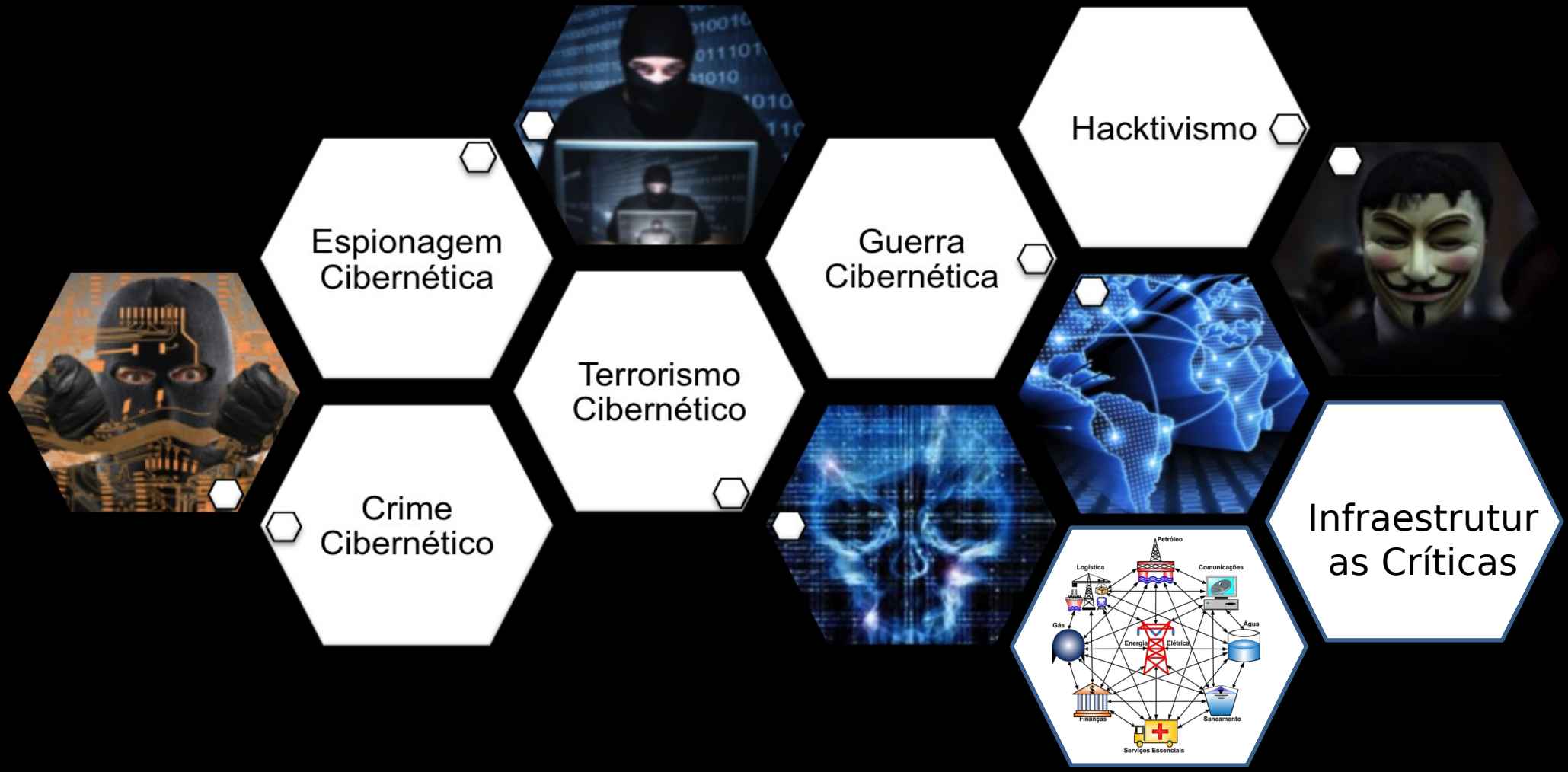
Exercício Guardião Cibernético:
Um estudo de caso de sucesso no Brasil

GTER 48 | GTS 34

34ª GTS - Grupo de Trabalho em Segurança de Redes

Major Campos – Comando de Defesa Cibernética (ComDCiber)

CENÁRIO CIBERNÉTICO



Níveis de Decisão e Atores

NÍVEL POLÍTICO – PRESIDÊNCIA DA REPÚBLICA
(SEGURANÇA DA INFORMAÇÃO, SEGURANÇA CIBERNÉTICA E
SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS)

NÍVEL ESTRATÉGICO – MD, EMCFA E FORÇAS
(DEFESA CIBERNÉTICA)

NÍVEL OPERACIONAL– COMANDO OPERACIONAL
(GUERRA CIBERNÉTICA)

NÍVEL TÁTICO – F Cj G Ciber
(GUERRA CIBERNÉTICA)

Doutrina Militar de Defesa Cibernética – MD31-M-07, Pag.

Ameaça real às IEC (Segurança Nacional)

Russian hackers in 2016 cyber attack on Ukraine's power grid intended to damage transmissions stations

The attack that blacked out most of the capital city Kyiv was intended to cause physical damage, claims new report

Alto grau de sofisticação:

- Ataque integrado
- Altamente coordenado
- Sofisticação logística
- Mais de 6 meses no ambiente

Analysis of the Cyber Attack on the Ukrainian Power GridDefense Use CaseMarch 18, 2016
Disponível em: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Ameaça real às IEC (Segurança Nacional)

US $ 10 milhões foram roubados do Banco do Chile e canalizados para uma conta em Hong Kong

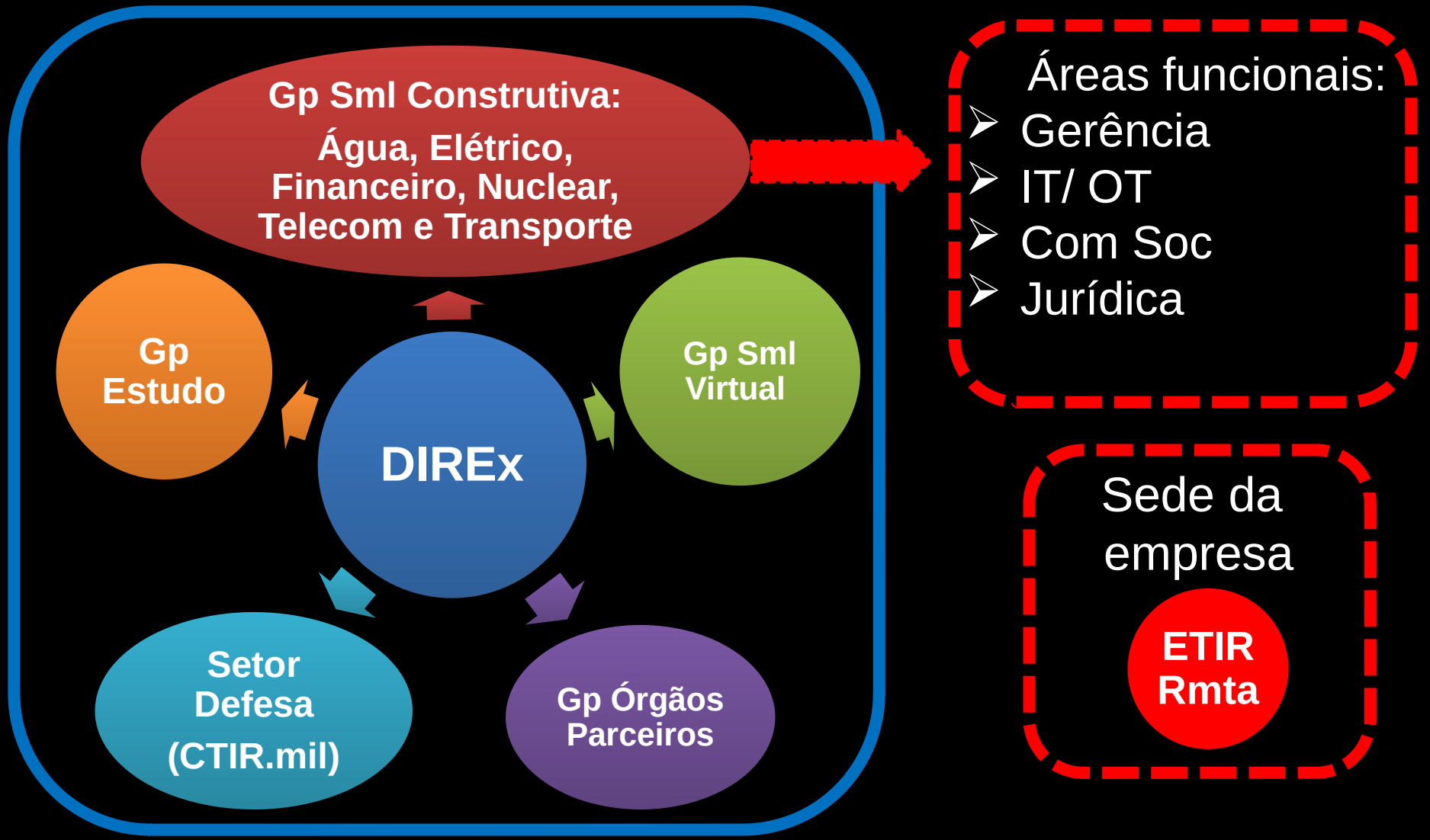
*Em 24 de maio houve um ciberataque contra a maior instituição financeira do Chile, que supostamente destruiu 9.000 estações de trabalho e 500 servidores, acredita-se que o objetivo do ataque foi comprometer os endpoints que lidam com transações na rede **SWIFT**.*

No domingo, o gerente-geral do banco, Eduardo Ebensperger, disse à mídia chilena *Latercera* que o ataque no final de maio permitiu que hachers completassem quatro transações fraudulentas no sistema SWIFT antes que o ataque fosse descoberto.

"Encontramos algumas transações estranhas no sistema SWIFT (onde os bancos remetem internacionalmente suas transações para diferentes países)", disse Ebensperger à emissora Chilena. "Então percebemos que o vírus não era necessariamente o problema subjacente, mas aparentemente os atacantes queriam defraudar o banco".

Eduardo Ebensperger – Foto: Latercera

CONCEPÇÃO DO EXERCÍCIO



Áreas funcionais:

- Gerência
- IT/ OT
- Com Soc
- Jurídica

Sede da empresa

ETIR Rmta

TIMELINE

Apresentação das primeiras impressões do EGC

DIREX

- Acompanhamento *online* (RT) dos problemas simulados de 41 organizações e empresas
- Eventos *table-top* estratégicos propostos pelas IEC

Simulação Construtiva

- Atuação colaborativa e integrada de especialistas nas áreas de IT, Com Soc, Jurídica e Alta Adm das empresas/ organizações
- Validação do PNTIR

Simulação Virtual

- Cooperação entre CIGE e SERPRO
- Atuação integrada nos setores estratégicos
- Identificação de vulnerabilidades e *report* para correção de falhas nas redes emuladas

Ativação do "Gabinete de Crise de Topázio"

- Participação de representantes de órgãos do Governo e da Defesa
- Deliberação sobre ações integradas em caso de paralisia estratégica no país

Grupo de Estudo

- **St Financeiro:** Avaliação de riscos do setor financeiro com abrangência nacional baseada em cenários de ameaças
- **St Nuclear:** Desenvolvimento e implementação de Marco Regulatório para a Segurança Cibernética do Setor Nuclear
- **St Elétrico:** Prática e Implementação do modelo do NIST Cybersecurity Framework
- **St Telecom:** Proteção contra ataques de interceptação telemática

Observadores de Nações Amigas

FIDC

IAEA

FINANCIAL SERVICES Information Sharing and Analysis Center

CCDCOE
NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

EMBRAER

SAAB

Visita da Comissão de Relações Exteriores e Defesa Nacional

SENADO FEDERAL

REUNIÕES SETORIAIS DE COORDENAÇÃO NA FASE PREPARATÓRIO

NÍVEIS DE DECISÃO

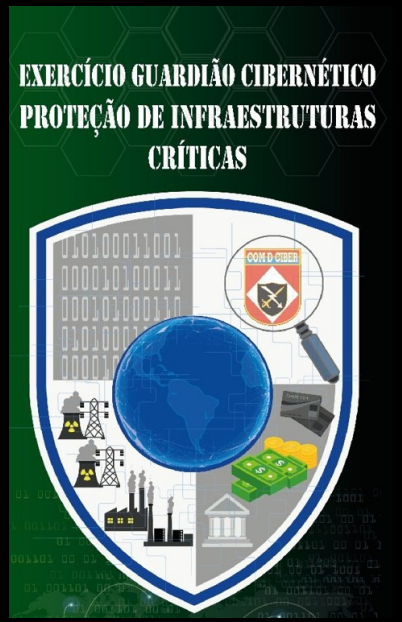
GUARDIÃO CIBERNÉTICO 1.0 - 3 a 6 de julho de 2018

COM D CIBER

Gabinete de Segurança Institucional
DA PRESIDÊNCIA DA REPÚBLICA

MARINHA DO BRASIL

MINISTÉRIO DA DEFESA



41 ORGANIZAÇÕES → 215 PARTICIPANTES E OBSERVADORES

Setor Elétrico

ITAIPU BINACIONAL
isa CTEEP
ONS Operador Nacional do Sistema Elétrico
FURNAS

Órgãos Parceiros

Agência Brasileira de Inteligência
Polícia Federal
CTIR Gov
cert.br
ANEEL Agência Nacional de Energia Elétrica
Ministério das Relações Exteriores
RNP
SERPRO

Setor Nuclear

SIPRON Sistema de Proteção ao Programa Nuclear Brasileiro
Eletrobras Eletronuclear
USP Universidade de São Paulo
IAEA
INB
CNEN Comissão Nacional de Energia Nuclear

Grupo de Observadores

EGC 2.0

(2019)

Telecomunicações

ANATEL
TIM
Claro
oi
Telefônica
TELEBRAS

Defesa

COM D CIBER

Setor Financeiro

BANCO CENTRAL DO BRASIL
cip
[B]3
Santander
FEBRABAN Federação Brasileira de Bancos
CAIXA
CVM
Itaú

VÍDEO

https://www.youtube.com/watch?v=a30GvHuYD64

Fonte: Site EB

OBJETIVOS ALCANÇADOS

GABIENTE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA

Secretaria de Coordenação de Sistemas

Departamento de Segurança de Informação e Comunicações

Coordenação Geral do Centro de Tratamento de Incidentes de Redes do Governo

Relatório da 1ª Oficina de Construção do Plano de Tratamento e Respostas a Incidentes de Redes

Data: 27 de Setembro de 2018.

COLABORAÇÃO DO EGC NOS SETORES ESTRATÉGICOS

BANCO CENTRAL DO BRASIL

FEBRABAN
FEDERAÇÃO BRASILEIRA DE BANCOS

- Comitê Executivo de Seg Ciber
- SOC do St Financeiro
- Criação do ITSec

COLABORAÇÃO DO EGC NOS SETORES ESTRATÉGICOS

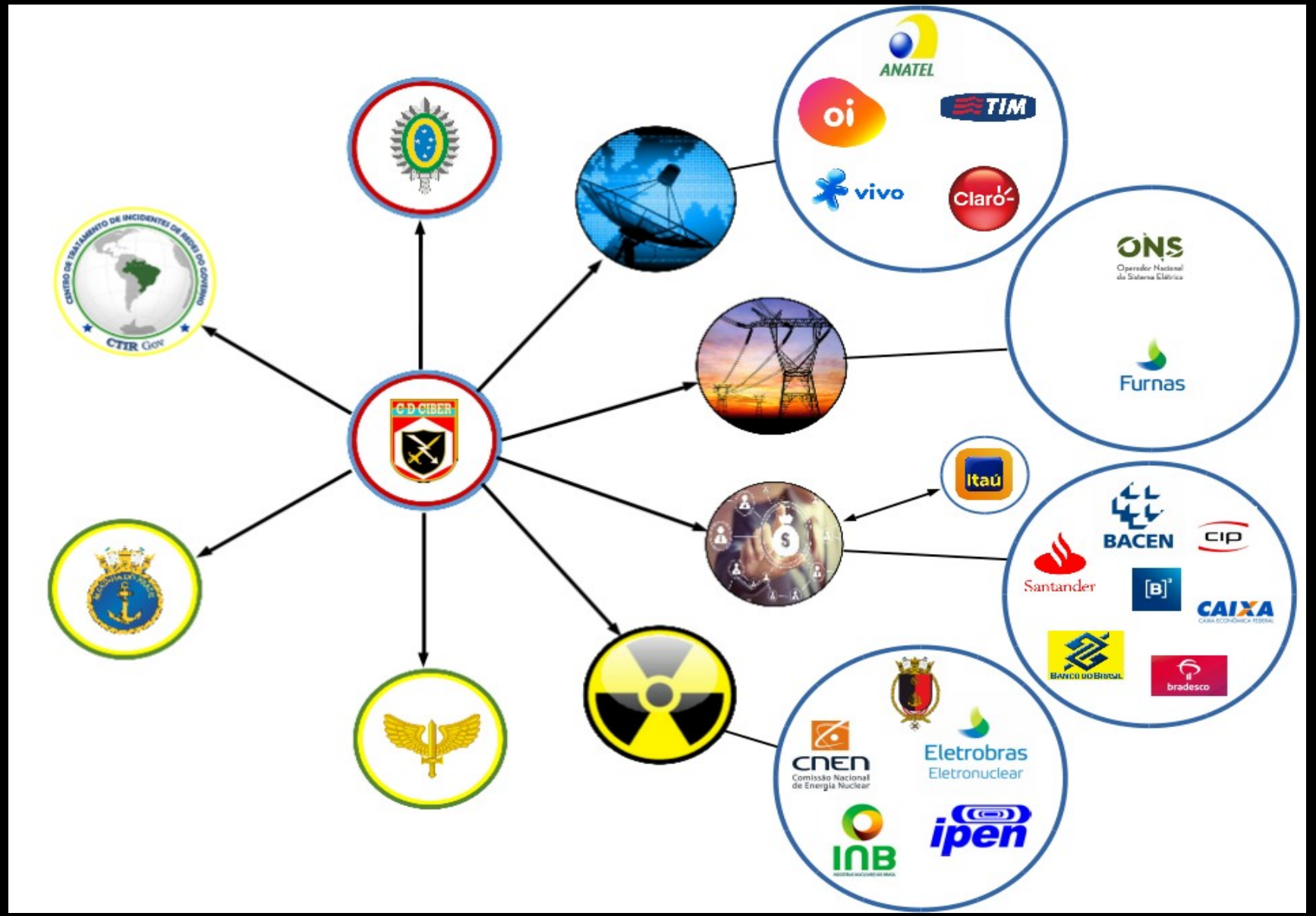
ONS
Operador Nacional do Sistema Elétrico

- Estudos para NOC/SOC em ambiente de automação SOC do St Financeiro
- Subsídios para Procedimento de Rede de Segurança Cibernética no Setor Elétrico

GUARDIÃO CIBERNÉTICO 2.0

WORKSHOP EM GESTÃO DE RISCOS CIBERNÉTICOS

MISP - Malware Information Sharing Platform and Threat Sharing



Setor Defesa

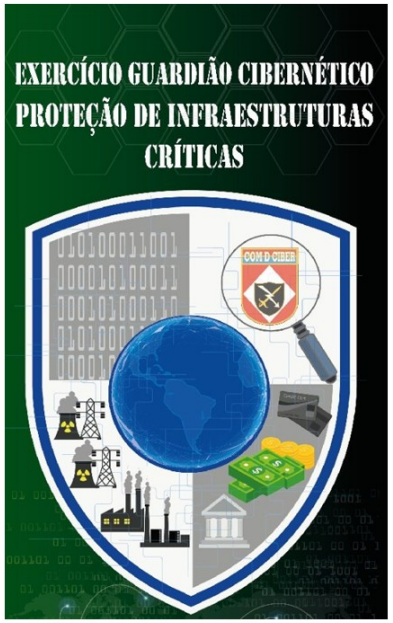
Cooperação entre o CTIR.mil e as infraestruturas críticas

REPERCUSSÃO DO EGC NOS SETORES ESTRATÉGICOS

Eletrobras
Eletronuclear

IAEA
International Atomic Energy Agency

Eletronuclear and The Cyber Guardian Exercise



The Cyber Guardian Exercise Logo
Image Source: Brazilian Army - ComDCiber

From July, 3rd to 6th 2018, Eletronuclear attended the first edition of the Cyber Guardian Exercise, that was an initiative by Brazilian Army, under Cyber Defense Command (ComDCiber) coordination, being a collaborative action in order to share experiences and technical skills in Cybersecurity as well as promote tight integration among Nuclear Energy, Finance and National Defense sectors on critical infrastructures protection.

The Cyber Guardian Exercise also had academic community participation and other government agencies of support or associated with cybernetic protection of the State and Brazilian society.

Simulador de Planta Nuclear

- Cooperação entre Defesa, Indústria, Governo e USP
- Lançamento mundial do Simulador, com a presença de pesquisador da AIEA

IAEA

Universidade de São Paulo

PREPARAÇÃO

Concepção EGC 2.0 - AGO 2018

1ª Reu Coor St 12 a 14 SET 2018

IPC 09 OUT 2018

2ª Reu Coor St 12 a 14 NOV 2018

3ª Reu Coor St 25 a 27 FEV 2019

Reu Intersetores 28 FEV 2019

4ª Reu Coor St 22 a 26 ABR 2019

Workshop e FCC 07 MAIO 2019

5ª Reu Coor St 5 a 7 JUN 2019

OBJETIVOS

Execução 2 a 4 JUL 2019

ATUAÇÃO COLABORATIVA

NORMATIVAS

PNTIR

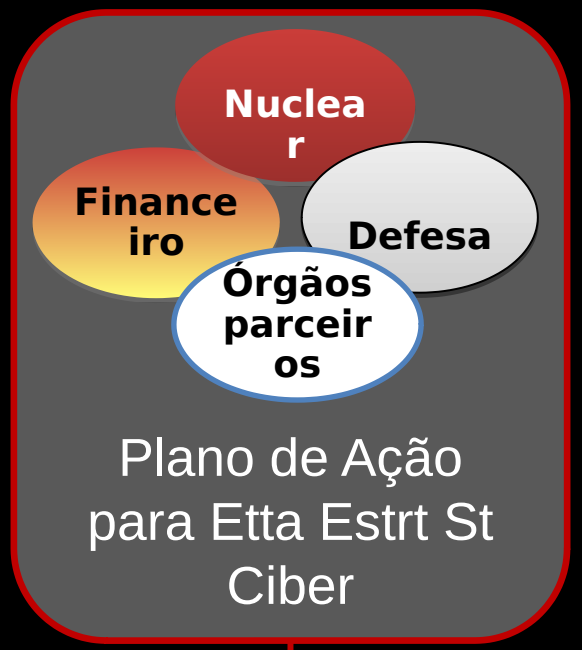
PROTEÇÃO IEC

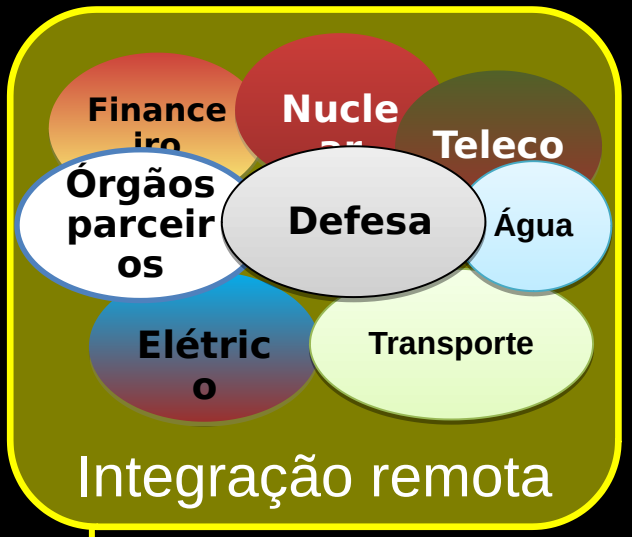
NIST CYBERSECURITY FRAMEWORK

MISP Threat Sharing


PREPARAÇÃO
OBJETIVOS
Concepção FGC
1ª Reu Coor St
IPC
ecução
JUL
TIVA
D IEC
Materializa a cooperação e integração entre o SMDC e a proteção de IEC para a Defesa Nacional
4ª Reu Coor St
22 a 26 ABR 2019
Workshop e FCC
07 MAIO 2019
5ª Reu Coor St
5 a 7 JUN 2019
RITY FRAMEWORK
MISP
Threat Sharing

Evolução do Guardião Cibernético





EGC 1.0 - 2018

EGC 2.0 - 2019

EGC 3.0 - 2020

EVOLUÇÃO DO EGC 3.0

Hub em SP

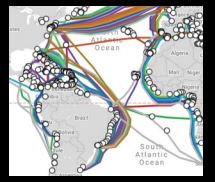
Sml Virtual remota

IEC Água e Transporte

2º Workshop Gestão Riscos Ciber

Cyber Law Toolkit e
Sml Planta Nu

Cenários “próxima década”
(Intlg Artificial, 5G, Comp Quântica, Criptomoeda, IoT...)



Cyber Hygiene
(Conscientização Seg Ciber)

Estrt Nac Seg Ciber
(alinhamento)

30 JUN a 02 JUL de 2020

Exercício Guardião Cibernético:
Um estudo de caso de sucesso no Brasil

GTER 48 | GTS 34

34ª GTS - Grupo de Trabalho em Segurança de Redes

Major Campos – Comando de Defesa Cibernética (ComDCiber)