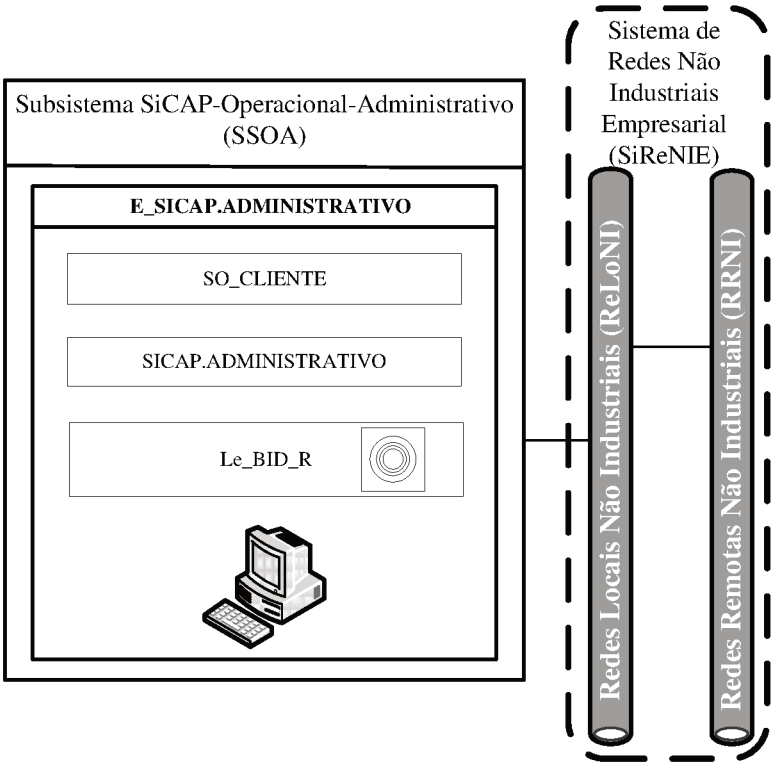

Figura 3.24 - Arquitetura do SSOA

3.10.2 Estação de trabalho SICAP.ADMINISTRATIVO (E_SICAP.ADMINISTRATIVO)

A "Estação de trabalho SICAP.ADMINISTRATIVO" (E_SICAP. ADMINISTRATIVO) é o equipamento que hospedará os *softwares* "SICAP.ADMINIDSTRATIVO" e "Sistema Operacional de Cliente" (SO_CLIENTE), permitindo também a conexão do leitor biométrico da impressão digital Le_BID_R. Além de hospedar esses *softwares*, deverá permitir a comunicação de dados com os respectivos equipamentos utilizados nos demais elementos do SiCAP, por meio de conexão com as redes locais ReLoNI. O *software* SICAP.ADMINISTRATIVO é executado sobre o sistema operacional SO_CLIENTE e permite ao operador de segurança OpS realizar suas atividades. O leitor biométrico Le_BID_R será utilizado nas operações que exigirem a extração de informações biométricas da impressão digital do usuário USR.

Como exemplos do sistema operacional SO_CLIENTE, podem ser citados os mesmos descritos na subseção "3.9.4". Na concepção do SiCAP estações de trabalho utilizadas na empresa poderão exercer as funções da estação de trabalho E_SICAP.ADMINISTRATIVO,

desde que, sejam adequadas e permitam a execução dos *softwares* hospedados pela estação em questão. Como tipo de equipamento que permite a implementação de estações de trabalho E_SICAP. ADMINISTRATIVO são indicados os computadores pessoais do padrão IArch ou compatíveis, sendo exemplo desses os mesmos descritos na subseção “3.9.4”.

Para expor as operações do *software* SICAP.ADMINISTRATIVO, serão utilizados fluxogramas analíticos, sendo um principal e outros referentes a subprocessos específicos existentes nesse principal. Na Figura 3.25, é exposto o fluxograma analítico principal, referente às operações do *software* SICAP.ADMINISTRATIVO.

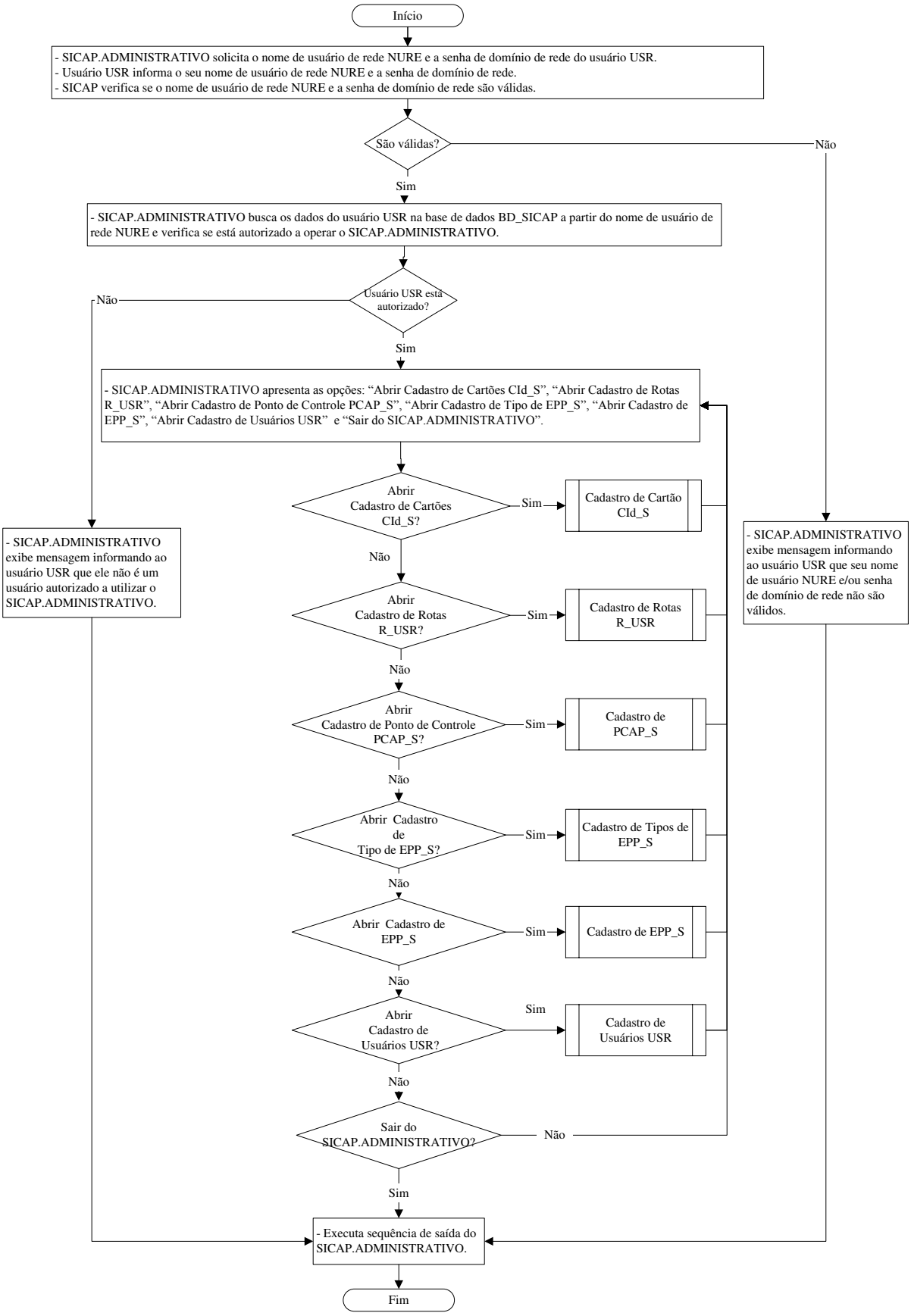

Figura 3.25 - Fluxograma analítico principal do *software* SICAP.ADMINITRATIVO

Na Figura 3.26, é exposto o fluxograma analítico referente ao subprocesso “Cadastro de Cartão CId_S”.

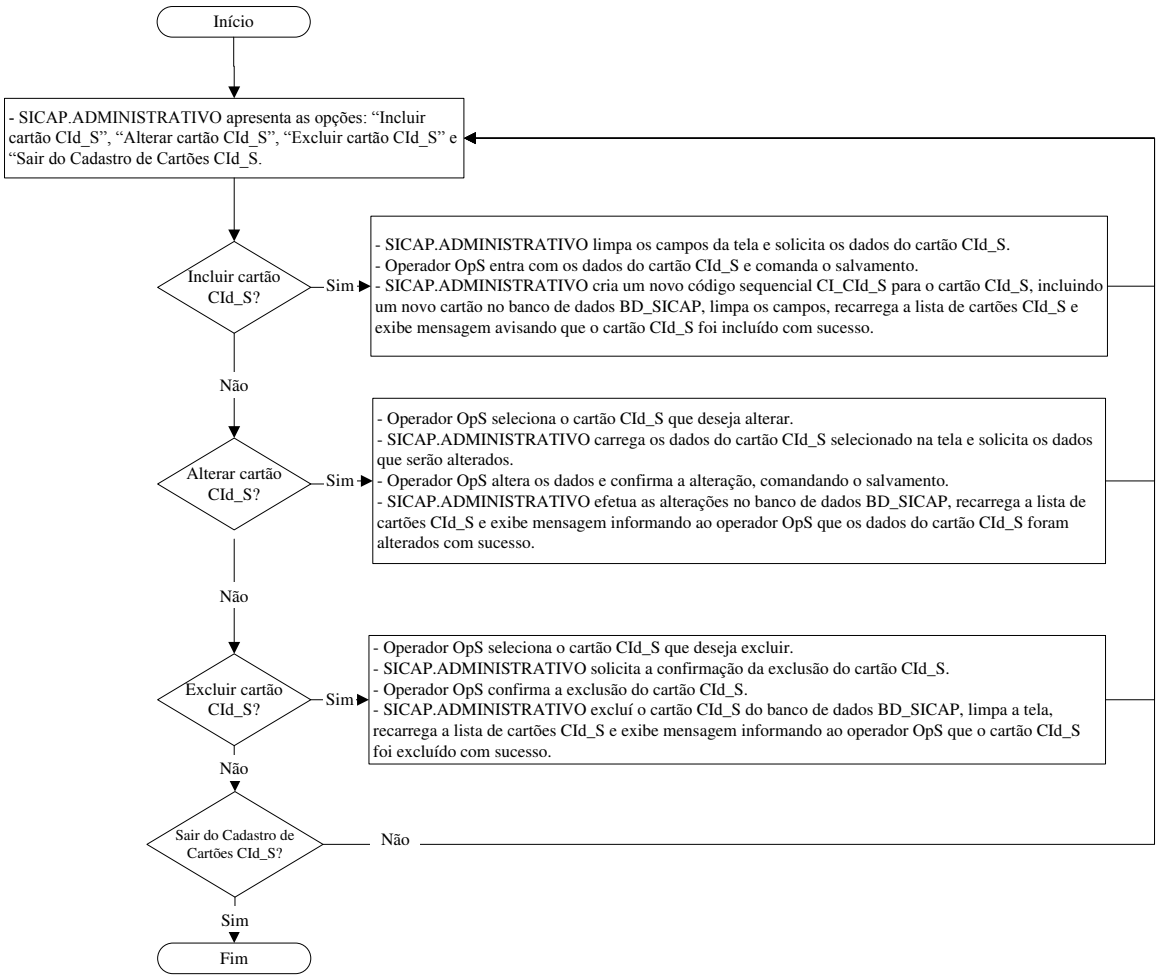

Figura 3.26 - Fluxograma analítico do subprocesso "Cadastro de Cartão CId_S”

Na Figura 3.27, é exposto o fluxograma analítico referente ao subprocesso “Cadastro de Rotas R_USR”.

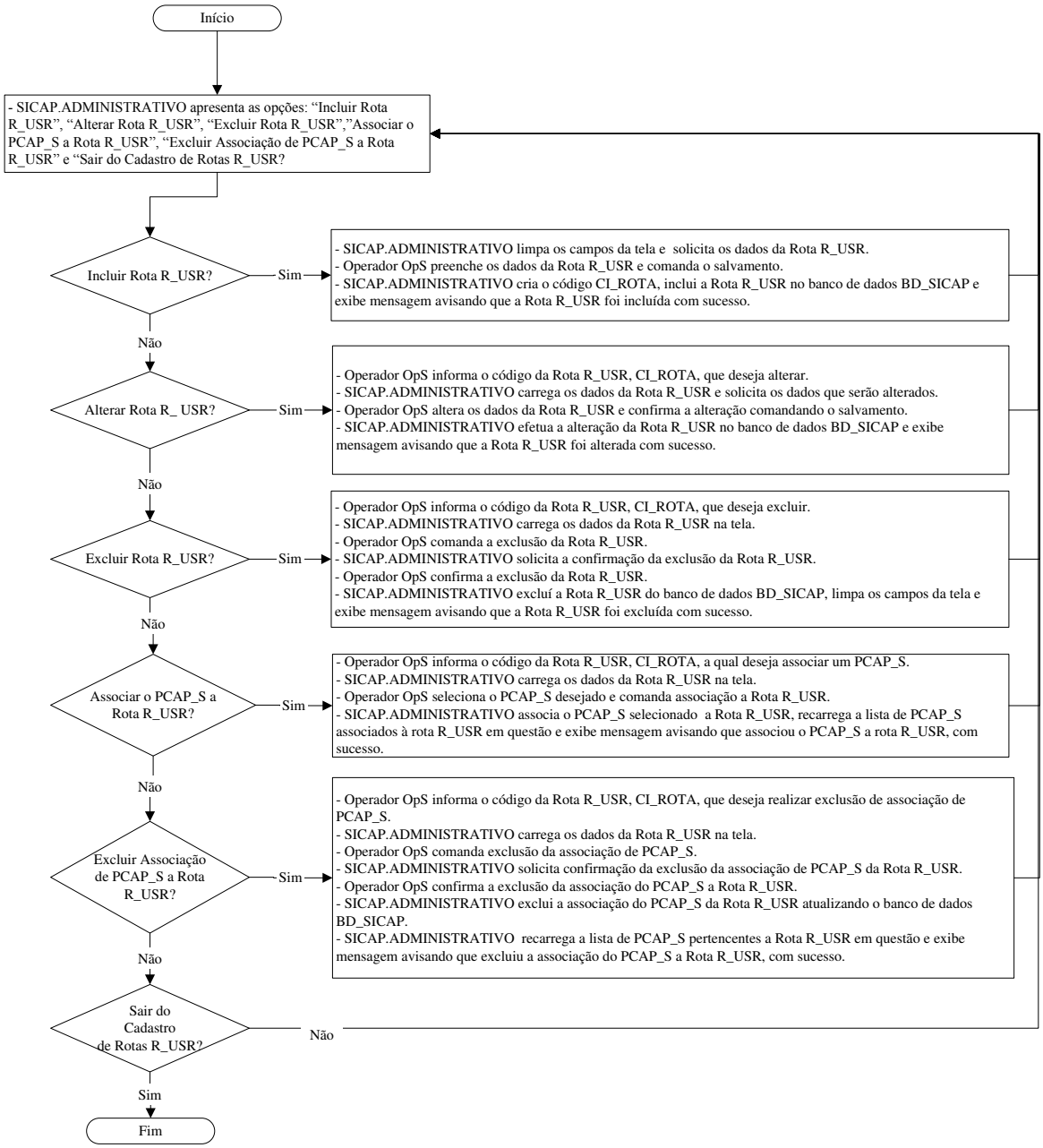

Figura 3.27 - Fluxograma analítico do subprocesso "Cadastro de Rotas R_USR"

Na Figura 3.28, é exposto o fluxograma analítico referente ao subprocesso "Cadastro de PCAP_S".

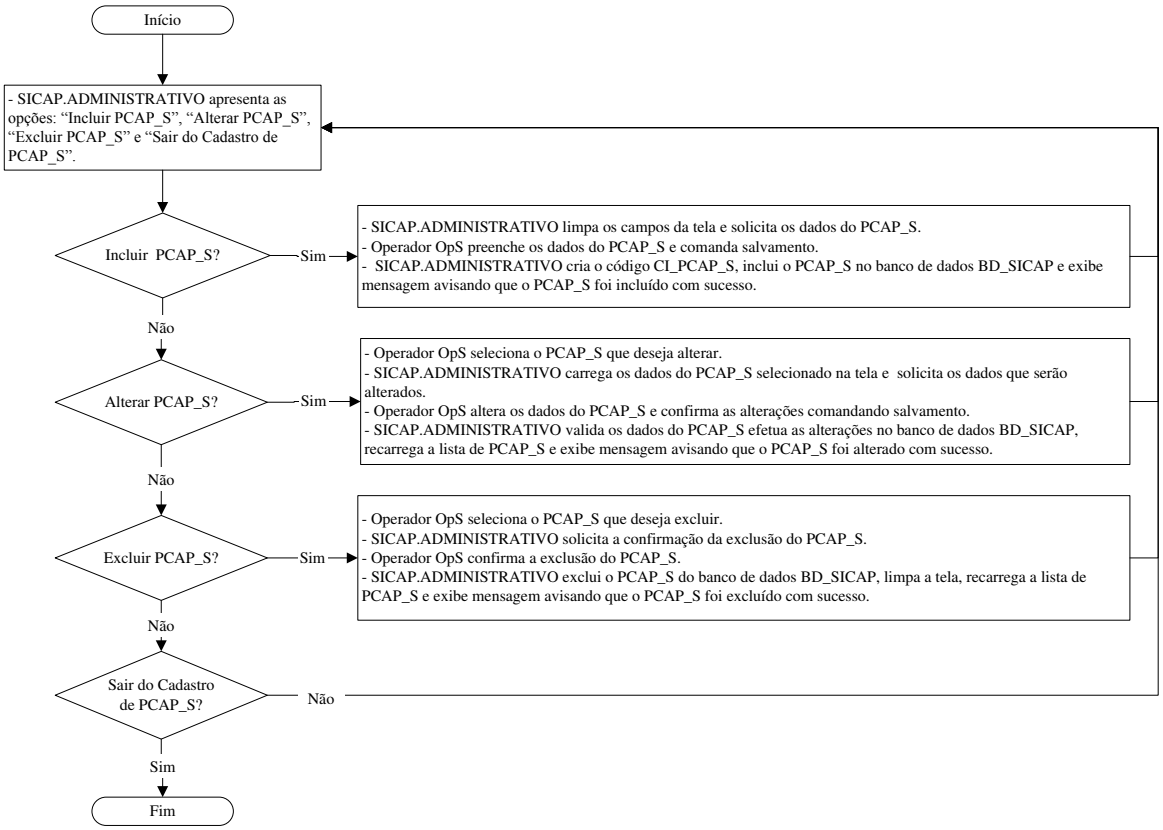

Figura 3.28 - Fluxograma analítico do subprocesso "Cadastro de PCAP_S"

Na Figura 3.29, é exposto o fluxograma analítico referente ao subprocesso “Cadastro de Tipos de EPP_S”.

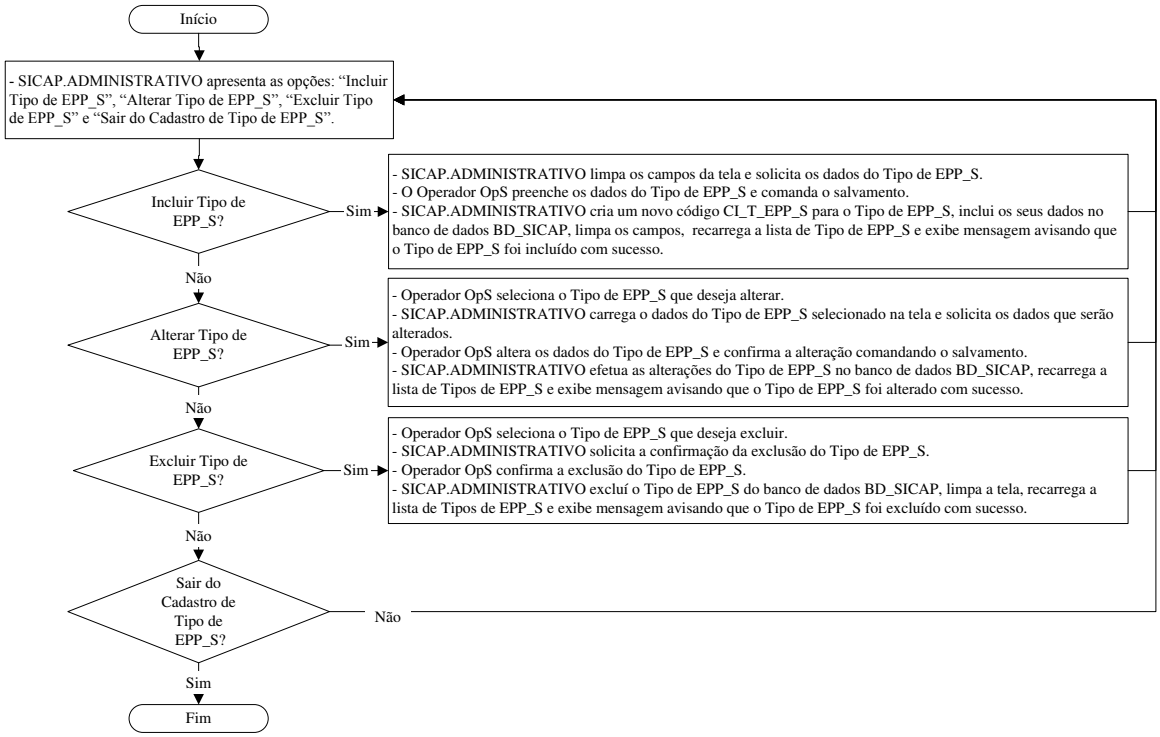

Figura 3.29 - Fluxograma analítico do subprocesso "Cadastro de Tipos de EPP_S"

Na Figura 3.30, é exposto o fluxograma analítico referente ao subprocesso "Cadastro de EPP_S".

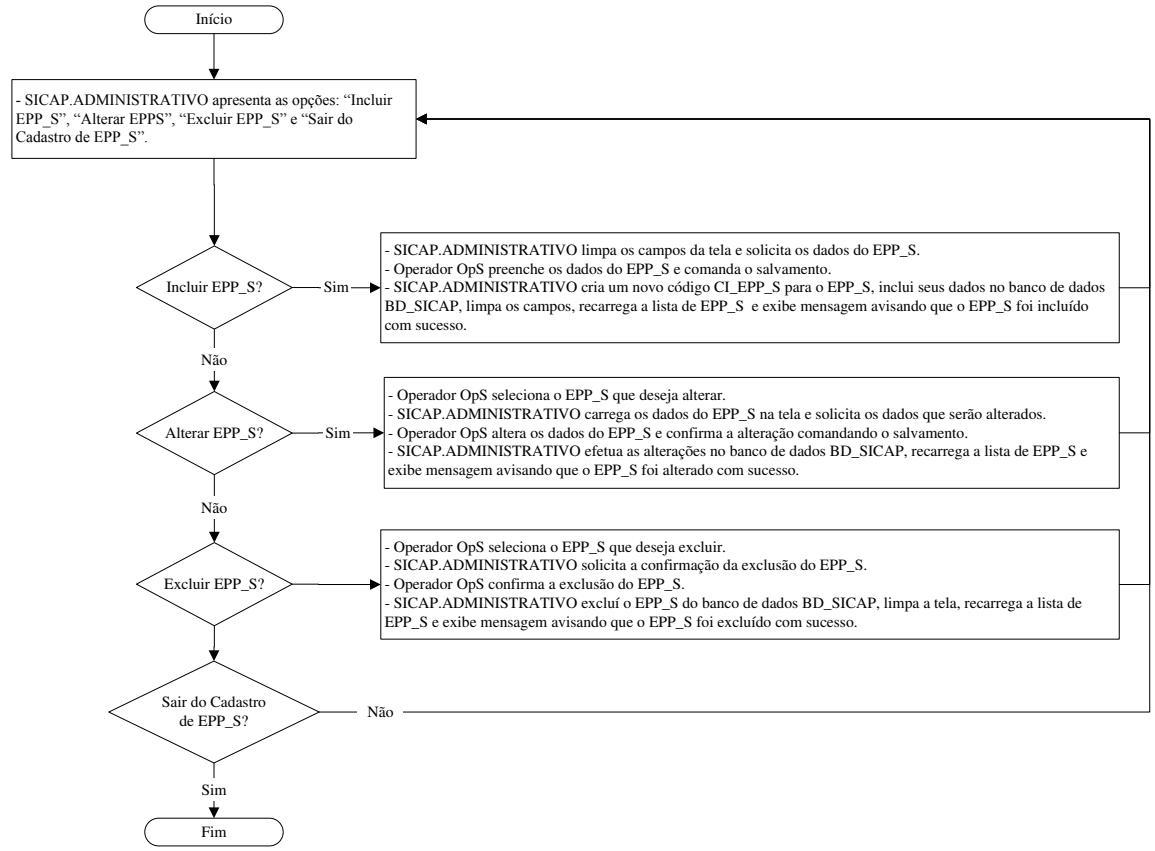

Figura 3.30 - Fluxograma analítico do subprocesso "Cadastro de EPP_S"

Na Figura 3.31, é exposto o fluxograma analítico referente ao subprocesso “Cadastro de Usuários USR”.

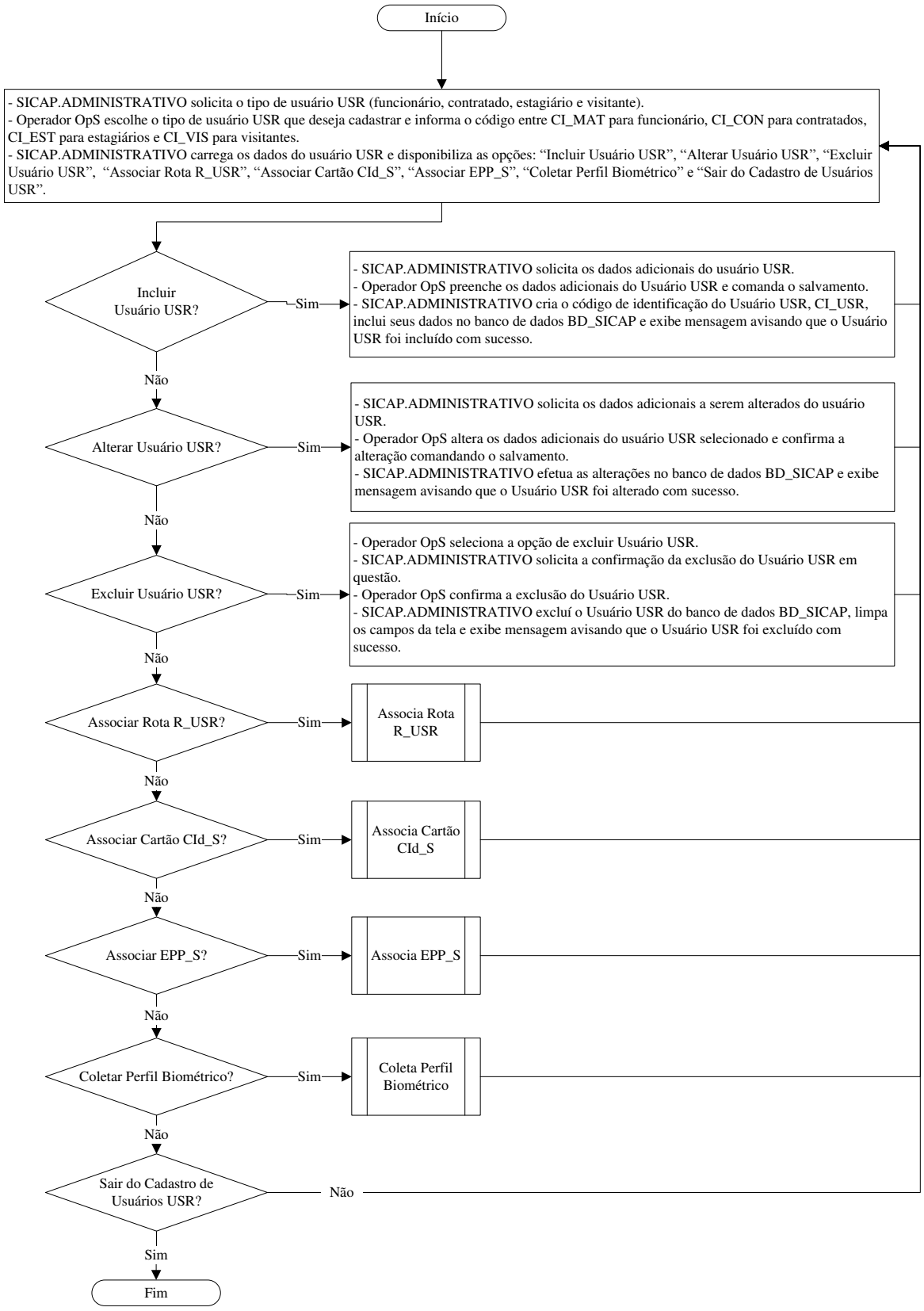

Figura 3.31 - Fluxograma analítico do subprocesso “Cadastro de Usuários USR”

Na Figura 3.32, é exposto o fluxograma analítico referente ao subprocesso “Associa Rota R_USR”.

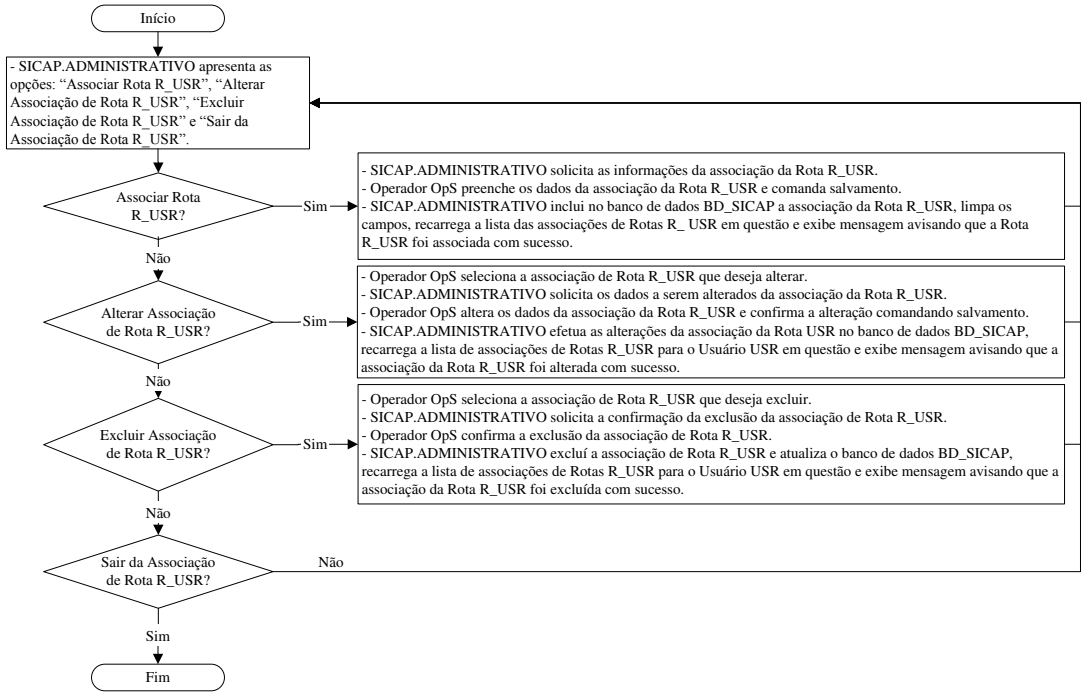

Figura 3.32 - Fluxograma analítico do subprocesso "Associa Rota R_USR"

Na Figura 3.33, é exposto o fluxograma analítico referente ao subprocesso “Associa Cartão CId_S”.

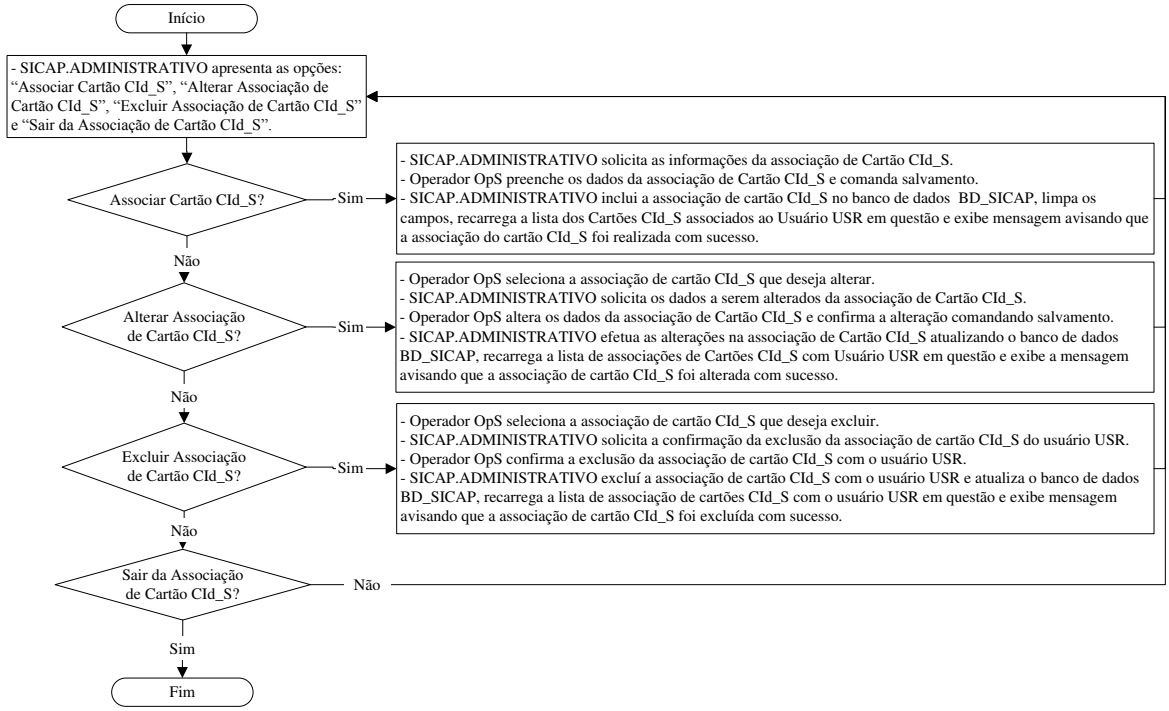

Figura 3.33 - Fluxograma analítico do subprocesso "Associa Cartão CId_S"

Na Figura 3.34, é exposto o fluxograma analítico referente ao subprocesso “Associa EPP_S”.

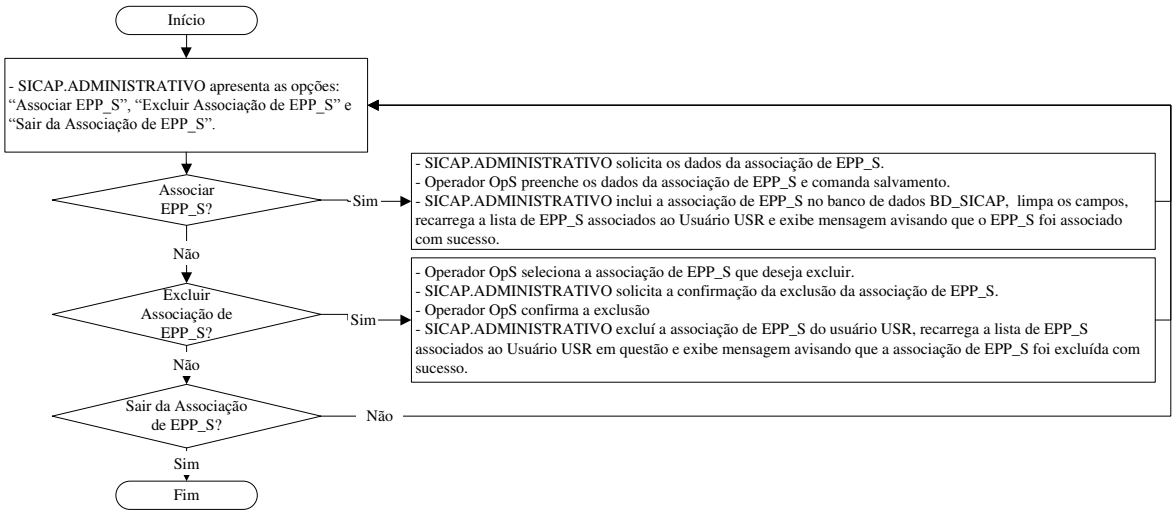

Figura 3.34 - Fluxograma analítico do subprocesso “Associa EPP_S”

Na Figura 3.35, é exposto o fluxograma analítico referente ao subprocesso “Coleta Perfil Biométrico”.

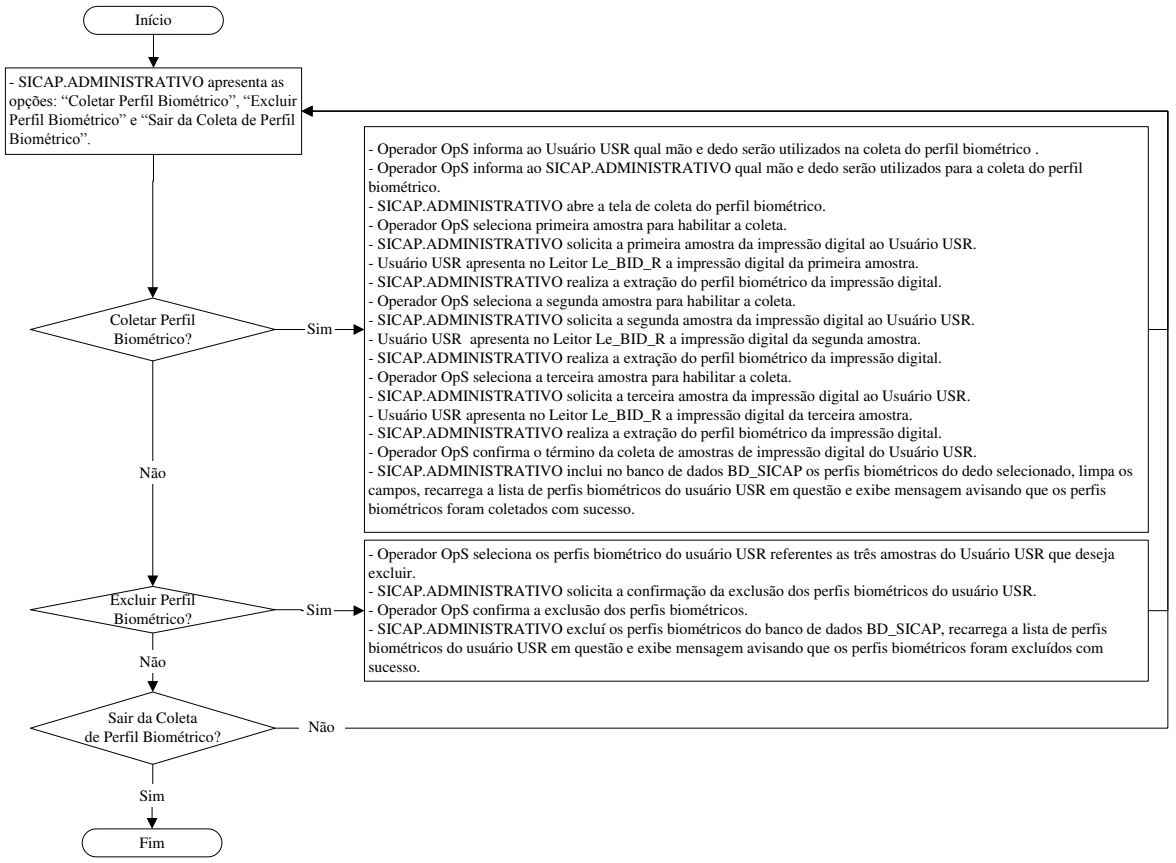

Figura 3.35 - Fluxograma analítico do subprocesso “Coleta Perfil Biométrico”

3.11 SUBSISTEMA SiCAP-OPERACIONAL-PCAP (SSOP)

3.11.1 Arquitetura do SSOP

O "Subsistema SiCAP-Operacional-PCAP" (SSOP) está alocado junto aos sistemas computacionais não industriais do nível operacional SCNINO, e se aplica à realização das operações de controle de acessos, proporcionadas pelo SiCAP, sendo seus equipamentos instalados em cada PCAP_S conforme mencionado na subseção "3.8". Essas operações envolvem: o usuário USR, que pretende acessar uma área industrial de segurança; o operador de segurança OpS, que atua na configuração dos PCAP_S; o segurança patrimonial SeP, que monitora as ocorrências no PCAP_S, libera o acesso forçado e interrompe o Alarme de PCAP_S; os equipamentos para controle de acessos de pessoas ECAP_S. Neste contexto, o controle de acessos proporcionado pelo SiCAP opera de forma automática, utilizando recursos do subsistema SSOP, sendo somente necessária a intervenção do segurança patrimonial SeP para: iniciação do subsistema SSOP, para partida a frio (*boot*); operação de acesso forçado; interrupção do Alarme de PCAP_S. Na Figura 3.36, é apresentada a arquitetura do subsistema SSOP, sendo a descrição de seus elementos expostas nas subseções a seguir, pertinentes a esta.

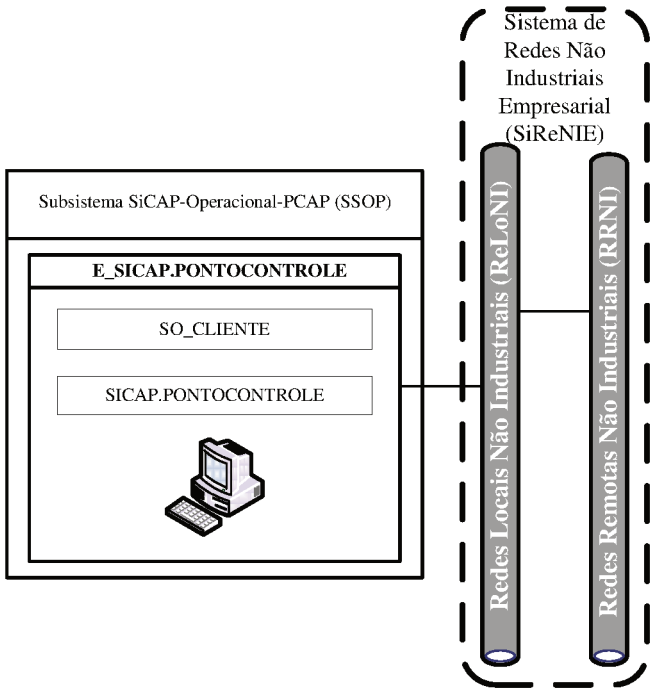

Figura 3.36 - Arquitetura do SSOP

3.11.2 Estação de trabalho SICAP.PONTOCONTROLE (E_SICAP. PONTOCONTROLE)

A "Estação de trabalho SICAP.PONTOCONTROLE" (E_SICAP. PONTOCONTROLE) é o equipamento que hospedará os *softwares* "SICAP.PONTOCONTROLE" e "Sistema Operacional de Cliente" (SO_CLIENTE), permitindo também a conexão do leitor biométrico da impressão digital Le_BID_R, leitor RFID Le_RFID e dos equipamentos para controle físico de acessos de pessoas ECoFAP. Além de hospedar esses *softwares*, deverá permitir a comunicação de dados com os respectivos equipamentos utilizados nos demais elementos do SiCAP, por meio de conexão com as redes locais ReLoNI. O *software* SICAP.PONTOCONTROLE é executado sobre o sistema operacional SO_CLIENTE e permite realizar as operações de controle de acessos de pessoas proporcionadas pelo SiCAP, dentre as quais, está o serviço de autenticação por senha de domínio de rede, que utiliza a IHM (Interface Homem-Máquina) da estação E_SICAP.PONTOCONTROLE para entrada de dados. O leitor Le_RFID será utilizado nas operações pertinentes ao serviço de identificação que utiliza a leitura do cartão CId_S. O leitor biométrico Le_BID_R será utilizado nas operações pertinentes aos serviços de identificação e/ou autenticação, que realizam a extração de informações biométricas da impressão digital do usuário USR, para comparação com perfis biométricos armazenados no SiCAP.

Como exemplo do sistema operacional SO_CLIENTE, podem ser citados os mesmos descritos na subseção "3.9.4". Na concepção do SiCAP deverá ser utilizado um equipamento exclusivo para a estação E_SICAP.PONTOCONTROLE. Para esse equipamento indica-se a utilização de computadores pessoais do padrão IArch ou equivalentes, sendo exemplo desses os mesmos descritos na subseção "3.9.4".

Para expor as operações do *software* SICAP.PONTOCONTROLE, serão utilizados fluxogramas analíticos, sendo um principal e outros referentes a subprocessos específicos existentes nesse principal. Na Figura 3.37, é exposto o fluxograma analítico principal, referente às operações do *software* SICAP.PONTOCONTROLE.

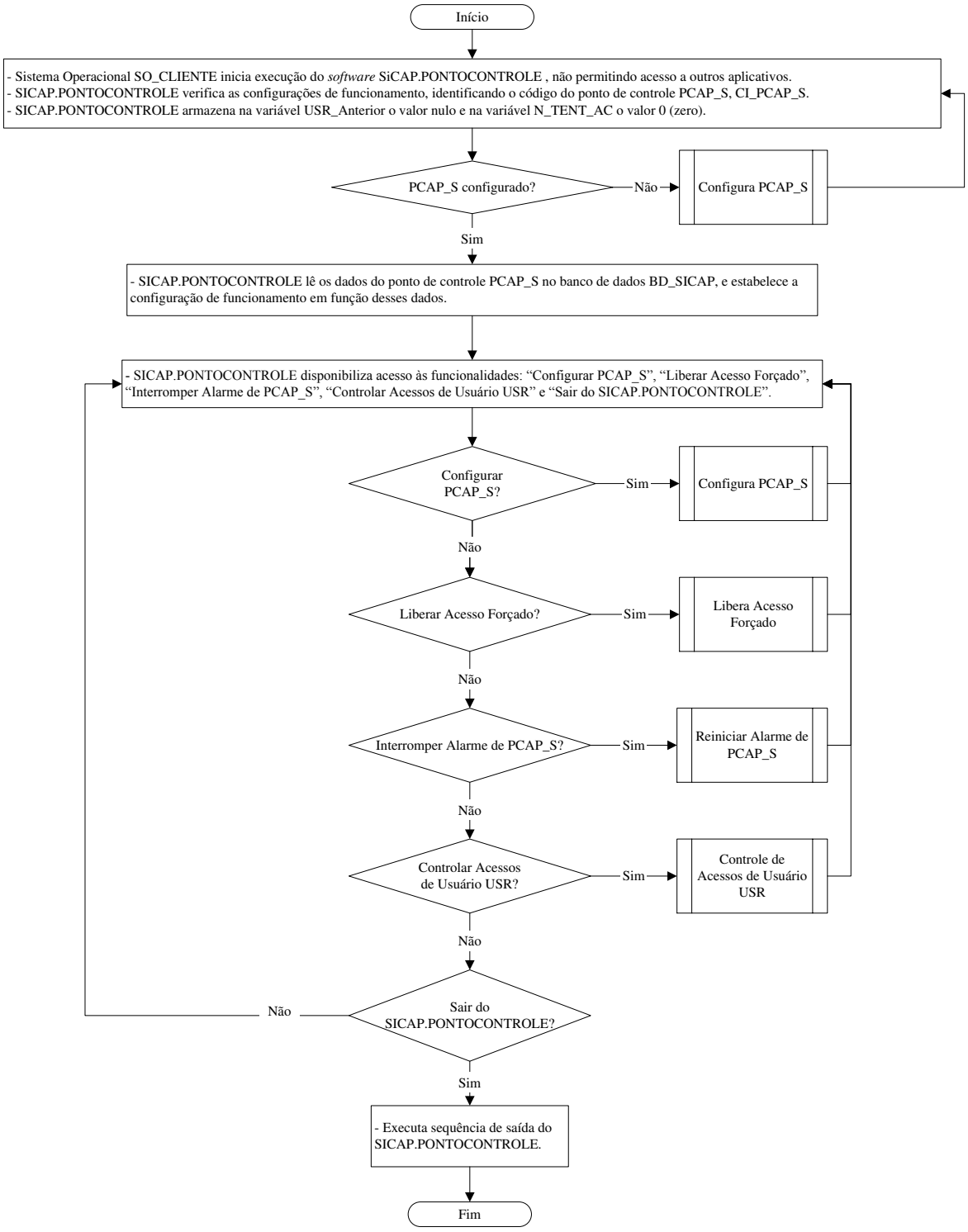

Figura 3.37 - Fluxograma analítico principal do *software* SICAP.PONTOCONTROLE

Na Figura 3.38, é exposto o fluxograma analítico referente ao subprocesso "Configura PCAP_S".

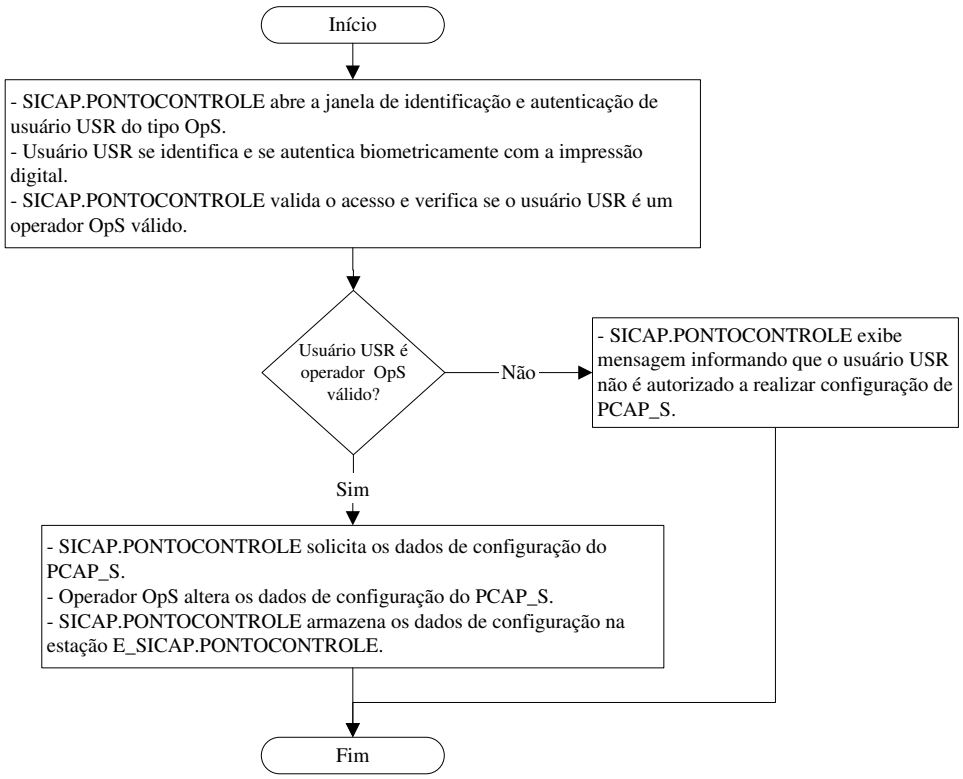

Figura 3.38 - Fluxograma analítico do subprocesso “Configura PCAP_S”

Na Figura 3.39, é exposto o fluxograma analítico referente ao subprocesso “Libera Acesso Forçado”.

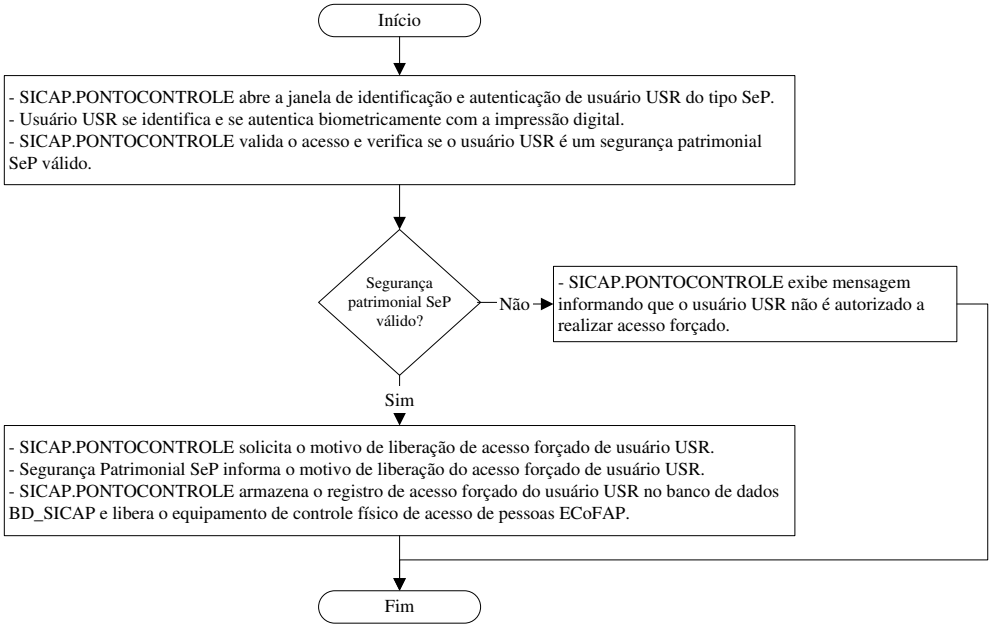

Figura 3.39 - Fluxograma analítico do subprocesso “Libera Acesso Forçado”

Na Figura 3.40, é exposto o fluxograma analítico referente ao subprocesso “Reiniciar Alarme de PCAP_S”.

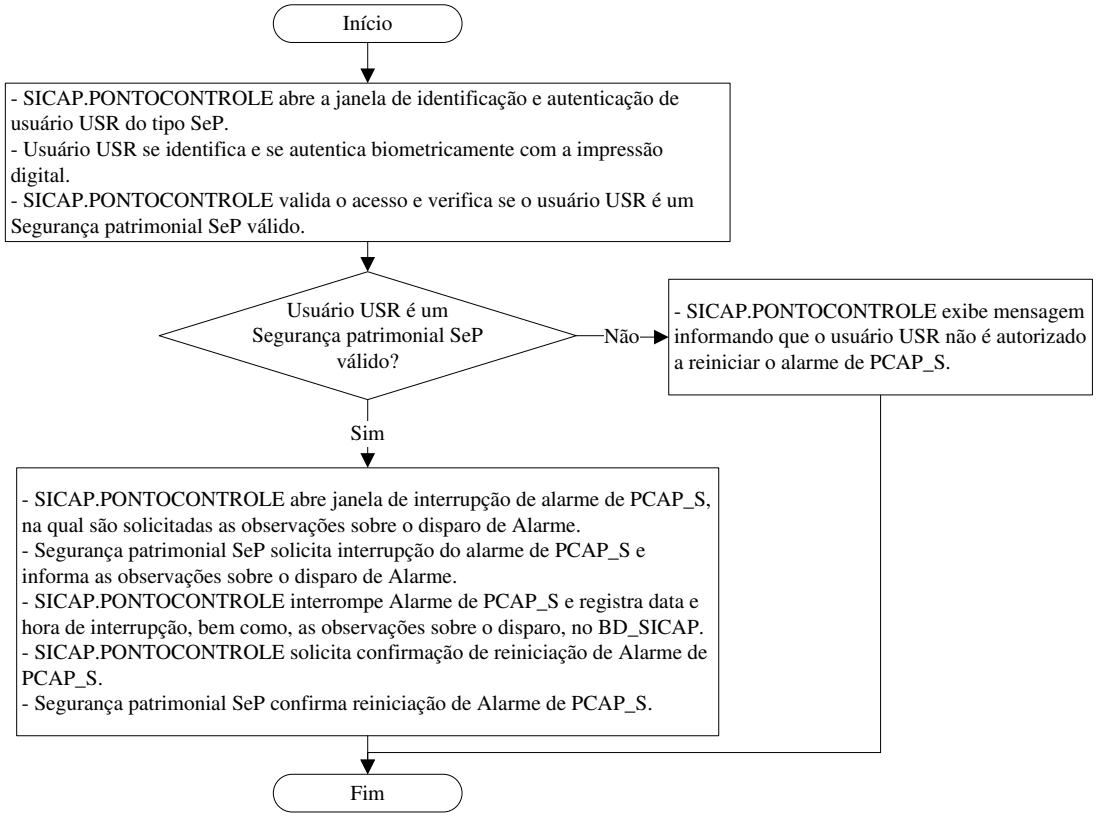

Figura 3.40 - Fluxograma analítico do subprocesso “Reiniciar Alarme de PCAP_S”

Na Figura 3.41, é exposto o fluxograma analítico referente ao subprocesso “Controle de Acessos de Usuário USR”.

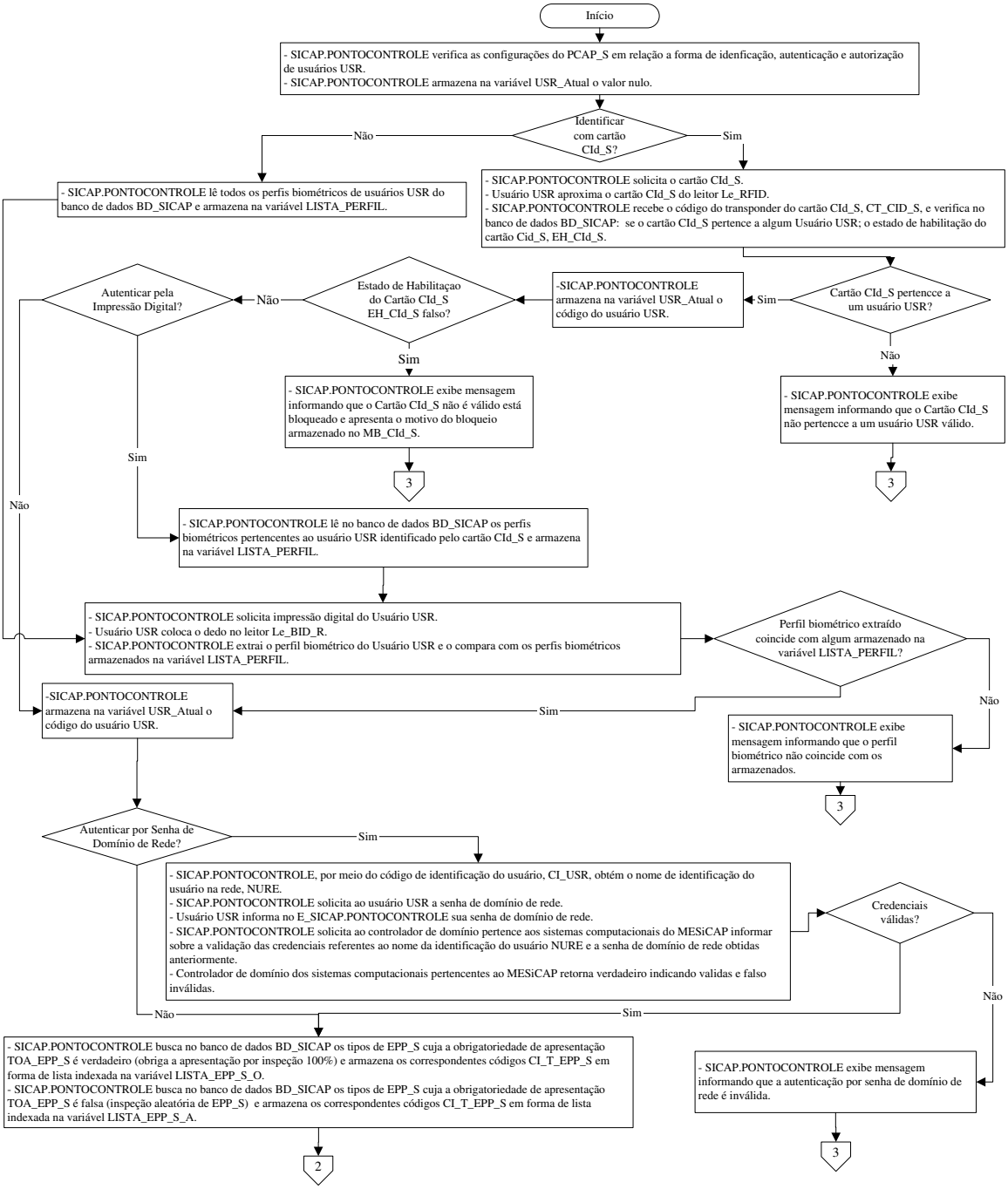

Figura 3.41 - Fluxograma analítico do subprocesso “Controle de Acessos de Usuário USR”

Na Figura 3.42, é exposta a continuação do fluxograma analítico referente ao subprocesso “Controle de Acessos de Usuário USR”.

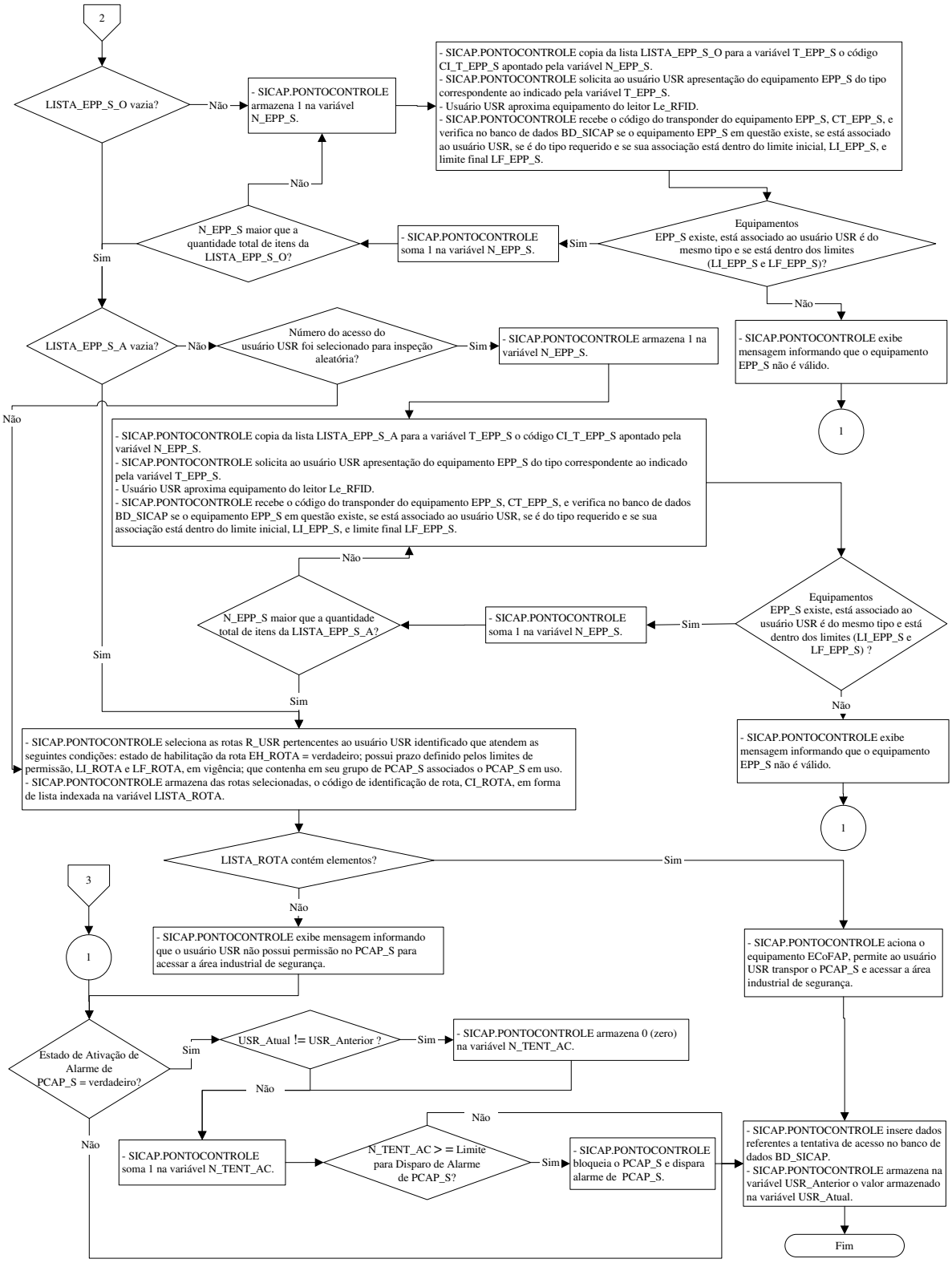

Figura 3.42 - Continuação do fluxograma analítico do subprocesso “Controle de Acessos de Usuário USR”

4 PROTÓTIPOS E TESTES PRÁTICOS

Nesta seção são apresentados os protótipos e os testes práticos referentes ao “Sistema de Controle de Acessos de Pessoas a Áreas Industriais por RFID e Biometria da Impressão Digital” (SiCAP), sendo esses pertinentes a avaliações sobre validação dos princípios de funcionamento de elementos do projeto conceitual do sistema em questão.

4.1 PROTÓTIPOS

4.1.1 Arquitetura para prototipagem da aplicação SiCAP-MESiCAP

Desenvolveu-se uma arquitetura para a prototipagem de elementos da aplicação SiCAP-MESiCAP, a qual é dedicada à realização dos testes práticos referentes ao SiCAP e cuja ilustração é apresentada na Figura 4.1.

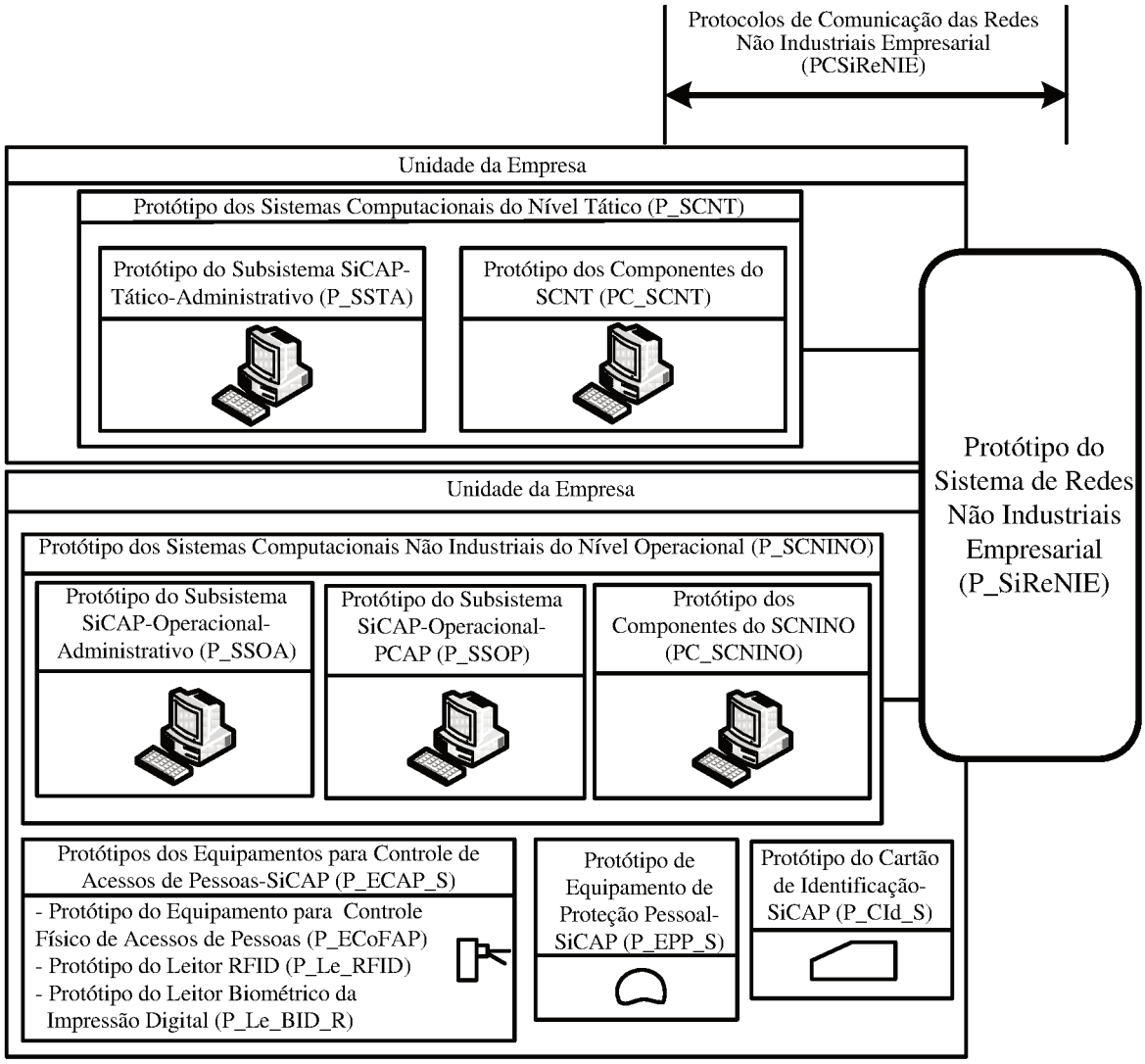

Figura 4.1 - Arquitetura para prototipagem da aplicação SiCAP-MESiCAP

De forma compatível com essa arquitetura, foram obtidos os respectivos protótipos detalhados nas subseções a seguir, relativas a esta. Entretanto, apresenta-se na Figura 4.2 imagem do *hardware* relativo aos protótipos em questão.

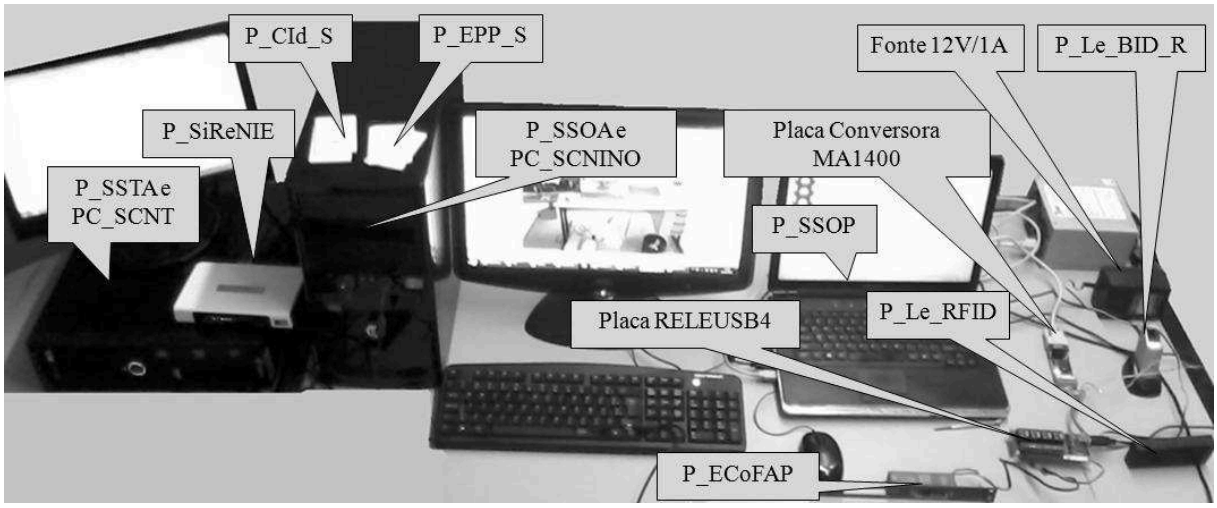

Figura 4.2 - Imagem do *hardware* relativo aos protótipos da aplicação SiCAP-MESiCAP

Nas subseções a seguir é realizada a descrição sobre os protótipos dos equipamentos que compõe a prototipação da aplicação SiCAP-MeSiCAP

4.1.2 Protótipo do Cartão de Identificação-SiCAP (P_CId_S)

Para o "Protótipo do Cartão de Identificação CId_S" (P_CId_S) foi utilizado transponder RFID do tipo cartão, passivo, que opera com baixa frequência em aplicações de identificação à curta distância. Esse transponder é do modelo Indala FlexISO, fornecido pela empresa HID Global (HID, 2012), que opera com frequência de 125kHz, sendo compatível com o protótipo do leitor RFID, P_Le_RFID. A Figura 4.3 apresenta imagem de exemplar do modelo de trasnponder em questão.

Figura 4.3 - Transponder FexISO referente ao P_CId_S (HID, 2012)

Para a realização dos testes práticos foram obtidos 5 transponders do modelo mencionado anteriormente, para utilização como exemplares do protótipo P_CId_S. Os conteúdos desses transponders, em caracteres ASCII, são: 35576; 35581; 35582; 35583; 35584.

4.1.3 Protótipo de Equipamento de Proteção Pessoal-SiCAP (P_EPP_S)

Para o "Protótipo do Equipamento de Proteção Pessoal-SiCAP" (P_EPP_S), foi utilizado transponder RFID do tipo cartão, do mesmo modelo descrito na subseção "4.1.2". Para a realização dos testes práticos foram obtidos 5 transponders do modelo em questão, para utilização como exemplares do protótipo P_EPP_S. Os conteúdos desses transpoders, em caracteres ASCII, são: 35577; 35578; 35580; 35585; 35586.

4.1.4 Protótipos dos Equipamentos para Controle de Acessos de Pessoas-SiCAP (P_ECAP_S)

4.1.4.1 Protótipo do Equipamento para Controle Físico de Acessos de Pessoas (P_ECoFAP)

Para o "Protótipo do Equipamento para Controle Físico de Acessos de Pessoas" (P_ECoFAP), utilizou-se uma tranca eletromagnética modelo Fecho Eletromagnético 12V, fornecida pela Thevear (THEVEAR, 2012). Para permitir a conexão dessa tranca com computador pertencente ao protótipo do subsistema operacional-PCAP (P_SSOP), utilizou-se uma placa controladora de relé com interface USB (*Universal Serial Bus*, Barramento Serial Universal), designada por RELEUSB4 e fornecida pela Andri Elétrica (ANDRI, 2012). Essa placa controladora possibilita ao computador enviar pulso elétrico para o respectivo protótipo do equipamento para controle físico de acessos de pessoas P_ECoFAP, estabelecendo a conexão por sinais elétricos que permite comandar a representação de liberação ou travamento de barreira física, respectivamente correspondentes a trinco destravado e travado. Uma fonte de 12V e 1A, modelo FTP 1201EC, fornecida pela HAYONIK (HAYONIK, 2012), foi utilizada para alimentar a tranca eletromagnética, sendo enviado pulso elétrico com duração de 1s para a liberação. O travamento ocorre com movimentação mecânica, sem a emissão de pulso elétrico. Na Figura 4.4, é apresentada imagem da tranca modelo Fecho Eletromagnético 12V.

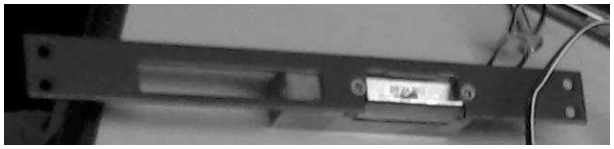

Figura 4.4 - Fecho Eletromagnético referente ao protótipo P_ECoFAP (THEVEAR, 2012)

Na Figura 4.5, apresenta-se imagem da placa RELEUSB4, fornecida pela Andri Elétrica.

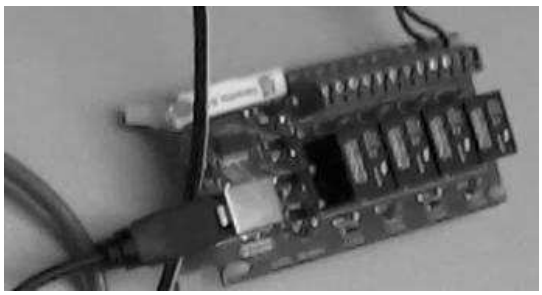

Figura 4.5 - Placa RELEUSB4 referente a protótipo P_ECoFAP (ANDRI, 2012)

Na Tabela 4.1, são apresentadas as características da placa RELEUSB4, disponibilizadas pelo fornecedor.

Tabela 4.1 - Características da placa RELEUSB4 (ANDRI, 2012)

Característica	**Valor**
Quantidade de Saídas	4.
Corrente máxima por saída	2A.
Voltagens	120VCA, 277VCA e 24VCC.
Dimensões	107x50x20mm (CxLxH).
Sistemas Operacionais	Microsoft Windows e Linux.
Linguagens de Programação Suportadas	VB.Net, Object Pascal, C#, C, Java e PHP.

Juntamente com a placa RELEUSB4 foi fornecida uma biblioteca para acessar os recursos de acionamento de relé, sendo essa biblioteca compatível com a linguagem C# utilizada para desenvolvimento de aplicativos empregados nos protótipos do SiCAP.

4.1.4.2 Protótipo do Leitor RFID (P_Le_RFID)

Para o “Protótipo do Leitor RFID” (P_Le_RFID) foi utilizado um leitor do tipo fixo, que opera com frequência de 125kHz, modelo Indala Classic Reader 603, fornecido pela empresa HID Global (HID, 2012), cuja descrição é realizada na subseção “2.4.2”. Na Figura

4.6 apresenta-se imagem do leitor em questão, que é compatível com os transponders referentes aos protótipos P_CId_S e P_EPP_S.

Figura 4.6 - Leitor RFID Indala Classic Reader 603 referente ao P_Le_RFID (HID, 2012)

Para conectar esse leitor ao computador pertencente ao protótipo do subsistema operacianal-PCAP (P_SSOP), utilizou-se uma placa conversora Wiegand-RS232, modelo MA1400, fornecida pela empresa MaCaPS (MACAPS, 2012). Essa placa é necessária devido ao fato do leitor utilizado para o P_Le_RFID transmitir dados no padrão Wiegand e o computador do P_SSOP aceitar interface em RS232 (*Recommended Standard* 232, Padrão Recomendado 232) . Na Figura 4.7, é apresentada imagem da placa conversora MA1400.

Figura 4.7 - Placa conversora MA1400 (MACAPS, 2012)

Na Tabela 4.2, são apresentados os terminais referentes às linhas de transmissão e recepção, na placa conversora em questão, e a designação dos respectivos sinais RS232 associados.

Tabela 4.2 - Terminais na placa conversora MA1400 e sinais RS232

Terminais (conector DB9)	**Sinal RS232**
02	RX.
03	TX.
05	GND.

Na Tabela 4.3, são apresentados os terminais e a designação dos respectivos sinais associados, referentes à conexão Wiegand na respectiva placa conversora MA1400.

Tabela 4.3 - Terminais Wiegand na placa conversora MA1400

Terminal (conector em linha)	**Sinal**
01	10 à 30 Vcc.
02	GND.
03	5Vcc.
04	GND.
05	Protocolo de saída: Data0 (WIEGAND), Data (ABA), Wand.
06	Protocolo de saída: Data1 (WIEGAND), Clock (ABA).
07	Protocolo de entrada: Data0 (WIEGAND), Data (ABA).
08	Protocolo de entrada: Data1(WIEGAND), Clock (ABA), Wand.

Para conectar a placa MA1400 ao computador pertencente ao protótipo do subsistema operacional-PCAP (P_SSOP), utilizou-se um cabo conversor USB/Serial (RS232) fornecido pela empresa MULTILASER (MULTILASER, 2012). Esse cabo foi necessário pelo fato do computador em questão não dispor de porta serial RS232, possuindo somente portas USB.

4.1.4.3 Protótipo do Leitor Biométrico da Impressão Digital por Reflexão (P_Le_BID_R)

Para o "Protótipo do Leitor Biométrico da Impressão Digital por Reflexão" (P_Le_BID_R), obteve-se um equipamento do mesmo modelo apresentado na subseção "2.3.3", ou seja, equipamento modelo HAMSTER HFDU04, fornecido pela empresa NITGEN (NITGEN, 2012). Esse equipamento funciona com conexão ao computador do padrão IArch ou compatível, por meio de porta USB e o fabricante dispõe um conjunto de bibliotecas que oferecem recursos para obter o perfil biométrico da impressão digital e realizar os processos de cadastramento e verificação requeridos pelo SiCAP, incluindo-se a etapa de comparação referente ao último. Na Figura 4.8, é apresentada imagem do leitor Le_BID_R utilizado para o protótipo P_Le_BID_R.

Figura 4.8 - Leitor Le_BID_R HAMSTER HFDU04 referente ao P_Le_BID_R (NITGEN, 2012)

4.1.5 Protótipo do Subsistema SiCAP-Operacional-PCAP (P_SSOP)

O "Protótipo do Subsistema SiCAP-Operacional-PCAP" (P_SSOP) possui composição para representar os seguintes elementos pertencentes ao subsistema operacional-PCAP SSOP: estação de trabalho E_SICAP.PONTOCONTROLE; *softwares* SO_CLIENTE e SICAP.PONTOCONTROLE. Para representar a estação de trabalho utilizou-se um computador do padrão IArch, *notebook*, modelo Vaio PCG-5K1L, da marca Sony (SONY, 2012), sendo as características de *hardware* e *software* de interesse para o trabalho, apresentadas na Tabela 4.4.

Tabela 4.4 - Características da E_SICAP.PONTOCONTROLE referente ao P_SSOP

CARACTERÍSTICAS DO COMPUTADOR UTILIZADO PARA O E_SICAP.PONTOCONTROLE	
Hardware	• Processador: Core 2 Duo 1,83GHz. • Memória RAM: 4GB DDR2. • Disco Rígido: 250 GB. • Monitor: LCD de 14.1 polegadas. • Portas USB: 3. • Teclado: Português (Brasileiro ABNT). • Interface para rede de comunicação com fios: 01, padrão ETHERNET. • Interface para rede de comunicação sem fios: 01, WiFi.
Software	• **Sistema operacional:** o Windows Vista Home Premium (MICROSOFT, 2012). • **Aplicativo:** o SICAP.PONTOCONTROLE. o .NET Framework 4.0 (MICROSOFT, 2012).

Os *softwares* hospedados e executados na estação de trabalho em questão, são descritos nos itens a seguir:

- Windows Vista Home Premium: Este sistema operacional representa o SO_CLIENTE pertencente ao SSOP.
- SICAP.CONTROLE: Este aplicativo representa o *software* de mesmo nome pertencente ao SSOP e foi desenvolvido especialmente para utilização no protótipo P_SSOP. Para esse desenvolvimento empregou-se os seguintes recursos de *software*: linguagem C# (MICROSOFT, 2012) com a .NET Framework 4.0 (MICROSOFT, 2012); IDE Microsoft Visual Studio Professional 2010 (MICROSOFT, 2012); SDK (*Software Development Kit*, Conjunto para Desenvolvimento de *Software*) para biometria da impressão digital da NITGEN (NITGEN, 2012), compatível com o protótipo P_Le_BID_R.

- .NET FrameWork 4.0: É uma plataforma que permite a execução dos aplicativos desenvolvidos para representação do SSOP.

4.1.6 Protótipo do Subsistema SiCAP-Operacional-Administrativo (P_SSOA) e dos Componentes do SCNINO

O "Protótipo do Subsistema SiCAP-Operacional-Administrativo" (P_SSOA) possui composição para representar os seguintes elementos pertencentes ao subsistema operacional-administrativo SSOA: estação de trabalho E_SICAP.ADMINISTRATIVO; *softwares* SO_CLIENTE e SICAP.ADMINISTRATIVO.

Para permitir representação desses elementos do SSOA, bem como, do "Protótipo dos Componentes do SCNINO" (PC_SCNINO), utilizou-se um computador do padrão IArch, *desktop*, modelo E4600, da marca SEMP TOSHIBA (SEMPTOSHIBA, 2012), designado por CPH2, sendo as características de *hardware* e *software*, de interesse para o trabalho, apresentadas na Tabela 4.5. Nesse computador foi instalada uma máquina virtual (MV1) para representação do PC_SCNINO, sendo a real destinada para representação dos mencionados elementos do SSOA. Nesse contexto, o P_SSOA, o PC_SCNINO e o P_SSOP, formam o protótipo P_SCNINO com representatividade de integração de elementos do SiCAP ao MESiCAP.

Tabela 4.5 - Características do computador CPH2 referente ao P_SSOA e PC_SCNINO

CARACTERÍSTICAS DO COMPUTADOR CPH2 UTILIZADO PARA REPRESENTAÇÃO DE ELEMENTOS DO SSOA E SCNINO	
Hardware	• Processador: Core 2 Duo 2.4 GHz. • Memória RAM: 2GB DDR2. • Disco Rígido: 250GB. • Monitor: LCD 17 polegadas. • Teclado: Português (Brasileiro ABNT2). • Interface para rede de comunicação com fio: 01 padrão ETHERNET.
Software	**MÁQUINA REAL (E_SICAP.ADMINISTRATIVO)**
	• **Sistema operacional:** o Windows Seven Professional (MICROSOFT, 2012). • **Aplicativo:** o SICAP.ADMINISTRATIVO.
	MÁQUINA VIRTUAL MV1 (PC_SCNINO)
	• **Máquina Virtual:** o Oracle Virtual Box 4.1. (ORACLE, 2012) • **Sistema operacional:** o Windows XP (MICROSOFT, 2012). • **Aplicativo:** o Windows Explorer (MICROSOFT, 2012).

Os *softwares* hospedados e executados na máquina real do computador CPH2, referentes a estação de trabalho E_SICAP.ADMINISTRATIVO do P_SSOA, são descritos nos itens a seguir:

- Windows Seven Professional: Este sistema operacional representa o SO_CLIENTE pertencente ao SSOA.
- SICAP.ADMINISTRATIVO: Este aplicativo representa o *software* de mesmo nome pertencente ao SSOA e foi desenvolvido especialmente para utilização no protótipo P_SSOP. Para esse desenvolvimento empregou-se os seguintes recursos de *software*: linguagem C# com a .NET Framework 4.0; IDE Microsoft Visual Studio Professional 2010 (MICROSOFT, 2012); SDK para biometria da impressão digital da NITGEN (NITGEN, 2012), compatível com o protótipo P_Le_BID_R.

Os *softwares* hospedados e executados na máquina virtual MV1, no computador CPH2, referentes ao PC_SCNINO, são descritos nos itens a seguir:

- Windows XP: Este sistema operacional representa aqueles pertencentes aos componentes do sistemas computacionais não industriais do nível operacional SCNINO.
- Windows Explorer: Este aplicativo representa aqueles pertencentes aos componentes do sistemas computacionais não industriais do nível operacional SCNINO.

4.1.7 Protótipo do Subsistema SiCAP-Tático-Administrativo (P_SSTA) e dos Componentes do SCNT

O "Protótipo do Subsistema SiCAP-Tático-Administrativo" (P_SSTA) possui composição para representar os seguintes elementos pertencentes ao subsistema tático-administrativo SSTA: sistema gerenciador de banco de dados central SGBD_C; sistema de *web services* e importação de dados SWSID; estação de trabalho E_SICAP.AUDITORIA.

Para permitir a representação desses elementos do SSTA, bem como, do "Protótipo dos Componentes do SCNT" (PC_SCNT), utilizou-se um computador compatível com o padrão IArch, *desktop*, modelo InfoWay, da marca Itautec (ITAUTEC, 2012), designado por CPH1, sendo as características de *hardware* e *software*, de interesse para o trabalho, apresentadas na Tabela 4.6. Nesse computador foram instaladas três máquinas virtuais para representação dos mencionados elementos do SSTA, sendo a real destinada para representação PC_SCNT. Nesse contexto, o P_SSTA e o PC_SCNT, formam o protótipo P_SCNT com representatividade de integração de elementos do SiCAP no MESiCAP.

Tabela 4.6 - Características do computador CPH1 referente ao P_SSTA e PC_SCNT

CARACTERÍSTICAS DO COMPUTADOR CPH1 UTILIZADO PARA REPRESENTAÇÃO DE ELEMENTOS DO SSTA E SCNT	
Hardware	• Processador: Phenom II X4 945 Processor 3.00 GHz. • Memória RAM: 4GB DDR2. • Disco Rígido: 300GB. • Monitor: LCD 19 polegadas. • Teclado: Português (Brasileiro ABNT2). • Interface para rede de comunicação com fio: 01, padrão ETHERNET.
Software	**MÁQUINA REAL (PC_ SCNT)**
	• **Sistema operacional:** o Windows Seven Professional (MICROSOFT, 2012). • **Aplicativo:** o Windows Explorer (MICROSOFT, 2012).
	MÁQUINA VIRTUAL MV1 (SGBD_C)
	• **Máquina Virtual:** o Oracle Virtual Box 4.1 (ORACLE, 2012). • **Sistema operacional:** o Windows 2003 Server (MICROSOFT, 2012). • **Aplicativo:** o Microsoft SQL-Server 2005 (MICROSOFT, 2012).
	MÁQUINA VIRTUAL MV2 (SWSID)
	• **Máquina Virtual:** o Oracle Virtual Box 4.1 (ORACLE, 2012). • **Sistema operacional:** o Windows 2003 Server (MICROSOFT, 2012). • **Aplicativo:** o Internet Information Server 6.0 (MICROSOFT, 2012). o SICAP.MODEL. o SICAP.WEBSERVICES. o SICAP.IMPORTAÇÃO. o .NET Framework 4.0 (MICROSOFT, 2012).
	MÁQUINA VIRTUAL MV3 (E_SICAP.AUDITORIA)
	• **Máquina Virtual:** o Oracle Virtual Box 4.1 (ORACLE, 2012). • **Sistema operacional:** o Windows XP SP3 (MICROSOFT, 2012). • **Aplicativo:** o SICAP.AUDITORIA. o .NET Framework 4.0 (MICROSOFT, 2012).

Os *softwares* hospedados e executados na máquina real do computador CPH1, referentes ao PC_SCNT, são descritos nos itens a seguir:

- Windows Seven Professional: Este sistema operacional representa aqueles pertencentes aos componentes do sistemas computacionais do nível tático SCNT.
- Windows Explorer: Este aplicativo representa aqueles pertencentes aos componentes do sistemas computacionais do nível tático SCNT.

Os *softwares* hospedados e executados na máquina virtual MV1 do computador CPH1, referentes ao SGBD_C, são descritos nos itens a seguir:

- Oracle Virtual Box 4.1: Esta máquina virtual representa a estação de trabalho SERV_SGBD_C, pertencente ao sistema SGBD_C do SSTA.
- Windows 2003 Server: Este sistema operacional representa o SO_SERV pertencente ao sistema SGBD_C do SSTA.
- Microsoft SQL-Server 2005: Este aplicativo representa o sistema de gerenciamento de banco de dados SGBD e a base de dados do SiCAP BD_SiCAP, pertencente ao sistema SGBD_C do SSTA.

Os *softwares* hospedados e executados na máquina virtual MV2 do computador CPH1, referentes ao SWSID, são descritos nos itens a seguir:

- Oracle Virtual Box 4.1: Esta máquina virtual representa a estação de trabalho SERV_SWSID, pertencente ao sistema SWSID do SSTA.
- Windows 2003 Server: Este sistema operacional representa o SO_SERV pertencente ao sistema SWSID do SSTA.
- Internet Information Server 6.0: Este aplicativo representa o servidor SW_HTTP, pertencente ao sistema SWSID do SSTA.
- SICAP.MODEL: Este aplicativo representa o *software* de mesmo nome pertencente ao sistema SWSID do SSTA, e foi desenvolvido especialmente para utilização no protótipo P_SSTA. Para esse desenvolvimento empregou-se os seguintes recursos de *software*: linguagem C# com a .NET Framework 4.0; IDE Microsoft Visual Studio Professional 2010 (MICROSOFT, 2012).
- SICAP.WEBSERVICES: Este aplicativo representa o *software* de mesmo nome pertencente ao sistema SWSID do SSTA, e foi desenvolvido especialmente para utilização no protótipo P_SSTA. Para esse desenvolvimento empregou-se os seguintes recursos de software: linguagem C# com a .NET Framework 4.0; IDE Microsoft Visual Studio Professional 2010 (MICROSOFT, 2012).
- SICAP.IMPORTAÇÃO: Este aplicativo representa o *software* de mesmo nome pertencente ao sistema SWSID do SSTA, e foi desenvolvido especialmente para utilização no protótipo P_SSTA. Para esse desenvolvimento empregou-se os seguintes recursos de *software*: linguagem C# com a .NET Framework 4.0; IDE Microsoft Visual Studio Professional 2010 (MICROSOFT, 2012).
- .NET FrameWork 4.0: É uma plataforma que permite a execução dos aplicativos desenvolvidos para representação do sistema SWSID do SSTA.

Os *softwares* hospedados e executados na máquina virtual MV3 do computador CPH1, referentes a estação E.SICAP.AUDITORIA, são descritos nos itens a seguir:

- Oracle Virtual Box 4.1: Esta máquina virtual representa o computador compatível com o padrão IArch utilizado para a estação de trabalho E_SICAP.AUDITORIA, pertencente ao sistema SSTA.
- Windows XP SP3: Este sistema operacional representa o SO_CLIENTE pertencente a estação de trabalho E_SICAP.AUDITORIA do SSTA.
- SICAP.AUDITORIA: Este aplicativo representa o *software* de mesmo nome pertencente a estação de trabalho E_SICAP.AUDITORIA do SSTA, e foi desenvolvido especialmente para utilização no protótipo P_SSTA. Para esse desenvolvimento empregou-se os seguintes recursos de software: linguagem C# com a .NET Framework 4.0; IDE Microsoft Visual Studio Professional 2010 (MICROSOFT, 2012).
- .NET FrameWork 4.0: É uma plataforma que permite a execução dos aplicativos desenvolvidos para execução na estação de trabalho E_SICAP.AUDITORIA do SSTA.

4.1.8 Protótipo do sistema de redes não industriais empresarial (P_SiReNIE)

Para o "Protótipo do Sistema de Redes Não Industriais Empresarial" (P_SiReNIE) foram utilizados recursos de *software* dos sistemas operacionais existentes nas máquinas reais e virtuais referentes a arquitetura da Figura 4.1, bem como, os respectivos recursos de *hardware* pertinentes a essas máquinas. Utilizou-se também um roteador *wireless* TP-Link modelo TL-MR3420 (TPLINK, 2012), que possui suporte para conexão à rede por cabo, com conector RJ45. Esses recursos permitiram representar o Protocolo de Comunicação das Redes Não Industriais Empresarial (PCSiReNIE), sendo utilizados os protocolos TCP/IP e SSL. Para as comunicações entre o SGDB_C e SWSID, utilizou-se protocolo TCP/IP. Para as comunicações entre o SWSID e os componentes P_SSOP, P_SSOA e E_SICAP.AUDITORIA, utilizou-se protocolos TCP/IP e SSL.

Para configuração do P_SiReNIE, foi atribuído para cada máquina real e virtual, um IP fixo da família 192.168.1.X, conforme descrito na Tabela 4.7.

Tabela 4.7 - Distribuição dos IPs do protótipo P_SiReNIE

IP	Equipamento ou Máquina
192.168.1.1	Roteador wireless TP-Link TL-MR3420.
192.168.1.2	SGBD-C.
192.168.1.3	SWSID.
192.168.1.4	E_SICAP.AUDITORIA.
192.168.1.5	E_SICAP.ADMINISTRATIVO.
192.168.1.6	E_SICAP.PONTOCONTROLE.
192.168.1.7	PC_SCNT.
192.168.1.8	PC_SCNINO.

Na Figura 4.9, é apresentada a imagem do roteador *wireless* TP-Link modelo TL-MR3420, utilizado no P_SiReNIE.

Figura 4.9 - Roteador *wireless* modelo TL-MR3420 (TPLINK, 2012)

4.2 TESTES PRÁTICOS

Com os protótipos descritos anteriormente, realizou-se testes práticos para avaliações sobre funcionalidades pertinentes ao SiCAP, com especial observância às expostas nas subseções “3.9”, “3.10” e “3.11”. Nos testes em questão, os protótipos funcionaram corretamente permitindo validar os princípios de funcionamento referentes aos respectivos elementos do projeto conceitual do SiCAP. Nas subseções a seguir, são apresentados detalhes sobre os principais testes.

4.2.1 Detalhes referentes ao teste de cadastramento de cartão CId_S

Este teste é direcionado para avaliações sobre os princípios de funcionamento das operações de cadastratamento de cartão CId_S. O cadastro de cartões CId_S é realizado pelo *software* SICAP.ADMINISTRATIVO, sendo realizados testes de inclusão, alteração e exclusão de protótipos de cartões, P_CId_S. Na Figura 4.10 é apresentada imagem da janela de cadastro de cartões CId_S, que possibilita incluir, alterar e excluir cartões CId_S do banco de da dos BD_SICAP.

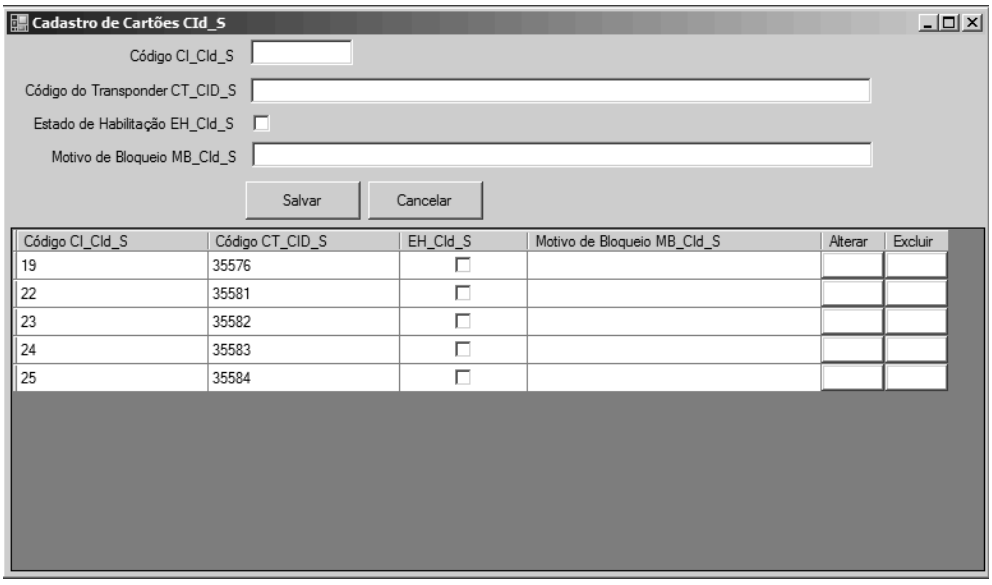

Figura 4.10 - Janela de cadastro de cartão CId_S

4.2.2 Detalhes do teste de cadastramento de equipamento EPP_S

Este teste é direcionado para avaliações sobre os princípios de funcionamento das operações de cadastratamento de equipamento EPP_S. O cadastro de equipamento EPP_S é permitido pelo *software* SICAP.ADMINISTRATIVO, sendo realizados testes de inclusão, alteração e exclusão de equipamentos EPP_S, representados pelos protótipos P_EPP_S. Na Figura 4.11, é apresentada imagem da janela de cadastro de equipamentos EPP_S, que possibilita incluir, alterar e excluir equipamentos EPP_S no banco de dados BD_SICAP.

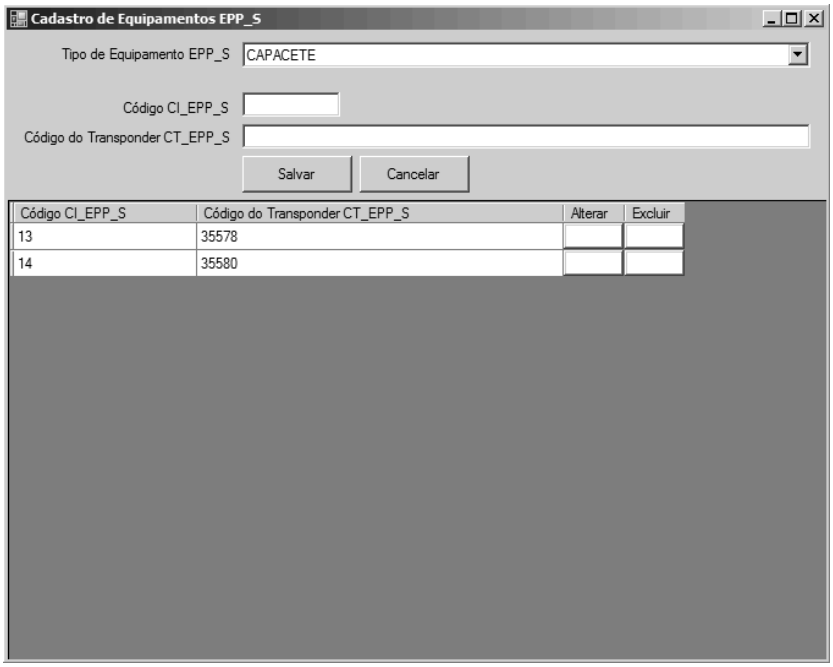

Figura 4.11 - Janela de cadastro de equipamento EPP_S

4.2.3 Detalhes do teste de cadastramento de ponto de controle PCAP_S

Este teste é direcionado para avaliações sobre os princípios de funcionamento das operações de cadastratamento do ponto de controle PCAP_S. O cadastro do ponto de controle PCAP_S é permitido pelo *software* SICAP.ADMINISTRATIVO, sendo realizados testes de inclusão, alteração e exclusão de pontos de controle PCAP_S. Na Figura 4.12, é apresentada imagem da janela de cadastro de pontos de controle PCAP_S, que possibilita incluir, alterar e excluir ponto de controle PCAP_S no banco de dados BD_SICAP.

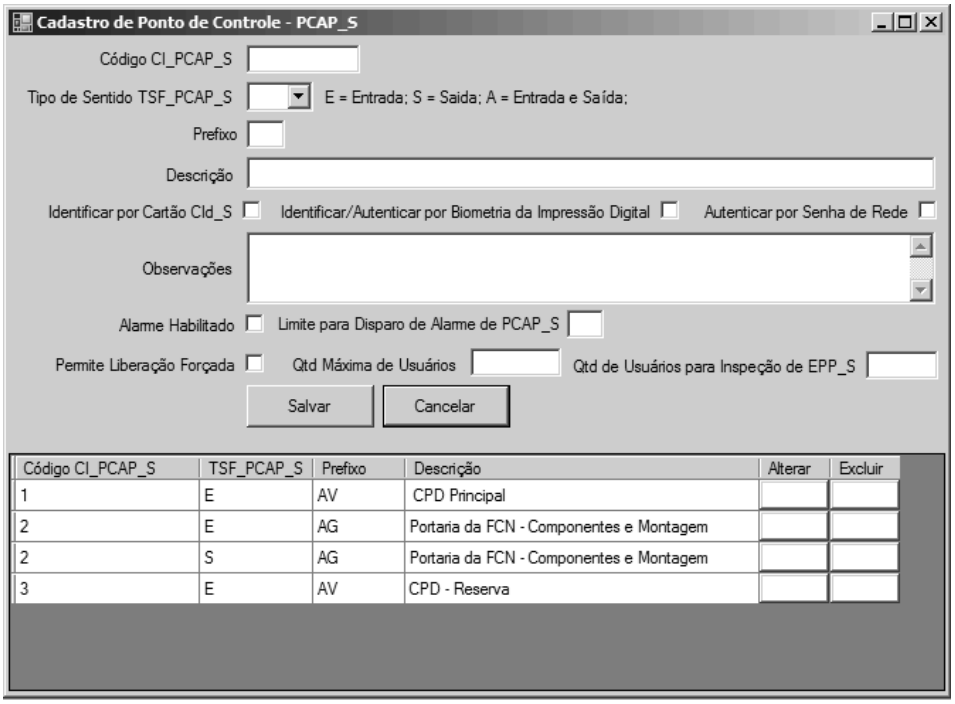

Figura 4.12 - Janela de cadastro de ponto de controle PCAP_S

4.2.4 Detalhes do teste de cadastramento de usuário USR no SiCAP

Este teste é direcionado para avaliações sobre os princípios de funcionamento das operações de cadastramento de usuários USR no SiCAP, sendo importadas de representações dos sistemas externos (existentes no PC_SCNINO), as informações necessárias para o cadastramento em questão. Esse cadastro de usuários é permitido pelo *software* SICAP.ADMINISTRATIVO, sendo realizados testes de importação, seleção e alteração de dados do usuário USR. Na Figura 4.13, é apresentada imagem da janela de cadastro de usuários USR, que possibilita alterar os dados dos usuários no banco de dados BD_SICAP, bem como, associar cartões CId_S, rotas R_USR, equipamentos EPP_S e obter o perfis biométricos referentes aos usuários USR.

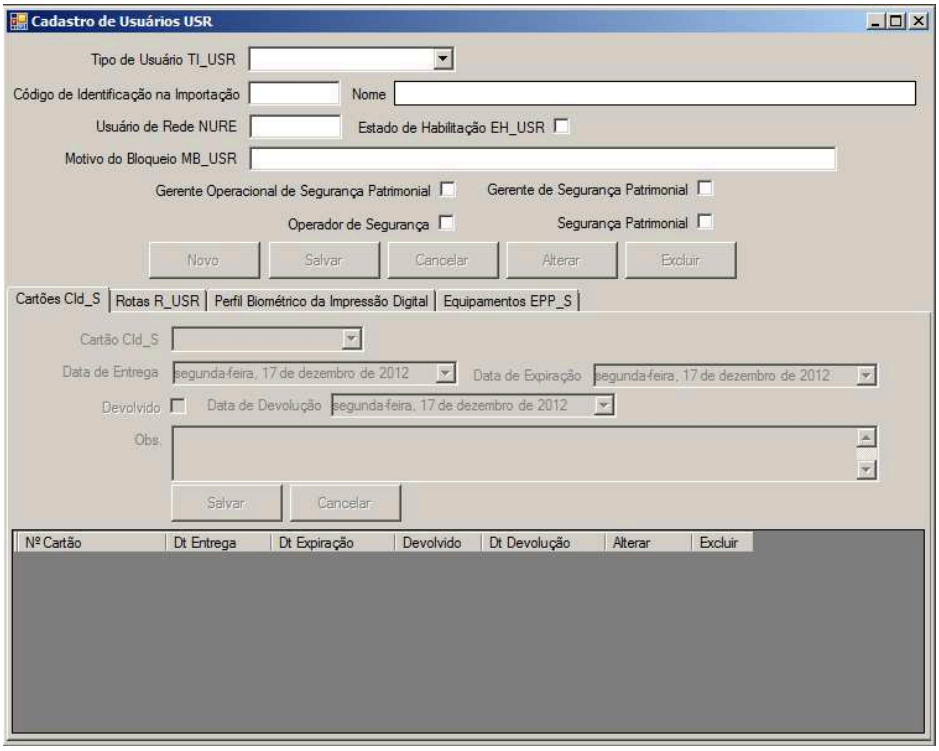

Figura 4.13 - Janela de cadastro de usuários USR

4.2.4.1 Detalhes da obtenção e armazenamento do perfil biométrico do usuário USR

Esta é uma parte importante do teste de cadastramento do usuário USR no SiCAP, sendo direcionada para avaliações sobre os princípios de funcionamento das operações referentes à obtenção das características biométricas da impressão digital do usuário USR, geração dos perfis biométricos da impressão digital e respectivos armazenamentos no banco de dados BD_SICAP. Foram realizados testes de geração, inclusão e exclusão de perfis biométricos da impressão digital de usuário USR. Na Figura 4.14, é apresentada a imagem da janela de seleção de dedo para obtenção de amostras biométricas.

Figura 4.14 - Janela de seleção do dedo para obtenção das amostras biométricas

Na Figura 4.15, é apresentada imagem da janela de captura das impressões digitais e geração dos respectivos perfis biométricos, sendo realizados acessos ao protótipo do leitor biométrico P_Le_BID_R, para as operações afins.

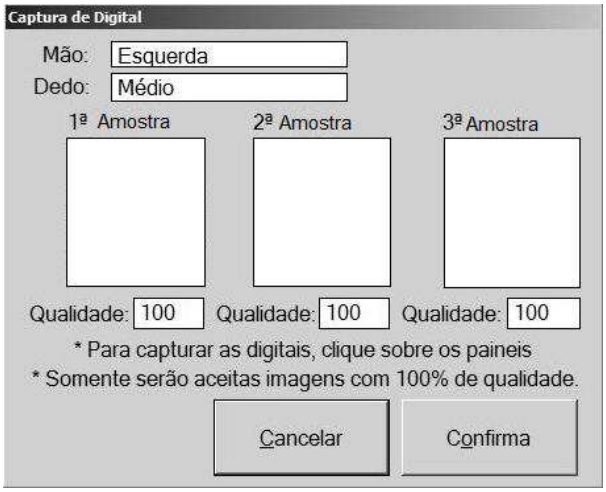

Figura 4.15 - Janela para geração dos perfis biométricos do usuário USR

4.2.5 Detalhes do teste de identificação por RFID com autenticação por biometria da impressão digital e autorização com solicitação de equipamento EPP_S

Este teste é direcionado para avaliações sobre os princípios de funcionamento das operações de identificação com recursos de RFID, autenticação com recursos de biometria da impressão digital e autorização com solicitação de equipamento de proteção pessoal EPP_S.

Para sua realização o PCAP_S foi configurado para funcionar com identificação por cartão CId_S, autenticação por biométrica da impressão digital e inspeção 100% de EPP_S.

Na Figura 4.16, é apresentada imagem da janela principal do *software* SICAP.PONTOCONTROLE, enquanto aguarda aproximação de cartão CId_S para proceder a identificação de usuário USR, sendo realizados acessos ao protótipo do leitor RFID, P_Le_RFID, para verificar se ocorreu leitura de transponder de P_CId_S, ou não.

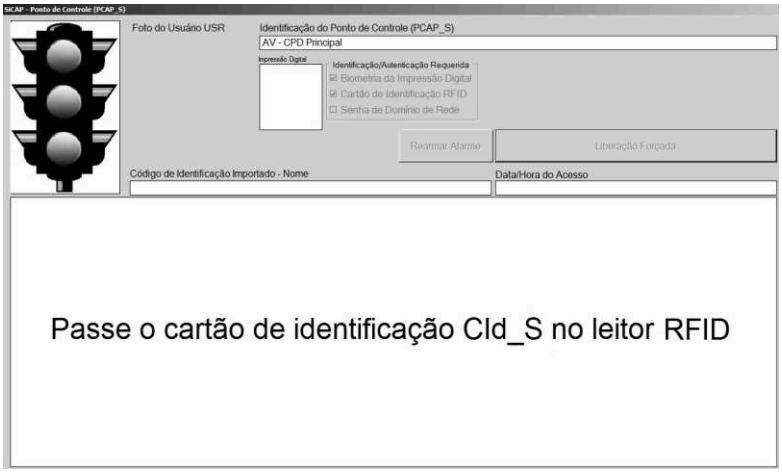

Figura 4.16 - Janela do SICAP.PONTOCONTROLE aguardando por cartão CId_S

Após a identificação do usuário USR, o *software* SICAP.PONTOCONTROLE seleciona somente os perfis biométricos pertencentes ao usuário identificado, para o processo de verificação. Na Figura 4.17, é apresentada imagem da janela principal do *software* em questão, após a identificação bem sucedida do usuário USR, sendo aguardada a apresentação de impressão digital referente ao processo de verificação por biometria da impressão digital, que inclui a respectiva etapa de comparação de perfil biométrico. Para o processo em questão, o SICAP.PONTOCONTROLE faz acessos ao protótipo do leitor biométrico da impressão digital, P_Le_BID_R, para realizar as etapas do processo de verificação descritas na subseção "2.3", que compreendem, de forma aplicada a biometria da impressão digital, o que segue: captura, processamento e comparação.

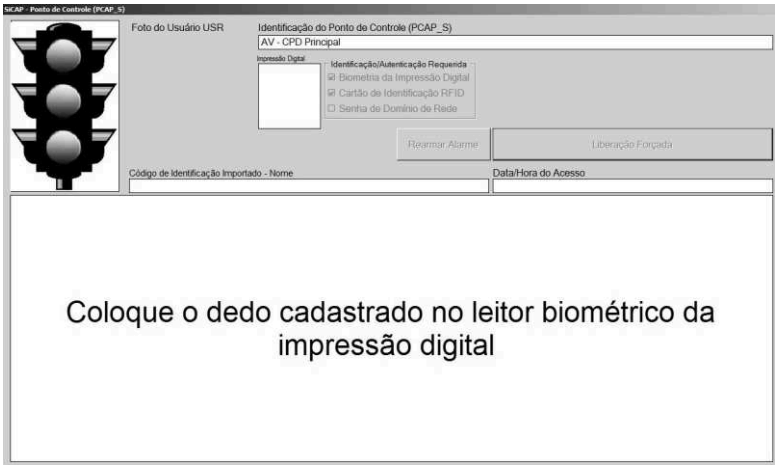

Figura 4.17 - Janela do SICAP.PONTOCONTROLE aguardando apresentação de digital

Na Figura 4.18, é apresentada imagem da janela em questão, porém, após realizar identificação e autenticação de usuário USR, sendo então solicitada a apresentação de equipamento EPP_S, representado pelo P_EPP_S correspondente a um capacete.

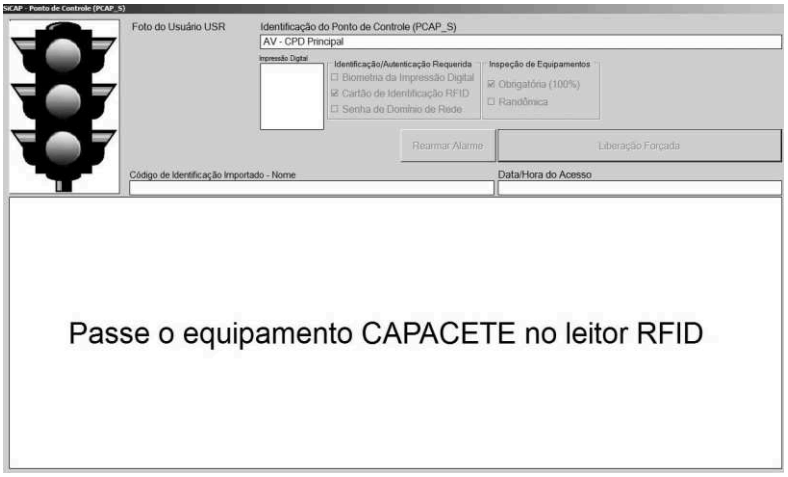

Figura 4.18 - Janela do SICAP.PONTOCONTROLE solicitando EPP_S do tipo capacete

Na Figura 4.19, é apresentada imagem da janela em questão, porém, após realizar identificação, autenticação e autorização de usuário USR cujos dados do transponder pertencente ao P_CId_S formam lidos por meio do P_Le_RFID, o processo de comparação que envolve a biometria da impressão digital foi realizado utilizando-se o P_Le_BID_R e os dados do transponder pertencente ao P_EPP_S formam lidos por meio do P_Le_RFID.

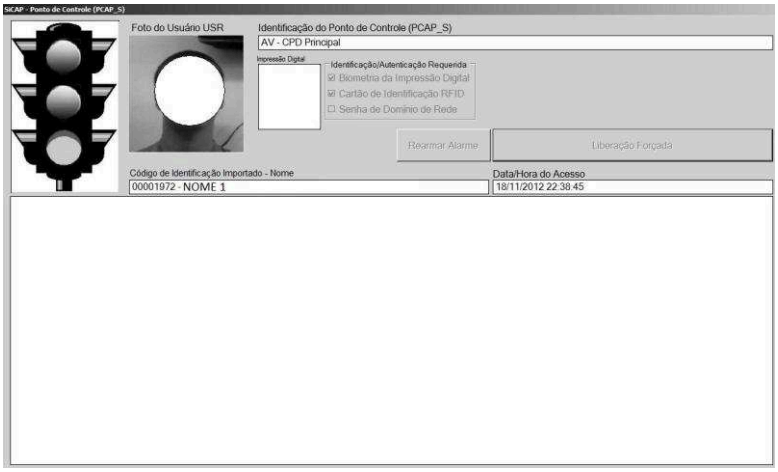

Figura 4.19 - Janela do SICAP.PONTOCONTROLE após conceder acesso ao usuário USR

5 CONCLUSÕES

O presente trabalho abordou estudos sobre elementos do projeto conceitual de um sistema de controle de acessos de pessoas a áreas industriais, voltado para o propósito de oferecer contribuição para o segmento particular daqueles tipos que exigem a utilização de automatização para atender a respectiva viabilização operacional relativa às atividades pertinentes ao controle de acessos em questão, atingindo o objetivo proposto. Nesse contexto foram expostos elementos da integração de recursos das identificações por radiofrequência e biometria da impressão digital, em aplicação direcionada para o controle de acessos abordado.

Os testes práticos realizados com os protótipos apresentaram resultados satisfatórios, validando os princípios de funcionamento dos elementos envolvidos, haja vista que foram verificadas as realizações das operações previstas pelo sistema, que possui as características de: identificação por radiofrequência fundamentada em tecnologia voltada para aplicações de identificação à curta distância com leitor fixo e transponder *read-only*; identificação por biometria da impressão digital fundamentada em tecnologia de captura de imagem com utilização de leitura óptica; utilização de equipamentos para controle físico do acesso de pessoas, cujas previsões de instalação permitam atender fluxos nos sentidos unidirecional e bidirecional com relação a área controlada; aplicação de recursos disponíveis por *Web Services* para atendimento das necessidades afins exigidas para o desenvolvimento do sistema; segurança no transporte de dados fundamentada na utilização do protocolo SSL; estações de trabalho e servidores constituídos por computadores pessoais do tipo IArch ou compatível; utilização de elementos de integração de sistemas direcionados para a abrangência de sistemas computacionais empresariais empregados em indústrias.

Como proposta de trabalhos futuros, sugere-se a realização de pesquisas referentes ao desenvolvimento de implementações do sistema abordado para gerar produtos destinados ao mercado de controle de acessos de pessoas, sendo também desenvolvida sua ampliação para incorporar o controle de acessos de veículos.

REFERÊNCIAS BIBLIOGRÁFICAS

AGUIAR, W. Aquisição de Dados de Inventário em Organização de Sistemas Computacionais Empresariais com Abrangência de Redes Industriais. Taubaté, 2011, Dissertação (Mestrado em Engenharia Mecânica) – Universidade de Taubaté.

ANDRI, Andri Elétrica. Home Page. Disponível em: <http://andrieletrica.com.br/>. Acesso em: 10/04/2012.

APACHE, The Apache Software Foundation. Home Page. Apache Tomcat. Disponível em: <http://tomcat.apache.org/>. Acesso em: 24/11/2012.

APORTEC, Aportec Tecnologia em Segurança Eletrônica. Home Page. Catraca Evolution Pedestal. Disponível em: <http://www.aportec.com.br/produtos_det.php?LISTA= menu&MENU=10&ID=37>. Acesso em: 10/11/2012.

BAZEN, A. M. Sistemas de Identificação Biométricos – A tênue fronteira entre a ciência e a eletrônica. Revista Elektor eletrônica & microinformática. Ano 5: nº 52. 2006.

BERNARDO, C. G. A Tecnologia RFID e os Benefícios da Etiqueta Inteligente para os Negócios. Revista Eletrônica Unibero de Iniciação Científica. São Paulo, 2004.

BHUPTANI, M. e MORADPOUR, S. RFID: Implementando o Sistema de Identificação por Radiofreqüência. São Paulo: IMAM, 2005.

BOECHAT, G. C. Investigação de um Modelo de Arquitetura Biométrica Multimodal para Identificação Pessoal. Recife, 2008, Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Pernambuco.

CARVALHO, M. Segurança Patrimonial – Organização e Planejamento. Rio de Janeiro: Agents Editores Ltda, 1982.

CF, Constituição da República Federativa do Brasil de 1988. Disponível em : <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 20/11/2012.

COELHO, L. C. Prospecção e Implantação de Tecnologia de Identificação Biométrica. XIII Semana Tecnológica e Cultural. 2009. Disponível em: <http://www.slideshare.net/IstRio/prospeco-e-implantao-de-tecnologia-de-identificao-biomtrica>. Acesso em: 25/05/2012.

D'ANGELO, V. e FERLINI, M. Gestão Estratégica da Segurança na Indústria. Disponível em: <http://www.fiesp.com.br/download/palestras/abseg_politica_seg.pdf>. Acesso em: 13/02/2012.

DELL, Dell Inc. Home Page. Disponível em: <http://www.dell.com.br/>. Acesso em: 24/11/2012.

DIMEP, Dimep Sistemas. Catraca Gabinete Francy Line. Disponível em: <http://www.dimep.com.br/produtos-ficha/3/35/sistemas-de-acessos/catraca-gabinete-fancy-line>. Acesso em: 10/02/2012.

EPC, EPCglobal®. Home Page. Disponível em <http://www.gs1.org/epcglobal>. Acesso em: 19/11/2012.

ERL, T. Introdução às tecnologias Web Services: SOA, SOAP, WSDL e UDDI - Parte1. Revista Web Mobile. ed. 1. Ano 1. Março. 2005.

FERREIRA, A. B. de H. Novo dicionário da língua portuguesa. Rio de Janeiro: Editora Nova Fronteira, 1998.

HAYONIK, Hayonik Ind. & Com. de Produtos Eletrônicos Ltda. Home Page. Disponível em: <http://www.hayonik.com/>. Acesso em: 12/10/2012.

HDL, HDL Legrand. Home Page. Porteiro Eletrônico com Vídeo Pinhole Color 60Hz com Teto (D&N). Disponível em: <http://www.hdl.com.br/produtos/interfonia-com-video/linha-classica/ porteiro-eletronico-com-video-pinhole-color-60hz-com>. Acesso em: 19/11/2012.

HID, HID Global. Home Page. Disponível em: <http://www.hidglobal.com/>. Acesso em: 20/10/2012.

HUA, HUAYUAN Shanghai Huayuan Smart Information Technology Co., Ltd. RFID Tag Worm. Disponível em: <http://portuguese.alibaba.com/product-gs/rfid-worm-tag-651094393.html>. Acesso em: 19/11/2012.

IECO, IECO Top Security. Home Page. Disponível em: <http://www.ieco.com.br/>. Acesso em: 19/10/2012.

IIS7, Internet Information Service. Conheça o IIS7. Outubro, 2009. Disponível em: <http://technet.microsoft.com/pt-br/library /cc753734%28v=ws.10%29.aspx>. Acesso em: 03/07/2012.

ISO, International Organization for Standardization. Information technology - Security techniques - Code of practice for information security. 2005.

ITAUTEC, Itautec S/A. Home Page. Disponível em: <http://www.itautec.com.br/>. Acesso em: 24/11/2012.

LEI, Lei nº 6.015/73 de 31 de dezembro de 1973. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L6015original.htm>. Acesso em: 20/11/2012.

LINUX, Linux Foundation. Home Page. Disponível em: <http://br-linux.org/>. Acesso em: 24/11/2012.

LOURENÇO, G. F. da F. Reforço da Segurança das Biométricas utilizando Codificação de Fonte Distribuída. Lisboa, 2009, Dissertação (Mestrado em Engenharia Eletrotécnica e Computadores) - Instituto Superior Técnico da Universidade de Lisboa.

MACAPS, MaCaPS Inc. Home Page. Disponível em: <http://www.macapsinc.com/ php/converter.php>. Acesso em: 24/11/2012.

MALTONI, D. et al. Handbook of Fingerprint Recognition. Second Edition. Editora Springer, 2009.

MICROSOFT, Microsoft® Corporation. Home-Page. Disponível em: < http://www. microsoft.com/pt-br/ default.aspx>. Acesso em: 24/11/2012.

MOTOROLA. Leitor RFID modelo DS908-R. Disponível em: < http://www.motorola.com/ Business/US-EN/Business+Product+ and+Services/RFID/RFID+ Readers/DS9808-R_US-EN>. Acesso em: 10/11/2012.

MSDN, Microsoft® Developer Network. Data Types. Disponível em: <http://msdn .microsoft.com/en-us/library/aa258271(v=sql.80).aspx>. Acessado em 02/11/2012.

MULTILASER, MULTILASER Tecnologia e Transformação. Home Page. Disponível em: <http://www.multilaser.com.br>. Acesso em: 24/11/2012.

MYSQL, MySQL. Home Page. Disponível em <http://www.mysql.com/>. Acesso em: 24/11/2012.

NE2.01, Proteção Física de Unidades Operacionais da Área Nuclear. Resolução CNEN 110/2011. 2011.

NEWMAN, R. Security and Access Control Using Biometric Technologies: Application, Technology, and Management. 1. ed. Course Technology, 2009.

NITGEN, NITGEN&COMPANY. Especificação do FingKey Hamster. Disponível em: <http://www.nitgen.com.br/Produtos/HamsterDX.aspx>. Acesso em: 15/01/2012.

ORACLE, Oracle® Brazil. Home Page. Disponível em <http://www.oracle.com/br/index. html>. Acesso em: 24/11/2012.

PINHEIRO, J. M. Biometria nos Sistemas Computacionais. 1. ed. Ciência Moderna, 2008.

RAMOS, A. et al. Security Officer – 2: Guia Oficial para Formação de Gestores em Segurança da Informação. Módulo Security Solutions, 2008.

ROSÁRIO, J. M. Automação Industrial. São Paulo, Editora Baraúna, 2009.

SANTINI, A. G. RFID: Rádio Frequency IDentification. Conceitos, Aplicabilidades e Impactos. Rio de Janeiro: Ciência Moderna, 2008.

SEMPTOSHIBA, Semp Toshiba. Home Page. Disponível em: <http://www. semp toshiba. com.br/>. Acesso em: 24/11/2012.

SEUFITELLI, C. B. et al. Tecnologia RFID e seus benefícios. Revista Vértices. V. 11. nº 1. 2009.

SILVA, L. G. C. et al. Certificação Digital - Conceitos e Aplicações. Editora Ciência Moderna, 2008.

SOARES, L. F. et al. Redes de Computadores: das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus, 1995.

SONY, Sony Inc. Home Page. Disponível em: <http://www.sony.com>. Acessado em: 01/02/2012.

SOUZA, Marcelo Barbosa. Controle de Acesso: Conceitos, Tecnologias e Benefícios. 1. ed. Sicurezza, 2010.

SQLSERVER, Microsoft® SQL-Server™ 2005. Home-Page. Disponível em: <http:// technet.microsoft.com/en-us/sqlserver/bb671245.aspx>. Acesso em: 24/11/2012.

THEVEAR, Thevear Eletrônica Ltda. Fecho Eletromagnético 12 Volts. Disponível em: <http://www.thevear.com.br/New/VerProdutos.aspx?IDSubCat=143>. Acesso em: 10/02/2012.

TITTEL, E. Coleção Schaum - Rede de Computadores. Porto Alegre: Bookman, 2003.

TORRES, G. H. Hardware Curso Completo. 4. ed. Rio de Janeiro: Axcel Books do Brasil Editora, 2001.

TPLINK, TP-LINK Technologies Co. Ltd. Home Page. Disponível em: <http://www.tp-link.com.br/>. Acesso em: 24/11/2012.

WCF, Windows Communication Foundation. Introdução aos serviços do Windows Communication Foundation no Visual Studio. Disponível em: <http://msdn.microsoft.com/ pt-br/library/bb907578(v=VS.90).aspx>. Acesso em: 10/02/2012.

WOLPAC, Wolpac Controles Eficientes. Home Page. Torniquete Woltor Plus. Disponível em: <http://www.wolpac.com/produto.php?codProd=22&codCat=1&codCatSub=15>. Acesso em: 10/02/2012.

ANEXO

ANEXO A - Descrição dos códigos de representação dos conteúdos dos campos referentes às estruturas de dados do SiCAP

Para os códigos de representação dos conteúdos dos campos referentes às estruturas de dados do SiCAP, adotou-se o padrão oriundo do Microsoft® SQL-Server™ (MSDN, 2012) cujos tipos são descritos na Tabela 5.1.

Tabela 5.1 - Padrão de tipos oriundos do Microsoft® SQL-Server™ (MSDN, 2012)

Tipos oriundos do Microsoft® SQL-Server™	
Designação	**Descrição**
BIGINT	Valores numéricos inteiros entre -9.223.372.036.854.775.808 e 9.223.372.036.854.775.807.
BINARY	Binário de tamanho fixo com tamanho máximo de 8.000 *Bytes*.
BIT	Valor booleano. 1 para verdadeiro e 0 para falso.
CHAR	Array de caracteres de tamanho fixo, armazenado de acordo com a tabela ASCII, permitindo no máximo 8.000 caracteres.
DATETIME	Valores de data e hora com range que varia de 1º de janeiro de 1753 a 31 de dezembro de 9999 com precisão de 3.33 milissegundos.
DECIMAL	Valores numéricos com casas decimais entre $-10^{+38}+1$ e $10^{+38}-1$.
IMAGE	Binário de tamanho variável com tamanho máximo de 2.147.483.647 *Bytes*.
INT	Valores numéricos inteiros entre -2.147.483.648 e 2.147.483.647.
MONEY	Valores monetários entre -922.337.203.685.477,5808 e 922.337.203.685.477,5807.
NCHAR	Array de caracteres de tamanho fixo, armazenado de acordo com a tabela Unicode, permitindo no máximo 4.000 caracteres.
NTEXT	Array de caracteres de tamanho variado, armazenado de acordo com a tabela Unicode, permitindo no máximo 1.073.741.823.
NVARCHAR	Array de tamanho variável, armazenado de acordo com a tabela Unicode, permitindo no máximo 4.000 caracteres.
SMALLDATETIME	Valores de data e hora com range que varia de 1º de janeiro de 1900 até junho de 2079 com precisão de 1 minuto.
SMALLINT	Valores numéricos inteiros entre -32.768 e 32.767.
SMALLMONEY	Valores monetários entre -214.748,3648 e 214.748,3647.
TEXT	Array de caracteres de tamanho variado, armazenado de acordo com a tabela ASCII, permitindo no máximo 2.147.483.647 caracteres.
TINYINT	Valores numéricos inteiros entre -32.768 e 32.767.
VARBINARY	Binário de tamanho variável com tamanho máximo de 8.000 *Bytes*.
VARCHAR	Array de caracteres de tamanho variado, armazenado de acordo com a tabela ASCII, permitindo no máximo 8.000 caracteres.