UNIVERSIDADE DE SÃO PAULO
ESCOLA POLITÉCNICA

**METODOLOGIAS DE AUTOMAÇÃO INTEGRADAS
AO CENTRO DE CONTROLE, COMUNICAÇÃO,
OPERAÇÕES E SEGURANÇA - CCCOS PARA O
SISTEMA DE SEGURANÇA PORTUÁRIO**

FÁBIO PIRES

SÃO PAULO
2011

FÁBIO PIRES

**METODOLOGIAS DE AUTOMAÇÃO INTEGRADAS
AO CENTRO DE CONTROLE, COMUNICAÇÃO,
OPERAÇÕES E SEGURANÇA - CCCOS PARA O
SISTEMA DE SEGURANÇA PORTUÁRIO**

Dissertação apresentada à Escola
Politécnica da Universidade de São
Paulo, para obtenção do grau de
Mestre em Engenharia.

Área de Concentração:

Engenharia de Energia e Automação
Elétricas

Orientador:

Prof. Dr. Eduardo Mario Dias

**SÃO PAULO
2011**

FICHA CATALOGRÁFICA

Pires, Fabio

Metodologias de automação integradas ao Centro de Controle, Comunicação, Operações e Segurança – CCCOS para o sistema de segurança portuário / F. Pires. -- São Paulo, 2011. 156 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Energia e Automação Elétricas.

1. Automação portuária 2. Portos (Segurança) I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Energia e Automação Elétricas II. t.

DEDICATÓRIA

Dedico esta obra acadêmica a Deus, nossa fonte vital da vida, a minha esposa Teresa, filhos Felipe, Fabio e Fabrício e aos meus pais Nelson e Luzia, que sempre me ensinaram a respeitar as leis naturais da vida e me dedicar aos estudos e com sapiência adquirir conhecimento. E a todos que direta ou indiretamente me auxiliaram nesta caminhada acadêmica e científica.

AGRADECIMENTOS

Primazmente agradeço ao Ser Supremo Deus, quiescência universal presente em todas as dimensões quânticas e cósmicas do universo (relativo e absoluto), a minha família, pai, mãe, filhos e, em especial, minha amada esposa, verdadeira companheira das horas difíceis, aos amigos (as) e professores (as), Drs. Eduardo Dias (meu orientador, mestre, amigo e desbravador do sistema de automação portuário brasileiro), Miguel Udaeta, Sergio Pereira, Mauro Zilbovicius, Cícero Couto, Guilherme Plonski e Israel Brusntein (IM), fomentadores e colaboradores do enriquecimento de meu saber e conhecimento, a Luzia, Tosta e Caio que sempre me ajudaram nos momentos críticos, a Universidade de São Paulo, Escola Politécnica e seus funcionários, a todos os Centros de Pesquisas, Faculdades e Universidades.

Aos demais docentes, em especial professor Kalil (eterno mestre), aos colegas de classe, engenheiros, cientistas, pesquisadores e também aos meus amigos de Santos e principais colaboradores da Codesp engenheiros João Fernando e Álvaro Luiz deixo expresso a todos, toda minha gratidão.

Muito obrigado!

“As Ciências Exatas, a Inovação Tecnológica e a Engenharia transmutam o conhecimento e tornam a alma jovem e diminui a amargura da velhice. Colhe, pois, a sapiência, armazena suavidade para os olhos e para o coração, na busca de um novo amanhã com discernimento e sabedoria”.

Adaptado pelo autor a frase do Engenheiro, Cientista e Inventor **Leonardo da Vinci**.

RESUMO

PIRES, F. **Metodologias de Automação Integradas ao Centro de Controle, Comunicação, Operações e Segurança – CCCOS para o Sistema de Segurança Portuário**. 2011. 156 p. Dissertação de mestrado. Escola Politécnica. Universidade de São Paulo. São Paulo. 2011.

A dissertação de mestrado apresenta as metodologias utilizadas com a integração de sistemas dos equipamentos de campo ao Centro de Controle, Comunicação, Operações e Segurança - CCCOS, visto ser o concentrador que recebe, gerencia, armazena e envia todas as informações dos equipamentos, seja do sistema de controle de acesso, através dos dados enviados e recebidos pelas placas de comunicação das leitoras das catracas, cancelas, torniquetes, sensores, sistema OCR, leitura automática de placas, contêineres, biometria facial, etc, ou do sistema de CFTV, através das imagens enviadas pelas câmeras fixas e móveis, via *encoders* e *switches* ou do sistema de comunicação *VOIP*, rádio ou telefonia. O sistema de segurança, preferencialmente, deverá estar com todos os subsistemas integrados e, na medida do possível, com um sistema de acesso especial e restrito para entrada de pessoas não autorizadas na área do centro de controle, com níveis de permissões em cada terminal de computador, acesso ou servidor, e neste trabalho, se descreve as tecnologias aplicadas dos equipamentos e dos subsistemas utilizados no sistema de segurança integrada e, como resultado, demonstra melhoria substancial da gestão, quando utilizados gerenciadores integrados, visto que o processo de entrada e saída para atender o sistema de segurança ou ISPS Code é otimizado e auxilia na gestão operacional e de segurança dos terminais e portos. Como proposta de customização, se terá vários Centros de Controles integrados, em portos públicos e privados de cada unidade da federação, com política de segurança criptografada, com confidencialidade, integridade e disponibilidade, tornando possível integrar todas as autoridades portuárias, alfandegárias e demais autoridades federais, estaduais e municipais, respeitando suas atribuições legais, em um único centro de controle global virtual, que permitirá inclusive se comunicar *on line* com demais sistemas portuários do mundo, que tenha o mesmo sistema de

segurança aplicado. Como caso de estudo, foi elaborado um estudo sobre o Porto de Santos, junto à autoridade portuária e demais terminais portuários, do *ISPS Code* implantado com os seus respectivos sistemas e centros de controles objetivando a gestão integrada de segurança eletrônica para o controle de pessoas, veículos e cargas, na interface cais-navio, para atracção de navios, logística de cargas, sinalização e tráfego de caminhões e demais veículos pelas vias principais e secundárias de acesso ao porto.

Palavras-chave: Sistema de Automação; Centro de Controle, Tecnologia da Informação; Hardware e Software; Segurança Portuária.

ABSTRACT

PIRES, F. **Methodologies for Integrated Automation Control Center, Communications, Operations and Safety - CCCOS for Port Security System** 2011. 156 páginas. Dissertação de mestrado. Escola Politécnica. Universidade de São Paulo. São Paulo. 2011.

The dissertation presents the methodologies used by integrating systems equipment field to control center, communications, Operations and safety-CCCOS, because it is the hub that receives, manages, stores, and sends all the information from the equipment, either from the access control system, through the data sent and received by boards of communication for the readers of ratchets, wickets, enclosures, sensors, OCR system, automatic reading of plates, containers, biometrics, facial, etc or CCTV system, through photographs sent by fixed and mobile cameras, encoders and switches or via the communication system, radio or VOIP Telephony. The security system, preferably, should be integrated with all subsystems and where possible, with a special access system and restricted to entry of unauthorized persons in the area control centre, with levels of permissions on each computer terminal, access or server, and in this work, describing the technologies applied in the equipment and subsystems used in integrated security system and, as a result, demonstrates substantial improvement of management, when used integrated managers, since the process of input and output to meet the security system or ISPS Code is optimized and assists with the operational management and security of the terminals and ports. As proposed, if customization has several integrated Controls Centers, public and private ports of each unit of the Federation, with encrypted security policy, with confidentiality, integrity, and availability, making it possible to integrate all port authorities, customs and other federal, State and municipal, respecting statutory duties, into a single global virtual control center, which will also communicate online with other port systems in the world, that has the same security system applied. As case study, a study was prepared on the port of Santos, next to the port authority and port terminals, the ISPS Code deployed with their systems and

aiming controls centers integrated electronic security for the control of persons, vehicles and loads in pier-ship, interface to lure ships, cargo logistics, signalling and traffic of trucks and other vehicles by major and minor routes of access to the port.

Keywords: Automation Systems, Control Centers, Information Technology, Hardware and Software, Safety Harbor.

LISTA DE ILUSTRAÇÕES

Figura 01. Integração entre empresas e pesquisadores da área portuária	25
Figura 02. Estrutura do Governo Federal para o Sistema Portuário Brasileiro	33
Figura 03. Mapa de localização dos portos brasileiros	35
Figura 04. Site da Supervia Eletrônica de Dados	38
Figura 05. Integração das Companhias Docas Brasileiras	39
Figura 06. Integração dos principais portos brasileiros.....	50
Figura 07. Modelo de Centro de Controle, Comunicação, Operação e Segurança...	52
Figura 08. Modelo do Centro de Controle e Comunicação do Porto de Santos	53
Figura 09. Sistema de CFTV Integrado	59
Figura 10. Arquitetura de Sistema OCR	77
Figura 11. Combinações Geométricas para Biometria Facial.....	78
Figura 12. Sistema LAP	79
Figura 13. Sistema LAP interligado ao Centro de Controle	79
Figura 14. Sistema LAC interligado ao Centro de Controle	80
Figura 15. Desenho dos equipamentos instalados de OCR no Gate	81
Figura 16. Painel de monitoramento com quadro sinótico	87
Figura 17. Balança Dinâmica.....	88
Figura 18. Sistema de Alarme e Comunicação por Voz	89
Figura 19. Característica do cartão Smart Card	102
Figura 20. Transações Eletrônicas	102
Figura 21. Imagem do Gestor de Eventos do OPC Cliente de Monitoração.....	103
Figura 22. Imagem da Tela do Sistema de Vídeo SmartSight.....	104
Figura 23. Análise da pesquisa sobre o sistema de segurança dos terminais dos portos brasileiros	105
Figura 24. Disposição física das salas de Controle, Técnica, Gerencial e Operacional.	107

LISTA DE GRÁFICOS

Gráfico 01. Movimentação geral dos portos brasileiros de 1996 e 2006	43
Gráfico 02. Movimentação geral dos portos brasileiros de 2006 a 2007	43
Gráfico 03. Movimentação geral dos portos brasileiros de 2007 a 2008	44
Gráfico 04. Movimentação geral dos portos brasileiros de 2008 a 2009	45
Gráfico 05. Sistema de segurança das empresas pesquisadas	106

LISTA DE TABELAS

Tabela 01. Movimentação geral dos portos brasileiros em 1996.....	40
Tabela 02. Movimentação geral dos portos brasileiros em 2006.....	41
Tabela 03. Movimentação geral dos portos brasileiros de 1996 e 2006.....	42
Tabela 04. Movimentação geral dos portos brasileiros de 2006 e 2007.....	43
Tabela 05. Movimentação geral dos portos brasileiros de 2007 e 2008.....	44
Tabela 06. Movimentação geral dos portos brasileiros de 2008 e 2009.....	44

LISTA DE SIGLAS E ABREVIATURAS NO SETOR PORTUÁRIO

SIGLAS	DESCRIÇÃO
ABNT	Associação Brasileira de Normas Técnicas
ABRATEC	Associação Brasileira dos Terminais de Contêineres de Uso Público
AIS	<i>Automatic Identification System</i>
ANTAQ	Agência Nacional de Transportes Aquaviários
ANVISA	Agência Nacional de Vigilância Sanitária
BL	<i>Bill of Lading</i>
CAP	Conselho de Autoridade Portuária
CBC	Câmara Brasileira de Contêineres
CBP	<i>Customs and Border Protection</i>
CC	Centro de Controle
CCCOM	Centro de Controle e Comunicação
CCO	Centro de Controle Operacional ou de Operações
CCOS	Centro de Controle Operacional e Segurança
CCCOS	Centro de Controle, Comunicação, Operações e Segurança
CECOL	Centro de Controle, Operações e Logística
CESPORTOS	Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis
CODESP	Companhia Docas do Estado de São Paulo
CFTV	Circuito Fechado de Televisão
CIFS	<i>Common Internet File System</i>
CONPORTOS	Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis.
COMCONTRAM	Comando do Controle Naval do Tráfego Marítimo
COV	Central de Operações e Vigilância
CSI	<i>Container Security Initiative</i>
DC	Declaração de Cumprimento
DNIT	Departamento Nacional de Infra-Estrutura dos Transportes
DP	Departamento de Portos
DPF	Departamento de Polícia Federal

DPRF	Departamento de Polícia Rodoviária Federal
EDI	<i>Electronic Data Interchange</i>
ETA	<i>Estimated Time of Arrival</i>
ETD	<i>Estimated Time of Departure</i>
EUA	Estados Unidos da América
FUSP	Fundação de Apoio a Universidade de São Paulo
IMCO	<i>Intergovernmental Maritime Consultative Organization</i>
IMO	<i>International Maritime Organization</i>
INFOCRIM	Sistemas de Informações Criminais
INFOSEG	Sistema de Informações de Justiça e Segurança Pública
ISPS Code	<i>International Ship and Port Facility Security Code</i> (Código Internacional para a segurança de navios e instalações portuárias).
ISCSI	<i>Internet Small Computer System Interface</i>
ISSC	<i>International Ship Security Certificate</i>
LRIT	<i>Long Range Identification and Tracking of Ships</i>
NFS	<i>Network File System</i>
NAPV	Normas de Controle de Acesso e circulação de pessoas e veículos
NEPOM	Núcleos Especiais de Polícia Marítima
NM	Navios Mercantes
NORMAM	Normas da Autoridade Marítima para Tráfego e Permanência de Embarcações em Águas Jurisdicionais Brasileiras
MS	Microsoft.
MSC	<i>Maritime Safety Committee</i>
OGMO	Órgão Gestor de Mão de Obra
ONU	Organização das Nações Unidas
PIMOP	Programa Integrado de Modernização Portuária
OCR	<i>Optical Character Recognition</i>
OLE	<i>Object Linking and Embedding</i>
OPC	<i>OLE for Process Control.</i>
PMAF	Polícia Marítima, Aérea e de Fronteiras
PNSA	Plano Nacional de Segurança Aduaneira

PNSPP	Plano Nacional de Segurança Público Portuário
PORTOBRAS	Empresa de Portos do Brasil S.A.
SAR	<i>Search and Rescue</i>
SED	Supervia Eletrônica de Dados
SEP	Secretaria Especial de Portos
SENASP	Secretaria Nacional de Segurança Pública
SISNC	Sistema Naval de Comando e Controle
SISTRAM	Sistema de Informações sobre o Tráfego Marítimo
SOLAS	<i>Safety of Life at Sea</i>
SSL	<i>Secure Sockets Layer</i>
SSPP	Sistema de Segurança Pública Portuário
STA	Secretaria de Transportes Aquaviários
SRF	Secretaria da Receita Federal
SVD	Servidor de Vídeo Digital
RAP	Prioridade e Requisição de Atracação
RPPS	Roteiro para Elaboração e Análise dos Planos de Segurança Pública Portuária
TA	Termo de Aptidão
TEU	<i>Twenty Feet Equivalent Unit</i>
TPA	Trabalhadores Portuários Avulsos
VAN	<i>Value Added Network</i>
VHF	<i>Very High Frequency</i>
VOIP	<i>Voice Over IP</i>
VTMIS	<i>Vessel Traffic Management and Information Service</i>
VTs	<i>Vessel Traffic Service</i>
USP	Universidade de São Paulo
UTC	<i>Universal Time Coordination</i>
WMD	<i>Weapons of Mass Destruction</i>

SUMÁRIO

1 INTRODUÇÃO	20
1.1 OBJETIVOS	20
1.2 RELEVÂNCIA DA DISSERTAÇÃO	21
1.3 DELIMITAÇÃO SOBRE O TEMA	21
1.4 FORMULAÇÃO DO PROBLEMA	22
1.5 HIPÓTESE E DESENVOLVIMENTO	23
1.6 JUSTIFICATIVAS	23
1.7 ORGANIZAÇÃO DO ESTUDO E PESQUISA	24
1.8 ESTADO DA ARTE NA ÁREA.....	25
 2 METODOLOGIA.....	26
2.1 FORMULAÇÃO DA PESQUISA E COMPOSIÇÃO DA AMOSTRA.....	26
2.2 MÉTODO DE ABORDAGEM E DE PROCEDIMENTO	27
2.3 TÉCNICAS E TIPOS DE PESQUISA	27
2.4 FUNDAMENTAÇÃO TEÓRICA	28
2.5 RESULTADOS PARCIAIS E DISCUSSÃO	28
2.6 PLANO DE TRABALHO DA PESQUISA	28
 3 COMPONENTES DO SISTEMA DE SEGURANÇA PORTUÁRIO	31
3.1 PANORAMA DO SISTEMA PORTUÁRIO BRASILEIRO	31
3.1.1 Lei de Modernização dos Portos	32
3.1.2 Secretaria Especial dos Portos – SEP.....	34
3.1.2.1 Localização dos Portos Brasileiros	35
3.1.2.2 Companhias Docas Administradas pela SEP	35
3.1.3 Modelo para o Sistema Integrado dos Portos Brasileiros	36
3.1.3.1 Sistema de Integração Digital de Dados, Vídeo, VoIP via SED – Supervia Eletrônica De Dados.....	36
3.1.3.2 Modelo para Integração de Sistemas Digitais das Autoridades Portuárias via SED	39
3.1.4 Movimentação geral dos portos brasileiros	40
3.1.5 Questões levantadas sobre o sistema portuário.....	45

3.1.6 Portos Brasileiros.....	46
3.1.6.1 Portos Marítimos.....	46
3.1.6.2 Portos Fluviais	47
3.1.6.3 Portos Secos	48
3.1.7 Modelo de Integração de Sistemas dos Portos Brasileiros.....	50
3.2 PORTOS INTEGRADOS EM SISTEMA GLOBAL VIRTUAL	51
3.3 MODELO PARA CENTRO DE CONTROLE, COMUNICAÇÃO, OPERAÇÃO E SEGURANÇA.....	52
 4 EQUIPAMENTOS E SISTEMAS DE SEGURANÇA INTEGRADA.....	54
4.1 SISTEMA DE CIRCUITO FECHADO DE TELEVISÃO (CFTV).....	54
4.1.1 Considerações importantes do Sistema de CFTV	54
4.1.2 Tecnologias de Gravação	55
4.1.3 Sistema de Segurança Físico e Lógico do CFTV	55
4.1.4 Transmissão do Sistema de CFTV	56
4.1.5 Sistemas de Integração físicos e lógicos integrados ao CFTV	56
4.1.6 Funcionalidade e Confiabilidade do Sistema de CFTV.....	56
4.1.7 Equipamentos utilizados em CFTV.....	57
4.1.8 Sistema de Monitoramento Físico	58
4.1.9 Sistema de CFTV utilizado em Portos e Terminais	58
4.1.10 Câmeras Fixas e Móveis	59
4.1.11 Encoders	60
4.1.12 Sistema de Gestão e Armazenamento de Vídeo.....	60
4.1.13 Detecção Automática de Riscos por Análise de Vídeo.....	60
4.1.14 Estação de Pesquisa em Vídeo Gravado	61
4.2 SISTEMAS DE CONTROLE DE ACESSO.....	62
4.2.1 Sistema de Identificação.....	62
4.2.2 Sistema de Gestão de Acesso.....	69
4.2.3 Sistema contra Intrusão.....	70
4.2.4 Sistema contra Incêndio	72
4.3 SISTEMA OCR E BIOMETRIA FACIAL	74
4.3.1 Componentes do Sistema e Funcionamento do OCR.....	75
4.3.2 Central de Comunicação	76

4.3.3	Arquitetura do Sistema de Reconhecimento	77
4.3.4	Leitura de Biometria Facial – LBF	77
4.3.5	Leitura Automática de Placas – LAP	78
4.3.6	Leitura Automática de Contêineres – LAC.....	80
4.3.7	Localização dos Equipamentos de OCR em Gate.....	81
4.4	INFRAESTRUTURA E BACKBONE ÓPTICO	81
4.5	MODELAGEM E ARQUITETURA DO SISTEMA DE SEGURANÇA.....	82
4.5.1	Equipamentos de Segurança Perimetral de Dados	82
4.5.2	Sistemas de Gerenciamento	82
4.5.3	Servidores de Arquivo	82
4.5.4	Contingenciamento do Sistema de Comunicação	83
4.5.5	Storage (Armazenamento)	83
4.5.6	Redundância de Conectividade	84
4.5.7	Administração e Gerenciamento do Sistema.....	84
4.6	FORNECIMENTO DE ENERGIA ELÉTRICA	84
4.7	SISTEMA DE DETECÇÃO E COMBATE À INCÊNDIO AUTOMÁTICO	85
4.8	PAINEL DE MOVIMENTAÇÃO VARIÁVEL – PMV	85
4.9	QUADRO SINÓTICO.....	86
4.10	BALANÇA DINÂMICA	87
4.11	SISTEMA DE ALARME E COMUNICAÇÃO SONORA	88
5	COMPONENTES DO SISTEMA DE SEGURANÇA PORTUÁRIO	90
5.1	PLANO NACIONAL DE SEGURANÇA PÚBLICA PORTUÁRIA	91
5.2	AGENTES DO SISTEMA PORTUÁRIO	91
5.2.1	Agentes Governamentais	91
5.2.2	Agentes Não-Governamentais no setor portuário.....	92
5.3	CONPORTOS - COMISSÃO NACIONAL DE SEGURANÇA PÚBLICA NOS PORTOS, TERMINAIS E VIAS NAVEGÁVEIS.	94
5.4	CESPORTOS - COMISSÃO ESTADUAL DE SEGURANÇA PÚBLICA NOS PORTOS, TERMINAIS E VIAS NAVEGÁVEIS	95
5.5	ISPS CODE - CÓDIGO INTERNACIONAL PARA PROTEÇÃO DE NAVIOS E INSTALAÇÕES PORTUÁRIAS	96
5.5.1	Código ISPS Code nos Portos Brasileiros.....	97

5.6 SISTEMAS COMPLEMENTARES PARA O SISTEMA DE SEGURANÇA PORTUÁRIO	98
5.7 SEGURANÇA PÚBLICA PORTUÁRIA NO PORTO DE SANTOS	99
6 CONSIDERAÇÕES FINAIS E ESTUDOS FUTUROS	105
6.1 ANÁLISE DA PESQUISA SOBRE O SISTEMA DE SEGURANÇA DOS TERMINAIS DOS PORTOS BRASILEIROS	105
6.1 ESTUDOS FUTUROS	107
6.2 POLÍTICAS DE SEGURANÇA NO CCCOS	107
6.3 SISTEMAS DE SEGURANÇA POR BIOMETRIA PARA ACESSAR O CENTRO DE CONTROLE E EQUIPAMENTOS.....	108
6.4 BENEFÍCIOS DE UM SISTEMA DE AUTOMAÇÃO NA SEGURANÇA PORTUÁRIA.....	108
7 CONCLUSÃO.....	110
REFERÊNCIAS E OBRAS CONSULTADAS	111
APÊNDICES.....	116
APÊNDICE A – ARTIGO SOBRE TECNOLOGIA DA INFORMAÇÃO NA GESTÃO PORTUÁRIA.....	117
APÊNDICE B – PESQUISA SOBRE O SISTEMA DE SEGURANÇA DOS TERMINAIS E PORTOS.....	134
ANEXOS	137
ANEXO A – PLANO NACIONAL DE SEGURANÇA PÚBLICA PORTUÁRIA.....	138

1 INTRODUÇÃO

A dissertação descreve a importância dos equipamentos instalados, nas áreas portuárias, e sua comunicação com o Centro de Controle, que é responsável por receber e enviar os dados para gerenciar, armazenar e controlar todas as informações dos equipamentos de campo, tanto para o sistema de controle de acesso, sistema OCR, quanto ao sistema de CFTV ou sistema de comunicação por fibra óptica, rádio ou cabos.

O sistema de segurança tem que estar com todos os seus subsistemas integrados, para melhor desempenho, e para fortalecer a idéia de integração o conteúdo para a metodologia deste trabalho objetiva descrever as tecnologias aplicadas dos equipamentos e os subsistemas utilizados no sistema de segurança integrada, que tem como meta a melhoria substancial da gestão, visto que o processo de entrada e saída é otimizado e auxilia na gestão técnica e operacional dos terminais e portos.

Com os Centros de Controles otimizados, em portos públicos e privados de cada unidade da federação, com política de segurança criptografada, com confidencialidade, integridade e disponibilidade é possível integrar todas as autoridades portuárias, alfandegárias e demais autoridades federais, estaduais e municipais, respeitando suas atribuições legais, em um único centro de controle global, que permita inclusive se comunicar *on line* com demais sistemas portuários do mundo, que tenha o mesmo sistema de segurança aplicado.

Como *Case*, foi feito uma pesquisa no Porto de Santos, junto à autoridade portuária e demais terminais, sobre o *ISPS Code* e centro de controle implantado, com os seus respectivos sistemas.

1.1 OBJETIVOS

Este trabalho tem por objetivo pesquisar as boas práticas de seguranças integradas aos centros de controles, nas áreas públicas e privadas, utilizadas pelos terminais e portos brasileiros para atender o Plano Nacional de Segurança Pública

Portuária (Anexo A) e o ISPS Code, que foi tema de dissertação de mestrado da Mestra Claudia de Oliveira Gomes, do GAESI. Tem caráter exploratório e consiste nos modelos de gestão de segurança, com os equipamentos utilizados e o nível de segurança eletrônica dos Centros de Controles para evitar quebra do sistema aplicado e também sobre a integração destes terminais e portos, com um único centro de informação integrado.

Apresenta a importância da segurança que se deve ter com os centros de controles e a situação atual dos portos brasileiros e terminais portuários, com os modelos de gestão de segurança eletrônica e respectivas ferramentas de qualidade para as melhores práticas portuárias, atendendo o mercado internacional globalizado.

Também visa apresentar a evolução de novas tecnologias de segurança, com sistemas integrados de governança portuária, conforme Apêndice A - Artigo sobre Tecnologia da Informação na Gestão Portuária, objetivando a integração dentro das normas internacionais de gestão de segurança da informação ISO 27001, num modelo próprio, que ajuste as necessidades dos vários agentes portuários dos portos brasileiros.

1.2 RELEVÂNCIA DA DISSERTAÇÃO

O tema é relevante e importante, pois permite apresentar aos portos e terminais brasileiros as vantagens que se tem ao utilizar um sistema de segurança integrado, com inteligência aplicada dos recursos tecnológicos existentes, desde os equipamentos de campo como dos centros de controles, resultando numa melhora consubstancial dos ativos aplicados.

1.3 DELIMITAÇÃO SOBRE O TEMA

Apresenta o modelo de gestão integrada de segurança eletrônica, com os equipamentos utilizados em campo, junto ao centro de controle, e como poderá

melhorar a qualidade dos serviços, através da troca de informações e, também, na integração dos portos brasileiros, inclusive como exemplo, o de Santos, o maior porto da América Latina com seus respectivos terminais. Portanto, se faz necessário maior integração da segurança com as autoridades portuárias e demais agentes participantes.

São colocados dados fornecidos pela Antaq, dos últimos anos da movimentação de cargas dos portos brasileiros, depois da Lei de Modernização dos Portos, que permite fazer uma projeção das perspectivas futuras, com um novo modelo de automação e gestão de segurança eletrônica integrada e como a automação melhora os resultados produtivos do tempo aplicado nas operações portuárias.

Consideram-se apenas, os portos e terminais com maior relevância para a economia do país e, as investigações das práticas adotadas têm caráter mais descritivo que analítico, visto que não se pretende fazer nenhuma análise destes portos e também não avalia o desempenho em segurança das empresas pesquisadas, nem tampouco pesquisa o que as levou a ter um bom ou mau sistema de segurança.

1.4 FORMULAÇÃO DO PROBLEMA

A falta de investimentos no setor portuário brasileiro tem trazido consequências lastimáveis para os portos, visto que o setor tem crescido mais de 5% ao ano, (ANTAQ, 2009) e a falta de uma política estratégica e financeira para os portos brasileiros em infraestrutura tem gerado um grande problema logístico, de segurança e de transporte.

Devido a problemas estruturais, há necessidade de buscar soluções para resolver os problemas dos Portos através da integração das três esferas das administrações públicas – municipal, estadual e federal com todos os agentes portuários numa gestão de excelência única. Caso não haja essa integração, os portos perderão competitividade nacional e internacional com os exportadores e

importadores que usam os vários serviços de logísticas, segurança de cargas, pessoas e patrimoniais.

1.5 HIPÓTESE E DESENVOLVIMENTO

Nos anos de 2000 a 2009 os Portos brasileiros têm aumentado, de forma significativa, sua movimentação de cargas e o porto de Santos, maior porto brasileiro e da América latina, movimenta aproximadamente 25% das exportações marítimas brasileiras (ANTAQ 2010) sendo que nos modais de transportes terrestres, tem no rodoviário a movimentação de 80 % das cargas, 16% no ferroviário e 4% nos dutoviários e, em função dessa movimentação, na região da Baixada Santista existem alguns gargalos, que causam grandes problemas e que dificultam a expansão das atividades do Porto, entre eles estão a circulação de caminhões e carretas pelas cidades de Santos, Guarujá, Cubatão, São Vicente e nas vias internas do porto, ocasionando também congestionamentos nos acessos rodoviários provocados pelo grande número de caminhões que transportam safras agrícolas, açúcar e contêineres.

Para uma análise do setor portuário foram feitos levantamentos das áreas portuárias, com segmentação de produtos e serviços, que servem como base para a importância de ter um sistema integrado e seguro.

1.6 JUSTIFICATIVAS

A relevância desta dissertação está, primeiramente, ligada aos aspectos econômico e social, trazendo também reflexos nos aspectos político, ambiental e cultural.

O material pesquisado visa apresentar a importância da segurança integrada, dos equipamentos, com os respectivos centros de controles e as soluções tecnológicas adequadas para a segurança dos terminais de grãos líquidos e

sólidos, contêineres, passageiros e cargas gerais com seus modais (dutos, malhas ferroviárias, rodoviárias e marítimas) através de controle de acesso, comunicação e sistema de vídeo.

Focar e dar ênfase da necessidade da qualificação dos principais agentes do processo de segurança para integração de todos os sistemas e processos de serviços e produtos. Aplicar novas metodologias que auxiliam na renovação dos processos e apresentar tendências, no sentido de novas proposições, visto que haverá várias contribuições teóricas e práticas nesta dissertação.

1.7 ORGANIZAÇÃO DO ESTUDO E PESQUISA

No primeiro capítulo, com os objetivos, encontram-se o delineamento do tema desta dissertação. Em seguida, são apresentados os objetivos centrais do trabalho, geral e específico, sendo de grande importância por mostrar os objetos de discussões que serão apresentados ao longo da pesquisa.

O segundo capítulo corresponde ao levantamento da literatura disponível em bibliotecas, Internet, acervos e áreas portuárias sobre o tema central da dissertação e também sobre assuntos correlatos, Plano de Pesquisa e Trabalho, com os objetivos, métodos, recursos aplicados, etc.

Quanto à literatura encontrada, mesma escassa, existe uma contribuição positiva dos trabalhos desenvolvidos pela Universidade de São Paulo, através do Grupo de Pesquisa GAESI, coordenado pelo Prof. Dr. Eduardo Mario Dias e outros docentes da área, pois auxiliaram nesta dissertação, apesar da necessidade de se fomentar mais publicações sobre o tema.

O terceiro e quarto capítulos apresentam o conteúdo, com os órgãos, atores e agentes envolvidos no sistema portuário, subsistemas integrados de CFTV, Controle de Acesso, OCR e Comunicação;

No capítulo cinco, descrevem-se as análises dos dados, o sistema de segurança do CCCOS e os resultados obtidos com a pesquisa.

Por fim, a conclusão do trabalho e a relação com as referências utilizadas e obras consultadas, o Anexo A sobre o Plano Nacional de Segurança Pública

Portuário e Apêndices A e B: Artigo sobre Tecnologia da Informação na Gestão Portuária e o questionário utilizado na pesquisa sobre a segurança dos portos e terminais.

1.8 ESTADO DA ARTE NA ÁREA

Na busca de materiais bibliográficos, sejam livros, apostilas, artigos ou encadernados do tema escolhido, sobre sistema de automação integrado ao centro de controle e segurança portuária, se percebe que a quantidade de material no mercado é escassa, como também na internet e quando encontrado, só em forma fracionada, seja parcialmente sobre segurança, equipamentos, CFTV, controle de acesso ou automação portuária.

Nota-se, portanto o trabalho importante que a Universidade de São Paulo, através do GAESI/PEA, tem feito nos últimos anos quanto ao tema em questão, por apresentar vários trabalhos, dissertações, teses e artigos sobre as atividades portuárias, na área de automação dos vários terminais, seja de Granéis sólidos ou líquidos, como também terminais de contêineres ou cargas gerais.

Quanto ao quesito sobre os materiais bibliográficos dos temas portuários, como sugestão, figura 01, é o incentivo que as empresas portuárias podem dar aos pesquisadores e estudantes da área, junto às faculdades e universidades, com apoio financeiro necessário para o desenvolvimento de publicações, tais como: manuais, livros, cadernos, artigos, monografias, teses ou apostilas sobre as tecnologias aplicadas no setor portuário e a inovação tecnológica que se pode ter com novas propostas de Automação Portuária e Gestão em TI integrada.

Sugestão de integração entre empresa e pesquisadores da área portuária

Figura 01. Integração entre empresas e pesquisadores da área portuária.

2 METODOLOGIA

A metodologia utilizada é a indutiva e segue as etapas normais de qualquer processo acadêmico e tem como objetivo colher e analisar as características dos vários métodos disponíveis em sua utilização (AGNES, 2006), sendo detalhada, numa direção de pesquisa científica e acadêmica.

2.1 FORMULAÇÃO DA PESQUISA E COMPOSIÇÃO DA AMOSTRA

Em função da necessidade de atingir os objetivos desse trabalho, se optou pelo método de pesquisa realizada pela Internet, via e-mail. Essa escolha foi desenvolvida pela facilidade de se alcançar um grande número de portos e terminais espalhados geograficamente pelo Brasil e até no exterior, num período de tempo menor, quando comparado com outros métodos baseados em entrevistas físicas e pessoais, visto que se tem uma redução do custo da pesquisa, em função da facilidade do envio do questionário por correio eletrônico.

O autor visitou os principais portos do Brasil, Santos, Rio de Janeiro, Paraná, Santa Catarina, Rio Grande do Sul, Bahia, Pernambuco, Espírito Santo e europeus, tais como o porto de *Amsterdam* e *Roterdam* na Holanda, Antuérpia na Bélgica, *Le Havre* na França, *Edinburg* na Escócia, *Belfast* na Irlanda do Norte, *Civitavecchia* (Roma) na Itália, *Hamburg* na Alemanha, *Cardiff* no País de Gales, *Dublin* na Irlanda, *London* na Inglaterra e Barcelona na Espanha. Com esta visita foi possível perceber a diferença na infraestrutura, organização logística e operacional dos terminais e o modelo de segurança eletrônica e humana utilizado por eles.

Para a pesquisa, além das visitas *in loco* foi utilizado bancos de dados, contendo contatos dos principais terminais e portos brasileiros e internacionais através de *e-mails*. Os profissionais que receberam as pesquisas possuíam cargos de diretoria, gerência, coordenação, supervisão ou engenheiros ligados à área de tecnologia e segurança.

As informações solicitadas tiveram por objetivo operacionalizar variáveis que viabilizassem os sistemas de segurança e as práticas operacionais utilizadas.

Para fortalecer o trabalho de pesquisa, de que se precisam criar mecanismos de integração entre todos os envolvidos nos portos, se utilizam pesquisas qualitativas e quantitativas que se desenvolveram através das seguintes fases:

- Levantamento e pesquisa de campo;
- Programas de segurança e sistemas integrados;
- Topologia de desenvolvimento de pesquisa;
- Conclusivas dos métodos de pesquisas e desenvolvimento utilizados.

2.2 MÉTODO DE ABORDAGEM E DE PROCEDIMENTO

A pesquisa realizada adota o método indutivo (abordagem), pelo fato da amplitude a ser pesquisada e também porque pode auxiliar nas conclusões dos argumentos apresentados e dos dados obtidos com os atores participantes do processo de pesquisa. Também é utilizado o método observacional (procedimento), que terá como referência algumas experiências anteriores, com uma investigação mais concreta dos dados históricos, estatísticos obtidos e o levantamento físico das informações necessárias para conclusão real do objetivo da pesquisa.

O universo da pesquisa está relacionado diretamente aos Portos e Terminais Portuários, sobre a segurança eletrônica e os modelos de centros de controles e equipamentos utilizados, objetivando a melhoria contínua da eficiência da segurança eletrônica e dos modais de transportes aquaviários e terrestres.

2.3 TÉCNICAS E TIPOS DE PESQUISA

A técnica de pesquisa consistiu na coleta de dados existentes, tais como bibliografias, documentos, artigos científicos, etc., e os tipos de pesquisas realizadas são as classificadas como *descritivas*, que apresenta a descrição das características

dos sistemas de segurança, agentes portuários e as *explicativas* que identificará os fatores que determinam a necessidade de um novo modelo de gestão de segurança portuária nos centros de controles.

2.4 FUNDAMENTAÇÃO TEÓRICA

São apresentados os embasamentos teóricos que fundamenta o trabalho com os elementos de pesquisa e, também, a definição dos conceitos empregados. A finalidade desta dissertação não será apenas um relatório ou descrição de fatos levantados empiricamente, mas objetivará o desenvolvimento interpretativo dos dados obtidos fornecendo uma direção no sentido de melhorar a segurança integrada dos agentes participantes do processo portuário.

Para isto, foram feitas perguntas direcionadas a área de segurança, com os diversos equipamentos utilizados e respectivo centro de controle.

2.5 RESULTADOS PARCIAIS E DISCUSSÃO

Através dos resultados obtidos, pela pesquisa realizada junto aos terminais e portos, no sentido de contribuir para as melhores praticas de segurança e também, em função do compromisso com os entrevistados, de não serem identificados na pesquisa. As respostas foram analisadas com critérios quantitativos, com os objetivos propostos neste trabalho.

2.6 PLANO DE TRABALHO DA PESQUISA

O plano de pesquisa visa apresentar as fases, o desenvolvimento dos estudos à dissertação para obtenção do mestrado e também a importância

estratégica dos Centros de Controles para o Sistema de Automação para o Plano de Segurança Pública Portuário exigido a todos os portos brasileiros, sejam públicos ou privados, para atender às exigências do *ISPS Code* – Código Internacional para Segurança de Navios e Instalações Portuárias.

O Centro de Controle permite ao operador de segurança, em tempo integral, o monitoramento, a observação e avaliação dos eventos que ocorrem nos pontos de controle (entradas e saídas), e tomar as medidas adequadas para o acionamento dos dispositivos de segurança do controle de acesso e vídeo.

Atualmente vários portos do Brasil têm feito instalações de monitoramento e controle, sem dar a devida atenção ao CCCOS, que tem que ter acesso restrito e ambiente de trabalho com boa ergonomia dos espaços, mobílias e climatização, além do sistema de controle de incêndio e, também, atender a demanda operacional e logística das informações geradas pelos equipamentos e dispositivos de campo.

O CCCOS, além do monitoramento do controle de acesso e CFTV, sensoriamento e comunicação por rádio ou VOIP (voz sobre IP) centraliza e armazena todos os dados dos eventos e vídeos gerados pelo sistema.

Diante da necessidade portuária de implantar o sistema de segurança para o *ISPS Code* e, principalmente, a centralização das informações vindas dos dispositivos e equipamentos de controle de acesso (catracas, cancelas, torniquetes, sensores), sistema OCR (leitura de placas e contêineres), biometria facial e monitoramento dos vídeos do circuito fechado de televisão (câmeras fixas e móveis), todos deverão estar integrados ao Centro de Controle, Comunicação, Operações e Segurança para o monitoramento *full time* e *on line* de usuários ou não, sejam eles visitantes, prestadores de serviços, pessoal de manutenção, funcionários, autoridades, trabalhadores portuários avulsos (TPA), tripulantes ou passageiros, transportadores, funcionários de praticagem e usuários especiais, etc.

Para a integração dos subsistemas do porto santista se utiliza um gerenciador de eventos (Gestor de Eventos), que é uma aplicação desenvolvida pela equipe do GAESI/PEA da USP, para integrar o sistema de monitoramento baseado em vídeo digital, com sistemas emissores de alarmes e eventos.

O Gestor de Eventos baseado em sistema OPC, que possibilita a integração com os sistemas de vídeo (câmeras fixa e móvel) e controle de acesso (catraca, cancela, torniquete, sensores, switch e laço indutivo) se comunicam via rede Giga Bit

no CCCom. Portanto, um tema bastante interessante para se buscar soluções integradas para atender as necessidades dos terminais e portos brasileiros.

Neste trabalho pode-se perceber uma relação interessante entre o ser humano (sistema manual) e os equipamentos do campo e o CCCOS (sistema automático).

Cabeça / cérebro (processamento e gerenciamento das informações) -
Centro de Controle com hardware e software;

Olhos / Visão (visualização e monitoramento) – Câmeras Fixas e Móveis;

Ouvido / Audição (som) – Sensores acústicos;

Boca / Voz (fala) – Comunicação VOIP;

Etc.

3 COMPONENTES DO SISTEMA DE SEGURANÇA PORTUÁRIO

O conteúdo da dissertação foi estruturado, de forma a apresentar os principais equipamentos de segurança utilizados nos sistemas de CFTV, Controle de Acesso, OCR, hardwares e softwares integrados ao centro de controle, nos portos e terminais do Brasil e no mundo, com os ambientes e atores participantes do sistema de segurança portuário.

3.1 PANORAMA DO SISTEMA PORTUÁRIO BRASILEIRO

O Brasil possui um setor portuário com uma costa navegável de 8,5 mil quilômetros, que movimentou, em 2009, aproximadamente 733 milhões de toneladas (ANTAQ, 2010), das mais diversas mercadorias, e responde sozinho, por mais de 80% das exportações.

Em função das reformas administrativas foi promulgada e implementada pelo governo brasileiro a Lei nº. 8.630, de 25 de fevereiro de 1993, denominada de Lei de Modernização dos Portos, que incentivou a privatização dos serviços portuários, criando áreas arrendadas dentro dos limites do porto organizado. Com ela, surgiu a figura do operador portuário, pessoa jurídica com a função de realizar as operações portuárias, cuja pré-qualificação para o desempenho dessas atividades deve ser obtida junto à Administração do Porto.

Dentro das limitações a Lei de Modernização dos Portos atuou de forma que o sistema brasileiro de gestão portuária se aproximasse dos modelos de gerenciamento vigentes nos países mais industrializados, nos quais as decisões sobre os assuntos relacionados ao arrendamento de terminais, alteração na execução das tarefas, mudanças nas jornadas de trabalho, dentre outros, tinham sido tomadas a nível local, atendendo o máximo possível das necessidades comerciais regionais onde atua.

Devido a problemas estruturais e falta de segurança nos portos brasileiros, fez com que o governo criasse a Comissão Nacional de Segurança Pública nos Portos,

Terminais e Vias Navegáveis (CONPORTOS) pelo Decreto 1.507 de 30 de maio 1995, alterado pelo Decreto 1.972 de 30 de julho de 1996, que teve por objetivo elaborar e implementar o sistema de prevenção e repressão a atos ilícitos nos portos.

No âmbito do tráfego internacional as questões de segurança também foram objeto de discussões e de criação de normas para o setor portuário. A Conferência Diplomática da Organização Marítima Internacional - IMO, em 12 de Dezembro de 2002, adotou as alterações à Convenção Internacional para a Salvaguarda da Vida Humana no Mar de 1974 (Convenção SOLAS) e um Código Internacional para a Proteção de Navios e Instalações Portuárias (Código ISPS).

3.1.1 Lei de Modernização dos Portos

A Lei nº. 8.630/93 de Modernização dos Portos promulgada pelo governo brasileiro em 25/02/93 transformou os portos brasileiros e exigiram grandes mudanças no setor portuário, tais como organizar o sistema de gerenciamento das operações e de mão-de-obra, eliminar o corporativismo e processos burocráticos e aproveitar, de forma racional, os espaços e instalações.

Dentre todos os avanços significativos, os resultados imediatos da implementação da Lei nº. 8.630 foram:

- A exploração dos portos organizados e das instalações portuárias;
- A substituição do setor público pelo setor privado nas operações portuárias, o que antes era exercido pela Administração do Porto Público, passou a ser executado por operadores portuários; e
- A quebra do monopólio dos sindicatos de trabalhadores avulsos no fornecimento e escalação da mão-de-obra para as operações portuárias com a constituição de 26 Órgãos Gestores de Mão-de-Obra (OGMO).

Ainda traçou três grandes eixos para realizar a transformação no sistema portuário brasileiro, promovendo a competição entre:

- Portos públicos (portos que se situam em uma mesma área de influência);

- Portos públicos e terminais de uso privativo (dentro ou fora do porto organizado); e
- Intraportos (entre terminais existentes no mesmo porto).

Por porto organizado, conforme a Lei nº 11.314 de 2006, Presidência da República, entende-se como aquele “construído e aparelhado para atender às necessidades da navegação, da movimentação de passageiros ou da movimentação e armazenagem de mercadorias, concedido ou explorado pela União, cujo tráfego e operações portuárias estejam sob a jurisdição de uma Autoridade Portuária”.

A Medida Provisória (MP) 369, de 7 de maio de 2007, criou a Secretaria Nacional de Portos com “*status*” de ministério, e conseqüentemente ficou com quase todo o organograma do DNIT, do Ministério dos Transportes, que permanece com as atribuições de formular, coordenar, supervisionar as políticas nacionais dos meios de transporte sob sua jurisdição e de promover o seu planejamento estratégico.

O sistema portuário brasileiro é composto por 37 portos públicos (2009), entre marítimos e fluviais. Desse total, 18 são concedidos ou tem sua operação autorizada à administração por parte dos governos estaduais e municipais. Existem ainda 42 terminais de uso privativo e três complexos portuários que operam sob concessão à iniciativa privada.

Os portos fluviais e lacustres são de competência do Ministério dos Transportes, conforme estrutura governamental para política dos portos brasileiros (figura 02).

a) Estrutura do Governo Federal para os portos brasileiros

Figura 02. Estrutura do Governo Federal para o sistema portuário brasileiro.

3.1.2 Secretaria Especial de Portos – SEP

A Secretaria Especial de Portos da Presidência da República (SEP/PR) foi criada por meio da Medida Provisória nº 369 de 07 de maio de 2007. Após aprovação pelo Congresso Nacional, o Presidente da República sancionou, em setembro daquele mesmo ano, a Lei 11.518 que consolidou o funcionamento da SEP/PR e o novo modelo de gestão do setor portuário com a revogação das leis, decretos-lei e dispositivos legais diversos (SEP, 2009).

A criação do novo órgão tem, entre os seus objetivos, colocar os terminais portuários brasileiros, figura 03, no mesmo patamar de competitividade dos mais eficientes do mundo, reduzindo assim as deficiências e o custo Brasil.

Entre as atribuições e competência da Secretaria está a formulação de políticas e diretrizes para o fomento do setor, além da execução de medidas, programas e projetos de apoio ao desenvolvimento da infraestrutura portuária. Compete ainda à SEP a participação no planejamento estratégico e a aprovação dos planos de outorgas, tudo isso visando assegurar segurança e eficiência ao transporte aquaviário de cargas e de passageiros no país.

Já quanto às metas estabelecidas pela Secretaria Especial de Portos, destaca-se a elaboração do Plano Nacional Estratégico dos Portos – PNE/PORTOS, que vai priorizar investimentos públicos e viabilizar o conceito dos portos concentradores e alimentadores, tendência operacional verificada mundialmente. Além disso, a consolidação dos marcos regulatórios do setor, buscando estimular a livre iniciativa e atrair mais investimentos privados, desonerando as cargas tributárias no âmbito das áreas alfandegadas e a disponibilização dos serviços públicos portuários, conforme previsto em lei, promovendo um modelo de gestão pautado por resultados previamente definidos também figuram como objetivos da SEP.

Existem sete companhias docas administradas pela Secretaria Especial de Portos, entre elas está a CODESP, que administra o maior porto da América Latina, o Porto de Santos.

5. Companhia Docas do Pará (CDP) – Responsável pela administração dos portos de Belém, Santarém e Vila do Conde.

6. Companhia Docas do Rio de Janeiro (CDRJ) – Responsável pela administração dos portos do Rio de Janeiro, Niterói, Angra dos Reis e Itaguaí.

7. Companhia Docas do Estado de São Paulo (Codesp) – Responsável pela administração do Porto de Santos.

3.1.3 Modelo para o Sistema Integrado dos Portos Brasileiros

Modelo de integração para a gestão integrada dos portos e terminais brasileiros com objetivo de dar respostas mais rápidas às decisões administrativas e operacionais.

3.1.3.1 Sistema de Integração Digital de Dados, Vídeo, VOIP Via SED – Supervia Eletrônica De Dados

Como sugestão para o sistema integrado portuário, todas as informações poderão ser trafegadas através da Supervia Eletrônica de Dados - SED, que foi desenvolvida pela equipe da USP, pelos colaboradores do grupo GAESI-PEA-POLI-USP e já utilizada no Porto de Santos, numa política de segurança, com confidencialidade, integridade e disponibilidade da informação, codificada e criptografada não só nos sistemas computacionais e de armazenamento, como também nos sistemas de integrações.

A) Sistema Supervia Eletrônica de Dados (SED)

O Sistema Supervia Eletrônica de Dados - SED resulta nas informações gerenciais por meio EDI (*Eletronic Data Interchange*), do serviço de VAN (*Value*

Added Network) e internet (figura 04). Trata-se de um sistema desenvolvido pela USP para atender as pessoas jurídicas ligadas à comunidade de atividade Portuária, disponibilizando a troca de informação em tempo integral, 24 horas por dia. Através dele a comunidade portuária envia e recebe informações sobre atracação e desatracação de navios, a movimentação e liberação de cargas junto a autoridade aduaneira via Internet, simplificando e otimizando seus processos e controles, reduzindo custos operacionais. Proporciona mecanismos de maior controle dos diferentes processos, com redução de erros, fluxo de papéis e acompanhamento de cláusulas contratuais referentes aos contratos de arrendamento de área a serem cumpridas por partes dos arrendatários. Permitindo ainda a fiscalização do fluxo das embarcações e mercadorias na importação e exportação, de operação de descarga e embarque de responsabilidade dos operadores portuários.

A SED teve seu primeiro módulo RAP (Prioridade e Requisição de Atracação), em abril de 2001, os demais módulos como Manifesto de Navios e Boletins de Carga e Descarga foram implantados em janeiro de 2004.

A SED recepciona os dados relativos aos seguintes módulos:

- Atracação;
- Manifesto de Carga;
- Boletim de Embarque /Descarga.

Todos os navios, abrangidos pelo Código ISPS, que pretendam entrar no porto de Santos deverão prestar à Autoridade Portuária via SED informações sobre a Livre Prática e número do certificado ISPS Code do navio.

Também pela SED será feito o envio dos arquivos de dados para o credenciamento de usuários às áreas restritas do Porto de Santos.

B) Site da SED – Supervia Eletrônica de Dados

Através da Home Page “www.superviadados.com.br”, figura 04, poderá ter acesso às informações de atracação de navios on-line do Porto de Santos.

Figura 04. Site da Supervia Eletrônica de Dados. Fonte: Codesp

3.1.3.2 Modelo para Integração de Sistemas Digitais das Autoridades Portuárias via SED

Como proposta de integração, entre todas as docas administradas pela SEP, será ampliar a Supervia Eletrônica de Dados entre as autoridades portuárias, visto ser uma realidade utilizada pelos terminais no Porto de Santos, conforme figura 05.

Figura 05. Integração das Companhias Docas Brasileiras.

3.1.4 Movimentação geral dos portos brasileiros

Através das tabelas 01, 02, 03, 04 e 05, de 1996, 2006, 2007, 2008 e 2009 e gráficos 01, 02, 03 e 04 foram verificadas as movimentações dos portos brasileiros e pode-se notar um crescimento na ordem de 100% (quase que dobrou neste período analisado), na movimentação de contêineres, granéis sólidos, líquidos e cargas gerais. A carga movimentada está expressa em toneladas (ton).

Tabela 01 - Movimentação geral dos portos brasileiros em 1996

Portos	Granéis Sólidos	Granéis Líquidos	Carga Geral	Total
Macapá (AP)	1.448.201	327	7.566	1.456.094
Porto Velho (RO)	-	52.693	1.312.601	1.365.294
Santarém (PA)	-	87.355	181.469	268.824
Manaus (AM)	-	3.487.709	876.921	4.364.630
Vila do Conde (PA)	2.451.782	366.912	451.516	3.270.210
Belém (PA)	9.500.389	1.513.066	1.206.426	12.219.881
Itaqui (MA)	45.298.052	3.830.902	339.835	49.468.789
Fortaleza (CE)	795.747	1.812.705	482.826	3.091.278
Areia Branca (RN)	4.151.285	-	-	4.151.285
Natal (RN)	-	5.017.358	91.385	5.108.743
Cabedelo (PB)	107.434	837.698	68.845	1.013.977
Recife (PE)	1.401.111	239.557	590.552	2.231.220
Suaape (PE)	2.498	3.040.382	180.952	3.223.832
Maceió (AL)	1.115.174	2.266.190	144.844	3.526.208
Aracaju (SE)	186.134	2.023.330	161.071	2.370.535
Salvador (BA)	477.747	-	1.156.765	1.634.512
Aratu (BA)	2.144.361	12.728.502	-	14.872.863
Ilhéus (BA)	123.778	184.700	113.945	422.423
Pirapora (MG)	47.748	-	-	47.748
Regência (ES)	-	397.840	-	397.840
Barra do Riacho (ES)	78.055	23.144	1.758.425	1.859.624
Praia Mole (ES)	10.106.850	10.011	6.234.115	16.350.976
Tubarão (ES)	62.856.811	1.345.997	-	64.202.808
Vitória (ES)	2.704.656	130.093	2.121.686	4.956.435
Ponta do Ubu (ES)	9.785.474	-	-	9.785.474
Forno (RJ)	758.237	3.660	2.011	763.908
Niterói (RJ)	127.460	-	-	127.460
Rio de Janeiro (RJ)	868.699	9.320.707	3.297.903	3.487.309
Sepetiba (RJ)	23.908.074	-	2.053	23.910.127
Angra dos Reis (RJ)	100.157	11.910.781	468.502	12.479.440
Panorama (SP)	76.207	-	-	76.207

Portos	Granéis Sólidos	Granéis Líquidos	Carga Geral	Total
Presidente Epitácio (SP)	101.518	-	-	101.518
São Sebastião (SP)	275.543	36.797.544	67.215	37.140.302
Santos (SP)	16.678.102	7.821.486	11.839.772	36.339.360
Antonina (PR)	672.710	-	47.936	720.646
Paranaguá (PR)	11.475.591	3.172.875	2.986.689	17.635.155
São Francisco do Sul (SC)	1.826.855	8.150.971	1.166.366	11.144.192
Itajaí (SC)	62.110	675.390	1.471.529	2.209.029
Imbituba (SC)	134.036	58.204	192.378	384.618
Charqueadas (RS)	371.366	-	-	371.366
Estrela (RS)	590.627	35.018	-	625.645
Porto Alegre (RS)	1.004.828	4.725.908	64.982	5.795.718
Pelotas (RS)	293.367	-	-	293.367
Rio Grande (RS)	5.564.863	2.440.663	1.677.965	9.683.491
Cáceres (MT)	22.384	-	440	22.824
Corumbá/Ladário (MT)	1.393.704	-	17.142	1.410.846
Total	221.089.725	124.509.678	40.784.628	386.384.031

Fonte: ANTAQ, 2010

Tabela 02 - Movimentação Geral dos Portos Brasileiros (em t) - 2006

Portos	Granéis Sólidos	Granéis Líquidos	Carga Geral	Total
Macapá (AP)	1.410.800	-	5.623	1.416.423
Porto Velho (RO)	2.054.278	5.787	151.654	2.211.719
Santarém (PA)	1.819.067	63.173	311.520	2.193.760
Manaus (AM)	-	-	1.271.793	1.271.793
Vila do Conde (PA)	13.093.122	1.658.233	1.119.663	15.871.018
Belém (PA)	171.052	1.809.412	825.355	2.805.819
Itaqui (MA)	6.582.964	5.639.027	307.350	12.529.341
Fortaleza (CE)	1.193.608	1.602.094	608.059	3.403.761
Areia Branca (RN)	4.096.932	-	-	4.096.932
Natal (RN)	88.335	2.533	218.040	308.908
Cabedelo (PB)	339.044	495.522	111.473	946.039
Recife (PE)	1.943.865	70.617	282.795	2.297.277
Suape (PE)	25.131	2.874.275	2.317.603	5.217.009
Maceió (AL)	2.180.863	1.015.598	314.746	3.511.207
Aracaju (SE)	-	-	-	-
Salvador (BA)	388.251	-	2.411.120	2.799.371
Aratu (BA)	1.582.578	3.809.508	-	5.392.086
Ilhéus (BA)	727.619	-	45.912	773.531
Pirapora (MG)	-	-	-	-
Regência (ES)	-	-	-	-
Barra do Riacho (ES)	-	-	-	-
Praia Mole (ES)	-	-	-	-
Tubarão (ES)	-	-	-	-
Vitória (ES)	2.338.572	265.847	5.327.614	7.932.033
Ponta do Ubu (ES)	-	-	-	-
Forno (RJ)	243.095	-	-	243.095

Portos	Granéis Sólidos	Granéis Líquidos	Carga Geral	Total
Niterói (RJ)	-	-	3.778	3.778
Rio de Janeiro (RJ)	1.511.628	371.346	6.629.421	8.512.395
Itaguaí (RJ)	8.512.395	-	4.778.135	29.694.079
Angra dos Reis (RJ)	-	-	164.315	164.315
Panorama (SP)	-	-	-	-
Presidente Epitácio (SP)	-	-	-	-
São Sebastião (SP)	450.875	-	-35.692	486.567
Santos (SP)	24.245.024	13.043.188	30.534.321	67.822.533
Antonina (PR)	-	-	-	-
Paranaguá (PR)	20.316.486	3.861.061	7.808.084	31.985.631
São Francisco do Sul (SC)	4.392.143	204.059	3.310.389	7.906.591
Itajaí (SC)		9.782	6.437.790	6.447.572
Imbituba (SC)	810.263	103.742	558.867	1.472.872
Charqueadas (RS)	-	-	-	-
Estrela (RS)	369.940	19.692	-	389.632
Porto Alegre (RS)	547.943	1.799	26.654	576.396
Pelotas (RS)	39.979	-	-	-
Rio Grande (RS)	12.249.670	3.966.775	6.212.519	22.428.964
Cáceres (MT)	174.812	-	-	174.812
Corumbá/Ladário (MT)	-	-	4.691	4.691
Total	415.727.739	175.541.324	101.564.405	692.833.468

Fonte: ANTAQ, 2010

Tabela 03 - Movimentação Geral dos Portos Brasileiros de 1996 e 2006

ANO	Granéis Sólidos	Granéis Líquidos	Carga Geral	Total
1996	221.089.725	124.509.678	40.784.628	386.384.031
2006	415.727.739	175.541.324	101.564.405	692.833.468
CRESCIMENTO (%)	88,03	40,99	149,03	79,31

Fonte: ANTAQ, 2010

Gráfico da Movimentação Geral dos Portos Brasileiros de 1996 e 2006

Gráfico 01. Movimentação geral dos portos brasileiros de 1996 e 2006.

Tabela 04 - Movimentação Geral dos Portos Brasileiros de 2006 e 2007

ANO	GRANEL SÓLIDO	GRANEL LÍQUIDO	CARGA GERAL	TOTAL
2006	415.727.739	175.541.324	101.564.405	692.833.468
2007	457.435.373	194.598.576	102.682.706	754.716.655
Diferença de Carga	41.707.634	19.057.252	1.118.301	61.883.187
Crescimento (%)	9,12%	9,79%	1,09%	8,20%

Fonte: ANTAQ, 2010

Gráfico de Movimentação Geral dos Portos Brasileiros de 2006 a 2007

Gráfico 02. Movimentação geral dos portos brasileiros de 2006 a 2007.

Tabela 05 - Movimentação Geral dos Portos Brasileiros de 2007 a 2008

ANO	GRANEL SÓLIDO	GRANEL LÍQUIDO	CARGA GERAL	TOTAL
2007	457.435.373	194.598.576	102.682.706	754.716.655
2008	460.184.343	195.637.355	112.501.852	768.323.550
Diferença de Carga	2.748.970	1.038.779	9.819.146	13.606.895
Crescimento (%)	0,60%	0,53%	8,73%	1,77%

Fonte: ANTAQ, 2010

H) Gráfico de Movimentação Geral dos Portos Brasileiros de 2007 a 2008

Gráfico 03. Movimentação geral dos portos brasileiros de 2007 a 2008.

Tabela 06 - Movimentação Geral dos Portos Brasileiros de 2008 a 2009

ANO	GRANEL SÓLIDO	GRANEL LÍQUIDO	CARGA GERAL	TOTAL
2008	460.184.343	195.637.355	112.501.852	768.323.550
2009	432.985.386	197.934.640	102.011.115	732.931.141
Diferença de Carga	-27.198.957	2.297.285	-10.490.737	-35.392.409
Crescimento (%)	-6,28%	1,16%	-10,28%	-4,83%

Fonte: ANTAQ, 2010

Gráfico de Movimentação Geral dos Portos Brasileiros de 2008 a 2009

Gráfico 04. Movimentação geral dos portos brasileiros de 2008 a 2009.

3.1.5 Questões levantadas sobre o sistema portuário

1. Se todos os portos e terminais tivessem sistemas automatizados e integrados de segurança e gestão, com centros de controles integrados, poderiam ter aumentado sua movimentação operacional e logística?

2. Com as autoridades portuárias integradas on-line a SEP, não poderia ter mais transparência nas administrações públicas portuárias?

3. Com todos os sistemas integrados nos terminais e portos não se reduziriam custos com TI e aumentariam a eficiência da gestão portuária e de segurança?

4. Podem os sistemas automatizados melhorar a qualidade dos serviços prestados pelos terminais portuários e aumentar sua produtividade?

5. Existe alguma relação entre o crescimento econômico do país e a movimentação de cargas dos portos brasileiros após a lei de modernização dos portos?

6. Os portos públicos e Autoridades Portuárias estão preparados para uma nova política de transparência administrativa e de segurança?

3.1.6 Portos Brasileiros

Os portos brasileiros são áreas abrigadas, localizadas a beira mar, oceano, rios e lagoas e são destinados ao atracamento de embarcações, com pessoal, serviços e recursos necessários ao carregamento e descarregamento e estoque temporário de cargas, bem como instalações para o movimento também de pessoas na área portuária, sendo compostos pelos portos marítimos, fluviais, lacustres e secos.

3.1.6.1 Portos Marítimos

São portos localizados a beira mar ou oceano.

- Porto de Angra dos Reis (Rio de Janeiro)
- Porto de Antonina (Paraná)
- Porto de Aratu (Bahia)
- Porto de Areia Branca (Rio Grande do Norte)
- Porto de Barra dos Coqueiros (Sergipe)
- Porto de Barra do Riacho (Espírito Santo)
- Porto de Belém (Pará)
- Porto de Cabedelo (Paraíba)
- Porto de Charqueadas (Rio Grande do Sul)
- Porto do Forno (Rio de Janeiro)
- Porto de Ilhéus (Bahia)
- Porto de Imbituba (Santa Catarina)
- Terminal de Itacoatiara (Amazonas)

- Porto de Itaguaí (Rio de Janeiro)
- Porto de Itajaí (Santa Catarina)
- Porto do Itaqui (Maranhão)
- Porto de Jaraguá ou Porto de Maceió (Alagoas)
- Porto Pesqueiro de Laguna (Santa Catarina)
- Porto de Luís Correia (Piauí) (planejado)
- Porto de Macapá (Amapá)
- Porto do Mucuripe ou Porto de Fortaleza (Ceará)
- Porto de Natal (Rio Grande do Norte)
- Porto de Niterói (Rio de Janeiro)
- Porto de Paranaguá (Paraná)
- Terminal de Pecém (Ceará)
- Porto de Pelotas (Rio Grande do Sul)
- Terminal da Ponta da Madeira (Maranhão)
- Terminal de Praia Mole (Espírito Santo)
- Porto do Recife (Pernambuco)
- Porto do Rio de Janeiro (Rio de Janeiro)
- Porto de Rio Grande (Rio Grande do Sul)
- Porto de Salvador (Bahia)
- Porto de Santos (São Paulo)
- Porto de São Sebastião (São Paulo)
- Porto de São Francisco do Sul (Santa Catarina)
- Porto de Suape (Pernambuco)
- Terminal de Tubarão (Espírito Santo)
- Porto de Vila do Conde (Pará)
- Porto de Vitória (Espírito Santo)

3.1.6.2 Portos Fluviais

São portos localizados e instalados na beira dos rios.

- Porto de Cáceres (Mato Grosso)

- Porto de Cachoeira do Sul (Rio Grande do Sul)
- Porto de Caracaraí (Roraima)
- Porto de Corumbá e Ladário (Mato Grosso do Sul)
- Porto de Estrela (Rio Grande do Sul)
- Porto de Juazeiro (Bahia)
- Porto de Manaus (Amazonas)
- Porto de Parintins (Amazonas)
- Porto de Petrolina (Pernambuco)
- Porto de Pirapora (Minas Gerais)
- Porto de Porto Alegre (Rio Grande do Sul)
- Porto de Porto Murtinho (Mato Grosso do Sul)
- Porto de Porto Velho (Rondônia)
- Porto Internacional de Porto Xavier (Rio Grande do Sul)
- Porto de Santarém (Pará)
- Porto de Tabatinga (Amazonas)

3.1.6.3 Portos Secos

São portos localizados e instalados para logísticas terrestres.

- Porto Rodo-Ferroviário de Santana do Livramento (Rio Grande do Sul)
- Porto Rodo-Ferroviário de Uruguaiana (Rio Grande do Sul)
- Porto Seco de Anápolis (Goiás)
- Porto Seco de Barueri (São Paulo)
- Porto Seco de Bauru (São Paulo)
- Porto Seco de Belém (Pará)
- Porto Seco de Campinas I e II (São Paulo)
- Porto Seco de Campo Grande (Mato Grosso do Sul)
- Porto Seco de Canoas (Rio Grande do Sul)
- Porto Seco de Cascavel (Paraná)
- Porto Seco de Caxias do Sul (Rio Grande do Sul)
- Porto Seco de Contagem (Minas Gerais)

- Porto Seco de Corumbá (Mato Grosso do Sul)
- Porto Seco de Cuiabá (Mato Grosso)
- Porto Seco de Curitiba I e II (Paraná)
- Porto Seco de Foz do Iguaçu (Paraná)
- Porto Seco de Franca (São Paulo)
- Porto Seco de Guarujá (São Paulo)
- Porto Seco de Guarulhos I e II (São Paulo)
- Porto Seco de Itajaí I e II (Santa Catarina)
- Porto Seco de Jacareí (São Paulo)
- Porto Seco de Jaguarão (Rio Grande do Sul)
- Porto Seco de Juiz de Fora (Minas Gerais)
- Porto Seco de Jundiaí (São Paulo)
- Porto Seco de Manaus (Amazonas)
- Porto Seco de Maringá (Paraná)
- Porto Seco de Nova Iguaçu (Rio de Janeiro)
- Porto Seco de Novo Hamburgo (Rio Grande do Sul)
- Porto Seco de Paranaguá (Paraná)
- Porto Seco de Piracicaba (São Paulo)
- Porto Seco de Recife (Pernambuco)
- Porto Seco de Resende (Rio de Janeiro)
- Porto Seco de Ribeirão Preto (São Paulo)
- Porto Seco do Rio de Janeiro (Rio de Janeiro)
- Porto Seco de Salvador I e II (Bahia)
- Porto Seco de Santo André (São Paulo)
- Porto Seco de Santos I, II, III e IV (São Paulo)
- Porto Seco de São Bernardo do Campo I e II (São Paulo)
- Porto Seco de São José do Rio Preto (São Paulo)
- Porto Seco de São Paulo I, II e III (São Paulo)
- Porto Seco de São Sebastião (São Paulo)
- Porto Seco de Sorocaba (São Paulo)
- Porto Seco de Suzano (São Paulo)
- Porto Seco de Taubaté (São Paulo)
- Porto Seco de Uberaba (Minas Gerais)

- Porto Seco de Uberlândia (Minas Gerais)
- Porto Seco de Varginha (Minas Gerais)
- Porto Seco de Vitória I, II e III (Espírito Santo)

3.1.7 Modelo de Integração de Sistemas dos Portos Brasileiros

O objetivo de apresentar este modelo de integração de portos é fazer, com que estes possam estar integrados fisicamente entre eles e a Secretaria de Portos, ou seja, todas as autoridades portuárias estarão interligadas entre si, com seus respectivos terminais e a SEP (figura 06). Através da integração de sistemas poder-se-á integrar os principais portos brasileiros, como os de Belém (PA), Fortaleza (CE), Imbituba, Itajaí e São Francisco do Sul (SC) Itaguaí e Rio de Janeiro (RJ), Itaqui e Rio Grande (RS), Manaus (AM), Paranaguá (PR), Salvador (BA), Santos (SP), São Luiz (MA), Suape (PE) e Vitória (ES).

Figura 06. Integração dos principais portos brasileiros.

3.2 PORTOS INTEGRADOS EM SISTEMA GLOBAL VIRTUAL

São apresentados os quantitativos dos principais portos do mundo, contendo os cinco continentes: África, América, Ásia, Europa e Oceania, que poderão estar integrados a um único sistema portuário global e virtual.

Como descrito no livro do francês Pierry Levi, o virtual e a virtualização afeta não só a informação e a comunicação, mas também os corpos, o funcionamento econômico, os quadros coletivos da sensibilidade ou exercício da inteligência, assim como as comunidades, empresas e democracia virtual (NEVES, 2007).

Quantitativo dos principais portos do mundo.

a) África

66 portos africanos.

b) Ásia

92 portos asiáticos.

c) Austrália e Oceania

52 portos australianos e Oceanía.

d) Europa

72 portos europeus

e) Mediterrâneo e Norte da África

55 portos do Mediterrâneo e norte-africanos.

f) Oriente Médio

40 portos do Oriente Médio.

g) América do Norte

42 portos norte-americanos.

h) América Central e Caribe

40 portos da América Central.

i) América do Sul

40 portos sul-americanos.

3.3 MODELO PARA CENTRO DE CONTROLE, COMUNICAÇÃO, OPERAÇÃO E SEGURANÇA

Como proposta, apresenta-se um modelo de Centro de Controle, figura 07, visando atender o ISPS Code, onde é composto por uma área de recepção (ante sala), sala de operação, sala Técnica e sala de Gestão. Pode-se integrar o CCCOS, com a SEP e demais portos, através da SED.

Figura 07. Modelo de Centro de Controle, Comunicação, Operação e Segurança – CCCOS.

a) Sala de Controle

A Sala de Controle é o ambiente de trabalho dos operadores, composta pelos terminais de computadores, telões e monitores, joysticks, mobiliários, telefonia e radiocomunicação, sistema de ar condicionado, sistema de incêndio, etc.

b) Sala Técnica

A Sala técnica é o local onde estão instalados os servidores, switches, racks, mobiliários, telefonia, sistema de ar condicionado, sistema de incêndio, etc.

c) Sistema de Ar condicionado da sala de servidores e ambiente dos operadores

Conjunto composto por equipamentos condicionadores de ar, com controle remoto e, respectivas linhas de alta e baixa pressão, além da drenagem necessária de forma a manter a temperatura ideal de operação dos servidores com capacidade suficiente para assegurar a estabilização da temperatura de operação na sala de servidores e operacional em torno de 20 a 22 °C.

d) Sistema de extinção de incêndio

Sistema de detecção, alarme e combate a incêndio em todos os ambientes, sala operacional e sala de Servidores através de detectores e tubulação de gás adequado para supressão e eliminação de chamas.

e) Modelo do Centro de Controle e Comunicação do Porto de Santos

A figura 08 apresenta o desenho tridimensional do centro de Controle do Porto de Santos.

Figura 08. Modelo do Centro de Controle e Comunicação do Porto de Santos. Fonte: Codesp.

4 EQUIPAMENTOS E SISTEMAS DE SEGURANÇA INTEGRADOS

São sistemas utilizados para a segurança portuária e são compostos por CFTV, Controle de Acesso, Comunicação e Gestão Integrada.

4.1 SISTEMA DE CIRCUITO FECHADO DE TELEVISÃO (CFTV)

O Sistema de Circuito Fechado de Televisão (CFTV) é composto por várias câmeras, conectadas a *encoders* com capacidade de capturar e digitalizar imagens, utilizando protocolos específicos via softwares, de uma ou mais entradas de vídeo, ou *switches* que envia dados para um servidor, que armazena, distribui, compartilha e reproduz tais imagens, onde podem ser incorporados recursos de captura e/ou armazenamento tais como: alarme, textos, áudio e outros dados relevantes para segurança eletrônica. Os principais objetivos do Sistema de CFTV são:

- Monitoramento preventivo de áreas, pessoas ou patrimônio;
- Gravação e reprodução de imagens, local e/ou remotamente;
- Buscar imagens gravadas, para detectar ou identificar eventos e situações específicas ocasionadas.

4.1.1 Considerações importantes do Sistema de CFTV

Devem ser observados alguns pontos importantes, tais como: qualidade da imagem, taxas de atualização de visualização ao vivo e na gravação, período máximo de gravação sem interrupções, facilidade na busca e resgate das imagens, capacidade de exportação de imagens para outras mídias, integração com outros sistemas e até mesmo acesso remoto.

Para ter o sistema de CFTV eficiente, tem que levar em consideração:

- Conhecimento das vulnerabilidades e riscos da segurança;

- Integração dos equipamentos e central de controle do sistema de CFTV;
- Utilizar equipamentos de qualidade.
- Ter política de segurança;

4.1.2 Tecnologias de Gravação

Existem dois tipos de tecnologias de gravação no mercado, a analógica e digital.

- **Analógica:** nos sistemas analógicos, a gravação é feita em baixa velocidade, a gravação de imagens é o *Time-Lapse* e a mídia de gravação é a fita *VHS*.
- **Digital:** os sistemas digitais são mais rápidos, flexíveis, expansíveis e fáceis de administrar. As tecnologias utilizadas para a gravação de imagens são NVR e DVR, que apresentam como recursos para a gravação de imagens o HD, CD e DVD.

4.1.3 Sistema de Segurança Física e Lógico do CFTV

O sistema de CFTV, para um bom funcionamento de segurança deverá ter, no mínimo, as seguintes diretrizes de segurança:

- Alarme e Indicação de perda de sinal de câmeras, falha de gravação e falha de HD;
- Criptografia da informação, de Comunicação – Rede *LAN* e Rede *Wireless*;
- Marca d'água;
- Níveis de hierarquia;
- *Login* e Senhas de Usuário;
- Política de segurança.

4.1.4 Transmissão do Sistema de CFTV

O sistema de CFTV deverá permitir as seguintes flexibilidades na comunicação:

- Câmeras: Analógicas e/ou IP.
- Gerenciamento: Local e/ou Remoto.
- Redes: Cabos Coaxiais; UTP; Fibra Óptica; Wireless.
- Visualização local, remota ou via Matriz Analógica: Câmeras virtuais.

4.1.5 Sistemas de Integração física e lógica integrados ao Sistema de CFTV

Para ter um sistema de CFTV completo é necessário que esteja integrado a todos os subsistemas de segurança, tais como:

- Sistemas Analógicos e Digitais;
- Sistemas de Automação;
- Sistemas de Alarmes e Contingências;
- Sistemas Digitais (IP – *Internet Protocol*);
- Sistemas de Controle de Acesso;
- Sistema OCR de Leitura de numeração de Contêineres.
- Sistema OCR de Reconhecimento de Face (biometria).
- Sistema OCR de Reconhecimento de Placas;

4.1.6 Funcionalidade e Confiabilidade do Sistema de CFTV

Para que se tenha a perfeita funcionalidade, operacionalidade e garantir a confiabilidade, o sistema de CFTV deverá, no mínimo, possuir os seguintes recursos:

- Redundância de Operação.
 - Monitoramento Local ou Remoto.
- Redundância de Gravação.
 - Arquivamento Redundante e Redundância por Falha de Servidor / Rede.
- Multi-Monitoramento.
 - Vários níveis de monitoramento para usuário.
- Estabilidade.
 - Sistema dedicado dotado de reinicialização automática para evitar perdas de informações.

4.1.7 Equipamentos utilizados em CFTV

Os equipamentos normalmente utilizados em sistema de CFTV são as câmeras fixas, móveis, controles, encoders, switches, panoramizadores, DVR's e NVR's, sendo:

- **DVR (digital video recorder) / NDVR (network digital video recorder):** Equipamento com capacidade de capturar e digitalizar imagens, utilizando protocolos específicos por hardware ou software, com uma ou mais entradas de vídeo, composto por um único hardware ou um conjunto de hardwares para armazenar em unidade(s) de memória, distribuir, compartilhar e reproduzir tais imagens, podendo ou não incorporar recursos de captura e/ou armazenamento de sinais de entrada e saída de alarmes, textos, áudios e outros dados relevantes para segurança eletrônica;
- **NVR (network video recorder):** Software que possui as funções de NDVR, para gerenciar câmeras IP ou câmeras analógicas conectadas a um encoder. Na própria câmera com IP, as imagens são captadas, e digitalizadas. O armazenamento das imagens é feito remotamente, em qualquer ponto da rede em unidades de disco (storages);

- **Câmeras Fixas:** equipamentos utilizados na captura e reprodução de imagens de um objeto ou uma área, em um ângulo de visão fixo e pré-estabelecido.
- **Câmeras Móveis (*Speed Dome*):** equipamentos com a mesma função das câmeras fixas; mas podendo ter movimentação de 360° na horizontal e mínimo de 90° na vertical, com lente de zoom, com grande capacidade de aproximação e afastamento das imagens;
- **Console (*Joystick*) ou mesa controladora:** equipamento utilizado pelos operadores para controlar as câmeras móveis.
- **Encoder:** dispositivo utilizado para transformar um sinal analógico em sinal digital.
- **Panoramizadores:** equipamentos que permitem a movimentação das câmeras na horizontal.
- **PTZ (*Pan-Tilt e Zoom*):** equipamentos utilizados para movimentar as câmeras na horizontal e na vertical, em conjunto com uma câmera com Lente Zoom.

4.1.8 Sistema de Monitoramento físico

Para um sistema de CFTV completo, se faz necessário uma central de monitoramento, que deve estar equipada e integrada com quantidade de equipamentos e câmeras fixas e móveis suficientes para atender o plano de segurança. A central de monitoramento deve ser protegida segundo as normas internacionais vinculadas aos *datas centers*, conforme determinação da ANSI/EIA/TIA 942.

4.1.9 Sistema de CFTV utilizado em Portos e Terminais

Devido à complexidade dos portos, como exemplo o de Santos, primeiro pela sua importância estratégica, segundo pelas suas dimensões físicas, o sistema de

CFTV, figura 09, utiliza dois tipos de câmeras, móveis e fixas, ambas tem a função de monitorar a área de interesse, objetivando levar as imagens de vídeos a um servidor de vídeo, para gerenciamento e gravação, e depois para o painel de controle e monitoramento, instalados numa central de controle. Para o sistema integrado, as câmeras enviam o sinal de vídeo para o *encoder*, e este para o switch, que transmite o sinal através de uma rede digital *Giga bit*, ou diretamente via IP, ao centro de controle.

Desenho esquemático do Sistema de CFTV integrado.

Figura 09. Sistema de CFTV integrado.

4.1.10 Câmeras Fixas e Móveis

a) Câmeras Fixas

As câmeras de vídeos fixas tem por objetivo monitorar áreas importantes para o sistema de CFTV, como entrada de pessoas nas catracas e torniquetes, de veículos nas cancelas, trânsito e pontos fixos patrimoniais. São utilizadas:

- a) Fixas;
- b) Mini Dome;

b) Câmeras Móveis

As câmeras móveis se dividem em dois modelos: as destinadas à vigilância local (entorno dos portões de entrada e saída) do tipo *dome* enquanto a do tipo *PTZ* a interface cais navio e estuário marítimo. Ambos os tipos possuem características ópticas e elétricas equivalentes e são ligadas a *encoders* (codificadores digitais) operando no padrão H.264, que por sua vez se interligam ao *switch* existente no *Gate*, são utilizadas para monitorar e auxiliar as câmeras fixas do sistema de CFTV, sendo compostas por:

- a) PTZ;
- b) Dome.

4.1.11 Encoders

Os codificadores de vídeos utilizados no sistema de CFTV podem de ser composto por 1, 2, 4, 8 e 16 portas e operam em padrão MPEG4 e H264.

4.1.12 Sistema de Gestão e Armazenamento de Vídeo

O sistema para gestão e armazenamento de vídeo poderá estar dentro de alguns parâmetros, entre eles estão:

- Padrões MPEG-4 / H.264 / MPEG-2 / MJPEG / Wavelet;
- Gestão de banda digital desde 8 Kbits/s até 20 Mbits/s por câmera;
- Até 60 fps por câmera (usual 15 fps);
- Resoluções desde 160x120(1/4 CIF) até multi-megapixels (usual 1 CIF);

4.1.13 Detecção Automática de Riscos por Análise de Vídeo

Considerando-se o Sistema de CFTV e controle de acesso de qualquer porto, pela dimensão a ser monitorada e sendo impraticável e ineficiente a supervisão das

imagens geradas apenas por simples observação, são incorporadas ao sistema facilidades de análise automática de vídeo, com as seguintes características funcionais:

a) Detecção de Movimento e Alarmes: As câmeras com esta funcionalidade são configuradas com zonas definidas pelo operador. Ao se detectar movimento em qualquer das zonas (eventualmente filtrado por horários programáveis) será acionado um alarme.

b) Detecção de Intrusão: As câmeras com esta funcionalidade são configuradas para gerar um alarme quando um objeto de tamanho maior que um patamar especificado cruzar uma linha imaginária.

c) Contagem de Objetos: Configuradas as dimensões máximas e mínimas do objeto de interesse, as câmeras especificamente configuradas para este fim geram uma contagem instantânea, atualizada periodicamente.

d) Identificação de Objetos: Os alarmes decorrentes de comportamentos inesperados de objetos (programáveis numa tabela acessível ao gestor do sistema). Todos os alarmes são gerados de forma independente pelo fato da câmera estar sendo visualizada ou não, mas podem (opcionalmente) causar o chaveamento do vídeo observado para a câmera que gerou o alarme.

4.1.14 Estação de Pesquisa em Vídeo Gravado

A estação de pesquisa permite ao usuário autorizado, utilizando o Gestor de Situação no Centro de Controle (ou em outro local) recuperar vídeo armazenado a partir de quaisquer metadados, e transferir os trechos de vídeo relevantes para mídia permanente, para providências posteriores ou arquivamento.

4.2 SISTEMA DE CONTROLE DE ACESSO

O sistema de controle de acesso tem que ter a capacidade de gerenciar, administrar e identificar o registro de pessoas, cargas e veículos, além de validar e autorizar os acessos às áreas controladas e restritas, sendo composto por:

- Identificação do usuário (pessoas e veículos);
- Dispositivos de bloqueio ou barreiras de acesso;
- Software de Gestão do Sistema;
- Armazenamento de dados;
- *Back-up*.

4.2.1 Sistema de Identificação

O sistema de controle de acesso necessita de recursos físicos e lógicos para reconhecer e identificar os usuários e, então, aplicar as regras de liberação ou não do acesso ao ambiente controlado ou restrito.

Meios de validação:

- Número de identificação pessoal, que pode ser associado a um cartão ou digitado em um teclado (*login* e senha);
- Identificação, através de uma característica biológica, do corpo da pessoa que se deseja controlar o acesso, sendo chamada de biometria.

Os cartões de acessos podem ter diversas tecnologias e para cada tecnologia de cartão uma leitora específica deverá ser utilizada e entre elas se destacam:

a) Controle de Acesso por Senha

Este controle de acesso é realizado por uma tecnologia que permite controlar a entrada ou saída de pessoas em determinados locais, através de senhas personalizadas ou identificadoras do lugar de acesso.

b) Controle de Acesso por Cartão

Controle de acesso realizado por tecnologia que permite controlar a entrada ou saída de pessoas em determinados locais, através de leitores de cartões instalados nos bloqueios (catracas, torniquetes, fechaduras, cancelas). Esses leitores fazem a verificação e a validação das informações contidas nos cartões das pessoas que pretendem acessar o local. Nessas informações, além de constar dados dos usuários, também existem indicações sobre locais, horários que se possa acessar.

As tecnologias de cartões utilizadas no controle de acesso são:

- **Cartão com Código de Barras** - possui código de barras distribuídas, que formam códigos alfanuméricos ou somente numéricos, podem possuir ou não criptografia e existem vários padrões de códigos de barras e de tecnologia de leitoras, não são recomendados para determinados níveis de segurança por ser de fácil adulteração e cópia.
- **Cartão Magnético** – com tarja magnética possui um conjunto de trilhas, normalmente três, para gravação das informações desejadas. É semelhante a um cartão utilizado pelos bancos e para determinados níveis de acesso não é recomendado, por ser facilmente clonado.
- **Cartão de Proximidade** - é lido através de uma antena (ondas de rádio) que aciona um chip interno que devolve o sinal captado por leitora apropriada, identificando assim o código associado ao usuário do cartão. São muito utilizados atualmente, sendo que uma de suas principais vantagens é o sistema de retorno e durabilidade, pode ser reutilizado por várias pessoas e seu nível de fraude é menor.
- **Cartão Inteligente - Smart Card** - possui um chip que pode ser acessado através de contato físico ou por uma antena (cartões sem contato ou *contactless*).

Possui um chip de memória com capacidade variável onde as informações relacionadas ao controle de acesso ficam registradas, podendo ser manipuladas ou não pelas leitoras de cartões. Atualmente tem menor índice de fraude.

- **Tag's** - São dispositivos de identificação que não necessitam de contato com as leitoras, pode ser apenas de leitura ou leitura / gravação. Os tags podem ser passivos (dependem da energia irradiada pelo dispositivo de leitura ou antena) ou ativos (possuem energia própria ajudando na captura de sinal aumentando o alcance da leitura). São muito utilizados no controle de acesso de veículos e sua aplicação é diversificada, sendo possível sua utilização na cadeia logística, pois é muito eficaz no controle de cargas, mercadorias e pessoas.

c) Controle de Acesso por Biometria

Permite controlar a entrada e/ou saída de pessoas em determinados locais, por meio da identificação de alguma característica biológica do corpo do usuário. Tal característica poderá estar ou não associada a uma senha ou cartão de identificação e será comparada com informações armazenadas em um sistema de banco de dados, permitindo ou não o acesso do usuário.

Diversas características biológicas podem ser utilizadas em um processo de identificação. A escolha da tecnologia biométrica a ser utilizada em cada local dependerá, principalmente, do grau de controle exigido, do perfil do usuário e do fluxo de pessoas. As principais tecnologias utilizadas atualmente são:

- **Assinatura**

Identificar a pessoa por meio da comparação de assinaturas, uma delas gravada no banco de dados.

- **Face**

Identificar a pessoa por meio da leitura dos traços do rosto da pessoa (biometria facial);

- **Geometria da mão**

Identificar a pessoa por meio da leitura do formato da mão da pessoa;

- **Impressão Digital**

Identificar a pessoa por meio da impressão digital. As tecnologias existentes, atualmente, para este método são:

- **Íris**

Identificar a pessoa através da leitura dos anéis existentes ao redor da pupila;

- **Retina**

Identificar a pessoa através da leitura da retina, isto é, análise dos vasos sanguíneos do fundo dos olhos da pessoa. Este é um dos métodos mais seguros de identificação biométrica;

- **Voz**

Identificar a pessoa através da identificação de sua voz;

Para casos especiais de controle de acesso, como exemplo, laboratórios nucleares, exigem-se como padrão internacional mais de uma conferência de biometria diferente para acesso nas áreas de risco.

d) Dispositivos de Bloqueio ou Barreira de Acesso

Os dispositivos de bloqueio ou barreira de acesso são equipamentos destinados a impedir a entrada ou a saída de pessoas ou veículos, sem autorização prévia.

d1) Controle de Acesso de Pessoas

Os sistemas de controle de acesso utilizam dispositivos e equipamentos eletro-eletrônicos, devidamente programados, para identificar o usuário, liberar ou não o acesso à área controlada ou restrita. Estes dispositivos estão associados a leitoras e/ou teclados.

- **Identificadores Biométricos**

Equipamentos que utilizam as tecnologias biométricas para liberar o acesso de pessoas e a escolha das tecnologias dos equipamentos a serem utilizados vai depender do grau de controle exigido.

- **Leitores de Cartões de Controle de Acesso**

São utilizados juntamente com cartões. Esses leitores auxiliam na identificação e autorização de acesso de pessoas e veículos. Para cada tipo de cartão existe um tipo de leitor diferente.

- **Portas e Fechos Eletromagnéticos**

Áreas como salas, laboratórios, etc, geralmente fazem parte do segundo nível da área controlada pelo sistema e são controlados por portas internas a instalação as quais utilizam fechos especiais para esta função e estão também associados a uma leitora ou outro dispositivo de controle. Podem liberar mecanicamente uma trava ou atuar como um eletroímã.

- **Catracas eletrônicas**

São equipamentos instalados na maioria dos casos em portarias, refeitórios, recepções e outros ambientes com necessidade de controle. Assim como as cancelas automáticas para o controle de acesso de veículos, as catracas ou bloqueios, são partes integrantes do primeiro nível do controle de acesso em uma instalação, ou seja, aquele um pouco mais periférico, antes de uma sala de acesso restrito, interna a área controlada.

- **Torniquetes**

São dispositivos com vários braços, ou barreiras, dispostos verticalmente em altura superior a uma pessoa. São utilizados em áreas de maior exposição para áreas controladas, funcionando como barreira total, visando a absoluta segurança, a fim de eliminar fraudes de entrada de intrusos.

- **Detectores de metais**

Têm a finalidade de detectar a presença de metais em pessoas, evitando a entrada de objetos que ameacem a segurança das pessoas e do local.

- **Detectores de Raio X**

Têm a finalidade de implantação em áreas de acesso para centrais de segurança direcionadas a visitantes e também áreas de embarque para monitoramento de objetos carregados em bolsas ou recipientes que passam pelo detector de metal de baixa frequência.

d2) Controle de Acesso de Veículos

- **Cancelas automáticas**

São equipamentos utilizados para o controle de acesso de veículos, com várias medidas de hastes, ou barreiras, e velocidades de movimentação. É importante que as cancelas tenham, associados a ela, sensores de detecção de veículos para evitar que a haste baixe sobre o mesmo, pode ser sensor de presença infravermelho ou laço indutivo.

- **Dilaceradores de pneus**

São equipamentos de segurança utilizados no controle de acesso de veículos para locais com alto risco de invasão / evasão. São utilizados quando o local a ser controlado exigir uma alta segurança e apresentar um grande volume de usuários.

- **Semáforos**

Equipamentos utilizados no controle de acesso de veículos por meio da sinalização de cores diferenciadas. Os semáforos são utilizados quando o local a ser controlado exigir uma baixa segurança e apresentar um grande volume de usuários, é utilizado para gerenciar fluxo e refluxo de acesso em horários de pico, invertendo posições de acesso de entrada ou saída.

- **Sensores**

Equipamentos utilizados para detectar a presença ou a ausência de estímulos e/ou matérias, podendo ser magnéticos, elétricos, ópticos.

e) Controle de Cargas e Bagagens

Para este tipo de controle são apresentados os principais equipamentos aplicados no controle e identificação de cargas e bagagens:

- **Balanças Ferroviárias** - Equipamentos utilizados para a pesagem de trens para se determinar o peso bruto ou líquido da carga.
- **Balanças Rodoviárias** - Equipamentos utilizados para a pesagem de caminhões ou equivalentes para se determinar o peso bruto ou líquido da carga.
- **Dinamômetros** - Dispositivos utilizados para medir a intensidade de tração ou compressão que é aplicada sobre ele, como resultado é possível determinar o peso de um material.
- **Etiquetas** - Dispositivos utilizados para identificar cargas ou bagagens com algumas informações, a fim de realizar um melhor controle e uma posterior identificação.

- **Leitores de Código de Barras** - Equipamentos utilizados para auxiliar no controle e identificação de cargas ou bagagens, realizando a leitura do código e barras. Há quatro tipos básicos de leitores de código de barras – fixo, manual, com memória e sem fio.

- **Leitores fixos e manuais:** equipamentos permanentemente ligados ao computador ou terminal que transmitem o dado, cada vez que o código de barras é lido.

- **Leitores portáteis:** equipamentos que possuem bateria e memória para armazenar os dados, a fim de transmiti-los, posteriormente, a um computador.

- **Leitores sem fio:** equipamentos que também possuem bateria e memória para armazenar, mas com capacidade de transmitir, em tempo real, os dados para o computador.

- **Scanner**

Equipamento utilizado para realizar a inspeção não intrusiva das cargas e / ou bagagens.

4.2.2 Sistema de Gestão de Acesso

As definições das características de integração com os diversos sistemas agregados determinam o grau de desempenho que será exigido do referido software. Especificar o sistema de controle de acesso de forma limitada, levando em consideração somente variáveis de entrada e saída, pode não agregar o grau de segurança esperado para o ambiente a ser controlado.

Desta forma, pode-se pensar nos grandes grupos de arquitetura de sistemas de controle de acesso, utilizando complexos sistemas de segurança integrada.

4.2.3 Sistema contra Intrusão

É o conjunto de dispositivos utilizados com o objetivo de detectar a intrusão em áreas protegidas.

Pode-se destacar como seus principais componentes:

a) Sensores Periféricos ou Perimetrais

São aqueles que possuem características adequadas para proteção de ambientes externos, tais como muros, cercas, ou ainda campo aberto.

Para esta aplicação destacam-se:

- **Sensor Infravermelho Ativo (IVA)** - Dispositivo que cria uma barreira eletrônica para detecção de intrusão em um ambiente protegido pelo sistema de alarme.
- **Barreira Microondas** - A barreira microondas é apropriada para a detecção de intrusão em áreas externas em que há necessidade de longo alcance. Ela é composta de duas bases, uma transmissora e outra receptora.
- **Cabo Microfônico** - Interfaces conectadas a cabos especiais, instalados em cercas ou enterrados, capazes de monitorar vibrações e variações mecânicas.
- **Cerca Elétrica ou Central de Choque Pulsativo** - Sistema composto por uma central, capaz de eletrificar e produzir um choque pulsativo nos fios instalados no perímetro da área a ser protegida.

b) Sensores de Abertura / Arrombamento

São aqueles que possuem características adequadas para proteção de portas, janelas e alçapões. Para esta aplicação destacam-se:

- **Sensores magnéticos** - Composto por um ímã e um contato, que quando afastados, geram uma variação de estado, enviando uma identificação de abertura para um painel ou central de alarme.
- **Sensores de quebra de vidro** - Desenvolvidos com microfones especiais, são capazes de distinguir no som ambiente, a onda de choque acústica, gerada pela quebra de um vidro.
- **Sensores de Vibração** - Componentes capazes de detectar vibrações em um ambiente protegido. Quando alcança determinado limite envia ao painel ou central de alarme a informação de violações em determinada área ou objeto.
- **Sensores volumétricos** - São aqueles que possuem características adequadas para detecção de movimentação em ambientes internos.
Para esta aplicação destacam-se os:
 - **Sensores de presença – infravermelho passivo (IVP)** - Também conhecido como Sensor PIR ou Sensor de Movimento ou Sensor Volumétrico é um dispositivo que detecta o movimento do intruso em um ambiente internamente protegido pelo sistema de alarme. Seu funcionamento baseia-se na detecção da aproximação e afastamento de uma fonte calórica (a qual emite raios infravermelhos).
 - **Sensor Dupla Tecnologia** - Também conhecido como Sensor Conjugado ou Sensor *Dual Safe* ou Sensor Volumétrico ou Pet, é um componente do sistema, que detecta o movimento do intruso em um ambiente internamente

protegido pelo sistema de alarme. Seu funcionamento baseia-se em duas tecnologias de detecção: Infravermelho Passivo e Microondas, o que permite que seja imune à detecção de pequenos animais.

4.2.4 Sistema contra Incêndio

Segundo a NBR 9441/98, sistema constituído pelo conjunto de elementos dispostos e adequadamente interligados, que fornece informações de princípios de incêndio, por meio de indicações sonoras e visuais, e controla os dispositivos de segurança e de combate automático instalados em edifícios.

Pode-se destacar como seus principais componentes:

- **Painel / Controlador de Alarme** - Sistema eletrônico responsável pela supervisão de sensores e módulos inteligentes a ele conectados, capaz de fazer acionamentos manuais ou automáticos, possibilitando a troca de informações com sistemas centralizados de monitoramento.
- **Teclado de Comando Local ou Remoto** - Utilizado para a programação e operação do painel de alarme.
- **Sensores ou Detectores** - Dispositivos que registram e analisam automaticamente a presença ou variação de certos fenômenos físicos ou químicos, transmitindo estas informações à Central de Controle.

De acordo com seu funcionamento, são agrupados em:

i) Sensores de Fumaça

São dispositivos encarregados de fazer a vigilância permanente de um local. Constituem a parte sensível da instalação de detecção automática de incêndio.

Sua ativação ocorre quando da presença de partículas e/ou gases, visíveis ou não, e de produtos de combustão, no ponto da instalação.

- **Iônicos** – Instalados em locais com presença de combustíveis inflamáveis, solventes.
- **Ópticos** – Instalados em corredores ou rotas de escape, locais com a presença de madeira ou papel. Não devem ser utilizados em áreas com presença de vapores, poeiras ou fumaças como em banheiros, cozinhas etc.

ii) Sensores de chama

- **Infravermelho ou Ultravioleta** - Ambos são constituídos por uma parte óptica e uma eletrônica, onde o sensor óptico responde à radiação emitida pelas chamas e envia o sinal de alarme, através do circuito eletrônico, à Central de Controle. São instalados onde a luz solar não penetre e onde a primeira consequência de um princípio de incêndio seja a produção de chama. Ex.: depósitos de gases e líquidos inflamáveis.

iii) Sensores lineares

- **Espectroscópicos** - Sua ativação ocorre quando da presença de partículas e/ou gases, visíveis ou não, ou mesmo variação de temperatura, em uma linha física de sensoriamento.
- **Eletroquímicos** - Composto por uma série de tubos que absorvem o ar do local e o analisam quanto à presença de determinados tipos de gases.

iv) Sensores de Temperatura - Sua ativação ocorre quando a temperatura ambiente (caso dos térmicos) ou o gradiente da temperatura (caso dos termovelocimétricos) ultrapassa um certo valor pré-determinado.

- **Térmico** – utilizados em processos que produzem calor.

- **Termovelocimétrico** - Utiliza termistores, elementos cuja resistência varia com a temperatura. São utilizados onde o ambiente está sujeito à presença de fumaça ou poeira e onde a velocidade do aumento da temperatura indique um princípio de incêndio (8 a 10°C por minuto). Exemplos: salas de aquecimento, cozinhas e lavanderias.

Para o sistema de segurança eletrônica, se deve primeiramente elaborar uma análise de riscos da segurança, um projeto e depois a aquisição dos equipamentos e aplicativos. Priorizando a proteção periférica, depois o controle das áreas com CFTV e por último o controle de acesso integrado, permitindo e monitorando acessos de pessoas e veículos.

4.3 SISTEMA OCR (OPTICAL CHARACTER RECOGNITION) E BIOMETRIA FACIAL

O sistema é baseado em tecnologia de reconhecimento de caracteres alfa-numéricos e também leitura de biometria facial, a partir de imagens, arquivos de imagens ou mapas de bits, sendo composto por:

1. Leitura de Biometria Facial – LBF;
2. Leitura Automática de Placas – LAP;
3. Leitura Automática de Contêineres – LAC.

A arquitetura é baseada no processamento distribuído, onde as imagens são processadas e enviadas para uma central de processamento e monitoramento, em banco de dados integrados, com arquitetura para reconhecimento de face e placa. Para o reconhecimento de contêineres o sistema está centralizado, uma vez que, é utilizado como auditoria ou verificação de numeração de contêiner.

4.3.1 Componentes do Sistema e Funcionamento do OCR

São partes integrantes para o funcionamento e operacionalidade do sistema OCR.

a) Crachá

Os crachás são cartões de proximidades fornecidos aos usuários do sistema. Dentre eles, têm-se os cartões de pessoa e veículo.

b) Leitoras de Cartão

As leitoras de cartões são responsáveis por realizar a leitura dos crachás eletrônicos dos usuários do sistema e após a leitura, são enviados os dados deste crachá para uma controladora.

c) Controladora

A controladora recebe os dados das leitoras de cartão, com os níveis de acesso, validação e permissão e envia às informações de controle a catraca, cancela, torniquete e Centro de Controle.

- Recebe dados de até três leitoras de um totem, com alturas baixa, média e alta;
- Recebe dados de duas leitoras no caso de ter duas direções no ponto de acesso.

d) Smartcapture

Sistema inteligente para o controle de acesso composto por software que permite fazer a leitura de placa, face e OCR.

d1) Software de Controle de Acesso

O software de controle de acesso é responsável por receber as mensagens de uma ou mais controladoras e enviar uma mensagem de resposta. Durante o processo, será necessário saber o IP da controladora. Esta informação não precisa ser enviada pela controladora, uma vez que pode ser identificada pelo software de controle de acesso através do socket.

d2) Reconhecimento - Placa e Biometria – Face

Estes softwares realizam o reconhecimento da placa/face e permite prover informações para o software de controle de acesso para que tome as decisões. Após o processamento, um evento deverá ser registrado no banco de dados na tabela de eventos.

4.3.2 Central de Comunicação

a) OCR – Contêiner

Este software realiza o reconhecimento do contêiner e, após o processamento, um evento deverá ser registrado no banco de dados na tabela de eventos.

b) Banco de Dados

Todas as informações para verificação e validação do sistema de controle de acesso (enviadas/recebidas) estão armazenadas no banco de dados, figura 10, bem como as tabelas locais e replicadas para os pontos de acesso.

4.3.3 Arquitetura do Sistema de Reconhecimento OCR

Figura 10. Arquitetura do sistema OCR.

4.3.4 Leitura de Biometria Facial – LBF

O sistema de reconhecimento facial avalia e seleciona em cada rosto (figura 11), aspectos que formam as diferentes características faciais. Estes são definidos como **pontos nodais**. A face humana possui em torno de oitenta pontos nodais. Alguns pontos que o software mede são:

- Distância entre os olhos; Contornos da cavidade orbital; Sobrancelhas; Comprimento e contorno do nariz;

Os pontos nodais são medidos e inter-combinados, criando-se um código numérico que representa o rosto no banco de dados. Esse código é chamado de **assinatura facial**.

Figura 11. Combinações Geométricas para Biometria Facial

Para atender às diferentes posições dos rostos dos motoristas, em função das alturas dos veículos, desde passeio até caminhões altos, cada totem possui 3 conjuntos de:

- a) Leitora de Crachá;
- b) Câmera digital;
- c) Iluminação eletrônica especial para reconhecimento de faces.

a) Integração ao Sistema de Credenciamento

O sistema de credenciamento, com o banco de dados no Centro de Controle, tem que interagir e estar integrado com o sistema OCR e CFTV.

4.3.5 Leitura Automática de Placas – LAP

O sistema LAP, figuras 12 e 13, com tecnologia de reconhecimento de caracteres (OCR) e câmeras dedicadas garantem altas taxas de reconhecimento, sob praticamente quaisquer condições de trabalho. A partir de algoritmos cruzados,

o sistema encontra a placa do veículo (dianteira ou traseira) na imagem, reconhece seus caracteres e o resultado do reconhecimento é armazenado em um banco de dados, incluindo imagens e outras informações gerenciais. A unidade de processamento pode gerar comandos para controlar elementos externos do sistema.

a) Sistema LAP

Figura 12. Sistema LAP.

b) Sistema LAP interligado ao Centro de Controle

Figura 13. Sistema LAP interligado ao Centro de Controle

4.3.6 Leitura Automática de Contêineres – LAC

O sistema de Leitura Automática de Números de Contêineres (LAC), figura 14, é utilizado para verificação e controle de acesso de entrada de caminhões com contêineres nos Gates.

a) Sistema LAC interligado ao Centro de Controle

Figura 14. Sistema LAC interligado ao Centro de Controle.

4.3.7 Localização dos Equipamentos de OCR no Gate

Figura 15. Desenho dos equipamentos instalados em Gate.

4.4 INFRA-ESTRUTURA E BACKBONE ÓPTICO

Refere-se a infraestrutura de encaminhamento físico de todo o cabeamento óptico da arquitetura do sistema com contingenciamento e arquitetura tolerante a falhas, em diversos níveis, visando a continuidade da comunicação através de soluções de última geração para comunicação e segurança lógica de dados.

Todas as imagens de vídeos e transmissão de dados são transmitidas por este meio físico entre os equipamentos instalados na área e Centro de Controle.

A redundância é importante para o processo óptico, visto ser um meio físico de transmissão de informação factível de ruptura e risco de perdas de informação.

Os equipamentos Ativos de Rede (LAN SWITCHING) são responsáveis por prover a conectividade de todos os dispositivos TCP-IP que trafegam na rede ótica.

4.5 MODELAGEM E ARQUITETURA DO SISTEMA DE SEGURANÇA

A arquitetura é composta por um conjunto de subsistemas de hardwares e softwares que permite a funcionalidade do sistema de segurança.

4.5.1 Equipamentos de Segurança Perimetral de Dados (Firewall)

Responsáveis pela garantia de segurança perimetral de dados da rede de comunicação e também pela provisão de acesso remoto seguro às aplicações desse ambiente.

4.5.2 Sistemas de Gerenciamento

São responsáveis pela provisão de monitoramento, gerenciamento e controle do ambiente lógico implantado no intuito de permitir a realização de operações de forma centralizada, com rastreabilidade das ações efetuadas, bem como manutenção do ambiente.

4.5.3 Servidores de Arquivo

Em função da necessidade de se dispor e avaliar quaisquer das informações de dados e imagens armazenadas, tem-se a arquitetura básica SAN – *Storage Área Network*, definido para a interconexão e utilização múltipla dos Servidores e

respectivos Discos Rígidos do Sistema de Armazenamento e Softwares de Controle, devidamente adequado ao Sistema.

4.5.4 Contingenciamento do Sistema de Comunicação

Todo sistema de comunicação tem que ter uma política de contingência, seja para a comunicação de dados ou energia elétrica, com sistemas de energia redundante para os circuitos que alimentam os equipamentos de CFTV , Comunicação e Controle de Acesso;

- Altos níveis de processamento e desempenho;
- Alta capacidade de vazão das informações trafegadas;
- Alta disponibilidade e tolerância a falhas em diversos níveis;
- Protocolos de gerenciamento, tratamento e comunicação de dados atualizados e aderentes as mais recentes normas e padrões tecnológicos;

O sistema de gestão de vídeo captura, visualiza, armazena, compartilha e a segurança lógica no acesso tem que ter as aplicações e informações no Centro de Controle.

4.5.5 Storage (Armazenamento)

O subsistema de armazenamento é compartilhável entre os servidores e clientes, ligado à rede através de uma porta Gigabit Ethernet. Para os aplicativos externos, ele aparece como um dispositivo ISCSI (não como compartilhamento de arquivos NFS ou CIFS) de modo a maximizar o desempenho da aplicação. As unidades de disco possuem interface SATA, em incrementos de 1 TB.

A troca de qualquer controlador, unidade de disco ou fonte de alimentação pode ser feita a quente, sem a necessidade de parar o sistema. O mesmo se aplica a um nó inteiro de armazenamento (isto é, um servidor completo). A configuração de redundâncias de disco e controladores é alterável dinamicamente.

O sistema suporta módulos de até 96 TB, suficientes para armazenar o dobro do tempo atual (30 dias) na suposição de adoção de encoders no padrão H.264.

4.5.6 Redundância de Conectividade

O sistema conecta-se à rede do Centro de Controle através de um switch dual, com redundância automática. No caso de perda de conectividade através de uma porta, a outra mantém o tráfego sem interrupção. A capacidade de tráfego por qualquer das portas é de 200 megabytes por segundo. Capacidade adicional, até 3 gigabytes por segundo, pode ser instalada sem interromper a operação das portas em uso.

4.5.7 Administração e Gerenciamento do Sistema

O sistema de armazenamento e gestão de vídeo apresenta uma interface gráfica de gestão de fácil aprendizado e uso. A configuração de hardware é automaticamente atualizada na tela, detectando as modificações, e as configurações de volumes, incluindo tipo de RAID e dinamicamente alteradas nesta interface sem interrupção da operação.

A prioridade entre as funções de migração de dados em caso de falha e acesso de dados é também configurável dinamicamente pelo operador. A priorização de recuperação e acesso pode ser feita volume por volume.

4.6 FORNECIMENTO DE ENERGIA ELÉTRICA

A fonte geradora para o fornecimento de energia elétrica para qualquer sistema de segurança é fundamental para o processo de monitoramento de imagens e controle de acesso. Como por exemplo a energia elétrica utilizada no Porto de Santos é própria e, para atender possíveis falhas, o sistema elétrico do centro de controle é composto por um estabilizador / no break de 40 KVA, com autonomia de 30 minutos e um Grupo Motor Gerador de 80 KVA, com sistema inteligente, para auxiliar nessa demanda. Como exemplo de conjunto de alimentação se tem:

- a) Conjunto Estabilizador / No-Break / Banco de Baterias.
- b) Grupo Motor-Gerador
- c) Controlador do Grupo Gerador

4.7 SISTEMA DE DETECÇÃO E COMBATE À INCÊNDIO AUTOMÁTICO

Sistema de detecção, alarme e combate a incêndio na sala do GMG interligando-o ao CCCOM, permite atender também a sala de servidores através da complementação de detectores e tubulação de gás adequado.

4.8 PAINEL DE MOVIMENTAÇÃO VARIÁVEL – PMV

São painéis utilizados em estradas, vias de acesso e área portuária para informar situações de trânsito e informações relevantes aos usuários deste sistema rodoviário.

a) Painei Tipo U

Para auxiliar os usuários com informações do trânsito e regramento se utilizam painéis alfanuméricos e gráficos, sobre estrutura metálica (Pórtico), dotadas de formato retangular, com apresentação colorida, utilizando-se combinações de LED's de cores primárias, reproduzindo uma região gráfica full-color com resolução de 64 x 64 pixels, com objetivo de informar os usuários portuários sobre as condições do Porto.

b) Painei Tipo L

Painei Alfanumérico e gráfico, sobre estruturas Semi-Pórticos, dotada de um formato retangular, utilizado em locais de grande circulação apoiada em apenas um

dos lados das pistas, comportando a fixação em qualquer dos lados. Estes painéis contêm duas (2) linhas de caracteres alfanuméricas, com doze (12) caracteres, com uma altura de caractere de 320 mm e uma resolução na área alfanumérica de 16 x 11 pixels por caracteres, com apresentação colorida, utilizando-se combinações de LED's de cores primárias, reproduzindo uma região gráfica full-color com uma resolução de 64 x 64 pixels, para informar os usuários portuários.

c) Painei Tipo C

Painéis semafóricos, com indicação de siga ou pare por pictograma fixo, nas faixas de entrada e saída dos Gates, para auxiliar o trânsito de veículos pesados e leves.

4.9 QUADRO SINÓTICO

O Gestor de Situação incorpora um quadro sinótico (mapa do porto) na qual são indicadas as posições dos elementos relevantes do sistema ISPS – câmeras, transmissores de rádio, guaritas, cancelas, torniquetes, etc.

O mapa permite, mediante escolha de quaisquer dos pontos na área visualizada, uma apresentação automática do vídeo das câmeras mais próximas dentro da região selecionada, onde apresenta:

- i. Locais de Ocorrências de Alarmes detectados pela Análise de Vídeo, ou pelo Sistema de Acesso;
- ii. Posicionamento dos Veículos da Guarda Portuária ou vigilância;
- iii. Trajetória dos veículos nos últimos 30 minutos, como uma trilha superposta ao mapa do Porto mostrado no Quadro Sinótico;
- iv. Eventos de alarme no caso do veículo rastreado sair dos limites do Porto;
- i. Visualização do Quadro Sinótico, figura 16, em diferentes níveis de zoom, de forma que o mais distanciado ofereça uma visão de toda a área portuária e o mais próximo a região de entorno (100 m aproximadamente) de cada Gate.

Figura 16 . Painel de monitoramento com quadro sinótico.

4.10 BALANÇA DINÂMICA

As Balanças Dinâmicas, figura 17, tem por objetivo o controle eletrônico e automático, para os veículos de cargas pesadas com os respectivos softwares, hardwares e acessórios.

A) Aplicação

- Pesagem automática;
- Dados de peso, placa, veículo;
- Reconhecimento de veículos;
- Balança unidirecional ou bidirecional;

B) Resultados

- Eliminação de fraudes.

- Eliminação de digitação e operadores.
- Aumento do fluxo de pesagem com a diminuição do tempo de presença do veículo na balança.
- Integração da balança com sistema de Gestão eliminando ticket de pesagem e digitação.

C) Desenho do Sistema de Balança Dinâmica.

Figura 17. Balança Dinâmica.

4.11 SISTEMA DE ALARME E COMUNICAÇÃO SONORA

Este sistema envia dados e mensagens a partir do Centro de Controle, de forma on-line a qualquer um dos Gates, distribuídos ou separados individualmente aos Gates, por região, ou para toda a área Portuária e destina-se a emitir avisos sonoros, figura 18, de condições de risco às pessoas presentes no Porto, de forma localizada ou setorizada. São amplificadores e cornetas acústicas instalados em cada um dos Gates que dão acesso à área primária, para sinalizar condições de alerta (som de sirene) e para comunicação de voz (anúncios emitidos a partir do CCom). A transmissão é feita pela mesma rede IP que recolhe imagens das câmeras, utilizando o canal de som já presente nos codificadores instalados nos Gates.

As condições de alarme (nível de segurança) no Porto são informadas, por Gate e vizinhanças, às pessoas presentes através de alarmes sonoros e avisos de voz.

a) Sistema de Alarme e comunicação por Voz

Sonofletores - utilizados para sonorização das áreas próximas aos Gates, visto ter longo alcance de difusão sonora e alta inteligibilidade.

Comunicador/microfone possibilita a execução de avisos a viva-voz. Possui haste flexível facilitando o melhor posicionamento ergonômico do operador.

Figura 18. Sistema de Alarme e comunicação por Voz

5. COMPONENTES DO SISTEMA DE SEGURANÇA PORTUÁRIO

Muitos fatores contribuem para o sistema portuário brasileiros, mas o mais importante são os componentes que fazem parte deste processo, como o PNSPP, ISPS Code, logística, Comex, os órgãos públicos e principalmente os atores e agentes portuários.

5.1 PLANO NACIONAL DE SEGURANÇA PÚBLICA PORTUÁRIA

Com a criação do PNSPP, Anexo A, se procurou buscar medidas integradas de segurança, desenvolvendo e aperfeiçoando a atuação dos organismos e instituições para a segurança pública nos portos, terminais e vias navegáveis, onde permitiu-lhes cooperação conjunta. Foi criada a Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CONPORTOS) e as Comissões Estaduais de Segurança Pública nos Portos Terminais e Vias Navegáveis (CESPORTOS), para suprir dificuldades encontradas no setor de segurança, tais como:

- Conciliação de ações de rotinas funcionais com aquelas decorrentes do delito considerado;
- Carência de recursos humanos e de equipamentos essenciais;
- Dificil levantamento das investigações a partir de registros de atos ilícitos e com inquérito policial instaurado, pelo fato de as pessoas não residirem no país.
- Elaboração de estatísticas sobre atos ilegais realizados em áreas marítimas brasileiras não confiáveis, perante a falta de registro de delitos de pequeno vulto;
- Inviabilidade de investigações pelo fato de os comandantes não comunicarem os atos ilícitos ocorridos em seus navios às autoridades locais, em portos brasileiros; e

- Nivelamento de assuntos tratados por setores diferentes da Administração Pública Federal e Estadual;

O PNSPP é um plano de ações, onde seu principal objetivo é aperfeiçoar o sistema de segurança pública nos portos, terminais e vias navegáveis, visando reprimir e prevenir o crime e a impunidade e aumentar a segurança portuária.

O PNSPP adotou quatro compromissos, os quais, suas respectivas ações são:

- Combate ao narcotráfico e ao crime organizado nos portos, terminais e vias navegáveis;
- Controle de entrada e saída de armas do país;
- Repressão ao roubo/furto de cargas;
- Utilização do subsistema de inteligência de Segurança Pública.

5.2 AGENTES DO SISTEMA PORTUÁRIO

São todos os envolvidos direta e indiretamente nas atividades portuárias.

5.2.1 Agentes Governamentais

A operacionalidade do porto se faz através da integração da Autoridade Portuária com todos os atores dos setores públicos e privados, tais como os Operadores e Agências Marítimas, OGMO e as Autoridades como a Secretaria Especial de Portos, Fazenda, Defesa, Justiça e Saúde.

Seguem os agentes governamentais participantes da segurança portuária, bem como as do governo Estadual e do CAP, suas atribuições e competências estão no Anexo A.

a. Conselho de Autoridade Portuária

b. Governo Estadual**b1) Polícia Civil****b2) Polícia Militar****b3) Corpo de Bombeiros****c. Ministério da Defesa / Marinha do Brasil / Capitania dos Portos****d. Ministério da Fazenda / Secretaria da Receita Federal****e. Ministério da Justiça / Polícia Federal****f. Ministério da Saúde / ANVISA****g. Secretaria Especial de Portos****5.2.2 Agentes Não-Governamentais no setor portuário**

Os agentes e órgãos não governamentais que prestam serviços na área portuária são compostos por:

A) Agente Marítimo

Representa o armador no país e tem a responsabilidade perante as autoridades pelas obrigações das embarcações, junto a alfândega e demais órgãos governamentais envolvidos nas operações de atracação e desatracação de embarcações, carga e descarga de mercadorias, embarque e desembarque de passageiros e tripulantes. Solicitar, à autoridade sanitária, a concessão de Livre Prática, e outros documentos como Manifesto de Carga/BL, Requisição e Prioridade

e Atracação, Declaração das provisões de bordo, Lista da tripulação, Lista de passageiros, Declaração dos bens da tripulação, Declaração marítima de saúde.

B) Órgão Gestor de Mão De Obra (OGMO)

Os OGMO's são responsáveis pelos cadastros e registros de Trabalhadores Portuários Avulsos – TPA's, com controle do ponto e requisição de mão-de-obra portuária para estes profissionais e administra as seguintes categorias de TPA's:

- **Arrumadores:** trabalham no costado, preparando a carga a ser movimentada;
- **Bloquistas:** encarregados de serviços tais como: peação e despeação da carga, forração, retirada de madeira ou limpeza em geral;
- **Conferentes:** encarregados do planejamento, da verificação de quantidades, marcas e lotes das cargas embarcadas ou desembarcadas dos navios;
- **Consertadores:** profissionais especializados nos reparos das embalagens e cargas avariadas;
- **Estivadores:** profissionais que atuam na movimentação da carga no interior das embarcações, efetuando a estivagem e desestivagem da carga;
- **Guindasteiros:** especializados na operação dos guindastes de terra.
- **Vigias portuários:** responsáveis pela vigilância a bordo das embarcações;

C) Operador Portuário

O operador portuário é responsável pela operação de carga e descarga de um navio na área do porto organizado, utilizando a mão-de-obra fornecida pelo OGMO.

5.3 CONPORTOS - COMISSÃO NACIONAL DE SEGURANÇA PÚBLICA NOS PORTOS, TERMINAIS E VIAS NAVEGÁVEIS.

A Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis foi criada pelo DECRETO Nº 1.507, DE 30 DE MAIO DE 1995, com o propósito de elaborar e implementar sistema de prevenção e repressão a atos ilícitos nos portos, terminais e vias navegáveis, sendo integrada por um representante e respectivo suplente dos Ministérios da Justiça, que a presidirá, Marinha, Fazenda, Relações Exteriores e dos Transportes.

Compete à Comissão Nacional de Segurança Pública nos Portos, Terminais e Via Navegáveis:

- I - baixar normas, em nível nacional, sobre segurança pública nos portos, terminais e vias navegáveis;
- II - elaborar projetos específicos de segurança pública nos portos, terminais e vias navegáveis e, por via diplomática, buscar junto à Organização Marítima Internacional (IMO) assistência técnica e financeira de países doadores e instituições financeiras internacionais;
- III - apresentar sugestões às autoridades competentes para o aperfeiçoamento da legislação pertinente, inclusive consolidação de leis e regulamentos;
- IV - avaliar programas de aperfeiçoamento das atividades de segurança pública nos portos, terminais e vias navegáveis;
- V - manter acompanhamento estatístico dos ilícitos penais ocorridos nos portos, terminais e vias navegáveis e dos resultados das investigações e das punições aplicadas;

VI - encaminhar aos órgãos competentes avaliações periódicas sobre as necessidades relativas à segurança pública nos portos, terminais e via navegáveis;

VII - elaborar seu regimento interno e submetê-lo à aprovação do Ministro de Estado da Justiça;

VIII - criar e instalar Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis, fixando-lhes as atribuições;

IX - orientar as Comissões Estaduais, no que for cabível.

Fonte: Ministério da Justiça, 2009.

5.4 CESPORTOS - COMISSÃO ESTADUAL DE SEGURANÇA PÚBLICA NOS PORTOS, TERMINAIS E VIAS NAVEGÁVEIS

A missão das Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CESPORTOS) são de prevenir e reprimir os atos ilícitos nos portos, terminais e vias navegáveis e estão constituídas e instaladas em 20 Estados no território nacional: Amazonas, Amapá, Pará, Maranhão, Piauí, Ceará, Rio Grande do Norte, Paraíba, Pernambuco, Alagoas, Sergipe, Bahia, Espírito Santo, Rio de Janeiro, São Paulo, Paraná, Santa Catarina, Rio Grande do Sul, Mato Grosso e Mato Grosso do Sul.

Cada CESPORTOS será composta, no mínimo por representantes de cada órgão:

- I. Departamento de Polícia Federal, que a coordenará;
- II. Capitania dos Portos;
- III. Secretaria da Receita Federal;
- IV. Administração portuária; e
- V. Governo do Estado.

Compete às CESPORTOS:

- Elaborar Plano de Segurança, na circunscrição de sua competência, contemplando as medidas de segurança necessárias a serem adotadas pelos órgãos públicos e privados que integram o sistema da segurança portuária.
- Elaborar e/ou apreciar os Estudos de Avaliação de Risco de Instalações Portuárias e os respectivos Planos de Segurança Pública Portuária e submetê-los à CONPORTOS para deliberação.
- Fiscalizar, em primeira instância, a implementação dos Planos de Segurança Pública Portuária das instalações portuárias localizadas em sua área de circunscrição, informando à CONPORTOS sobre as incorreções e as medidas necessárias a serem aplicadas na sua correção.
- Propor a CONPORTOS, a elaboração de normas, regulamentos e/ou a adoção de medidas, sempre que estas ações venham a melhorar o sistema de Segurança Pública Portuária.
- Manter e atualizar as informações sobre os ilícitos ocorridos nas instalações portuárias na área de sua atuação, dando a conhecer a CONPORTOS.
- Executar as ações da CONPORTOS, nas respectivas Unidades da Federação, quando acionadas.

Fonte: Ministério da Justiça, 2009.

5.5 CÓDIGO INTERNACIONAL PARA PROTEÇÃO DE NAVIOS E INSTALAÇÕES PORTUÁRIAS (CÓDIGO ISPS),

O Código ISPS, se reporta à Organização Marítima Internacional (IMO). que, consiste em uma Assembléia formada por representantes de todos os Estados-Membros das organizações não governamentais com estatuto consultivo, entre os quais se encontra, atualmente, a Comissão Européia. É constituído por 40 membros, eleitos por dois anos (ANTAQ, 2010).

A mais importante e abrangente de todas as convenções da IMO é a Convenção Salvaguarda da Vida no Mar (SOLAS) que foi Criada em 1912 e ratificada por treze países após o naufrágio do Titanic. Entrou em vigor em 1929, 1948 e 1960, sendo esta última revisão sob coordenação da IMO. Modificada em

1974 e complementada por dois protocolos em 1978 e 1988, tem como foco os equipamentos dos navios, as regras de segurança a cumprir, os procedimentos de alerta e de socorro, e controles do porto pelo Estado, etc.

O Código ISPS é um conjunto de medidas definidas pelo IMO objetivando segurança dos navios e das instalações portuárias nos terminais; tem como principais objetivos: constituir um quadro internacional de cooperação entre os Governos-contratantes da SOLAS, os órgãos públicos, as administrações locais e os setores portuário e dos transportes marítimos, visando identificar ameaças à segurança e tomar medidas para prevenção de incidentes que possam afetar a segurança dos navios ou das instalações portuárias utilizadas no tráfego internacional.

O Código ISPS estabelece 3 (três) níveis de segurança em que os navios e as instalações portuárias deverão operar, conforme as ameaças identificadas.

- Nível 1 de Proteção, normal; o nível no qual os navios e instalações portuárias normalmente operam;
- Nível 2 de Proteção, elevado; o nível aplicável enquanto houver um risco elevado de um incidente de proteção;
- Nível 3 de Proteção, excepcional; o nível aplicável pelo período durante o qual há um risco provável ou iminente de um incidente de proteção.

Segundo a IMO, para os 163 países signatários, o ISPS Code passou a ser obrigatório, inclusive o Brasil.

5.5.1 Código ISPS Code nos Portos Brasileiros

Todos os portos brasileiros terão que ter o ISPS Code implantado em suas instalações portuárias, visto ser uma resolução do Ministério da Justiça (nº. 12 de 18 de dezembro de 2003) que inclusive elaborou um “Roteiro para Análise dos Planos de Segurança Pública Portuária – RPPS” e permitiu uma orientação para elaboração das “Normas de Controle de Acesso e circulação de pessoas e veículos - NAPV”

ambos enviados para as instalações portuárias, para efetuarem um estudo de avaliação de risco; que em seguida, foram enviados à CONPORTOS.

Depois de implantado o ISPS Code caberá a CONPORTOS/CESPORTOS fazer uma verificação das instalações físicas e ver se está de acordo com o Plano de Segurança aprovado. Se tudo estiver nas conformidades será concedido ao Porto ou Terminal a certificação definitiva com a Declaração de Cumprimento (DC), caso contrário será fornecido um Certificado Provisório, com validade de 6 (seis) meses, denominado Termo de Aptidão (TA).

5.6 SISTEMAS COMPLEMENTARES PARA O SISTEMA DE SEGURANÇA PORTUÁRIO

A) Sistema Automático de Identificação (AIS) - é um sistema composto por um conjunto integrado de componentes AIS ou "*transponder AIS*", um modem de alta frequência, um computador e um software gráfico que processa as informações recebidas pelo equipamento, gerando um arquivo para transmissão ou recepção de mensagens de dados digitais padronizadas para o Comando do Controle Naval do Tráfego Marítimo - COMCONTRAM via e-mail, pela intranet ou internet, nas instalações localizadas em pontos fixos, distribuídas ao longo da costa brasileira, ou transmissão de mensagem por HF, via Estações Rádio da Marinha, quando os navios da Marinha do Brasil - MB estiverem em patrulha no mar. (ISPS Code, 2009)

B) Sistema de Identificação e Acompanhamento de Navios a Longa Distância (LRIT) - Sistema de Identificação e Acompanhamento de Navios a Longa Distância (LRIT - *Long Range Identification and Tracking of Ships*), é um sistema que permite saber com grande antecedência ameaças relacionadas a "*security*", sistema que transmite automaticamente informações relativas à identificação e ao seguimento de longo alcance do navio.

C) **Sistema de Gerenciamento do Tráfego de Navios (VTMIS)** - Sistema de controle de tráfego marítimo (VTS) é composto por estações costeiras e portuárias, que controlam a navegação visualmente, por radar, por rádio e por telecomunicações, assegurando a detecção 24 horas por dia, de forma *full time* e *on-line*, sob quaisquer condições atmosféricas. A adição de informações como administrativa, comercial, meteorológica e geográfica agregam valor para o VTS, que passa a designar-se Sistema de Informação e Gestão de Tráfego (VTMIS - *Vessel Traffic Management and Information*).

D) **Iniciativa de Segurança do Contêiner (CSI)** - *Container Security Initiative* - (CSI) é um plano estratégico desenvolvido pela “*U.S. Customs and Border Protection* (CBP)” propicia um regime de segurança para assegurar que todos os contêineres que apresentem um risco potencial do terrorismo sejam identificados e inspecionados em portos estrangeiros antes que eles sejam colocados em navios destinados aos Estados Unidos.

5.7 SEGURANÇA PÚBLICA PORTUÁRIA NO PORTO DE SANTOS

O porto de Santos, maior porto da América do Sul movimentou aproximadamente 96 milhões de toneladas em 2010. Com aproximadamente 13 km de extensão e administrado pela Companhia Docas do Estado de São Paulo – CODESP tem um papel relevante para a economia local e nacional.

O Sistema de Segurança Pública Portuário – SSPP do porto de Santos contou com o apoio e colaboração do GAESI/POLI/USP, através da Fundação de Apoio à Universidade de São Paulo (FUSP) por meio do Departamento de Energia e Automação Elétricas que foi responsável pela integração dos três subsistemas de Controle de Acesso, Circuito Fechado de TV – CFTV e Comunicação.

O SSPP era composto por subsistemas integrados e centralizados operacionalmente no centro de controle, entre eles estão:

- Subsistema de Cadastramento e Credenciamento de Usuários;
- Subsistema de Circuito Fechado de TV (CFTV);
- Subsistema de Comunicação;
- Subsistema de Controle de acesso;
- Subsistema Gestor de Eventos.

Todos os subsistemas foram implantados para atender a demanda do porto de Santos e são integrados aos 28 Gates e Centro de Controle operado pela guarda portuária (autoridade portuária).

Portões (Gates) Instalados no Porto de Santos.

Gate 01 – Acesso à Administração da Petrobrás – Alemoa

Gate 02 – Acesso á Alemoa

Gate 03 – Acesso aos Píeres da Alemoa

Gate 04 – Acesso a Deicmar e Píer do Saboó

Gate 05 – Rodrimar

Gate 06 – Píer dos armazéns 10/11

Gate 07 – Píer na DIROP

Gate 08 – VCP

Gate 09 – Teaçu

Gate 10 – Copersucar

Gate 11 – Concais

Gate 12 – T-Grão

Gate 13 – Canal 4

Gate 14 – Citrosuco/NST – Píer

Gate 15 – CBA TEAG – Píer

Gate 16 – Libra 35

Gate 17 – TEAG – Píer

Gate 18 – Libra 37

Gate 19 – Macuco

Gate 20 – Corredor de Exportação

Gate 21 – Acesso ao cais da Libra 37

Gate 22 – ADM

Gate 23 – Acesso a Presidência

Gate 24 – Saída da Presidência

Gate 25 – Entrada/Saída das oficinas – área da Presidência

Gate 26 – Acesso por terra à Ilha Barnabé

Gate 27 – Acesso aos Píeres da Ilha Barnabé

Gate 28 – Acesso por mar à Ilha Barnabé.

A tecnologia utilizada pela CODESP para fazer a comunicação de voz entre os Gates e o CCCOM é Voice Over IP (VOIP) ou Voz Sobre IP, onde permite estabelecer conversações telefônicas na Rede IP, tornando a transmissão de voz mais um dos serviços suportados pela rede de dados, além do sinal de vídeo.

A) Subsistema de Cadastramento e Credenciamento de Usuários

O Sistema de cadastramento, credenciamento de usuários do porto é o que estabelece uma hierarquia de acesso conforme o perfil dos usuários que permitirá o acesso ao Gates controlados eletronicamente pelo SSPP.

Com este modelo de cadastramento e crachá eletrônico utilizado pela CODESP impedirá que usuários, como o OGMO ou outros, tenham acesso ao cais sem sua identificação biométrica, o que acabaria com os tradicionais “cavalos”, que são indivíduos que trabalham esporadicamente usando a documentação de outras pessoas.

B) Subsistema de Controle de Acesso

Todos os funcionários, prestadores de serviços, terceiros e demais pessoas autorizadas a acessar a faixa portuária e demais áreas controladas deverão estar portando um crachá com tecnologia Mifare de proximidade (rádio frequência).

B1) Características Técnicas do Cartão de Acesso.

Para o porto de Santos foi adotado o cartão inteligente (*smart card*) com chip Mifare, figura 19, ícone em tecnologia no mercado nos últimos anos, devido às suas qualidades, desempenho, versatilidade, facilidade de utilização e compatibilidade com as normas internacionais.

Figura 19: Característica do cartão Smart Card. Fonte: Codesp

A Figura 20 mostra o processo de cadastramento e credenciamento de veículos e pessoas para a obtenção do acesso das áreas restritas da CODESP através de transações eletrônicas.

Figura 20: Transações eletrônicas. Fonte: FUSP

C) Subsistema de Comunicação

O *backbone* utilizado para a transmissão digital do sinal eletrônico é composto por uma rede Gigabit principal com velocidade de transmissão de 1 Gbit, via fibra óptica e também por sistema wireless. Esta comunicação se realiza entre os transmissores e receptores opto - eletrônicos dos Gates e Centro de Controle e Comunicação e Segurança.

D) Subsistema Gestor de Eventos

O Sistema Gestor de Eventos, figura 21, é uma aplicação desenvolvida para buscar informações dos usuários, quando necessário, normalmente quando um evento é gerado e precisa associar dado e vídeo. Solução Inteligente que permite simultaneamente visualizar, armazenar, e capturar em alta qualidade, vídeo e dados com sistemas emissores de alarmes e eventos.

Figura 21: Imagem do gestor de eventos do OPC cliente de monitoração. Fonte: Codesp

E) Subsistema de Circuito Fechado de TV (CFTV)

O sistema de vídeo SmartSight¹ constitui uma solução abrangente e dinâmica, para as várias câmeras implantada, oferecendo as funcionalidades e características necessárias ao CFTV. O sistema inclui dois módulos:

- Módulos do Servidor de Vídeo Digital (SVD)
- Módulos da Estação Cliente

O SmartSight, imagem de vídeos da figura 22, é compatível com a infraestrutura técnica para serviços de vídeo via IP denominada VSIP (*Open Technical Framework for Video Services*) que permite a terceiros o desenvolvimento de aplicativos e dispositivos tais como Servidores de Vídeo Digitais que podem ser integrados a sistemas aderentes a este padrão. O canal de controle VSIP é encriptado utilizando SSL.

Os registros de tempo nas gravações de vídeo utilizam UTC (*Universal Time Coordination*) para assegurar a precisão e confiabilidade da localização dos itens de interesse.

Figura 22: Imagem da tela do sistema de vídeo SmartSight. Fonte: Codesp

¹ SmartSight é marca registrada da Verint.

6 CONSIDERAÇÕES FINAIS E ESTUDOS FUTUROS

6.1 ANÁLISE DA PESQUISA SOBRE O SISTEMA DE SEGURANÇA DOS TERMINAIS DOS PORTOS BRASILEIROS E ESTUDOS FUTUROS

A pesquisa elaborada tem por objetivo fazer um levantamento acadêmico do nível de segurança em que se encontram os terminais e portos brasileiros, com caráter mais descritivo que analítico, conforme figura 23,, visto que não se pretende fazer nenhuma análise destas empresas quanto ao desempenho em segurança, nem tampouco pesquisar o que as levou a ter um bom ou mau sistema de segurança.

Figura 23. Análise da pesquisa sobre o sistema de segurança dos terminais dos portos brasileiros.

No gráfico 05, se tem o percentual das empresas pesquisadas no quesito segurança.

Gráfico 05. Sistema de segurança das empresas pesquisadas.

6.2 ESTUDOS FUTUROS

Serão elaboradas mais pesquisas em outros terminais portuários, como da Ásia e América, além dos portos brasileiros e europeus visitados pelo autor, com foco nas soluções encontradas para atender as necessidades portuárias locais e o que poderá ser melhorado nos equipamentos e centros de controles objetivando adequar os modelos de equipamentos, com biometria e segurança, que poderão ser utilizados nos centros de controles integrados.

6.2.1 POLÍTICAS DE SEGURANÇA NO CCCOS

As políticas de segurança são importantes dentro do CCCOS e devem ser adotadas tanto para o patrimônio físico dos ativos como a segurança da informação, através do controle de acesso à sala, aos Notebooks, Servidores, PC's, Sistema de segurança de biometria facial ou digital, utilização de mouse, portas de E/S e USB com proteção contra uso indevido para gravações das informações.

A figura 24 apresenta um desenho para o controle de acesso em equipamentos de controle e monitoramento, com segurança biométrica.

Figura 24. Disposição física das salas de Controle, Técnica, Gerencial e Operacional.

- Pontos para instalação de sistema de segurança por biometria, além da segurança de identificação nos equipamentos de CFTV, Controle de Acesso e Comunicação.

6.3 SISTEMAS DE SEGURANÇA POR BIOMETRIA PARA ACESSAR O CENTRO DE CONTROLE E EQUIPAMENTOS.

Normalmente quando se utiliza sistemas de biometria para áreas de acesso restrito, como exemplo os centros de controles, se tem um fator inibidor positivo que diminui significativamente o interesse de terceiros de estarem nesta área, pela dificuldade do acesso de pessoas não autorizadas. Por isso é muito importante a aplicação destas tecnologias como instrumento de segurança. O sistema biométrico poderá ser usado nos seguinte equipamentos e dispositivos:

- a) Radio de comunicação, com senha biométrica digital.
- b) Desktops e Workstations com senha biométrica de reconhecimento facial
- c) Servidores com senha biométrica de reconhecimento facial
- d) Notebooks com senha biométrica de reconhecimento facial e/ou digital
- e) Rede com identificação e senha de acesso - Switchs, Firewall, Roteadores, Proxy, VPN, Wireless

6.4 BENEFÍCIOS DE UM SISTEMA DE AUTOMAÇÃO NA SEGURANÇA PORTUÁRIA

Com sistemas integrados de automação nos terminais e portos, com gerenciador de comunicação de dados será possível fazer um regramento e planejamento de horário do transportes de cargas, evitando com isso as grandes filas e desordem do trânsito, que existem nos horários de picos por falta de um

planejamento mais eficaz durante o período diuturno. Maior interação na troca de informações de segurança, como dados, imagens, vídeos sobre suspeitos, infratores, embarcações, veículos, etc...

Benefícios da automação integrada.

- a) Informações *on-line* e *full time* relacionadas à segurança e operação;
- b) Tempo de operação otimizado;
- c) Planejamento gerencial das ações conjuntas;
- d) Dados estatísticos do trânsito, monitoramento, segurança e do gerenciamento administrativo;
- e) Redução de consumos desnecessários de energia, combustível e trabalho;
- f) Interatividade com os equipamentos de campo e Centro de Controle;
- g) Troca de informações *on-line* sobre veículos, pessoas e cargas;
- h) Controle semafórico e monitoramento de tráfego inteligente;
- i) Informação eletrônica nos painéis de mensagens;
- j) Outros.

CONCLUSÃO

Apresentadas as tecnologias disponíveis, os equipamentos, os subsistemas e o que se pode fazer com a integração desses sistemas de segurança, permite fornecer informações seguras para a metodologia empregada de integração dos equipamentos de campo com o Centro de Controle, visto ser o concentrador que recebe, gerencia, armazena e envia todas as informações dos equipamentos, seja do sistema de controle de acesso, através dos dados enviados pelas catracas, cancelas, torniquetes, sensores, sistema OCR, leitura automática de placas, contêineres, biometria facial, etc, ou do sistema de CFTV, através das imagens enviadas pelas câmeras fixas e móveis, via *encoders* e *switches* ou do sistema de comunicação *VoIP*, rádio ou telefonia.

Com os Centros de Controles otimizados, permitem aos portos públicos e privados se integrarem, com políticas de segurança adequadas, tornando possível integrar todas as autoridades portuárias, alfandegárias e demais autoridades, respeitando suas atribuições legais, em um único centro de controle global virtual, que permita inclusive se comunicar *on line* com demais sistemas portuários do mundo, que tenha o mesmo sistema de segurança aplicado.

Portanto se conclui que para ter um sistema seguro, eficiente e integrado, com sistema de automação entre os equipamentos e centros de controles, onde todos os terminais e portos possam trocar informações de dados, vídeos, etc, com segurança, se faz necessário políticas de segurança de comunicação, com acessos seguros na área das centrais de controles.

REFERÊNCIAS E OBRAS CONSULTADAS

AGNES, Clarice; **Normas para Apresentação de Trabalhos Acadêmicos - 8ª** Edição Ed. Edunisc, 2006

Levi, Pierry. **O que é Virtual**. Tradução de Paulo Neves, 2007. Editora 34, 1996

Braga. A. L. - **Proposição e Implementação de Modelo de Troca Eletrônica de Dados para Sistema Portuário Brasileiro**. 2002, 400 p. Tese de Doutorado. EPUSP. 2002.

Castrucci, P.L; Moraes, C.C - **Engenharia de Automação Industrial**. LTC Livros Técnicos e Científicos Editores S.A. 2001.

Empresa ATOS, **Curso do Software de programação A1 (IEC 61131-3), Manual Rev. 1.20 Ref. 5-085.120**, São Paulo, 2006.

FONTANA, C. F. – **Modelo de Automação de um sistema de Controle de Carga para a Aduana nos Portos Brasileiros**; 2004. 129 p. Qualificação (Mestrado). Escola Politécnica. Universidade de São Paulo. São Paulo. 2005.

LEVISON, M. – **The Box – How the Shipping Container Made the World Smaller and the World Economy Bigger**. New York: Princeton University Press, 2006. 390 p.

RUSSO FILHO, A. - **Comércio internacional, um modelo para segurança portuária e modernização da Aduana brasileira**. 2006. 122 p. Qualificação (mestrado). Escola Politécnica. Universidade de São Paulo. São Paulo. 2006.

Salvi. Levi - **Metodologia de Segurança para Intercâmbio Eletrônico de documentos aplicado ao sistema portuário brasileiro**. Tese de Doutorado – EPUSP – 2004, 408f.

OLIVEIRA, C. T. - **Modernização dos portos**. 3. ed. São Paulo: Aduaneiras, 2000.

GOMES, C.O. - **Estudo analítico e operacional do modelo tecnológico de um sistema de segurança pública portuária adequado ao ISPS Code implementado no porto de santos, 2007**. 114 p. Qualificação (mestrado). Escola Politécnica. Universidade de São Paulo. São Paulo. 2007.

INTERNET

AGÊNCIA NACIONAL DE TRANSPORTES AQUAVIÁRIOS – ANTAQ. Ministério dos Transportes. **Adoção do Código Internacional para a Proteção de Navios e Instalações Portuárias. Resolução 2 da Conferência**. Brasília: 2003. Disponível em: <<http://www.antaq.gov.br/NovositeAntaq/pdf/ISPSversaoportugues.pdf>> Acesso em: 18 Mar. 2009.

Associação Brasileira de Normas Técnicas - ABNT - www.abnt.org.br . Acesso em 12 Ago. 2008.

BRASIL. Decreto n. 1.507, de 30 de maio de 1995. Cria a Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis, e dá outras providências. Brasília: 1995. Sítio da Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto/1995/D1507.htm> Acesso em: 04 Jul. 2009

BRASIL. Decreto n. 1.972, de 30 de julho de 1996. Altera a redação do art. 2º do Decreto nº. 1.507, de 30 de maio de 1995, que cria a Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis, e dá outras providências. Brasília: 1996. Sítio da Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto/1996/D1972.htm> Acesso em: 04 Jul. 2009

BRASIL. Lei n. 10.233, de 5 de junho de 2001. Dispõe sobre a reestruturação dos transportes Aquaviários e Terrestres, cria o Conselho Nacional de Integração de Políticas de Transporte, a Agência Nacional de Transportes Terrestres, a Agência Nacional de Transportes Aquaviários e o Departamento Nacional de Infra-Estrutura de Transportes, e dá outras providências. Sítio da Agência Nacional de Transportes Aquaviários - ANTAQ. Ministério dos Transportes. Disponível em: <<http://www.antaq.gov.br/novositeantaq/pdf/Lei10233.pdf>> Acesso em: 21 Mar. 2009

Código ISPS Code - ANTAQ.

<http://www.antaq.gov.br/Portal/pdf/ISPSversoportugues.pdf>. Acesso em 12/04/2009.

COMISSÃO NACIONAL DE SEGURANÇA PÚBLICA NOS PORTOS, TERMINAIS E VIAS NAVEGÁVEIS - CONPORTOS. Ministério da Justiça. **Plano Nacional de Segurança Pública Portuária**. 1ª ed. Brasília: [s.n.], 2002, 23 p. Disponível em: <<http://www.mj.gov.br/senasp/biblioteca/documentos/planonacional.pdf>> Acesso em 26 Abr. 2009.

COMPANHIA DOCAS DO ESTADO DE SÃO PAULO. **Cartilha do Controle de Acesso nas Áreas Restritas do Porto de Santos**. Santos: 2005. Disponível em: <<http://www.superviadados.com.br/>> Acesso em: 11 jul. 2008.

COMPANHIA DOCAS DO ESTADO DE SÃO PAULO. Porto de Santos. **Informações e Dados Estatísticos sobre o Porto de Santos, relatórios gerenciais da Cia. Docas do Estado de São Paulo – CODESP**. Santos: 2007. Disponível em: <<http://www.portodesantos.com.br/authority/estatistica.html>>. Acesso em: 04 Ago. 2008.

COMPANHIA DOCAS DO ESTADO DE SÃO PAULO. **Porto de Santos: Realizações em 2006 e Perspectivas para 2007**. Santos: 2006. Disponível em: <<http://www.portodesantos.com/releases/arquivo2/0237.html>> Acesso em: 16 ago. 2008.

CONSELHO DE AUTORIDADE PORTUÁRIA DO PORTO DE SANTOS - CAP
 Porto de Santos. **São Deveres e Responsabilidades dos Operadores
 Portuários**. Santos: 1993. Disponível em:
 <<http://www.portodesantos.com/cap/deveres.html>>. Acesso em: 17/04/2009

DELL Computadores - www.dell.com.br . Acesso em 12 Dez. 2009.

DIRETORIA DE PORTOS E COSTAS. Marinha do Brasil. Normas da Autoridade
 Marítima para Operação de Embarcações estrangeiras em Águas Jurisdicionais
 Brasileiras NORMAM-04/DPC. Capítulo 3 - **Controle de Navios pelo Estado do
 Porto**. Brasília: 2003. Disponível em:
 < https://www.dpc.mar.mil.br/normam/N_04/N04cap3.pdf> Acesso em: 05 jun. 2009

NASCIMENTO, S.S. **A Logística do Comércio Exterior Brasileiro**.
 [S.l.:s.n.], [2007]. Sítio do Guia Logística e Transporte. Disponível em:
 <<http://www.guiadelogistica.com.br/Y661.htm>> Acesso em: 03 jul. 2009

ORGANIZAÇÃO MARÍTIMA INTERNACIONAL - IMO. **IMO Assembly elects new
 Council for 2006-2007 biennium**. Londres, 2005. Disponível em:
 <http://www.imo.org/dynamic/mainframe.asp?topic_id=1018&doc_id=5434>
 Acesso em: 03 jun. 2009

ORGANIZAÇÃO MARÍTIMA INTERNACIONAL - IMO. **AIS Transponder**.
 Londres : [s.n.]. Disponível em:
 <http://www.imo.org/Safety/mainframe.asp?topic_id=754> Acesso em: 12
 Mar. 2009

ORGANIZAÇÃO MARÍTIMA INTERNACIONAL - IMO. **Long Range
 Identification and Tracking (LRIT)**. Londres: Maio 2006.
 Disponível em: <http://www.imo.org/Safety/mainframe.asp?topic_id=905>
 Acesso em: 12 Mar. 2009

SONY Computadores - www.sony.com.br . Acesso em 12 Dez. 2009.

U.S. CUSTOMS AND BORDER PROTECTION. U.S. Government. **Container Security Initiative – 2006 – 2011 Strategic Plan**. Estados Unidos: Agosto 2008
Disponível em:
<http://www.cbp.gov/linkhandler/cgov/border_security/international_activities/csi/csi_strategic_plan.ctt/csi_strategic_plan.pdf>. Acesso em 12 Ago. 2008.

3COM Tecnologia - www.sony.com.br . Acesso em 12 Dez. 2009.

APÊNDICES

APÊNDICE A

ARTIGO SOBRE TECNOLOGIA DA INFORMAÇÃO NA GESTÃO PORTUÁRIA.

TECNOLOGIA DA INFORMAÇÃO NA GESTÃO PORTUÁRIA

Resumo: O artigo foi desenvolvido em função da necessidade, das autoridades portuárias, em integrar as várias tecnologias aplicadas nos portos brasileiros e dos pequenos, médios e grandes terminais portuários e retro-portuários em reduzir seus custos em TI e da integração dos vários sistemas utilizados, visto que o gasto é significativo em equipamentos de informática, softwares e hardwares. É importante lembrar que, tanto no Brasil quanto no mundo, a movimentação em TI está na ordem de bilhões de dólares e, com a utilização de vários softwares diferentes, se faz necessário o gerenciamento integrado para uniformização das informações e principalmente ganho de eficiência e redução de custos, além do aumento da velocidade, melhoria da comunicação e eficiência dos equipamentos. E as empresas de tecnologia estão buscando atender essas necessidades, conscientizando os fabricantes e fornecedores de hardwares e softwares nas soluções integradas que tornem mais eficiente as infra-estruturas de engenharia de dados e de segurança. Como resultado as empresas portuárias tem percebido vantagens operacionais, administrativas e econômicas na implantação desses sistemas de gestões, como exemplos: o Balanced ScoreCard, Return on Investment (ROI), Total Cost of Ownership (TCO), Economic Value Added (EVA), Activity Based Costing (ABC), CobiT - Control Objectives for Information and Related Technology, ITIL e CMM. E como resultado foi elaborado um estudo, no Porto de Santos, junto à autoridade portuária e terminais, objetivando uma gestão integrada no atracamento de navios, logística, regramento, transporte e tráfego de caminhões pelas vias principais e secundárias de acesso ao porto e região.

Palavras-chave: Gerenciamento Integrado; Tecnologia da Informação; Hardware e Software; Engenharia; Gestão de Qualidade.

Abstract: The article was developed on the basis of need, port authorities, to integrate the various technologies applied in Brazilian ports and small, medium and large port terminals and port back-to reduce their costs in IT and the integration of various systems used, as that the expense is significant in computer equipment, software and hardware. It is important to remember that, both in Brazil in the world, handling in IT is the order of billions of dollars and, using several different software, it is necessary to standardize the management of integrated information and especially to gain efficiency and reduce costs, in addition to increased speed, improved communication and efficiency of equipment. And the companies are seeking technology to meet those needs, conscious manufacturers and suppliers of hardware and software in integrated solutions that make it more efficient infrastructure for engineering and data security. As a result companies have perceived advantages port operational, administrative and economic in the deployment of these systems management, as examples: the Balanced Scorecard, Return on Investment (ROI), Total Cost of Ownership (TCO), Economic Value Added (EVA), Activity based costing (ABC), Cobit - Control Objectives for Information and Related Technology, ITIL and CMM. And the result was a study in the Port of Santos, near the port authority and terminal, to an integrated management in berthing of vessels, logistics, regulation, transportation and traffic of trucks by main and secondary roads for access to the port and region.

Keywords: Integrated Management, Information Technology, Hardware and Software, Engineering, Quality Management.

1 INTRODUÇÃO

O gerenciamento integrado em Tecnologia da Informação (TI), visa integrar as várias tecnologias aplicadas nos computadores das empresas, para o gerenciamento das mais diversas soluções de fornecedores e fabricantes de softwares e hardwares. Portanto, se percebe que o setor de informática começou a se conscientizar da necessidade da mudança de foco da TI, quanto à busca de soluções centralizadas em tecnologias, para melhorar a eficiência empresarial e operacional dos processos de gestão integrada.

Devido à necessidade de um gerenciamento eficiente, das várias plataformas, e de um sistema padrão, foram desenvolvidas algumas interfaces, como a IPMI - Intelligent Platform Management Interface para servidores; a DMI - Desktop Management Interface e o ASF - Alert Standard Format para estações de trabalho na arquitetura servidor-cliente; WFM - Wired for Management para todas as plataformas, e o WBEM - Web-Based Enterprise Management e CIM - WBEM - Common Information Model - WBEM, sendo um conjunto de tecnologias padrões para gerenciamento e Internet, desenvolvidas para integração e gerenciamento completo da empresa.

Pelo fato de muitas empresas apresentarem plataformas diferentes surge à necessidade de uma integração para o ambiente tecnológico comercial e industrial, ou do escritório digital. Os objetivos dessas iniciativas visam simplificar o ambiente de TI e realizar o gerenciamento de sistemas, permitindo reduzir despesas e custos desnecessário de suporte e, conseqüentemente, obter melhoria na qualidade do serviço em geral.

Entre pesquisas e estudos de várias empresas de tecnologia, se concluiu que existem quatro pilares tecnológicos para o escritório digital (Intel Next Generation, 2008):

1. TI integrada, diretamente nos componentes da plataforma e gerenciamento para PC's, com segurança e estabilidade do sistema.
2. Conectividade em todas as redes para todos os serviços de software em qualquer dispositivo.
3. Simultaneidade , no trabalho de equipe, permitindo a comunicação e colaboração entre as plataformas utilizadas.

4. Facilitar a utilização do assistente de informações, pelos usuários, de forma eficiente e com resultados satisfatórios.

2 FORMULAÇÃO DO PROBLEMA

Tanto na indústria, comércio, quanto na área portuária se tem um grande problema quanto aos custos dos ativos de informática e das tecnologias de gestão utilizadas pelas empresas, principalmente na integração das informações de logística, de transporte na chegada e saída de navios e caminhões para o transporte de cargas e, as empresas de um modo geral, para reduzir os custos de informática e principalmente as de tecnologias, buscam várias soluções nas grandes fornecedoras de TI e algumas respostas foram encontradas objetivando um melhor resultado, como exemplo, uma delas se concentrou em seu próprio setor de TI para viabilização de estudo de caso sobre os problemas comuns na área de informática. Entre os identificados se destacaram: gerenciamento, segurança, conectividade, custo de recursos humanos, etc, e, em função disso foi possível determinar o custo total de seus ativos na área de TI.

Entre os principais problemas das empresas que se utilizam destas tecnologias estão:

- Como devem ser alocados os recursos nas organizações de TI para aproveitar melhor os sistemas distribuídos, tais como CPUs e chips de memória nas soluções de gerenciamento, segurança e conectividade;
- Incompatibilidade entre os sistemas utilizados devido a complexidade da integração dos aplicativos utilizados;
- Gerenciamento e diagnóstico on-line remotamente, porque as organizações de TI gastam um tempo significativo para atualizar, diagnosticar e recuperar os sistemas com problemas, onde poderia reduzir em aproximadamente 40 % das visitas para sanar esses problemas na rede, mesmo com os PC's desligados ou travados;
- Gerenciamento do ativo, visto que as organizações da área de TI não conseguem localizar parte do seu ativo, sem saber o que realmente aconteceu com eles;

- Proteger as plataformas internamente, porque os ataques de vírus, worms e outros softwares maliciosos afetam no lado interno dos sistemas;

Para as várias situações descritas, não importa se os usuários estão numa rede LAN (Local Area Network) ou remotas WAN (Wide Area Network), as plataformas precisam de conectividade difundida, ser ininterrupta e não ter problemas de comunicação e deve funcionar independente do uso de um PC desktop, notebook, palm, telefone celular, plataforma móvel ou servidor e usar armazenamento não-volátil para proteção integrada contra ataques virtuais.

3 SOLUÇÃO DO PROBLEMA

Dentre as várias empresas de tecnologia, destacam às que mais investem em P&D e trabalham nas melhorias de gerenciamento integrado e segurança, diretamente na plataforma desses sistemas.

As empresas desenvolvem programas que permitem a integração de várias plataformas, com isso permite o sistema identificar e projetar a capacidade de gerenciamento, de interfaces e protocolos consistentes e comuns.

Para conformidade do sistema de todas as plataformas se requerem quatro principais capacidades:

- Consistência em todas as plataformas;
- Segurança integral, pois há hardware e firmware (software embutido nos processadores), resistentes à destruição, como serviços OOB (out-of-band), quando o sistema operacional está inoperável, para controle remoto e comunicações que não podem ser comprometidos por ataques de vírus, entre outros.
- Disponibilidade contínua das funções, porque as capacidades persistem independentemente do estado do host, seja bloqueado ou infeccionado por vírus. Inclusive com pré-inicialização, comunicação remota, etc.
- Capacidade de suportar diferenciações de terceiros, para que os fornecedores de terceiros usem mais os recursos de desenvolvimento para diferenciar seus aplicativos, ao invés de terem de desenvolver novos processos para funções comuns em todos os aplicativos.

Figura 01 – Vários micros integrados em rede, através de gestor de integração.

3.1 Estratégias para Gestão

Para o gerenciamento das várias tecnologias aplicadas, pode adotar algumas ferramentas, indicadores e metodologias para o dimensionamento e uso efetivo dos sistemas. Atualmente, somam-se às soluções já conhecidas e tradicionais, como Activity Based Costing, Balanced ScoreCard, Economic Value Added (EVA), Return on Investment (ROI), TCO (Total Cost of Ownership) e outros modelos que são empregados pelo setor corporativo, como o CobiT, ITIL e CMM. A metodologia CobiT – Control Objectives for Information and Related Technology desenvolvida pelo Information System Audit and Control Association (Isaca), a partir de ferramentas de auditoria, serve como guia para a gestão da TI nas empresas, como também incluiu uma série de recursos, tais como: sumário executivo, framework, controle de objetivos, mapas de auditoria e um conjunto de processos de trabalho já aceitos e empregados pelo mercado, entre os quais se incluem o CMM (Capability Maturity Model), ISO 9000 (para qualidade), BS7799/ISSO 17799 (normas para segurança da informação) e o ITIL (para gestão do departamento de TI).

O CobiT independe das plataformas de TI adotadas pelas empresas e seu uso é orientado a negócios, no sentido de fornecer informações detalhadas para gerenciar TCO, TVO e CAPT. O setor corporativo procura verificar até que ponto os

gastos estão sendo feitos de forma inteligente e quais os verdadeiros ganhos obtidos. Atualmente, uma das mais conhecidas e que se tornou padrão no mundo todo é o TCO -Total Cost of Ownership, que evolui para TVO – Total Value of Opportunity.

Devido as grandes transformações tecnológicas houve uma mudança significativa no ambiente de TI das empresas corporativas, tornando o gerenciamento mais complexo. Nesta evolução, dos antigos terminais aos atuais PC's, o gestor da informática limitou-se a administrar a tecnologia de forma técnica num ambiente centralizado, baseado em tecnologias proprietárias. A atenção do gestor da área estava basicamente focada no desenvolvimento de aplicativos, análise de sistemas, cuidados com a sua equipe, manutenção, atendimento às solicitações dos diferentes departamentos da empresa e atividades técnicas.

Esse modelo deixou de vigorar com a proliferação do ambiente cliente-servidor e da computação distribuída. Em curto espaço de tempo, novas empresas fornecedoras de hardware e software ampliaram consideravelmente a oferta de opções, tornando mais complicado o processo de escolha.

Com a complexidade das redes se fazem necessários à segurança, integração automatizadas e um gerenciamento integrado mais eficiente nos computadores pessoais, estações de trabalho, servidores e outras ferramentas e equipamentos, visto que elas foram projetadas, inicialmente, para possibilitar o compartilhamento de vários recursos, como programas, aplicativos específicos e bancos de dados, além de impressoras e demais periféricos. Só que além desta comunicação em rede micro a micro, se fez necessário também a customização entre os softwares e hardwares do sistema.

3.2 GERENCIAMENTO INTEGRADO DE SEGURANÇA

Além dos computadores, muitos outros dispositivos estão ligados nas redes, tais como as unidades móveis - hand helds, celulares, sistemas sem-fio - wireless ou outros pontos de acesso por funcionários, autorizados ou não, que

Os sistemas de gerenciamento de redes apresentam a vantagem de ter um conjunto de ferramentas para análise e depuração, como a notificação e o registro de problemas, por exemplo:

Alarmes que indicam, por meio de mensagens ou bips de alerta, anormalidades na rede; Geração automática de relatórios contendo as informações coletadas; Facilidades para integrar novas funções ao próprio sistema de gerenciamento; Geração de gráficos estatísticos em tempo real; Apresentação gráfica da topologia das redes.

Outro ponto que merece a atenção dos gestores da TI são os serviços de telecomunicações, que figuram como os gastos mais difíceis de serem administrados.

Ferramentas de gerenciamento: Cada vez mais poderosas e específicas, as ferramentas de gerenciamento permitem monitorar e controlar o ambiente de TI.

Modelos de gerenciamento: Existem alguns modelos para gerência de redes. Um deles é o modelo Internet, que adota uma abordagem gerente/agente. Os agentes mantêm informações sobre recursos, e os gerentes requisitam essas informações aos agentes. Outro modelo é o OSI, da ISO, que se baseia na teoria de orientação a objeto. Independentemente do modelo escolhido, protocolos e ferramentas empregadas, o gerenciamento permite monitorar a disponibilidade e performance de cada elemento da rede, medir o nível de utilização do parque de software, consumo de banda, e uma série de fatores que assegura a continuidade das operações e o melhor uso da infra-estrutura de TI.

Gerenciamento de dados e e-mail: Devido o grande uso das redes Internet, intranets e extranets, se faz necessário também outro tipo de gerenciamento: o de storage. Especialmente nas empresas de maior porte ou nas que contam com grande parque tecnológico, o crescimento do volume de dados requer a tomada de medidas apropriadas para seu correto armazenamento.

Gerenciamento da segurança: Ferramentas de segurança são importantes para o gerenciamento, principalmente na implementação de soluções em áreas que não precisam tanto de proteção e não deixar vulneráveis algumas áreas importantes.

Segurança em redes sem fio: **Com a evolução da tecnologia móvel e o aumento do seu uso pelas empresas, alguns cuidados também devem ser tomados em relação às redes wireless, sendo que as proteções convencionais usadas em**

redes cabeadas se aplicam ao ambiente sem fio. Mas, além delas, as redes wireless exigem cuidados adicionais e específicos. O padrão de criptografia para redes locais sem fio, denominado WEP - Wired Equivalent Privacy, é bastante seguro, mas ainda apresenta algumas restrições, por isso é recomendável que as empresas busquem outras alternativas tecnológicas.

Para se ter uma rede mais segura, algumas recomendações para gestor da TI, visando tornar a rede corporativa mais segura devem ser seguidas:

Não mencionar o nome da rede para qualquer pessoa; Desabilitar, no Access Point, a emissão automática de informações como o nome da rede, a chave criptográfica e a senha do administrador de rede; Fazer uma lista dos computadores confiáveis; A autenticação do computador à rede deve ser feita usando o MAC Address da placa de cada dispositivo. Essa ação impede que máquinas estranhas ao ambiente possam se conectar à rede; Não deixar o sinal vazar; O posicionamento do access point e a potência da antena podem ter um alcance que ultrapasse as fronteiras geográficas da empresa. O vazamento do sinal é perigoso. É preciso implementar mecanismos de autenticação e criptografia; Agir rápido se o notebook for roubado ou perdido. Roubo e perda de equipamentos têm consequências sérias para a segurança da rede corporativa; Definir que tipo de informação trafega na rede. É importante que o usuário do canal sem fio saiba o que pode e o que não pode ser trafegado pela rede wireless; Criptografar para não dar o mapa ao agente infrator. Dados estratégicos, e-mails profissionais, modelos de vendas, lista de clientes preferenciais e planos de novos negócios podem cair em mãos alheias; Autenticação de quem entra na rede. Além de garantir que determinado dispositivo é autorizado para entrar na rede, devem ser usados métodos de autenticação forte de usuário, por meio de tokens e senhas dinâmicas; A ligação com a rede local cabeada deve estar sempre protegida por firewall, como qualquer porta aberta para o mundo exterior; Realizar monitoração freqüente de todas as atividades da rede sem fio para verificar falhas e flagrar intrusos. Esse procedimento traz uma série de benefícios, como permitir a descoberta de instalação de placas não autorizadas nos equipamentos pelos usuários, checagem de dispositivos que não estão usando criptografia, detecção de ataques contra clientes wireless que não sabem que estão sendo hackeados; e visualização de acessos não autorizados, o que permite tomar

providências imediatas que impeçam o intruso de chegar aos dados estratégicos da empresa.

Segurança dos dados: O gerenciamento de dados envolve a realização de backup, restore e business continuity. Existem boas opções de ferramentas disponíveis, como a do Computer Associates BrightStor; Control Center Storage Scope; Softek Storage Manager; OpenView Builder; Tivoli Storage Resource Manager; Storage Resource Management Suíte; SANPoint Control/Storage Reporter.

Contingência: O setor corporativo está adotando uma política de contingência, principalmente após o atentado ao World Trade Center, em 11 de setembro de 2001, que serviu para ampliar o interesse pela Segurança da Informação, principalmente as que lidam com grandes volumes de dados e dependem muito da Tecnologia, como as do setor de finanças e de telecomunicações.

CIOs, CTOs e CSOs: Responsáveis pelo gerenciamento de TI, os CTOs (Chief Technology Officers) e CSOs (Chief Security Officers), cuidam das políticas de segurança e da aquisição de tecnologias específicas, deixando aos CIOs (Chief Information Officers) os assuntos relacionados à gestão dos negócios e a responsabilidade pela integração das áreas executivas com a área de TI.

O surgimento da Internet, entendida como o conjunto de redes de computadores interligadas no mundo inteiro, tendo em comum um conjunto de protocolos e serviços, foi um fator que, sem dúvida, trouxe muito impacto às empresas e potencializou o uso dos recursos internos. A Internet propiciou a criação de outros tipos de redes, como as de uso exclusivo interno - intranets e as destinadas ao relacionamento da empresa com seus parceiros de negócios através da extranet, configurando-se como o meio eficiente para agilizar e facilitar o intercâmbio de informações e de documentos via WebEDI. Além disso, ampliou as vulnerabilidades: riscos por vírus, acessos não-autorizados, invasões ao sistema, pirataria, etc. e proporcionou o excesso do tráfego de dados por e-mails e mensagens instantâneas, levando ao questionamento da dimensão das capacidades das máquinas e, conseqüentemente, tornando o gerenciamento mais complexo. A Internet precisa ser repensada como um instrumento de trabalho global, principalmente aumentando sua eficiência quanto às pesquisas como a comunicação de dados VoIP, Imagens, Vídeos, etc.

3.3 TERCEIRIZAÇÃO

Na avaliação de vários especialistas de mercado, a computação sob demanda levará algum tempo para amadurecer e o que poderá ganhar cada vez mais impulso é o processo de terceirização da TI. O outsourcing, como também é conhecido, há muitos anos vem sendo adotado, pelas empresas de diferentes ramos de atividade. Mas recentemente se começou a perceber que as desconfianças e resistências das áreas usuárias, que eram muito elevadas no passado recente, já não constituem empecilho para a maturação desse modelo. Motivadas pela necessidade de reduzir custos e por terem concluído que fazer tudo em casa, além de muito caro, é pouco produtivo, as empresas de grande, médio e pequeno porte estão gradativamente aumentando o repasse de algumas funções da TI para terceiros. Tão importante quanto a escolha da empresa prestadora, é fundamental elaborar o melhor acordo de nível de serviço SLA – Service Level Agreement.

3.4 SOLUÇÃO EM GERENCIAMENTO DE TI

As empresas enfrentam grandes obstáculos para implantação de novos programas gerenciais, principalmente em TI, visto que, levar novas práticas de gestão de gerenciamento para outros setores requer muita persistência para superar as resistências de mudanças. E para isso, a empresa terá que planejar, com eficiência as futuras implementações, envolver todos os colaboradores, de todas as áreas no processo, e intensificar o treinamento das equipes para alcançar o objetivo que é customizar custos, melhorar a tecnologia empregada e aumentar a eficiência empresarial.

A. Terminal Portuário

Os terminais portuários do Porto de Santos utilizam as mais variadas tecnologias, desde micros PC's antigos, com pouca capacidade, quanto aos novos quad core, notebooks, coletoras, impressoras, catracas, cancelas, câmeras de

vídeos, etc e necessita integrar estas várias tecnologias para ganho de eficiência operacional e administrativa. Para isso se faz necessários à utilização de uma TI, que atenda suas necessidades gerenciais através de gestores integradores.

Figura 03. Comunicação das várias tecnologias no terminal portuário.

B. Autoridade Portuária

A autoridade portuária necessita desenvolver políticas gerenciais integradas para fomentar uma comunicação mais eficiente com seus terminais portuários, melhorar sua logística e aumentar sua eficiência operacional e gerencial.

Figura 04. Comunicação da autoridade portuária com os terminais portuários.

Precisam-se realizar dois trabalhos de integração no porto santista:

1º) Uniformizar as tecnologias aplicadas nos terminais portuários, através de uma TI integrada, otimizando custos e recursos tecnológicos;

2º) Integrar todos os terminais portuários com a autoridade portuária através de um gerenciador de gestão operacional e administrativo.

4 CONCLUSÃO

Através do artigo apresentado se conclui que toda empresa, independentemente do seu tamanho, se faz necessário o gerenciamento das tecnologias aplicadas, seja pelas equipes próprias ou por empresas terceirizadas. Não se pode afirmar quais os melhores programas de gerenciamentos serão utilizados nas tecnologias da Informação no futuro ou atual, visto que o mercado está em expansão e muitas empresas estão buscando novas soluções de gerenciamento integrado de TI e na gestão da qualidade da engenharia de softwares. A terceirização é uma tendência que as empresas buscam, principalmente quando a atividade principal não é tecnologia e a computação sob demanda, a mobilidade, a convergência, a consolidação de sistemas, segurança e software livre são realidades atuais com grandes projeções futuras.

Além da Tecnologia, os novos gestores precisarão ter uma visão ampla e estratégica das empresas, pois deixará de ter somente o papel da gestão na tecnologia, mas também a integração de todos os dados corporativos com transparência, ética e responsabilidade social e empresarial, além da manutenção da infra-estrutura tecnológica e do gerenciamento de terceiros. Portanto o gerenciamento integrado de TI continuará a crescer muito nesse mercado globalizado e as empresas portuárias terão que se adequar nesse novo modelo de integração para se tornarem competitiva, visto que a diferença administrativa e operacional entre empresas que adotaram a gestão integrada de TI e as que não utilizam são muito grande.

OBRAS CONSULTADAS

AGNES, Clarice; **Normas para Apresentação de Trabalhos Acadêmicos** - 8ª Edição Ed. Edunisc, 2006

INTEL , **Curso de Gerenciamento Integrado**, INTEL NEXTGENERATION, 2007.

INTEL, **Curso de Tecnologia da Informação**, INTEL NEXTGENERATION, 2008.

INOVAÇÃO TECNOLÓGICA; <http://www.inovacaotecnologica.com.br>, acesso em 02/12/2008.

LAURINDO, Fernando José Barbin. **TECNOLOGIA DA INFORMAÇÃO** - Eficácia nas Organizações, 247 páginas. Editora: Futura. 2002.

LUCRATIVIDADE PELA INOVAÇÃO, Como eliminar ineficiência nos seus negócios e na cadeia de valor - Rio de Janeiro: Elsevier; São Paulo - Microsoft Brasil, 2005.

SEVERINO, Antônio Joaquim. **METODOLOGIA DO TRABALHO CIENTIFICO**. 22ª edição, São Paulo: Cortez, 2002.

TURBAN, Efrain. **TECNOLOGIA DA INFORMAÇÃO PARA GESTÃO**. Editora bookman. 2006.

APÊNDICE B

**PESQUISA SOBRE O SISTEMA DE SEGURANÇA DOS TERMINAIS
PORTUÁRIOS.**

Prezado(a) colaborador(a).

Esta pesquisa tem por objetivo fazer um levantamento acadêmico do nível de segurança em que se encontram os terminais e portos brasileiros, com caráter mais descritivo que analítico, visto que não se pretende fazer nenhuma análise destas empresas quanto ao desempenho em segurança, nem tampouco pesquisar o que as levou a ter um bom ou mau sistema de segurança.

A identificação dos(as) pesquisados(as) não entrarão na pesquisa, visto que será feito somente uma análise quantitativa das informações pesquisadas.

Opcional (caso queira nos informar):

Empresa:

Nome do Pesquisado:

Tel:

E-mail:

QUESTIONÁRIO

1. A empresa tem uma política de segurança implantada?

() Sim () Não Em Andamento: () 25% () 50% () 75%

2. Existe uma pessoa responsável pela segurança patrimonial e eletrônica?

() Sim () Não Em Andamento: () 25% () 50% () 75%

3. Já foi implantado o sistema de CFTV na empresa?

() Sim () Não Em Andamento: () 25% () 50% () 75%

4. Já foi implantado o sistema de Controle de Acesso na empresa?

() Sim () Não Em Andamento: () 25% () 50% () 75%

5. Já foi implantado o sistema de Comunicação na empresa?

() Sim () Não Em Andamento: () 25% () 50% () 75%

6. O sistema implantado é integrado: CFTV, Controle de Acesso e Comunicação?

() Sim () Não Em Andamento: () 25% () 50% () 75%

7. O Sistema de Controle de Acesso já está contemplado com o sistema OCR: Leitura de Placas, Contêineres e Biometria Facial ou das mãos?

() Sim () Não Em Andamento: () 25% () 50% () 75%

8. A empresa tem implantado o ISPS Code e já recebeu a Declaração de Cumprimento - DC?

a) ISPS Code

() Sim () Não Em Andamento: () 25% () 50% () 75%

b) Cumprimento - DC

() Sim () Não

9. Como se chama o Centro de Controle?

- () CC - Centro de Controle
- () CCCOM - Centro de Controle e Comunicação
- () CCO - Centro de Controle Operacional
- () CCOS - Centro de Controle Operacional e Segurança
- () CCCOS - Centro de Controle, Comunicação, Operações e Segurança

Outro: _____

10. O Centro de Controle está em conformidade quanto à ergonomia, climatização, iluminação, segurança de acesso, sistema contra incêndios?

() Sim () Não Em Andamento: () 25% () 50% () 75%

a) Ergonomia (Disposição física dos mobiliários, micros, monitores, telão...)

() Sim () Não

b) Sistema de Climatização (Ar Condicionado, Ventilação...)

() Sim () Não

c) Sistema de Iluminação (Lâmpadas...)

() Sim () Não

d) Segurança de Acesso (Leitoras de acessos, equipamentos...)

() Sim () Não

e) Sistema contra incêndios

() Sim () Não

11. Existe uma segurança geral da informática (hardware e software) na organização?

() Sim () Não Em Andamento: () 25% () 50% () 75%

12. Existe um ambiente on-line de comunicação de dados na empresa - Internet, Intranet, extranet?

() Sim () Não Em Andamento: () 25% () 50% () 75%

Qual: _____

ANEXOS

ANEXO A

PLANO NACIONAL DE SEGURANÇA PÚBLICA PORTUÁRIO

MINISTÉRIO DA JUSTIÇA
COMISSÃO NACIONAL DE SEGURANÇA
PÚBLICA NOS PORTOS, TERMINAIS E VIAS
NAVEGÁVEIS - CONPORTOS

PLANO NACIONAL DE SEGURANÇA
PÚBLICA PORTUÁRIA

- 1ª Edição -
BRASÍLIA
Dezembro 2002

SUMÁRIO

Introdução	03
 Capítulo I	
Missão, Composição e Atribuições da CONPORTOS	04
 Capítulo II	
Missão, Composição e Atribuições das CESPORTOS e de Seus integrantes.	06
 Capítulo III	
Compromissos	14
Compromisso nº 1	
Combate ao narcotráfico e ao crime organizado nos portos, terminais e vias navegáveis	14
Compromisso nº 2	
Controle de entrada e saída de armas do País	16
Compromisso nº 3	
Repressão ao roubo/furto de cargas	17
Compromisso nº 4	
Utilização do Subsistema de Inteligência de Segurança Pública	17
 Conclusão	 18

INTRODUÇÃO

Este é um plano de ações. Seu objetivo é aperfeiçoar o sistema de segurança pública nos portos, terminais e vias navegáveis, visando reprimir e prevenir o crime e a impunidade, aumentando a segurança e a tranquilidade dos mesmos, com diminuição do “custo Brasil”.

A solução para a complexa e desafiadora questão da segurança exige o efetivo envolvimento de diferentes órgãos governamentais em todos os níveis, entidades privadas e sociedade civil. Busca-se, com o estabelecimento de medidas integradas, aperfeiçoar a atuação dos órgãos e instituições voltadas à segurança pública nos portos, terminais e vias navegáveis, permitindo-lhes trabalhar segundo um enfoque de mútua colaboração. Somente com essa participação conjunta, este programa terá efetividade e criará condições para o desenvolvimento de ações mais eficazes.

Dentro deste contexto, visando dotar o Brasil com órgãos destinados, especificamente, à segurança dos portos, foi criada a Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CONPORTOS) e Comissões Estaduais (CESPORTOS). O Plano está estruturado em três capítulos que relacionam missões, atribuições e compromissos a serem assumidos pelos órgãos envolvidos.

CAPÍTULO I

MISSÃO, COMPOSIÇÃO E ATRIBUIÇÕES DA CONPORTOS

Referência: Decreto nº 1.507, de 30 de maio de 1995.

1. MISSÃO

A Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CONPORTOS) deverá elaborar e implementar o sistema de prevenção e repressão a atos ilícitos nos portos, terminais e vias navegáveis.

2. COMPOSIÇÃO

A CONPORTOS é integrada por um representante e respectivo suplente de cada Ministério a seguir indicado:

- a. da Justiça, que a presidirá;
- b. da Defesa (Comando da Marinha);
- c. da Fazenda;
- d. das Relações Exteriores; e
- e. dos Transportes.

3. ATRIBUIÇÕES

Compete à CONPORTOS:

- a. baixar normas, em nível nacional, sobre segurança pública nos portos, terminais e vias navegáveis;

- b. elaborar projetos específicos de segurança pública nos portos, terminais e vias navegáveis e, por via diplomática, buscar, junto à Organização Marítima Internacional (IMO), assistência técnica e financeira de países doadores e instituições financeiras internacionais;
- c. apresentar sugestões às autoridades competentes para o aperfeiçoamento da legislação pertinente, inclusive consolidação de leis e regulamentos;
- d. avaliar programas de aperfeiçoamento das atividades de segurança pública nos portos, terminais e vias navegáveis;
- e. manter acompanhamento estatístico dos ilícitos penais ocorridos nos portos, terminais e vias navegáveis e dos resultados das investigações e das punições aplicadas;
- f. encaminhar aos órgãos competentes avaliações periódicas sobre as necessidades relativas à segurança pública nos portos, terminais e vias navegáveis;
- g. elaborar seu regimento interno e atualizá-lo, quando necessário, submetendo-o à aprovação do Ministro de Estado da Justiça;
- h. criar e instalar Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis, fixando-lhes as atribuições;
- i. orientar as Comissões Estaduais, no que for cabível;
- j. gerenciar crises, relativas à segurança pública, quando necessário, em apoio às CESPORTOS.

CAPÍTULO II

MISSÃO, COMPOSIÇÃO E ATRIBUIÇÕES DAS CESPRTOS E DE SEUS INTEGRANTES

Referência:

Decreto nº 1.507, de 30 de maio de 2002-08-21

1. MISSÃO

As Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CESPORTOS) deverão prevenir e reprimir os atos ilícitos nos portos, terminais e vias navegáveis.

2. COMPOSIÇÃO

Cada CESPRTOS será composta, no mínimo, por representantes dos seguintes órgãos:

- a. Departamento de Polícia Federal, que a coordenará;
- b. Capitania dos Portos;
- c. Secretaria da Receita Federal;
- d. Administração portuária; e
- e. Governo do Estado.

3. ATRIBUIÇÕES

a. Compete às CESPRTOS:

- de acordo com a CONPORTOS, baixar normas, em nível estadual, sobre segurança pública nos portos, terminais e vias navegáveis;

- elaborar estatísticas dos ilícitos penais ocorridos nos portos, terminais e vias navegáveis e dos resultados das investigações e das punições aplicadas;
- elaborar seu regimento interno e plano de segurança portuária a ser submetido à CONPORTOS;
- controlar os pontos sensíveis de valor estratégico, nas áreas portuárias;
- constituir, de acordo com a necessidade, subcomissões em cada instalação portuária do Estado;
- realizar anualmente, até 30 de setembro, planejamento das atividades da Comissão, para o ano seguinte, articulando com os órgãos representados a inclusão dos respectivos recursos orçamentários necessários, observada a programação específica de cada organização e encaminhar o referido planejamento à CONPORTOS;
- encaminhar, aos órgãos competentes, as avaliações periódicas sobre as necessidades relativas à segurança pública nos portos, terminais e vias navegáveis;
- manter estreito relacionamento com os representantes do Programa de Harmonização das Atividades dos Agentes de Autoridades nos Portos – PROHAGE;
- propor alteração na legislação, justificando as propostas;
- solicitar o apoio da CONPORTOS no gerenciamento de crises, relativas à segurança pública, quando julgar-se insuficiente para tal.
- prevenir e reprimir os crimes de competência da Polícia Federal praticados na área portuária, adjacências e no mar territorial brasileiro, incluindo o tráfico de armas de fogo, de pessoas, armas químicas, nucleares, biológicas e congêneres e o terrorismo e outros crimes praticados no âmbito marítimo que tenham repercussão interestadual ou internacional e que exijam repressão uniforme;

- executar a fiscalização de migração de passageiros e tripulantes, quando da realização da visita oficial a bordo das embarcações de transporte marítimo internacional, sem prejuízo de outras providências de controle interno em relação ao cumprimento do Estatuto do Estrangeiro, nos navios afretados ou não, que estejam operando em cabotagem, em apoio marítimo ou em apoio portuário, observando-se o recolhimento das taxas devidas;
- Fiscalizar as embarcações que operam no transporte internacional de cargas e/ou de passageiros, por meio da expedição de passes de entrada e de saída, em cada porto habilitado para o transporte internacional, ressaltando-se as atribuições dos demais órgãos;
- manter uma central de comunicação com rádio, telefone, fax e “e-mail”, operando 24 horas, para receber denúncias de prática de ilícitos de competência da Polícia Federal nos portos e mar territorial e, conforme o caso, adotar as medidas pertinentes;
- policiar a área portuária, mediante o patrulhamento sistemático marítimo e terrestre;
- buscar a integração dos órgãos que compõem a CESPOTOS, para uma ação mais coordenada na prevenção e repressão aos atos ilícitos.

2) Capitania dos Portos

De acordo com a Lei nº 9.537/1997, que dispõe sobre a Segurança do Tráfego Aquaviário, cabe à Marinha do Brasil, na condição de autoridade marítima, promover a implantação e execução deste dispositivo, com o propósito de assegurar a salvaguarda da vida humana e a segurança da navegação, no mar aberto e hidrovias interiores, e a prevenção da poluição ambiental por parte de embarcações, plataformas ou suas instalações de apoio. Abaixo, estão relacionados os outros instrumentos legais que atribuem competência à Marinha do Brasil sobre segurança e que, de alguma forma, podem ter reflexos sobre a segurança pública portuária:

- Constituição da República Federativa do Brasil – Art 142;
- Lei Complementar nº 97/1999 – dispõe sobre as normas gerais para organização, o preparo e o emprego das Forças Armadas;
- Decreto nº 1.265/1994 – aprova a Política Marítima Nacional;
- Decreto nº 1.052/1994 – dispõe sobre a direção civil do transporte marítimo em situações de tensão internacional ou guerra, e
- Decreto nº 3.897/2001 – fixa as diretrizes para o emprego das Forças Armadas na garantia da Lei e de Ordem e da outras providências.

3) Secretaria da Receita Federal

A fiscalização e o controle sobre o comércio exterior, essenciais à defesa dos interesses fazendários nacionais, serão exercidos pelo Ministério da Fazenda. (Artigo 237 da Constituição Federal). Portanto, à Secretaria da Receita Federal (SRF) compete:

- dirigir, supervisionar, orientar, coordenar e executar os serviços de administração, fiscalização e controle aduaneiro, inclusive no que diz respeito a alfandegamento de áreas e recintos. (Decreto nº 3782 de 05/04/2001, artigos 7º, incisos XVI e artigo 35 e Portaria do MF nº 259 de 24/08/2001, artigo 1º, inciso XVI);
- participar, observada a competência específica de outros órgãos, nas atividades de repressão ao contrabando, ao descaminho e ao tráfico ilícito de entorpecentes e de drogas afins, e à lavagem de dinheiro. (Decreto nº 3782 de 05/04/2001, artigos 7º, inciso XIX e artigo 35 e Portaria do MF nº 259 de 24/08/2001, artigo 1º, inciso XIX);
- cumprir e fazer cumprir a legislação que regula a entrada, a permanência e a saída de quaisquer bens ou mercadorias no País. (LEI DOS PORTOS – Lei nº 8.630 de 25/12/93, artigo 36, inciso I);

- fiscalizar a entrada, a permanência, a movimentação e a saída de pessoas, veículos, unidades de carga e mercadorias, sem prejuízo das atribuições das outras autoridades no porto. (LEI DOS PORTOS – Lei nº 8.630 de 25/12/93, artigo 36, inciso II);
- exercer a vigilância aduaneira e promover a repressão ao contrabando, ao descaminho e ao tráfico de drogas, sem prejuízo das atribuições de outros órgãos. (LEI DOS PORTOS – Lei nº 8.630 de 25/12/93, artigo 36, inciso III);
- proceder ao despacho aduaneiro na importação e na exportação. (LEI DOS PORTOS – Lei nº 8.630 de 25/12/93, artigo 36, inciso V);
- proceder à apreensão de mercadorias em situação irregular, nos termos da legislação fiscal aplicável. (LEI DOS PORTOS – Lei nº 8.630 de 25/12/93, artigo 36, inciso VII);
- autorizar a remoção de mercadorias da área do porto para outros locais, alfandegados ou não, nos casos e na forma prevista na legislação aduaneira. (LEI DOS PORTOS – Lei nº 8.630 de 25/12/93, artigo 36, inciso VIII);
- zelar pela observância da legislação aduaneira e pela defesa dos interesses fazendários nacionais. (LEI DOS PORTOS – Lei nº 8.630 de 25/12/93, artigo 36, inciso XI).

São, ainda, prerrogativas da SRF:

1. A administração fazendária e seus servidores fiscais terão, dentro de suas áreas de competência e jurisdição, precedência sobre os demais setores administrativos, na forma da lei. (Constituição Federal 1988, artigo 37, inciso XVII);
2. No exercício de suas atribuições, a autoridade aduaneira terá livre acesso a quaisquer dependências do porto e às embarcações atracadas ou não, bem como aos locais onde se encontrem mercadorias procedentes do exterior ou a ele destinadas, podendo, quando julgar necessário, requisitar papéis, livros e outros documentos, inclusive, quando necessário, o apoio de força pública

federal, estadual ou municipal. (LEI DOS PORTOS – Lei nº 8.630 de 25/12/93, artigo 36, parágrafo 2º) 3. Em tudo o que interessar à fiscalização aduaneira na zona primária, a autoridade aduaneira tem precedência sobre as demais que ali exerçam suas atribuições.

§ 1º - O dispositivo neste item aplica-se igualmente à zona de vigilância aduaneira, devendo as demais autoridades prestar à autoridade aduaneira a colaboração que for solicitada.

§ 2º - A precedência de que trata este item implica, igualmente:

I - a obrigação, por parte das demais autoridades, de prestar auxílio imediato, sempre que requisitado, para o cumprimento das atividades fiscais e de colocar à disposição da autoridade aduaneira pessoas, equipamentos ou instalações necessárias à ação fiscal;

II - que, no que interessar à Fazenda Nacional, a disciplina da entrada, permanência, movimentação e saída de pessoas, veículos, unidades de carga e mercadorias, na zona primária, é de competência da autoridade aduaneira, sem prejuízo das atribuições dos outros órgãos (Artigo 10 do Regulamento Aduaneiro, aprovado pelo Decreto nº 91030, de 05 de março de 1985 e Decreto Lei nº 37/66, Artigo 35).

4. A autoridade aduaneira poderá proceder às buscas em veículos necessárias para prevenir e reprimir a ocorrência de infração à legislação aduaneira, inclusive em momento anterior à prestação das informações referidas no caput. (Artigo 37, § 3º, do Decreto – Lei 37/66, alterado pela Medida Provisória nº 38, de 14/05/2002).

4) Administração Portuária

À Administração Portuária, por meio de sua Guarda Portuária e consoante, também, com a Portaria nº 180, de 23 de maio de 2001, do Ministério dos Transportes, compete:

- promover a vigilância e a segurança no porto organizado. Na zona primária o porto organizado, a vigilância será levada a efeito com o objetivo de garantir o cumprimento da legislação que regula a entrada, a permanência, a movimentação e a saída de pessoas, veículos, unidades de carga e mercadoria;
- prestar auxílio às autoridades que exerçam suas atribuições no porto, sempre que requisitada. Portanto, a Guarda Portuária deverá colaborar com os órgãos de

segurança pública e demais autoridades que atuam na área portuária para manutenção da ordem e a prevenção de ilícitos no interior daquelas instalações;

- exercer o policiamento interno das instalações do porto;
- zelar pela segurança, ordem, disciplina e fiel guarda dos imóveis, equipamentos, mercadorias e outros bens existentes ou depositados na área portuária, sob a responsabilidade da administração portuária;
- deter, em flagrante delito, os autores de crimes ou contravenções penais e apreender os instrumentos e objetos que tiveram relação com o fato, entregando-os à autoridade competente;
- registrar a ocorrência, quando constatadas atividades ilícitas, acidentes de trabalho, sinistros ou avarias em equipamentos e veículos ou atividades irregulares que venham a prejudicar o andamento das operações portuárias, mantendo a preservação do local do delito, efetuando os levantamentos preliminares e encaminhando-os à autoridade competente.
- adotar as seguintes providências, quando da ausência da autoridade competente, em caso de sinistro, acidente, crime, contravenção penal ou ocorrência anormal:
 - ✓ remover os feridos para o pronto-socorro ou hospital, comunicando, de imediato, o setor de segurança do trabalho;
 - ✓ isolar o local para a realização de verificação e perícias, sempre que possível sem a paralisação das atividades portuárias;
 - ✓ acionar o grupo de combate a incêndio, sempre que necessário.
- buscar a integração dos órgãos que compõem a CESPOTOS, para uma ação mais coordenada na prevenção e repressão aos atos ilícitos.

5) Governo do Estado

Ao Governo do Estado, por meio da Polícia Civil, Polícia Militar e Corpo de Bombeiros, de acordo com o Artigo 144 da Constituição da República Federativa do Brasil compete:

a) Polícia Civil.

- desempenhar as funções de polícia judiciária;
- apurar infrações penais, exceto as militares.

b) Polícia Militar

- realizar policiamento ostensivo;
- preservar a ordem pública.

c) Corpo de Bombeiros

- executar atividades de defesa civil, além das atribuições definidas em Lei.

A Polícia Civil e a Polícia Militar deverão buscar a integração dos órgãos que compõem a CESPORTOS, para uma ação mais coordenada na prevenção e repressão aos atos ilícitos.

Compete ao Coordenador da CESPORTOS:

- exercer as atividades de secretaria executiva da CESPORTOS, oferecendo, inclusive, apoio administrativo durante a realização das reuniões ordinárias e extraordinárias da Comissão;
- convocar as reuniões ordinárias e, quando necessário, as extraordinárias da CESPORTOS;
- incentivar a ação integrada dos órgãos que compõem a CESPORTOS.
- elaborar e encaminhar à CONPORTOS, em até 15 (quinze) dias da realização, as atas das respectivas reuniões da CESPORTOS, após lida e aprovada;
- promover os atos necessários, perante as autoridades constituídas, à preservação da ordem pública e da incolumidade das pessoas e do patrimônio dos entes alcançados por esta norma;
- adotar as medidas necessárias, quando os atos de que trata o item anterior desta alínea “c” exigir a expedição de ordem judicial expressa que resguarde a ação a ser desencadeada;
- exercer outras atividades que lhe sejam atribuídas, em razão da deliberação, no mínimo, da maioria dos membros que integram a CESPORTOS.

CAPÍTULO III

COMPROMISSOS

COMPROMISSO Nº 1 - COMBATE AO NARCOTRÁFICO E AO CRIME ORGANIZADO NOS PORTOS, TERMINAIS E VIAS NAVEGÁVEIS.

AÇÕES

1. OPERAÇÕES DE COMBATE AO NARCOTRÁFICO

Desencadear nos portos do País operações integradas sistemáticas de repressão ao tráfico de drogas, a partir de uma atuação conjunta dos órgãos que compõem a CESPORTOS. Terão prioridade os portos dos estados de São Paulo, Rio de Janeiro, Pernambuco, Pará, Amazonas, Espírito Santo, Paraná, Rio Grande do Sul e Santa Catarina.

2. OPERAÇÕES DE COMBATE AO CONTRABANDO E AO DESCAMINHO.

Promover esforços conjuntos dos órgãos que compõem a CESPORTOS, para conter o contrabando e o descaminho de bens e valores nos portos, terminais e vias navegáveis.

3. VIGILÂNCIA NOS PORTOS, TERMINAIS E VIAS NAVEGÁVEIS.

Incrementar a vigilância nos portos, terminais e vias navegáveis, estabelecendo operações integradas inesperadas, a serem realizadas conforme orientação dos dados obtidos pelo Subsistema de Inteligência de Segurança Pública. Isto permitirá uma ação sistemática e planejada de repressão, além da otimização de recursos financeiros e humanos.

A Marinha do Brasil faz as seguintes recomendações aos comandantes das embarcações, constantes do seguinte Decálogo:

- vigie o navio e a carga;
- ilumine o navio e seu costado;
- estabeleça comunicações para apoio externo;
- controle o acesso à carga e aos compartimentos habitáveis;
- mantenha as vigias fechadas;
- não deixe objetos de valor expostos;
- mantenha as escadas recolhidas;
- em caso de assalto soar alarme geral para a tripulação, manter iluminação adequada, soar alarme através do Canal 16 VHF para os navios nas proximidades e para o sistema de escuta permanente das autoridades em terra, soar alarmes sonoros intermitentes, visuais como holofotes e sinalizadores náuticos;
- mantenha os vigias contratados sob o controle do Oficial de Serviço;
- comunique à Polícia Federal qualquer ocorrência relativa a furto, roubo e assalto.

4. CRIAÇÃO DOS NÚCLEOS ESPECIAIS DE POLÍCIA MARÍTIMA - NEPOM

Criar sete Núcleos Especiais de Polícia Marítima – NEPOM, nas unidades do Rio Grande/RS, Itajaí/SC, Vitória/ES, Paranaguá/PR, Foz do Iguaçu/PR, Recife/PE e Belém/PA, como instrumento de combate ao roubo/furto em embarcações, ao narcotráfico e ao contrabando e descaminho, com a colaboração dos órgãos que compõem a CESPOTOS.

Resultados esperados 2003 – 2006

- Redução anual da entrada de drogas ilícitas no Brasil, através dos portos.
- Redução anual do contrabando e do descaminho através dos portos.
- Portos adequadamente controlados e vigiados.
- Operações de repressão ao crime mais integradas entre os órgãos que compõem a CESPORTOS.

COMPROMISSO Nº 2 – CONTROLE DE ENTRADA E SAÍDA DE ARMAS DO PAÍS.

AÇÕES

5. INTENSIFICAÇÃO DA FISCALIZAÇÃO NOS PORTOS TERMINAIS E VIAS NAVEGÁVEIS

Incrementar a fiscalização da entrada e saída de armas do País, com a participação integrada dos órgãos que compõem a CESPORTOS.

6. RECOLHIMENTO DE ARMAS ILEGAIS

Realizar ações de recolhimento de armas ilegais na posse de infratores, nos portos, terminais e vias navegáveis.

Resultado esperado 2003 - 2006

- Redução de armas ilegais nas mãos de infratores, nos portos, terminais e vias navegáveis.

COMPROMISSO Nº 3 – REPRESSÃO AO ROUBO/FURTO DE CARGAS

AÇÃO

7. OPERAÇÕES DE REPRESSÃO AO ROUBO/FURTO DE CARGAS

Intensificar ações integradas de fiscalização, com vistas a diminuir os índices de roubo/furto de cargas em embarcações, “containers” e depósitos alfandegados.

Resultados esperados 2003 – 2006

- Portos, terminais e vias navegáveis seguras.
- Ações integradas para o combate ao roubo/furto de cargas.

COMPROMISSO Nº 4 – UTILIZAÇÃO DO SUBSISTEMA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

AÇÃO

8. INTEGRAÇÃO DAS CESPORTOS AO SUBSISTEMA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

As CESPORTOS, por intermédio dos representantes dos órgãos que as compõem, deverão integrar-se ao Subsistema de Inteligência de Segurança Pública, utilizando os dados ali produzidos e, ao mesmo tempo, alimentando o referido Sistema.

Resultados esperados 2003 – 2006

- Realizar ações integradas de segurança pública nos portos, terminais e vias navegáveis, orientadas pelo Subsistema de Inteligência de Segurança Pública.

CONCLUSÃO

O Plano apresentado é o resultado de um trabalho da CONPORTOS e das CESPORTOS.

A integração dos órgãos que compõem as CESPORTOS é fundamental e contribuirá para a criação de um Sistema Nacional de Segurança Pública que ofereça alcance amplo e eficaz na solução do complexo problema da violência.

As medidas aqui selecionadas visam difundir, junto ao povo brasileiro, a idéia precisa de segurança e justiça, bem como a percepção da presença e o sentimento de confiança no Poder Público, destacando os valores fundamentais ao desenvolvimento de uma sociedade organizada e democrática.

As referidas medidas visam, também, diminuir o “Custo Brasil”, facilitando as importações e exportações, por meio de portos, terminais e vias navegáveis seguras, caracterizando a importância da Segurança Pública no contexto da nação brasileira.

O presente Plano serve para dar as referências e o horizonte do como e para onde se deseja chegar, porém a consecução de seus resultados exige um compromisso efetivo de todos.