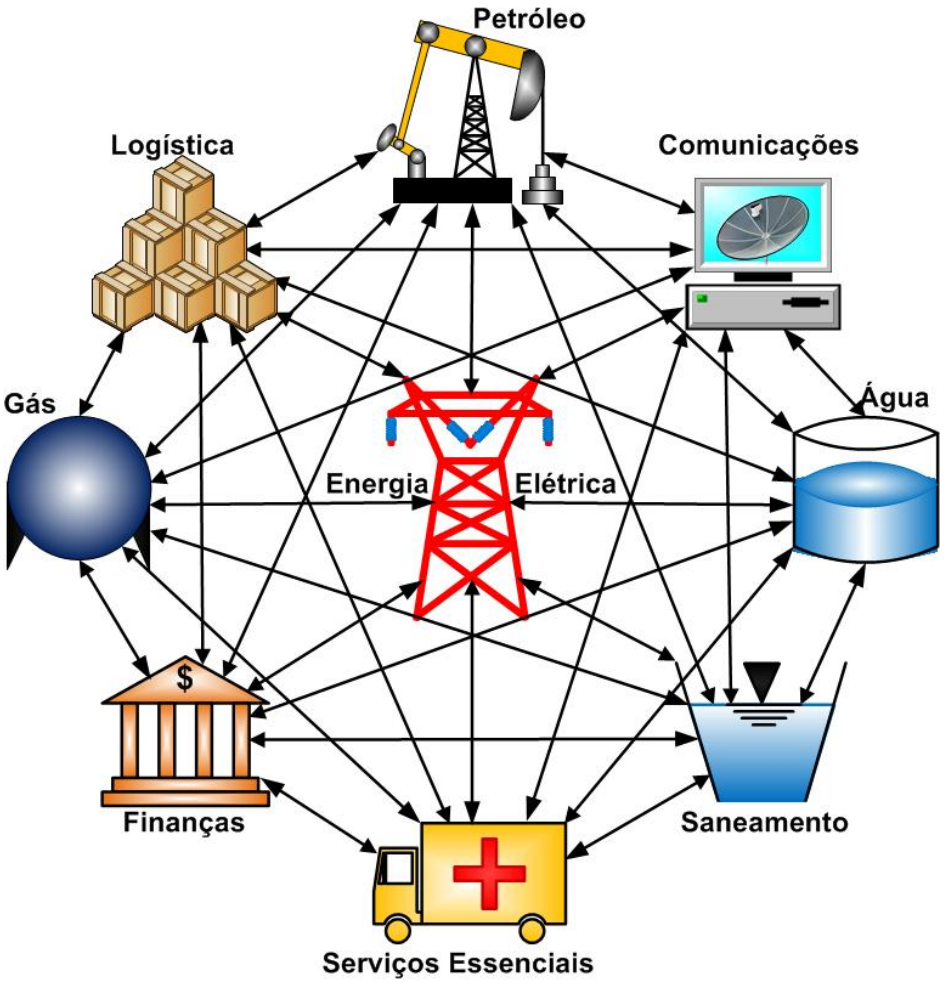
Laboratório de Segurança Cibernética em Ambiente de Tecnologias de Informação e Automação aplicada em Sistemas Elétricos – LaSC

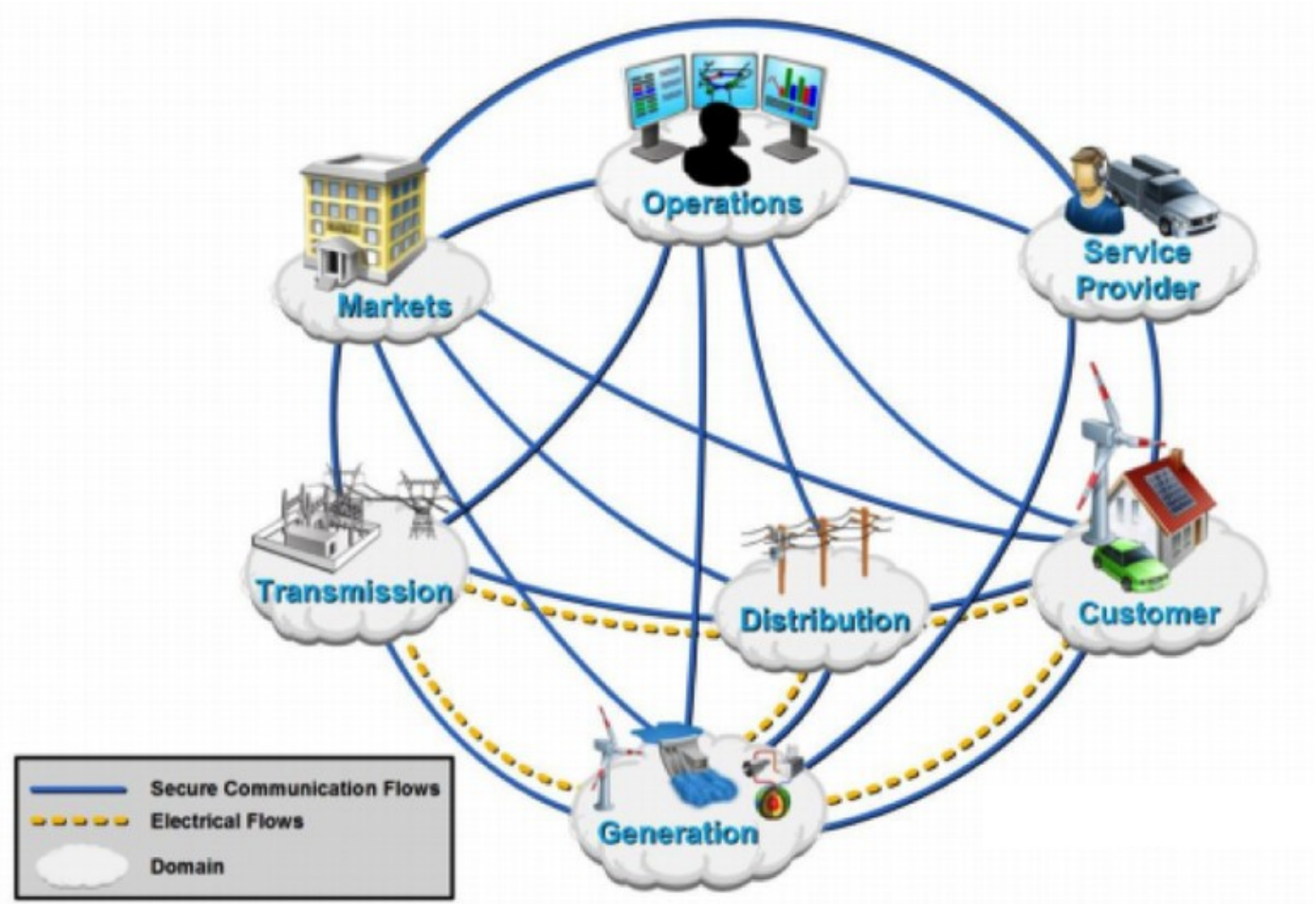
Parceria ITAIPU- Exército Brasileiro (IME) - Fundação PTI-BR (Ceape²/Lasse)

Infraestruturas Críticas - Setores

Estruturas físicas, serviços, bens e sistemas, que se forem interrompidos ou destruídos, total ou parcialmente, poderão provocar impactos social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade.



Sistema Elétrico no contexto da Indústria 4.0



Espaço Cibernético e suas implicações

Ambiente em permanente mudança

↓

Os sistemas de comunicação, sensoriamento e controle em todos os níveis, demandam o emprego extensivo de tecnologias da informação e comunicação.

↓

Com isso, proliferam também as ameaças e as vulnerabilidades

↓

Necessidade urgente do fortalecimento de uma cultura de segurança cibernética e de uma atuação estratégica que considere as suas diversas dimensões, tanto em termos das tecnologias utilizadas, quanto os aspectos sociais e seu inter-relacionamento (visão sistêmica).

Operador Nacional do Sistema - ONS

É atribuição do ONS propor regras para a operação das instalações de transmissão da rede básica do SIN, a serem aprovadas pela Agência Nacional de Energia Elétrica - ANEEL.

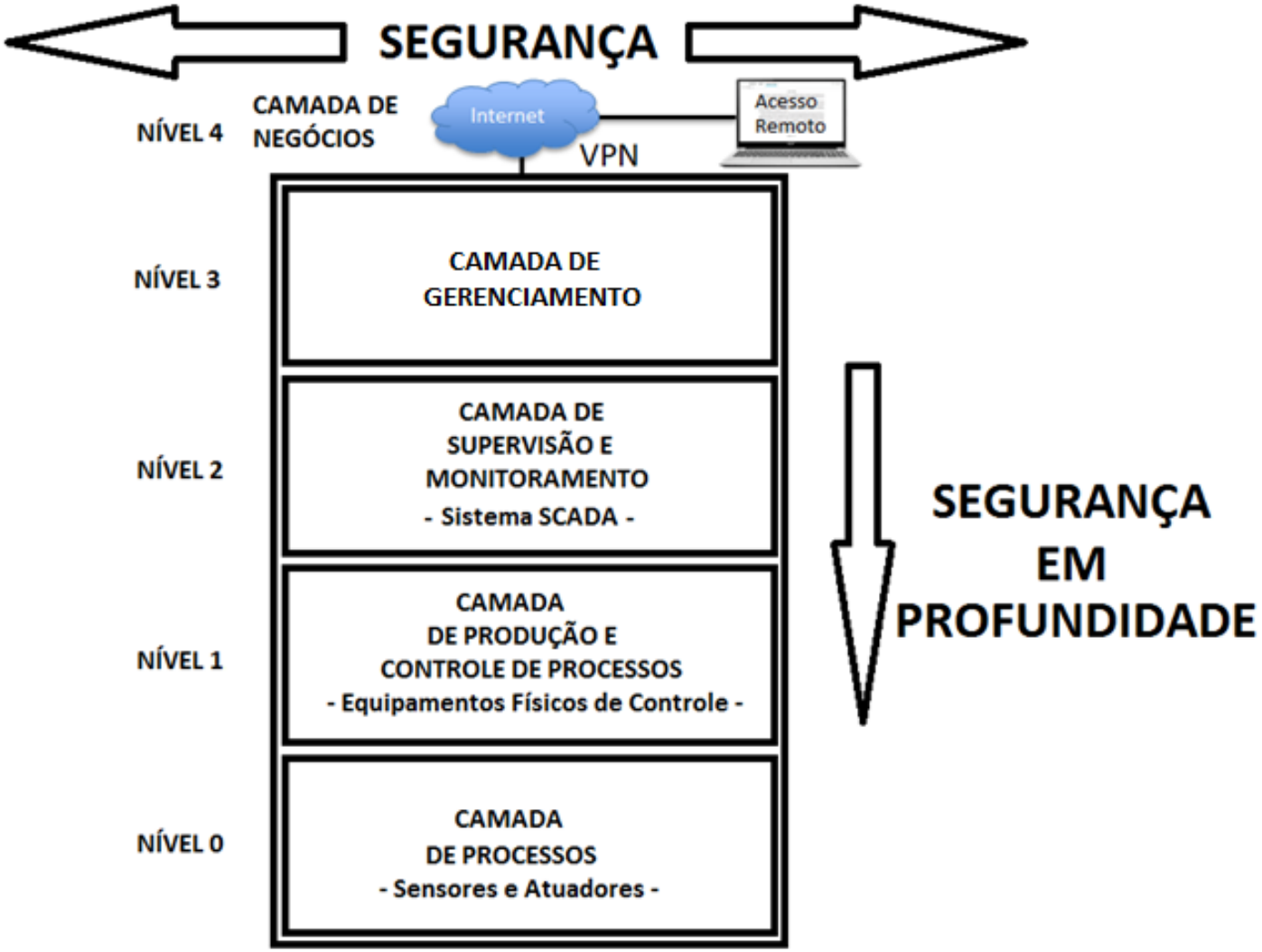
Essas regras são consolidadas nos **Procedimentos de Rede – PR** (atualmente são 25 PR vigentes), que são documentos de caráter normativo elaborados pelo ONS, com participação dos agentes.

ITAIPU BINACIONAL

Como um dos agentes, terá responsabilidades para com o sistema elétrico quanto à Segurança Cibernética.

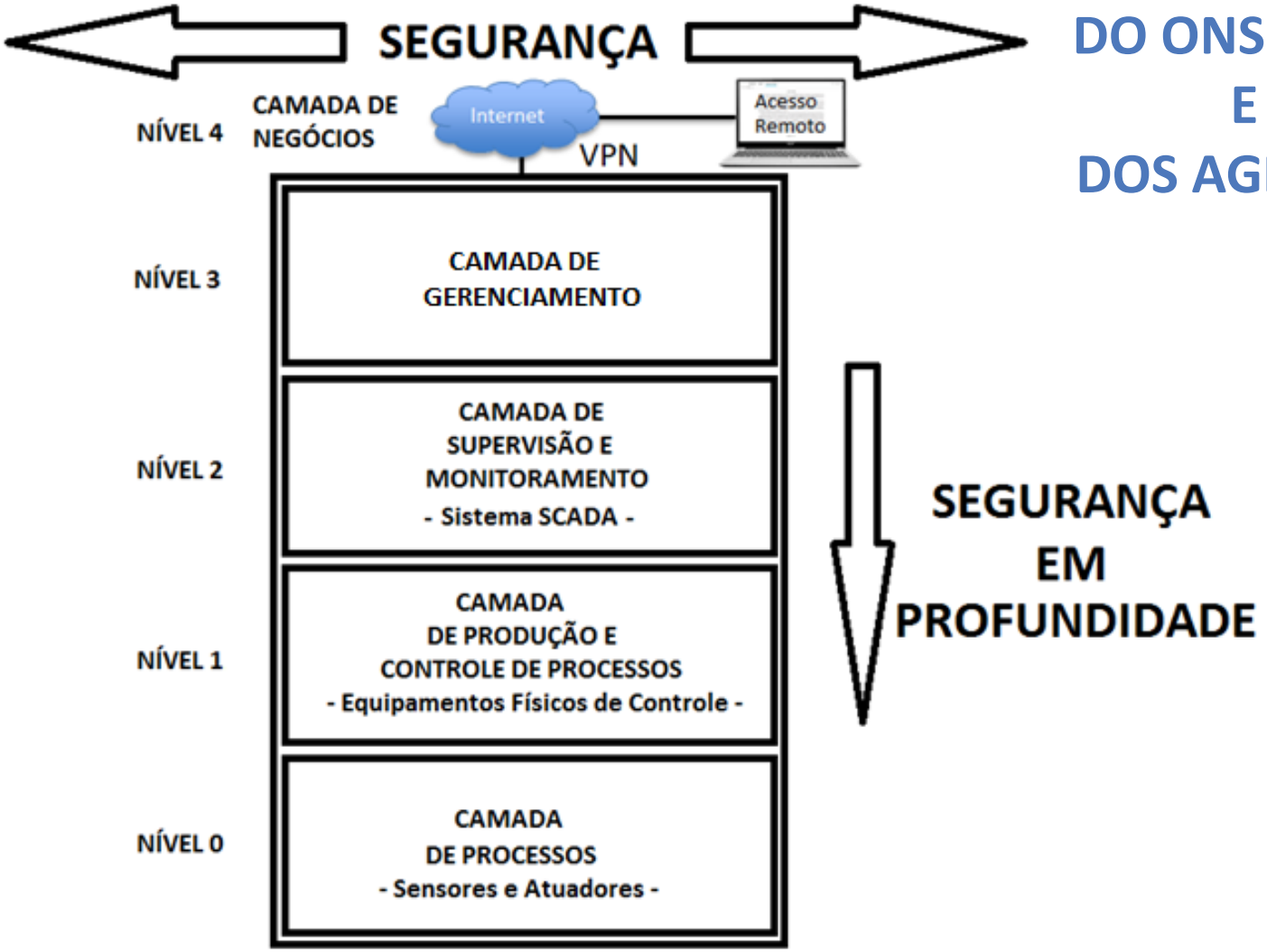
Atualização tecnológica da Usina – Presença massiva de dispositivos definidos por *software*.

SISTEMA INTERLIGADO – SEGURANÇA INTEGRADA

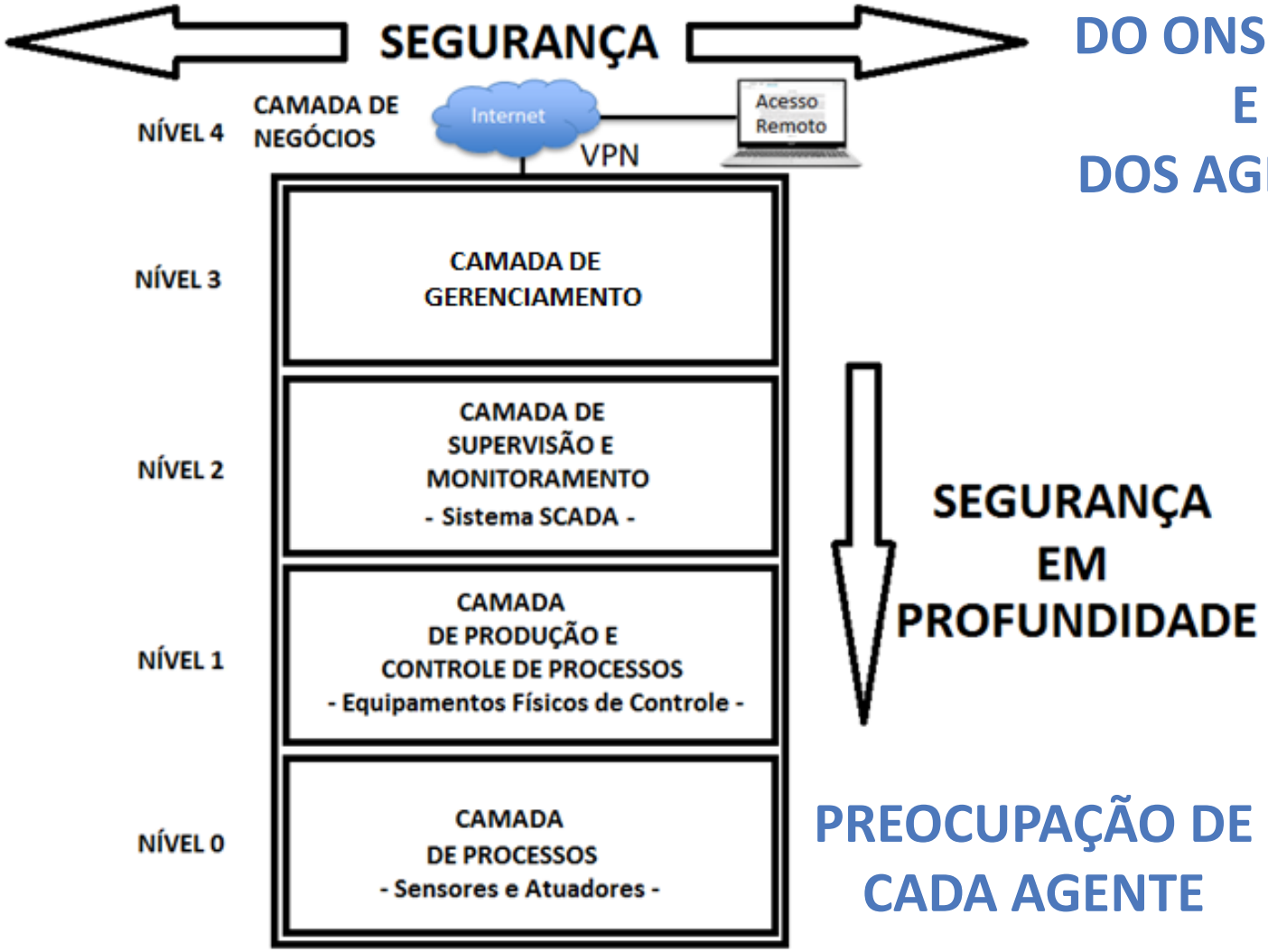


SISTEMA INTERLIGADO – SEGURANÇA INTEGRADA

PREOCUPAÇÃO DO ONS (CAG) E DOS AGENTES



SISTEMA INTERLIGADO – SEGURANÇA INTEGRADA

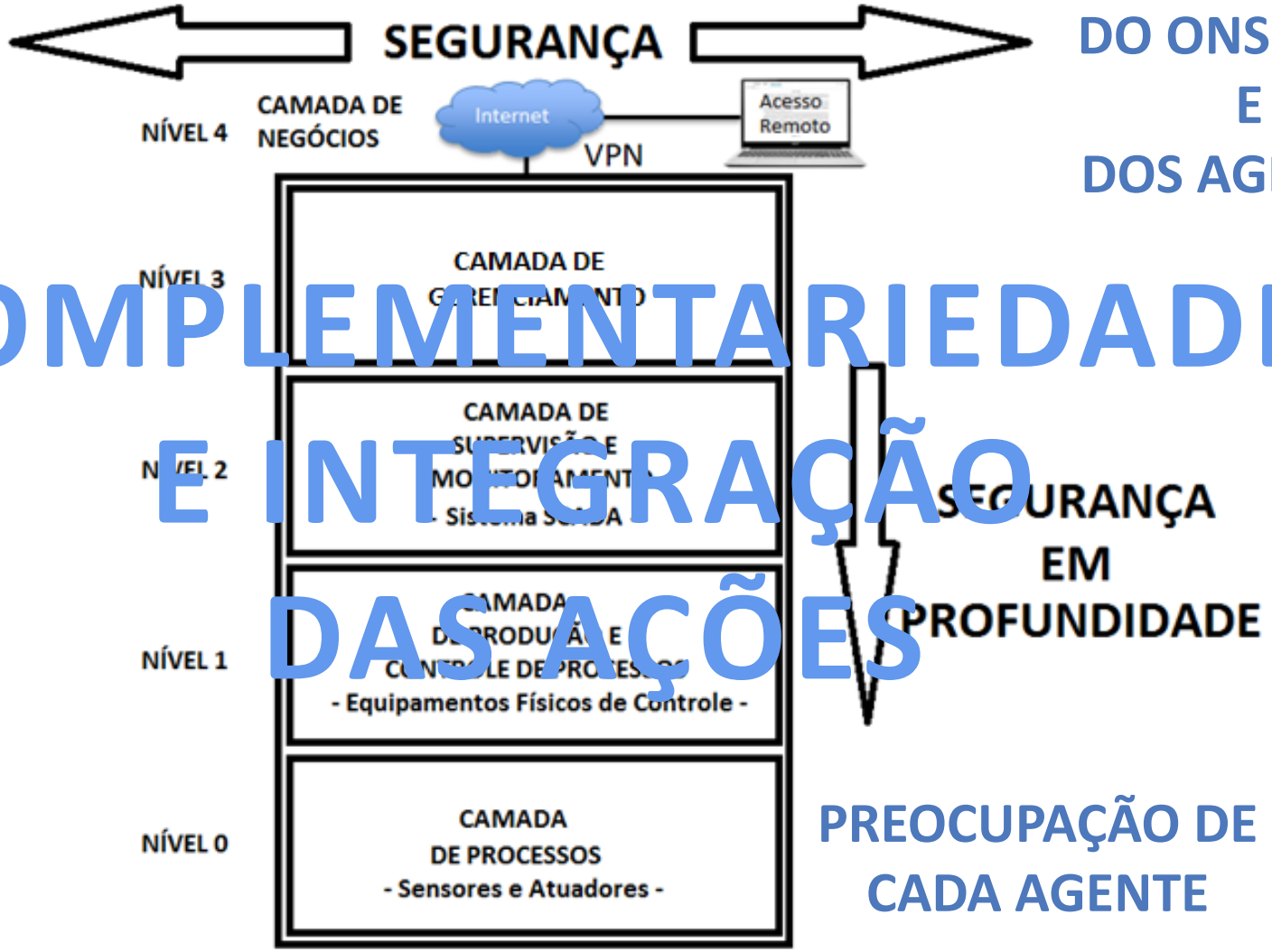


PREOCUPAÇÃO DO ONS (CAG) E DOS AGENTES

PREOCUPAÇÃO DE CADA AGENTE

SISTEMA INTERLIGADO – SEGURANÇA INTEGRADA

PREOCUPAÇÃO DO ONS (CAG) E DOS AGENTES



COMPLEMENTARIEDADE E INTEGRAÇÃO DAS AÇÕES

PREOCUPAÇÃO DE CADA AGENTE

O Projeto

Desenvolvimento de laboratório de Segurança Cibernética - LaSC voltado para estudos e análises da segurança em ambiente cibernético aplicado a infraestruturas críticas.

Início das tratativas em Abril de 2017.

Acordo de Parceria Nº EME 18-040-00 e Nº ITAIPU 4500049330, firmado entre a ITAIPU, o Comando do Exército Brasileiro e a Fundação Parque Tecnológico ITAIPU-Brasil (DOU 168, de 30 de agosto de 2018).

Integra o Programa Estratégico do Exército de Defesa Cibernética gerido pelo ComDCiber.

O Projeto no contexto do Exército Brasileiro

- A Estratégia Nacional de Defesa - END define que o EB é responsável pela Defesa Cibernética;
- ComDCiber hoje é o gestor do Programa Estratégico do Exército de Defesa Cibernética;
- O IME é responsável pelo Projeto de Pesquisa Cibernética;
- O LaSC faz parte do Projeto de Pesquisa Científica.

O Projeto no contexto do Exército Brasileiro

O Projeto no contexto do Exército Brasileiro

DEFESA CIBERNÉTICA

LABORATÓRIO DE ALTO DESEMPENHO

SUPERCOMPUTADOR

CRAY

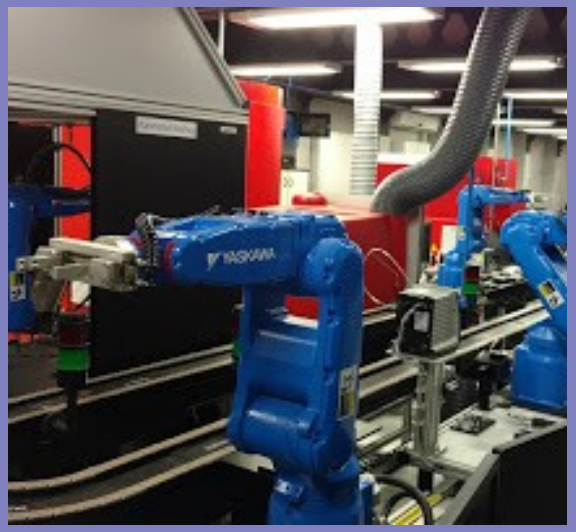
CLOUD

CLUSTER

2013

AUTOMAÇÃO

LABORATÓRIO DE MECATRÔNICA



2015

O Projeto – Descrição Geral

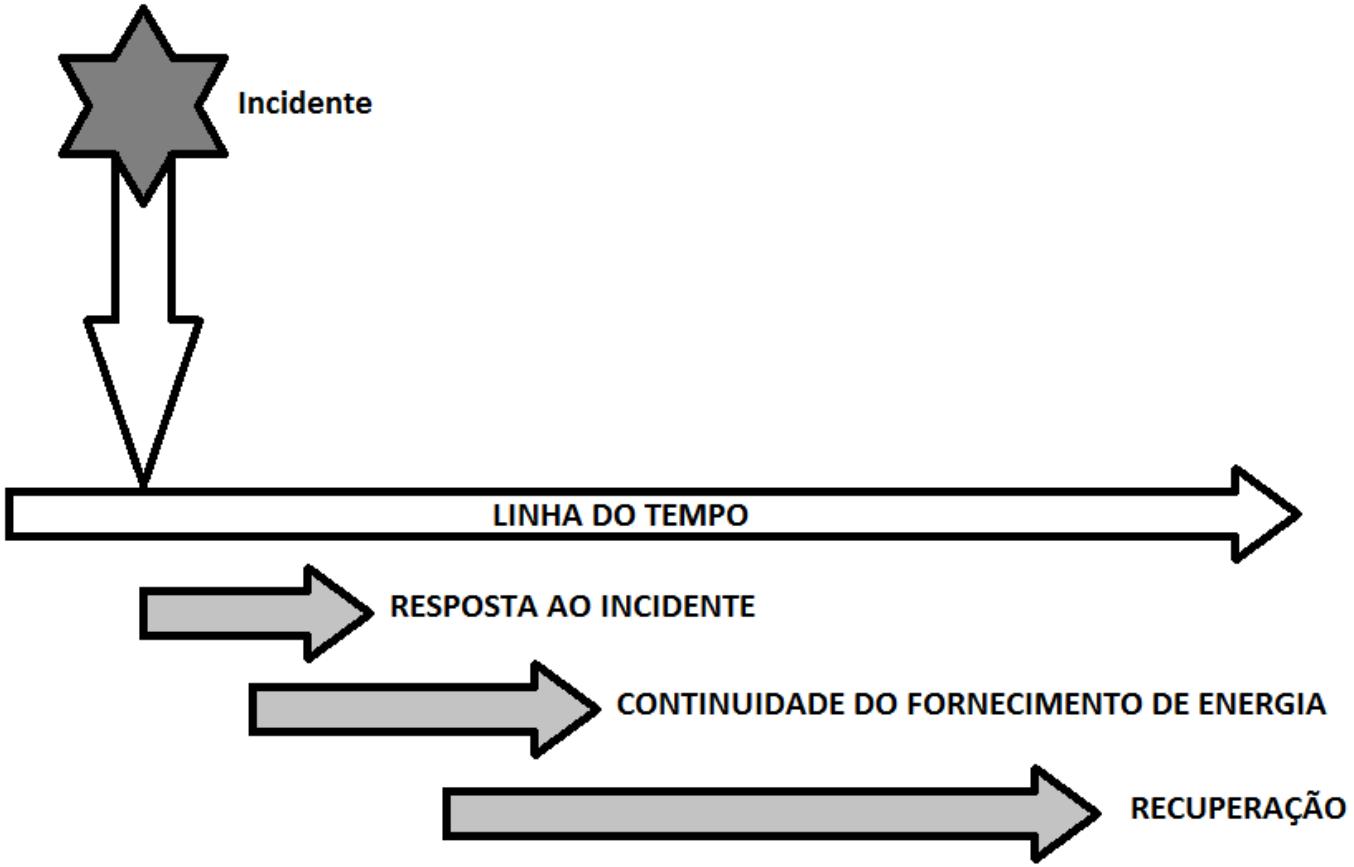
O projeto do LaSC, contempla um ambiente de simulação do tipo *hardware in the loop*, incluindo dispositivos físicos industriais que representarão infraestruturas críticas na área de Sistemas Elétricos e de Potência (SEP) e de Tecnologia de Automação.

Objetivo do Projeto

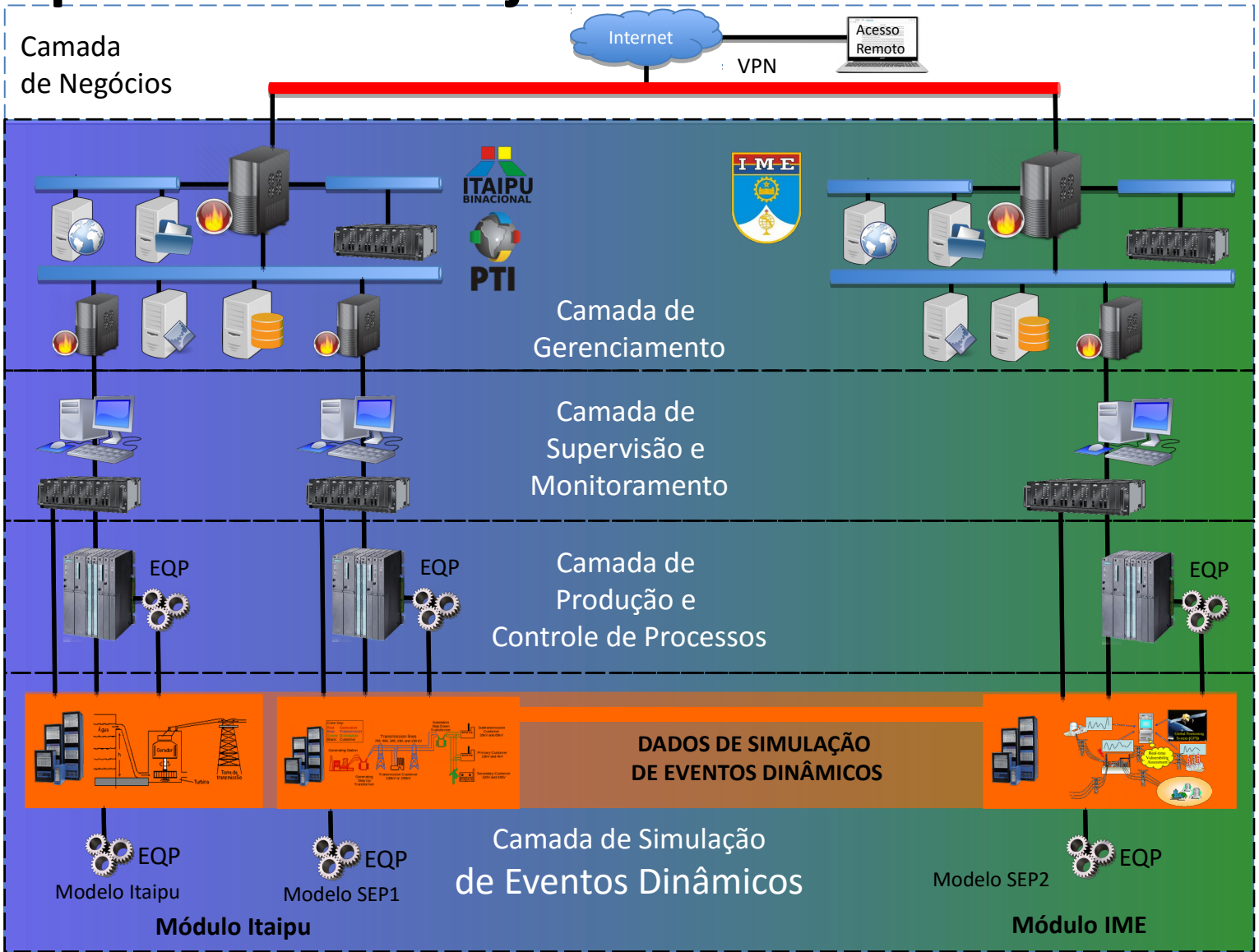
Instalar e operar um laboratório voltado para estudos e análises de segurança cibernética aplicada a infraestruturas críticas, atingindo os objetivos estratégicos das instituições parceiras.

Objetivo do Projeto

Ser um instrumento que permite gerir de forma mais eficiente a **Continuidade do Fornecimento de Energia**:



Arquitetura do Projeto



O LaSC na Proteção de Infraestruturas Críticas

Etapas dos estudos:

- Identificar os Ativos (Alvos);
- Analisar Riscos (Hierarquização);

Fase de Inventário

- Defender;

Camada Superior
Nível 4

- Detectar (*malware* ou invasão);
- Analisar os impactos;
- Definir Contramedidas;
- Mitigar Impactos.

Segurança em
Profundidade
Níveis 0 ao 3

O LaSC na Proteção de Infraestruturas Críticas

TIC e TA:

Raízes Diferentes

TIC

Padronização

Manipulação de informações

Manutenção da segurança
(confidencialidade, disponibilidade e integridade)

TA

Especialização

Manipulação de itens de risco

Manutenção da segurança
(confidencialidade, disponibilidade e integridade)

O LaSC na Proteção de Infraestruturas Críticas

Produtos

- Metodologias que permitam a execução e avaliação de ações em ambientes simulados de forma a não expor o sistema em produção a riscos cibernéticos;
- Requisitos de operação (topologias para minimizar os impactos, por exemplo);
- Instruções de operação para mitigar ataques de natureza cibernética;
- Promoção da consciência situacional com relação à segurança cibernética;
- Recursos humanos especializados;
- Pesquisa, desenvolvimento e inovação;
- Ampliação da capacidade da ITAIPU, do PTI-BR e do EB na área de segurança cibernética de infraestruturas críticas no setor elétrico.

O LaSC na Proteção de Infraestruturas Críticas

Produtos

Provas de conceito e validação (ou possivelmente certificação) de dispositivos e tecnologias (alguns exemplos):

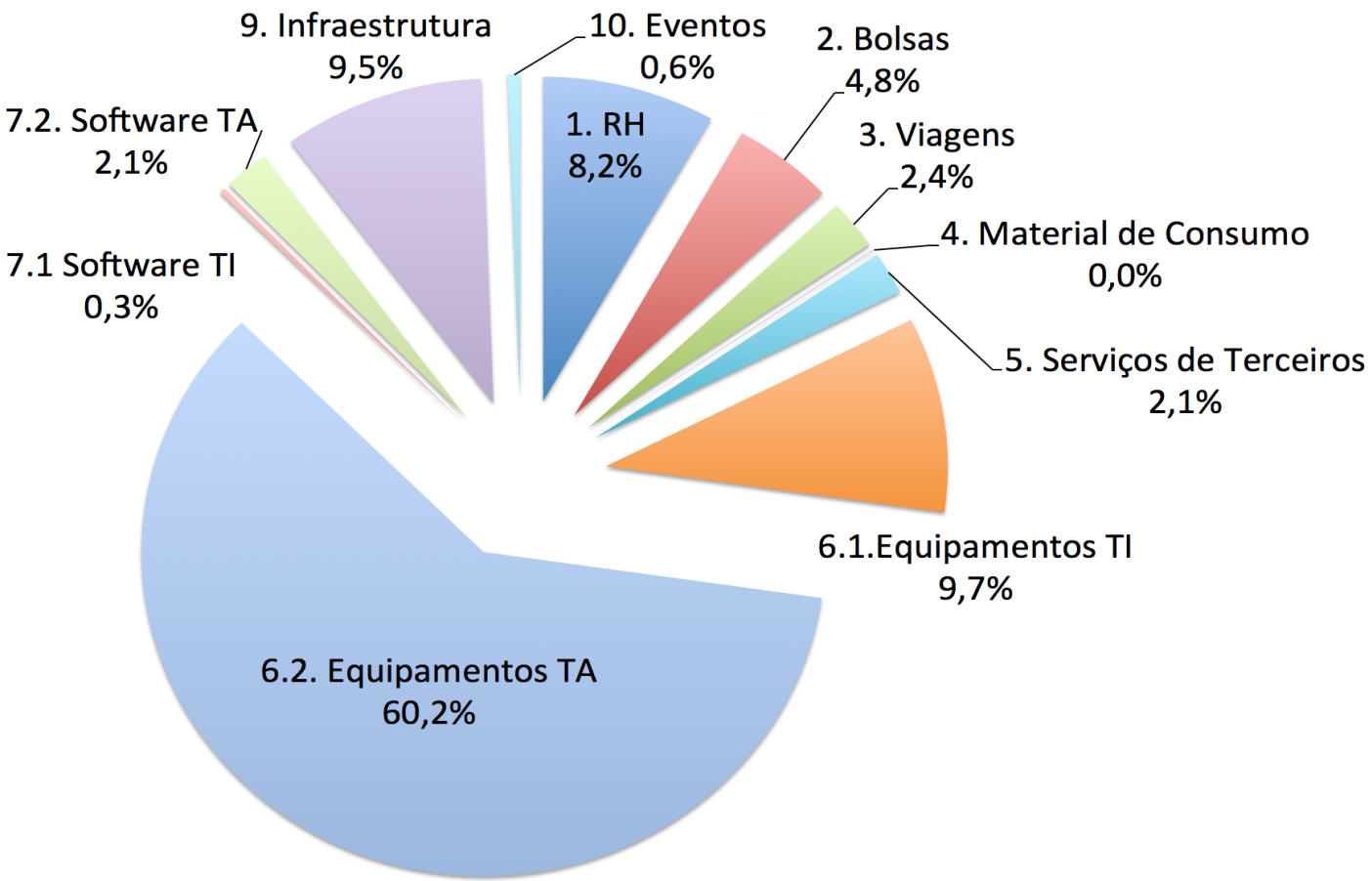
• Criar modelos de configurações padronizadas de segurança;

• Testar topologias no campo da segurança cibernética aplicada a dispositivos de automação e operação (relés e RTU - *Remote Terminal Units*) em uma réplica de sistemas elétricos;

• Testar novos firmwares antes de aplicar em campo;

• Testar e ensaiar novos equipamentos no que tange à segurança cibernética, autonomamente ao invés de contratar.

Projeto LaSC – Resumo da aplicação de recursos financeiros em percentual por natureza de despesa



Projeto LaSC – Resumo das Atividades Realizadas

- Concepção da estrutura do Laboratório de Segurança Cibernética (LaSC) – Módulos IME e PTI;
- Infraestrutura para instalação do LaSC – Módulos IME e PTI;
- Especificação de materiais e equipamentos para aquisição;
- Programa Doutorado Acadêmico para Inovação – DAI/CNPq;
- Alinhamento das pesquisas realizadas pelo IME, voltadas para o projeto, em nível mestrado e doutorado;

Projeto LaSC – Resumo das Atividades Realizadas

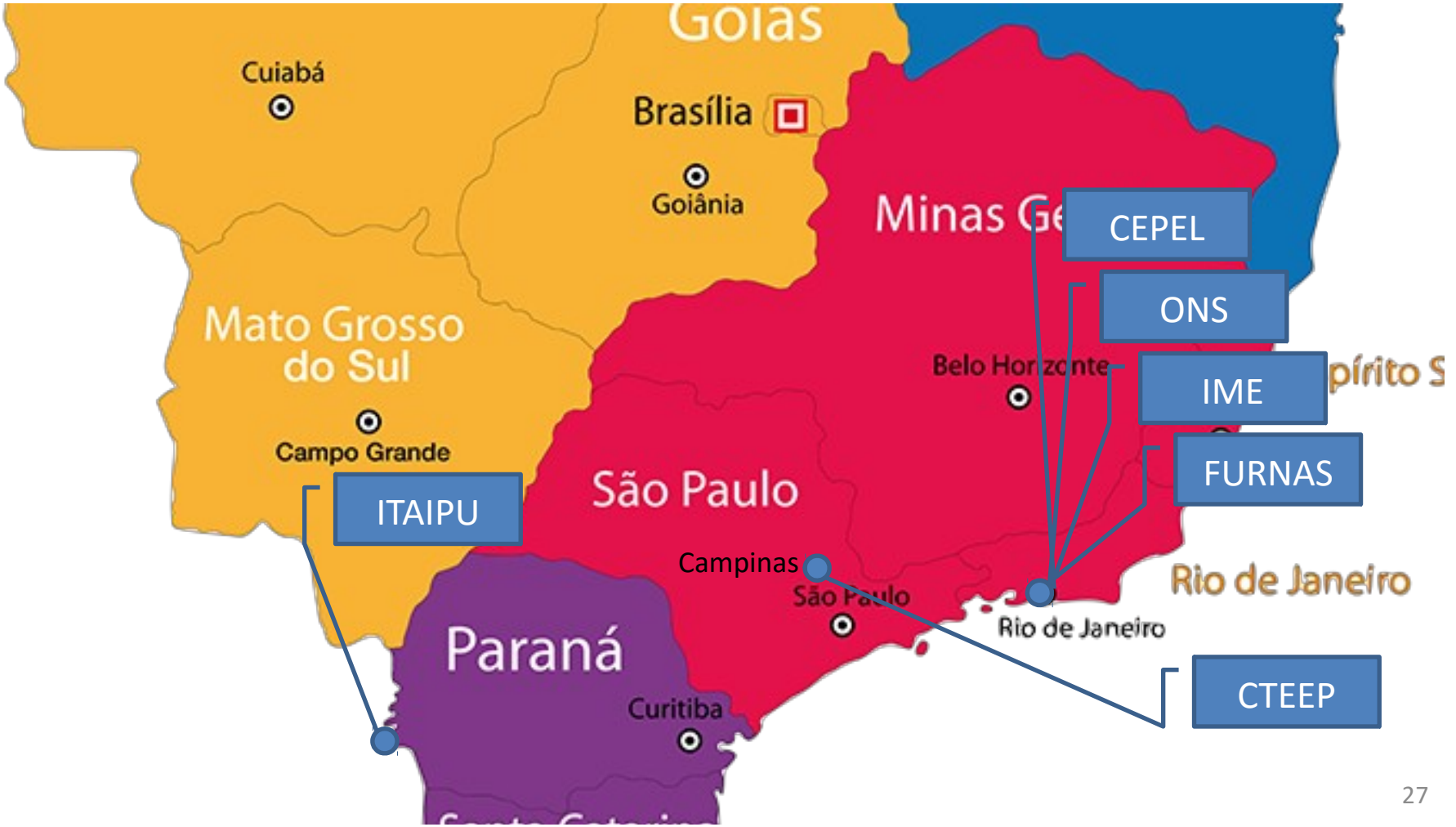
- Análises sobre a utilização do computador de alto desempenho em estudos e pesquisas do projeto;
- Estabelecimento de parcerias:

COPPE – UFRJ: Pesquisas conjuntas na área de automação/segurança cibernética.

ONS: Cooperação técnico-científico e interligação de simuladores RTDS e OPAL.

Cepel: Cooperação técnico-científica e do uso do programa SAGE, além de outros softwares voltados ao SEP.

ONS – Integração de Centros de Simulação em Tempo Real



Ações necessárias:

- Levantar os ativos de Itaipu – atualização tecnológica;
- Fomentar a formação de recursos humanos nas diversas áreas;
- Manter constante aperfeiçoamento do pessoal;
- Manter um canal de ligação permanente com Itaipu no que tange à segurança cibernética;
- Buscar “independência” na questão de Segurança Cibernética.


Ministério da Defesa
Exército Brasileiro
BRAÇO FORTE - MÃO AMIGA
PTI
Parque Tecnológico
Itaipu
ITAIPU
BINACIONAL

OBRIGADO!