Comitê Gestor da Internet Brasileira

12ª Reunião do GTS - Grupo de Trabalho em Segurança – 8 nov 2008

RENASIC – Rede Nacional de Segurança da Informação e Criptografia

Antonio Carlos Menna Barreto Monclaro

Assessor do Gabinete de Segurança Institucional

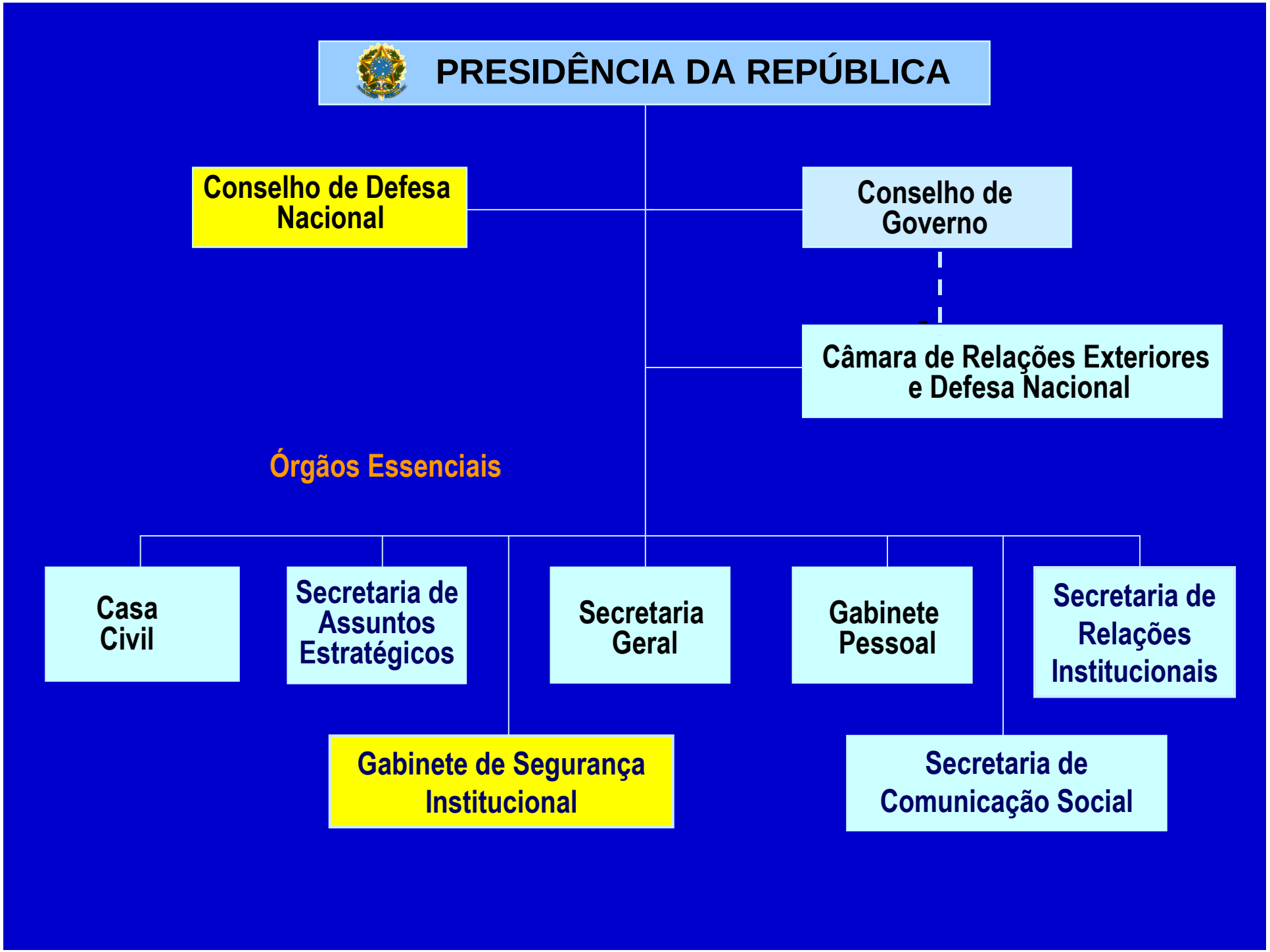
monclaro@planalto.gov.br

ÍNDICE

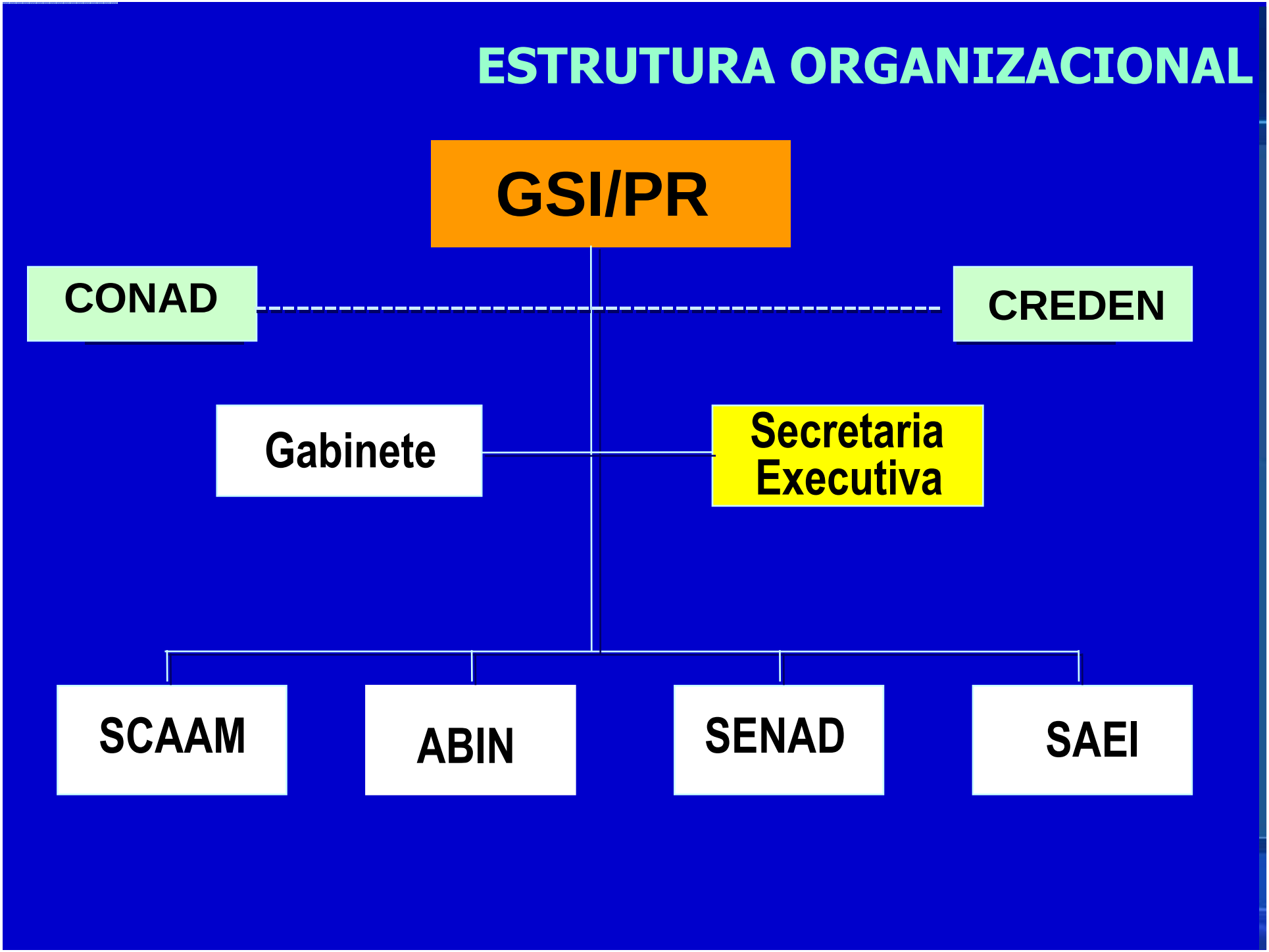
1. **GSI, o filme**
2. **Estrutura do GSI**
3. **A RENASIC**

ÍNDICE

1. GSI, o filme
2. Estrutura do GSI
3. A RENASIC


PRESIDÊNCIA DA REPÚBLICA
Conselho de Defesa Nacional
Conselho de Governo
Câmara de Relações Exteriores e Defesa Nacional
Órgãos Essenciais
Casa Civil
Secretaria de Assuntos Estratégicos
Secretaria Geral
Gabinete Pessoal
Secretaria de Relações Institucionais
Gabinete de Segurança Institucional
Secretaria de Comunicação Social

ESTRUTURA ORGANIZACIONAL



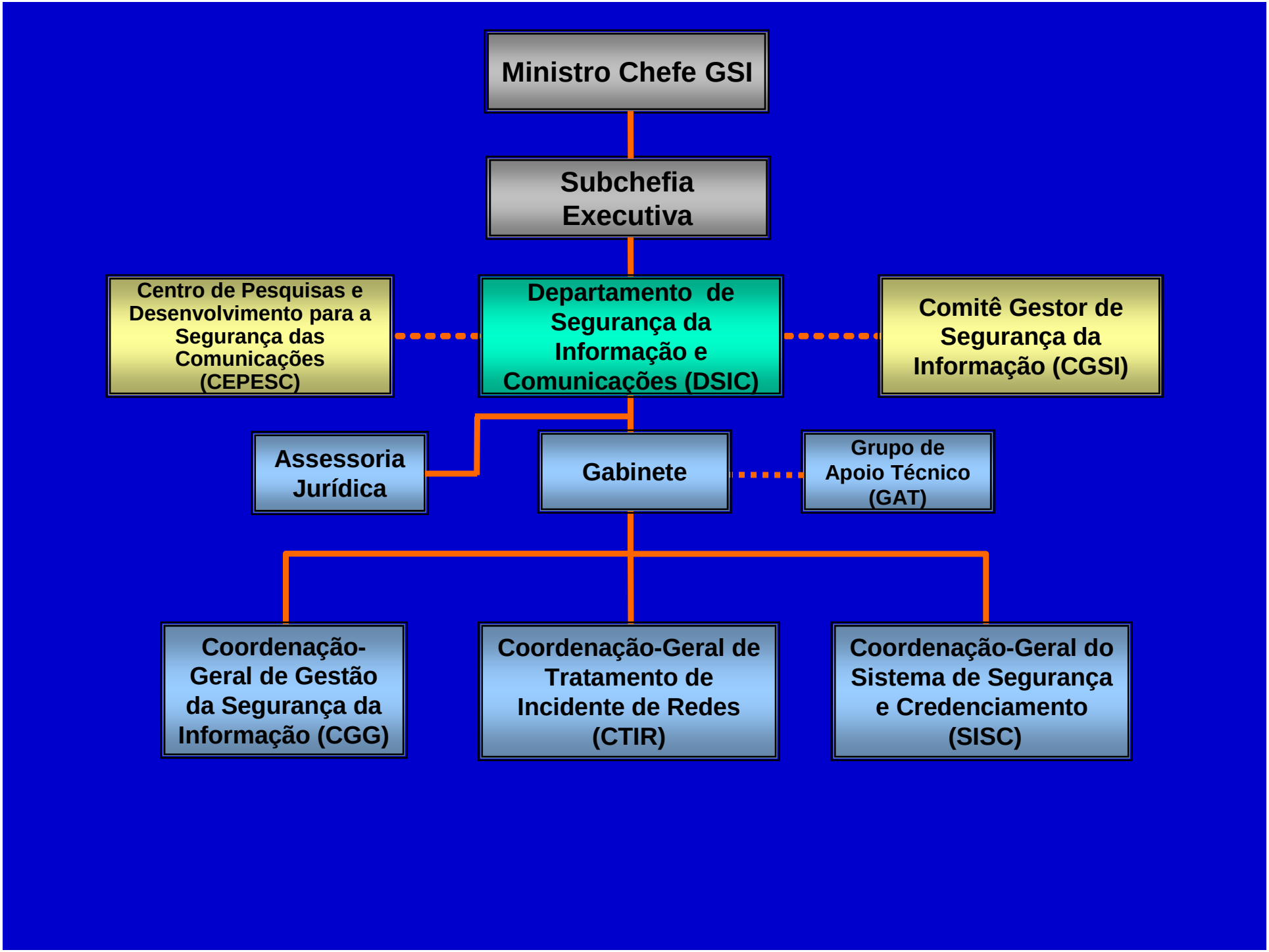
ENTRE AS MISSÕES DO GSI ESTÁ A COORDENAÇÃO DAS ATIVIDADES DE SEGURANÇA DA INFORMAÇÃO

(LEI Nº 10.683, DE 28 DE MAIO DE 2003)

Segurança da Informação e Comunicações

A SIC permeia praticamente todas as áreas de uma organização

ESTRUTURA ORGANIZACIONAL


Ministro Chefe GSI
Subchefia Executiva
Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC)
Departamento de Segurança da Informação e Comunicações (DSIC)
Comitê Gestor de Segurança da Informação (CGSI)
Assessoria Jurídica
Gabinete
Grupo de Apoio Técnico (GAT)
Coordenação-Geral de Gestão da Segurança da Informação (CGG)
Coordenação-Geral de Tratamento de Incidente de Redes (CTIR)
Coordenação-Geral do Sistema de Segurança e Credenciamento (SISC)

O DSIC FOI CRIADO PARA SER O BRAÇO EXECUTIVO DO GSI NAS AÇÕES DE COORDENAÇÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

DEVE ATUAR EM ESTREITA COLABORAÇÃO COM:

- ***CGSI – AÇÕES POLÍTICAS***
- ***CEPESC – AÇÕES TÉCNICAS***
- ***RENASIC – AÇÕES DE INTEGRAÇÃO***

Do DECRETO Nº 3.505, DE 13 DE JUNHO DE 2000, que instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, extraímos as seguintes missões para o GSI:

- **Capacitação dos segmentos das tecnologias sensíveis;**
- **Definição do uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;**
- **Capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado;**
- **Eliminação da dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;**

- **Promoção da capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;**
- **Promoção do intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;**
- **Promoção da capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como o estímulo ao setor produtivo para que participe competitivamente no mercado de bens e de serviços relacionados com a segurança da informação.**

- estabelecimento de programas destinados à formação e ao aprimoramento dos recursos humanos, com vistas à definição e à implementação de mecanismos capazes de fixar e fortalecer as equipes de pesquisa e desenvolvimento, especializadas em todos os campos da segurança da informação; e
- acompanhamento, em âmbito nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à segurança da informação.

Para coadjuvar o GSI no cumprimento dessas missões foi criada a RENASIC por meio da Portaria nº 31 de 6 de outubro de 2008

ÍNDICE

1. GSI, o filme
2. Estrutura do GSI
3. A RENASIC

HISTÓRICO

- Lista de distribuição da ComSic (160)
- Site WIKI (68)
- Visita do Min GSI ao MIN MCT
- Portaria da RENASIC
- Entrega do Termo de Referência

OBJETIVO

O principal objetivo da RENASIC é elevar a competência brasileira em Segurança da Informação e Criptografia (SIC) ao nível dos países mais desenvolvidos em C&T, pelo estabelecimento e efetivo aumento da integração das pesquisas brasileiras que acontecem nas universidades, institutos de pesquisa, órgãos governamentais e empresas.

Art.2º A RENASIC tem por objetivos:

I – promover o avanço científico-tecnológico no país da segurança da informação, em geral, e da criptografia e defesa cibernética em particular; e

II – integrar as atividades no país de grupos de pesquisa atuantes nas áreas mencionadas no inciso anterior.

Parágrafo único. No âmbito da RENASIC serão executadas as seguintes atividades:

I – análise, desenvolvimento e implementação de técnicas e ferramentas relacionadas com segurança da informação e criptografia; e

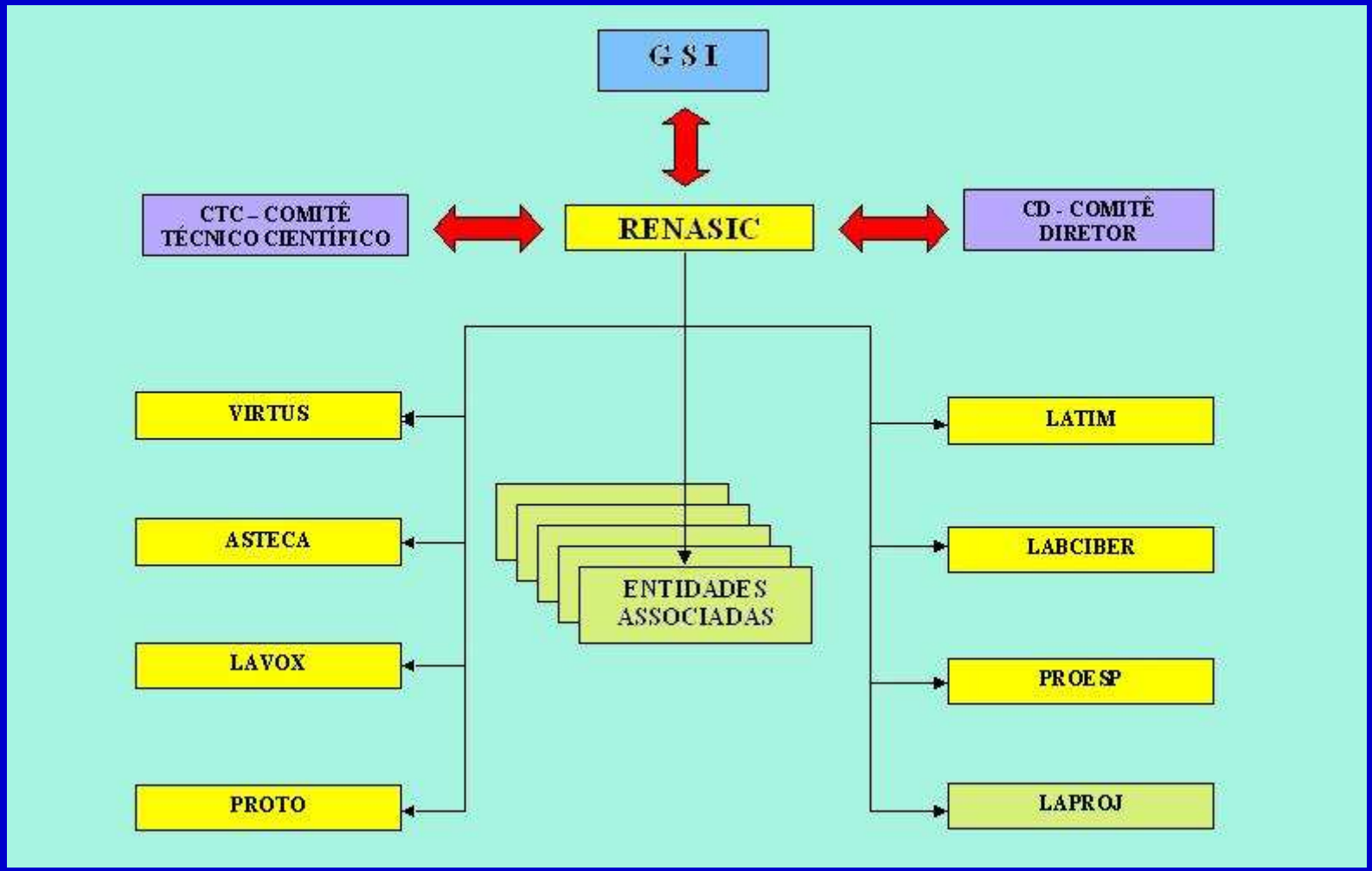
II – aproximação do conhecimento das comunidades acadêmicas com as necessidades dos potenciais usuários; e

III – realimentação das dificuldades e problemas práticos advindos das implementações aos grupos teóricos.

INSTRUMENTOS

- E-integração: portal colaborativo, fóruns virtuais e listas de distribuição de e-mails;
- Workshops, seminários e congressos para acolher as necessidades de todos os parceiros relevantes, criar consenso sobre as agendas de pesquisa integrada, apresentações científicas e sessões de interação coletiva (“brainstorming”);
- Visitas de intercâmbio entre os pesquisadores e doutorandos;
- Cursos de durações diversas;
- Concessão de bolsas de mestrado, e pós-doutorado em Universidades de excelência no país ou no estrangeiro;
- Desenvolvimento de uma infra-estrutura comum.

ORGANOGRAMA



COMITÊ DIRETOR (CD)
8 membros

Art. 8º O Comitê Diretor terá a seguinte composição:

I – dois representantes do GSI, sendo que um o presidirá;

II – um representante da Casa Civil da Presidência da República;

III – um representante do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações – CEPESC, unidade da Agência Brasileira de Inteligência - ABIN;

IV – um representante dos órgãos de fomento, indicado pelo Ministro de Estado Chefe do MCT;

V – um representante das entidades associadas; e

VI – dois pesquisadores de renome na área científica ou tecnológica indicados em lista tríplice pela Academia Brasileira de Ciência e pela Sociedade Brasileira para o Progresso da Ciência.

COMITÊ TÉCNICO-CIENTÍFICO (CTC) – 7 membros

Art. 10 O Comitê Técnico-Científico será composto por sete pesquisadores, com atuação reconhecida na área de segurança da informação e criptografia, designados mediante Portaria do Ministro de Estado Chefe do GSI.

§ 1º Na escolha dos pesquisadores, levar-se-á em consideração a estruturação dos Labs e GTs, devendo, sempre que possível, haver representação das diversas especialidades científicas.

§ 2º O Comitê Técnico-Científico será presidido por um dos seus integrantes, escolhidos por seus pares, na forma a ser estabelecida no Regimento Interno da RENASIC.

ENTIDADES ASSOCIADAS

Art. 4º A RENASIC poderá admitir entidades associadas, denominação dada às organizações públicas ou privadas que participarem ou fomentarem suas atividades.

Parágrafo Único. As entidades associadas deverão firmar acordos de cooperação com a RENASIC, por intermédio do GSI, visando a garantir apoio e ao desenvolvimento científico e tecnológico relacionados às áreas de segurança da informação e criptografia de seu interesse.

METODOLOGIA DE IMPLANTAÇÃO (1)

- Portal colaborativo e listas de distribuição de mensagens hospedadas no âmbito da Presidência da República
- Reuniões periódicas intra e inter Comitês Diretor e Científico Tecnológico
- Seminários no domínio de cada Laboratório Virtual
- Workshops na esfera de cada Grupo de Trabalho
- Ferramentas de web 2.0 que possibilitem reuniões virtuais
- Cursos presenciais interdisciplinares de curta duração (40 Hs)

METODOLOGIA DE IMPLANTAÇÃO (2)

- Concessão de bolsas de mestrado e de pós-doutorado anual por cada Grupo de Trabalho (GT) de cada Laboratório Virtual;
- Palestras e cursos de curta duração por renomados pesquisadores brasileiros ou estrangeiros em áreas específicas, particularmente aquelas de maior carência nacional
- Publicação da “Revista Brasileira de Segurança da Informação e Criptografia”
- Um Congresso anual
- Gradual adesão das Entidades Associadas por meio de convênios
- Desenvolvimento de projetos específicos, de interesse do governo ou das Entidades Associadas

VIRTUS

Congrega as seguintes áreas:

Fundamentos teóricos das técnicas simétricas

- **Algoritmos simétricos de bloco**
- **Algoritmos simétricos seqüenciais**
- **Códigos para autenticação de mensagens**
- **Funções Hash**
- **Modos de operação e uso de primitivas criptográficas simétricas**

Grupos de Trabalho (GT)

- **GT 1: Desenvolvimento e análise de algoritmos de bloco**
- **GT 2: Desenvolvimento e análise de algoritmos seqüenciais**
- **GT 3: Desenvolvimento e análise de Funções Hash**
- **GT 4: Técnicas complementares**

ASTECA

Coordena as pesquisa nas seguintes áreas:

- **Assinaturas digitais.**
- **Desenvolvimento e análise de algoritmos de chaves públicas.**
- **Segurança demonstrável.**

Compõe-se dos seguintes grupos de trabalho (GT):

- **GT 1: Técnicas assimétricas tradicionais.**
- **GT 2: Técnicas assimétricas especiais.**
- **GT 3: Segurança demonstrável.**

PROTO (1)

Coordena as pesquisas nas seguintes áreas:

- **Modelos e definições.**
- **Protocolos seguros de computação.**
- **Protocolos criptográficos racionais.**

Grupos de Trabalho:

GT 1 Modelos e definições, com os seguintes temas:

- **Protocolos de acordo de chaves e autenticação.**
- **Provas de zero-knowledge.**
- **Protocolos para identificação.**

PROTO (2)

GT 2: Protocolos seguros de computação

- Computação eficiente entre múltiplas partes (MPC)
- Segurança Demonstrável para protocolos:
- Votação
  - Leilão e licitação eletrônica segura
  - Criptografia no limiar
  - Protocolos de acordo assíncronos
- Protocolos incondicionalmente seguros

GT 3: Protocolos criptográficos racionais:

- Comportamento racional e modelos econômicos e de Teoria dos Jogos.
- Computação entre múltiplos participantes racionais.

LATIM (1)

Possui um duplo papel no âmbito do RENASIC. Por um lado, realiza intensas pesquisas em novas técnicas relacionadas a implementações seguras. Por outro, este laboratório serve como intersecção entre as comunidades teóricas e os potenciais usuários.

Seus objetivos podem ser assim sumarizados:

- desenvolvimento de novas e eficientes técnicas de implementação em hardware e software;
- desenvolvimento de sólida compreensão dos ataques secundários (side-channel attacks) e suas respectivas contramedidas;
- estudos e pesquisas dos hardwares criptoanalíticos e seus impactos nos parâmetros criptográficos

LATIM (2)

Existem também objetivos não técnicos, tais como o incremento da cooperação entre os desenvolvedores, os engenheiros e os teóricos da criptografia, interligando as comunidades das empresas com a Academia. Pretende também realimentar os grupos teóricos com as dificuldades e problemas práticos advindos das implementações.

É composto de 4 GTs:

- GT 1: Implementações em software;
- GT 2: Implementações em hardware;
- GT 3: Ataques secundários;
- GT 4: Avaliação de conformidade.

LAVOX

Seus principais objetivos consistem no:

- **desenvolvimento e análise das técnicas convencionais concernentes à segurança de voz;**
- **desenvolvimento e análise de novas e eficientes técnicas de implementação em hardware e sofware com vistas à segurança de voz;**
- **manter permanente discussão a respeito da segurança de Voip.**

O LAVOX é composto de três GTs:

- **GT 1: Sistemas Criptográficos de Voz convencionais;**
- **GT 2: Sistemas especiais;**
- **GT 3: Discussão sobre Segurança de Voip**

PROESP

O PROESP - Laboratório Virtual de Projetos Especiais reúne aqueles pesquisadores de temas específicos relacionados com a Segurança da Informação e Criptografia, porém não abrigados nos demais laboratórios. Hoje existem diversas técnicas sendo desenvolvidas em centros de excelência de outros países as quais devem ser acompanhadas, analisadas e difundidas pela RENASIC, com vistas ao desenvolvimento de projetos específicos (LAPROJ).

Os objetivos do PROESP podem ser assim sumarizados:

- acompanhamento a nível mundial das novas tecnologias relacionadas com a Segurança da Informação e técnicas criptográficas e de criptoanálise;
- estudos e pesquisas sobre computação e criptografia quântica;
- estudos sobre a utilização do processamento de alto desempenho como ferramenta indispensável à computação de estudos e pesquisas dos hardwares criptoanalíticos e seus impactos nos parâmetros critográficos.

Por enquanto, o PROESP é composto de dois GTs:

- GT 1: Computação e Criptografia Quântica;
- GT 2: Computação de Alto Desempenho

LAPROJ

Será implantado à medida que surgirem demandas específicas dos Associados da RENASIC, sejam oriundas de entidades governamentais ou privadas.

Para cada projeto será selecionado o gerente e a equipe que participará, criando-se tópicos específicos nesta web, que aglutinarão todas as informações referentes ao respectivo projeto.

LABCIBER (1)

O LABCIBER - Laboratório Virtual de Defesa Cibernética visa, no âmbito do RENASIC, congregar a comunidade de especialistas em segurança de redes numa discussão coletiva sobre assuntos específicos tais como, Centros de Tratamento de Incidentes de Rede (CTIRs), estudos dos artefatos nocivos correntes e suas contramedidas, forense computacional e outros temas relevantes à segurança das redes computacionais. Além dessas tarefas, deve também usar seus conhecimentos para incrementar o desempenho do LATIM, inclusive na sua análise dos ataques secundários (side-channel attacks) e respectivas contramedidas. Este laboratório serve assim, como intersecção entre as comunidades de criptografia teórica e sua implementação real nas atuais e futuras redes de computadores.

LABCIBER (2)

Seus objetivos podem ser assim sumarizados:

- desenvolvimento de novas e eficientes ferramentas para integração dos Centros de Tratamento de Incidentes de Rede do país;
- análise de artefatos;
- estudos das ferramentas para forense computacional;
- colaboração com o LATIM, inclusive na análise dos ataques secundários;
- servir de forum de discussão de temas relevantes à Segurança da Informação.

O LABCIBER é composto dos seguintes GTs:

- GT 1: Discussão sobre integração de CTIRs;
- GT 2: Discussão sobre artefatos;
- GT 3: Discussão sobre forense computacional;
- GT 4: Apoio ao LATIM em ataques secundários (side-channel atacks);
- GT 5: Segurança de Redes;
- GT 6: Gestão de Riscos de Segurança da Informação.

Questões?

Antonio Carlos Menna Barreto Monclaro
61 3411 1117 9696 9945
monclaro@planalto.gov.br
https://wiki.planalto.gov.br/comsic