“Oficina “EQUIPES DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS – ETIR“ 2018

Brasília – 15 de agosto de 2018

CDCIBER

ENAP

RNP
REDE NACIONAL DE ENSINO E PESQUISA

CENTRO DE TRATAMENTO DE INCIDENTES DE REDES DO GOVERNO
CTIR Gov

GSI-PR
DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

CAIS Centro de Atendimento a Incidentes de Segurança

Coordenação-Geral de Gestão de Segurança da Informação

Palavras do Diretor do DSIC

CENTRO DE TRATAMENTO DE INCIDENTES DE REDES DO GOVERNO

“Tratamento de Incidentes de Redes de Governo”

Brasília – julho de 2018

CTIR Gov

Democlydes Carvalho
Coordenador-Geral

Programação da Manhã

8:30 – 9:00	Credenciamento
9:00 – 9:30	Abertura e Ambientação – Cel Fontenele e Major Democlydes
9:30 – 10:00	MISP - Major Godinho
10:00 – 10:10	Perguntas – Major Godinho
10:10 – 10:40	NORMAS DSIC - Alexandre Santos
10:40 – 11:00	Break
11:00 – 11:45	Tratamento de Incidentes – Maurício Leite
11:45 – 12:00	Exercícios – Alexandre e Perguntas CTIR Gov

Ambientação

CTIR GOV: HISTÓRICO, SERVIÇOS E PARCERIAS

Papel dos CSIRTs

- **A redução do impacto de um incidente é consequência:**
  - da agilidade de resposta
  - da redução no número de vítimas
- **O papel do CSIRT é:**
  - auxiliar a proteção da infraestrutura e das informações
  - prevenir incidentes e conscientizar sobre os problemas
  - auxiliar a detecção de incidentes de segurança
  - responder incidentes – retornar o ambiente ao estado de produção

Fonte: cert.br

CSIRT

- **CSIRT (*Computer Security Incident Response Team*)**
- Acrônimo internacional para designar um Grupo de Resposta a Incidentes de Segurança, responsável por tratar incidentes de segurança para um público alvo específico.
- Pode ser um serviço prestado por uma empresa especializada ou uma unidade da própria empresa.
- Outros acrônimos: IRT, CIRC, CIRT, SERT, SIRT, CERT®.
- No Brasil também são usados: CTIR, ETIR, CAIS, GRA...

Fonte: cert.br

Papel dos CSIRTs

- **O sucesso depende da confiabilidade**
  - nunca divulgar dados sensíveis nem expor vítimas, por exemplo.

- **O CSIRT não é "investigador"**
  - foco é entender "**o que**" o que aconteceu, não "**quem**" originou a ação
    - ferramentas muitas vezes são as mesmas da investigação e da perícia
  - naturalmente pode identificar possíveis crimes e então:
    - atuar na preservação de evidências
    - auxiliar investigações posteriores, dependendo de sua missão

Fonte: cert.br

Termos Comuns

- **Incidente de Segurança em Computadores** – qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.
- **Tratamento de Incidentes (*Incident Handling*):** o processo de receber, triar, analisar e **responder** um incidente.
- **Artefato Malicioso:** é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizados ou interromper o funcionamento de sistemas e/ou redes de computadores
- **Público Alvo:** Comunidade ou *Constituency*. Conjunto de pessoas, setores, órgãos ou entidades atendidas por uma ETIR.
- **Notificação de Incidente:** informar eventos ou incidentes para uma ETIR ou grupo de segurança.
- **Vulnerabilidade:** qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa ou ocorrência de incidentes.

Evolução histórica: Tratamento de Incidentes no Brasil

- **Agosto/1996**: o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil" é publicado pelo CGI.br (1)
- **Junho/1997**: o CGI.br cria o CERT.br (naquele tempo chamado NBSO – NIC BR Security Office), com base nas recomendações do relatório, como um grupo com responsabilidade nacional (2)
- **Agosto/1997**: a RNP cria seu próprio CSIRT (CAIS) (3), seguida pela rede acadêmica do Rio grande do Sul (CERT-RS) (4)
- **1999**: o SERPRO cria o G.R.A. (Grupo de Respostas a Ataques), assim como outras instituições, incluindo Universidades e Operadoras de Telecomunicações, iniciaram a formação de seus CSIRTs
- **2002–2004** : grupos de trabalho para definição da estrutura de um CSIRT para a Administração Pública Federal
- **2004**: o CTIR-Gov foi criado, com a Administração Pública Federal como seu público alvo (5)

1 http://www.nic.br/pagina/grupos-de-trabalho-documento-gt-s/169
2 http://www.nic.br/pagina/gts/157
3 http://memoria.rnp.br/_arquivo/documentos/rel-rnp98.pdf
4 http://www.cert-rs.tche.br/index.php/missao
5 http://www.ctir.gov.br/sobre-CTIR-gov.html

Fonte: cert.br

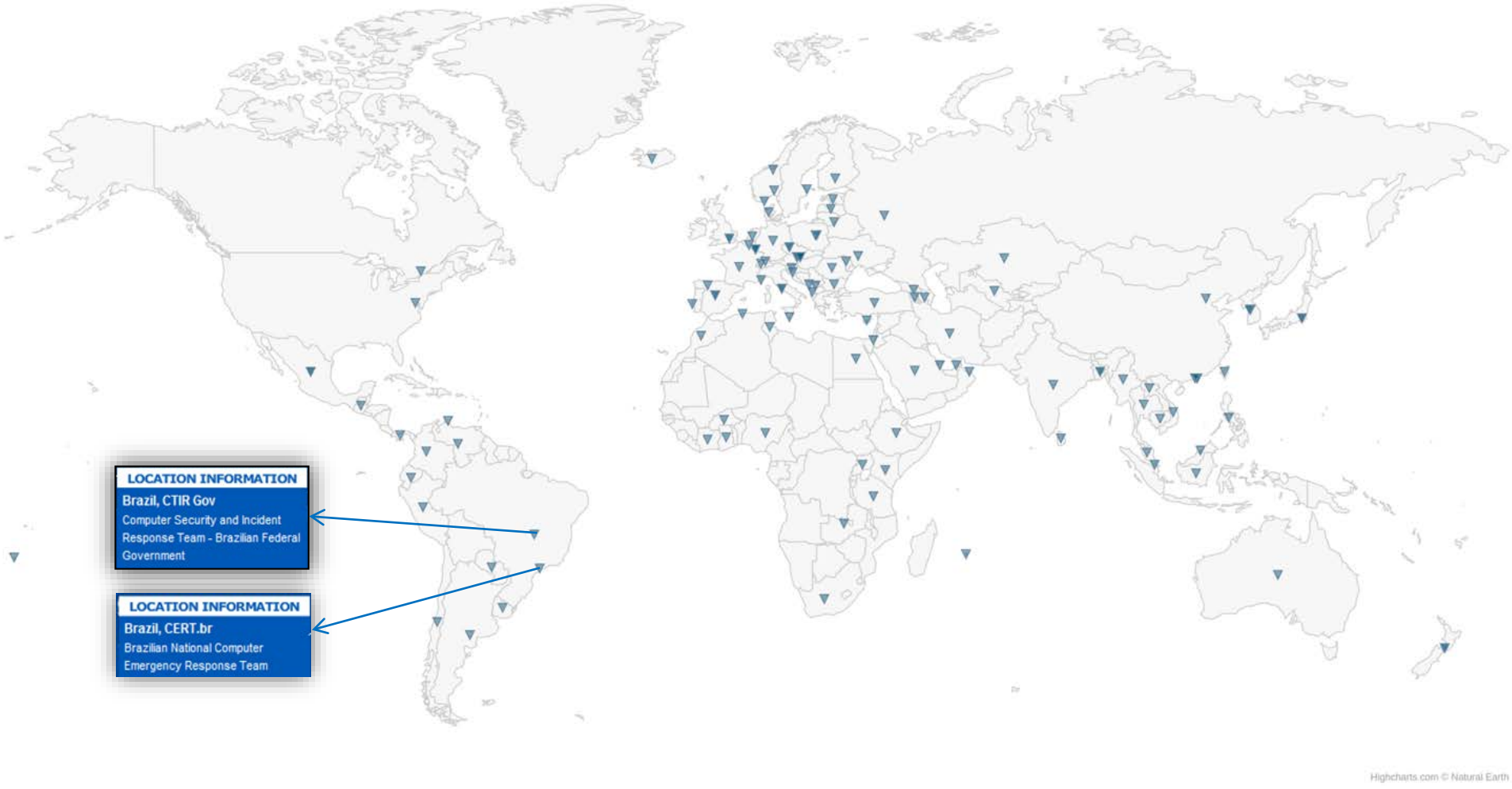
Detalhes da Criação

- Ago / 2004: Grupo de Trabalho no GSI conclui que é necessário criação **CSIRT** de coordenação para a **APF**;
- Dez / 2004: **Informalmente**, uma equipe é alocada para iniciar atividades de **tratamento de incidentes**;
- Mai / 2006: Decreto cria **DSIC** e enquadrou a Coordenação-Geral de Tratamento de Incidentes de Rede (CGTIR);
- Nov / 2006: Portaria dá **competências** e **denomina** a CSIRT da APF de **CTIR Gov**;

Histórico e Maturidade

2018	**Padronização** dos processos de tratamento de incidentes e **maior aproximação** com o público alvo e parceiros . **=> Cooperação / Compartilhamento / Comunicação / Confiança**
2016	Melhoria dos processos automatizados visando obter melhor performance, e atualizar a documentação dos processos existentes.
2014	**Implantação do Data Warehouse** de Incidentes integrado ao Sistema automatizado de incidentes.
2012	Aperfeiçoamento dos processos, ampliação do número de serviços oferecidos pelo CTIR Gov à APF e intensificação de trocas de informação com parceiros
2010	**Implantação do RT** (*Request Tracker*) como ferramenta para suportar o modelo de negócios do CTIR Gov
2008	Criação do "Modelo de melhoria de qualidade baseado em processos para tratamento de incidentes de rede na APF"
2006	**Competências** da CGTIR publicadas em Portaria Ministerial

CSIRTs com Responsabilidade Nacional

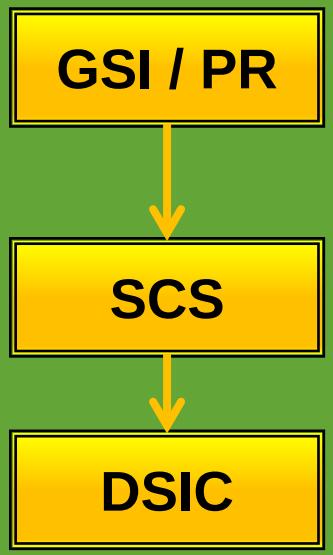


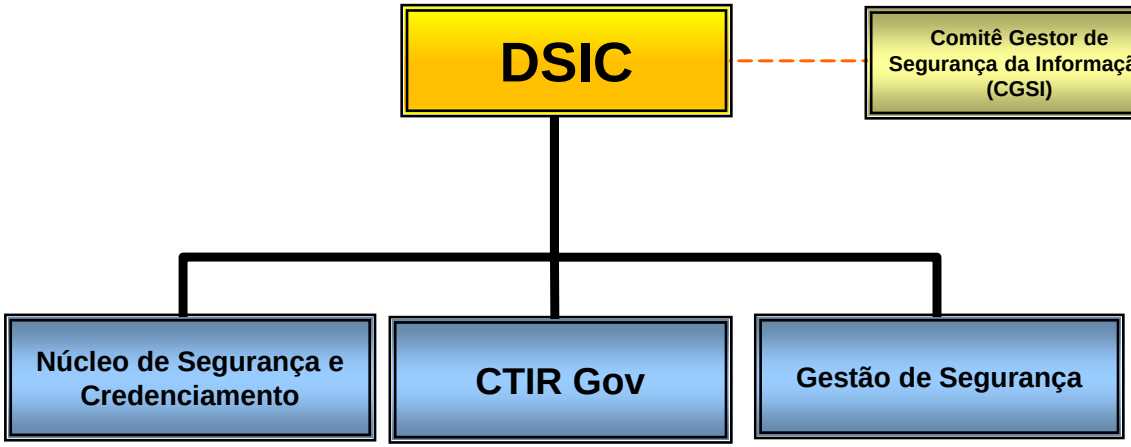
Fonte: https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/national-csirts/

Coordenação Nacional

- O CTIR Gov atua como **Centro de Coordenação Nacional**, trabalhando de forma colaborativa e **não tem a intenção de concorrer com as ETIR** dos órgãos APF, Estados e órgãos vinculados.
- Os órgãos e entidades da APF deverão **comunicar de imediato a ocorrência dos incidentes** de segurança nas redes de computadores ao CTIR Gov, com vistas a permitir que sejam dadas soluções integradas para a APF, bem como a geração de estatísticas (**NC n° 05 e 08 - DSIC/GSIPR**).
- O CTIR Gov **não realiza** procedimentos de **investigação criminal**. Eventuais desdobramentos dos incidentes são encaminhados às autoridades policiais competentes.

Estrutura do CTIR Gov





LEI Nº 10.683, de 28 de maio e 2003
(Organização da PR e dos Ministérios)

"Art. 6º Ao Gabinete de Segurança Institucional da Presidência da República compete:

.....

VI - coordenar as atividades de segurança da informação e das comunicações; (atualização de redação dada pela Lei nº 13.341, de 2016)

.....

Decreto Nº 9.031, de 12 de abril de 2017 **ANEXO I - Art. 11.**
Ao Departamento de Segurança da Informação e Comunicações compete:

.....

III - manter o centro de coordenação de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal.

.....

Competências do CTIR Gov

PORTARIA Nº 91, DE 26 DE JULHO DE 2017 - Regimento Interno do GSI/Pr

Art. 32. À Coordenação-Geral do Centro de Tratamento de Incidentes de Redes do Governo (CGCTIR) compete:

I - operar e manter o Centro de Tratamento de Incidentes de Redes do Governo (CTIR Gov);

II - promover o intercâmbio científico-tecnológico relacionado a incidentes de redes de computadores junto a outros centros;

III - apoiar órgãos e entidades do governo nas atividades de tratamento de incidentes de redes de computadores;

IV - acompanhar e analisar tecnicamente os incidentes de segurança nas redes do governo;

V - implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança nas redes do governo;

VI - apoiar, incentivar e contribuir no âmbito do governo para a capacitação no tratamento de incidentes de segurança em redes de computadores;

VII - orientar os administradores de redes do governo quanto aos procedimentos de proteção e recuperação de incidentes de rede, bem como quanto à redução de riscos, prevenção de ameaças e vulnerabilidades cibernéticas;

VIII - pesquisar e analisar possíveis impactos de vulnerabilidades e falhas de segurança de redes do governo;

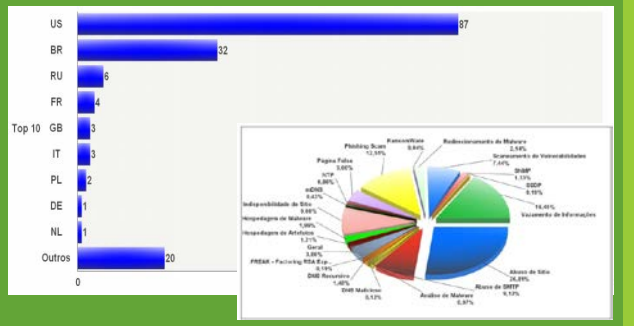
IX - expedir alertas, recomendações, relatórios técnicos e relatórios estatísticos de incidentes de redes do governo;

X - armazenar e analisar informações relativas a ameaças e tendências de vulnerabilidades cibernéticas;

XI - orientar as equipes de tratamento de incidentes de redes do governo na verificação da conformidade dos controles estabelecidos de segurança da informação; e

XII - realizar outras atividades determinadas pelo Diretor do DSIC.

Serviços



CENTRO DE TRATAMENTO DE INCIDENTES DE REDES DO GOVERNO
CTIR Gov

Tratamento de Incidentes

- Coordenação
- Notificação
- Suporte

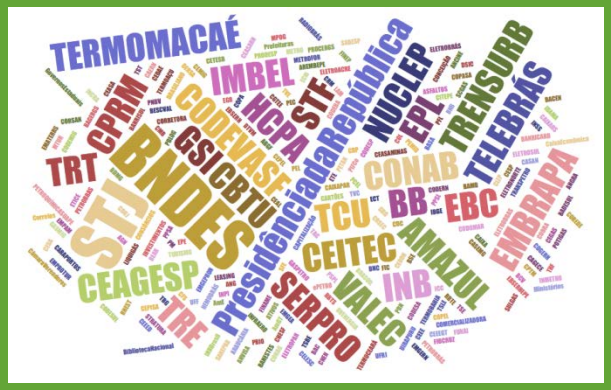
Sensibilização

- Oficinas e Colóquios Técnicos
- Normas e Padrões
- Apresentações e Visitas

Análise de Tendências e Estatísticas

- *Honeypots* Distribuídos
- Sensores de Detecção
- Alertas e Estatísticas

Atuação



Atuação em Grandes Eventos

- Rio+20 (2012)
- Copa das Confederações (2013)
- Jornada Mundial da Juventude (2013)
- Copa do Mundo FIFA (2014)
- Jogos Olímpicos RIO (2016)

Publico Alvo

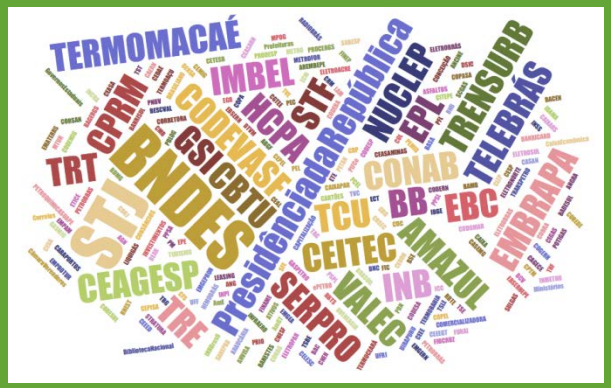
Órgãos de Governo:

- das esferas Federal, Estadual e Municipal
- dos poderes Executivo, Judiciário e Legislativo

Principais Domínios

*.gov.br, *.mil.br, *.jus.br, *.leg.br, *.mp.br e *.def.br

Atuação



Participação em Eventos, Grupos de Trabalhos e Fóruns

- OEA – Comitê Interamericano de Contraterrorismo
- FIRST – Nat CSIRTs
- LACNIC - – Reunião de Grupos de Segurança e Resposta a Incidentes (CSIRT) da América Latina e Caribe
- Fórum Brasileiro de CSIRTs
- DISI
- FEBRABAN – GT Fraudes
- Fórum de CSIRTs do CERT.br
- Defesa – GT Inter Forças
- Reuniões Coordenação do SISP
- Fórum do *National Cybersecurity and Communications Integration Center* (NCCIC)

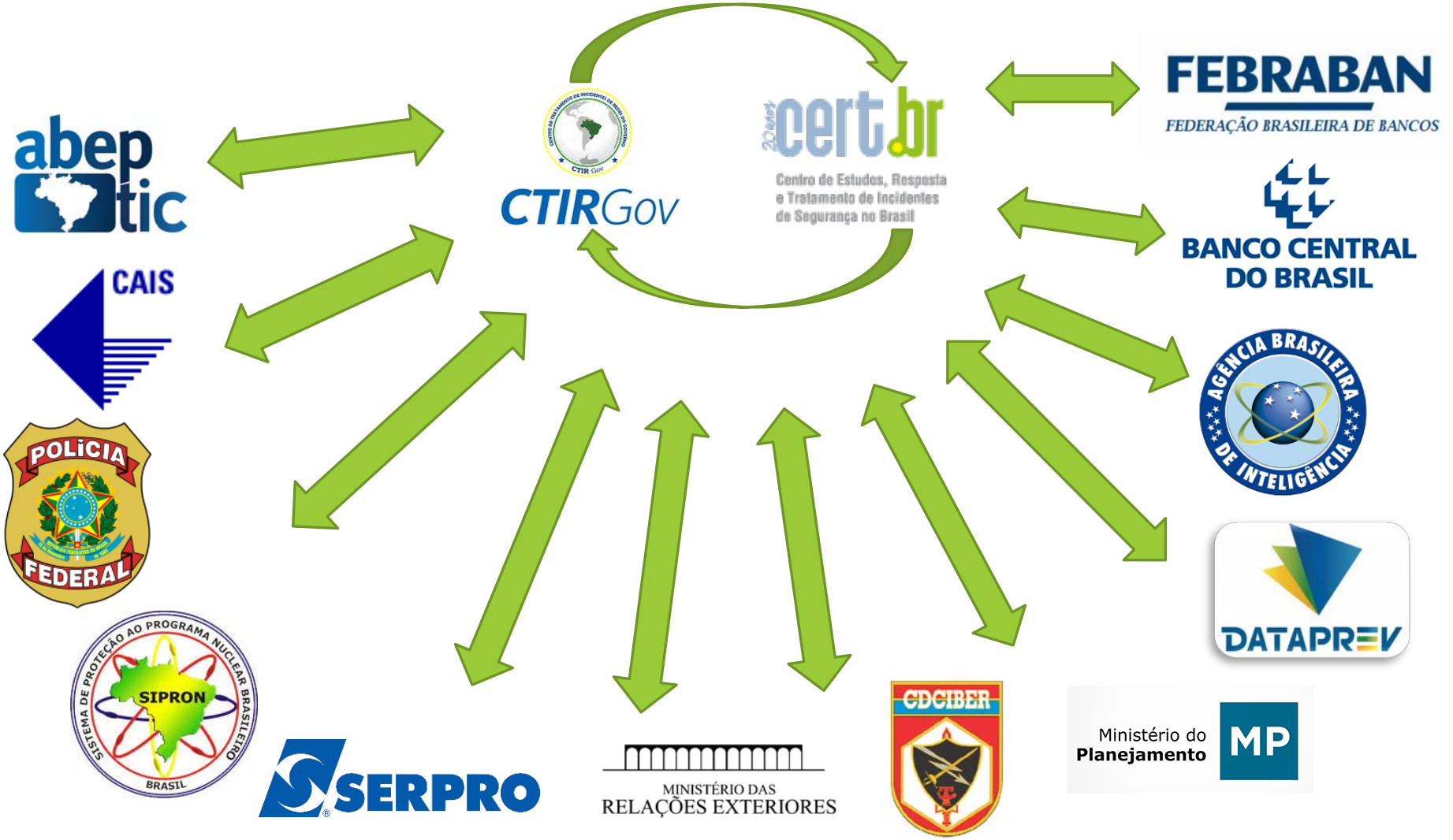
- Atualização técnica e operacional.
- Articulação institucional.
- Aumento do contato e consequentes ações de atendimento por parte dos representantes de AS (Sistemas Autônomos).
- Representatividade e reconhecimento internacional.
- Aumento na demanda de notificações de incidentes.
- Velocidade na ciência de eventos cibernéticos.

Atuação

Promoção de Eventos e atividades.

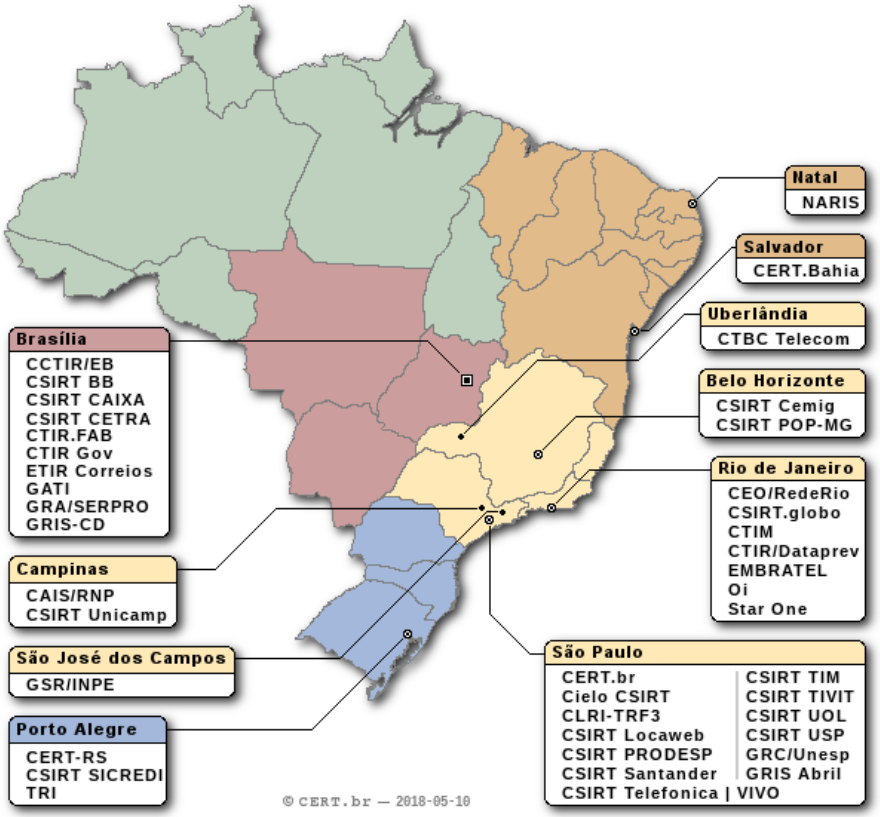
- Oficinas e Colóquios Técnicos.
- Visitas de Orientação Técnica.
- Levantamento para publicação do relatório OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE, mantido pela OEA e BID, levantado por pesquisados da Universidade de Oxford
- Exercício Cibernético Guardião Cibernético I.
- Grupo de Trabalho da Plataforma MISP (Plataforma de compartilhamento de ameaças livre e de código aberto que ajuda no compartilhamento de informações sobre inteligência de ameaças, incluindo indicadores de segurança cibernética).
- Encontro Regional de CSIRTs das Américas.
- Criação do GT para elaboração do Plano Nacional de Gestão e Resposta a Incidentes de Redes.

Parcerias


abep tic
CAIS
POLÍCIA FEDERAL
SISTEMA DE PROTEÇÃO AO PROGRAMA NUCLEAR BRASILEIRO
SIPRON
BRASIL
SERPRO
CTIRGov
cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
MINISTÉRIO DAS RELAÇÕES EXTERIORES
CDCIBER
FEBRABAN
FEDERAÇÃO BRASILEIRA DE BANCOS
BANCO CENTRAL DO BRASIL
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA
DATAPREV
Ministério do Planejamento
MP

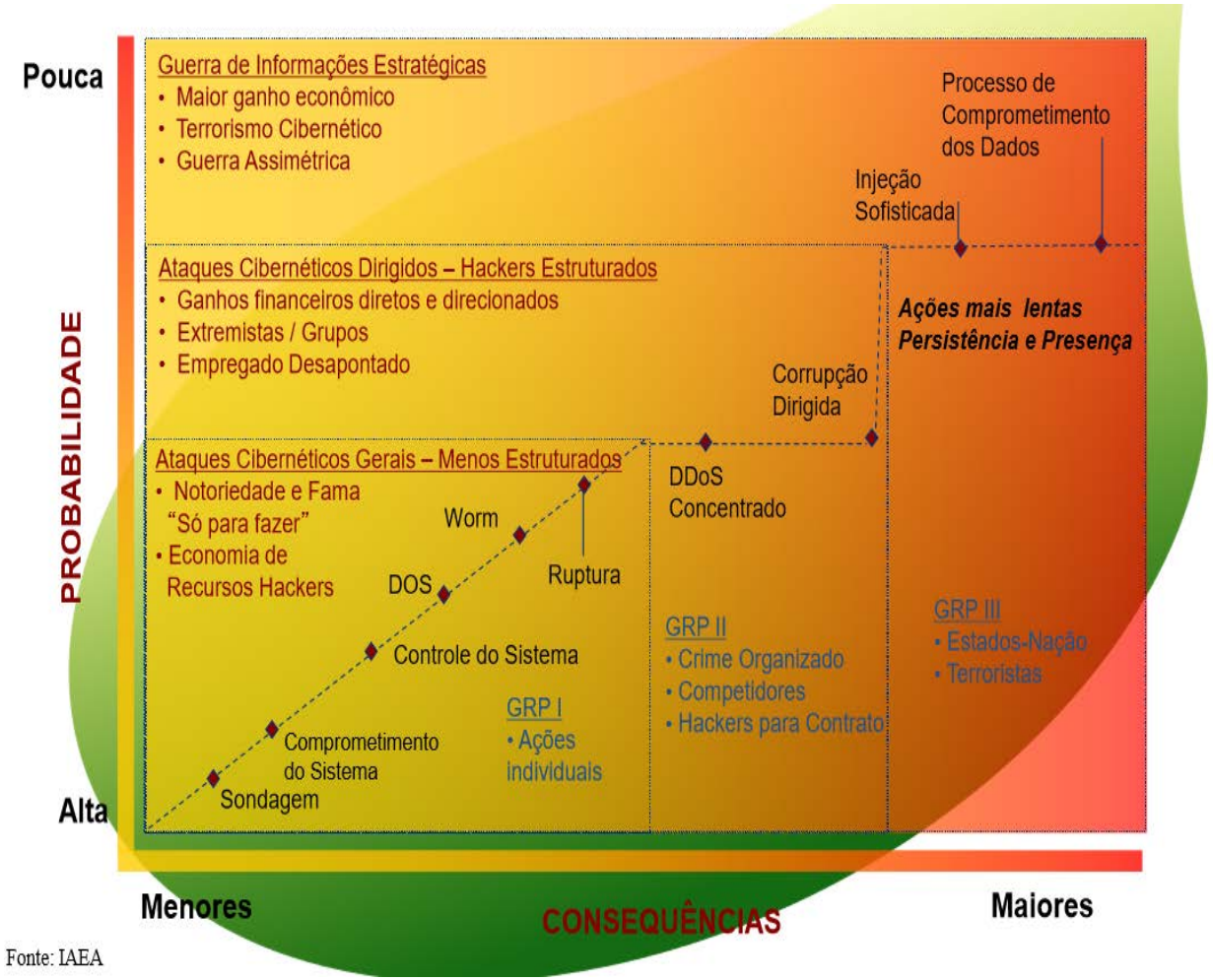
Coordenação Nacional - ETIRs Nacionais

Setor	ETIRs de Governo
Nacional – Todas Redes Brasileiras	CERT.br
Nacional – Todas as Redes de Governo	CTIR Gov
Militar	CCTIR/EB, CTIM, CTIR.FAB
Judiciário	GATI, CLRI-TRF-3
Legislativo	GRIS-CD
Energia	CSIRT Cemig
Financeiro	CSIRT BB, CSIRT CAIXA, CSIRT BASA, CSIRT BNB, CSIRT BRB, CSIRT Banese
Serviços de TI Telecom	CTIR/Dataprev, GRA/SERPRO, CSIRT PRODESP
Academia	CAIS/RNP, CEO/RedeRio, CERT-RS, CERT.Bahia, CSIRT POP-MG, CSIRT Unicamp, CSIRT USP, GSR/INPE, GRC/UNESP, NARIS, TRI
Outros	CSIRT CETRA, ETIR Correios, TCU SESTI



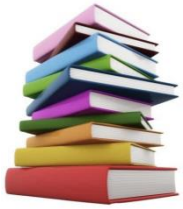
Fonte: https://www.cert.br/csirts/brazil

Estamos preparados?



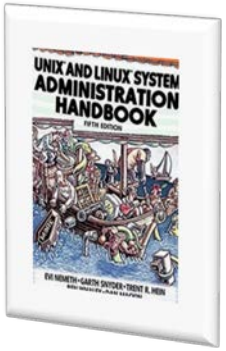
Fonte: IAEA

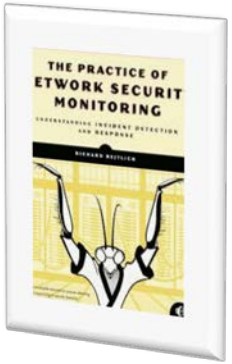
A Defesa

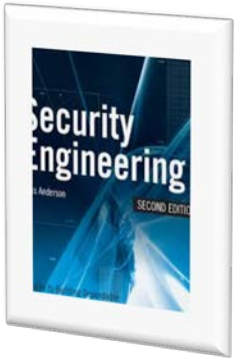


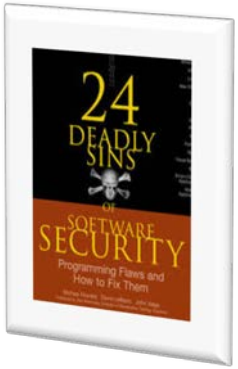
CULTURA DE SEGURANÇA DA INFORMAÇÃO

- **Normas Complementares do DSIC**
- **Padrões para Notificação de Incidentes de Redes do Governo ao CTIR Gov**
- **Cartilha de Segurança para Internet - CERT.br**
- **Boas Práticas para Desenvolvedores Web - OWASP Top 10**
- **Recomendações CAIS/RNP**
- **Projeto de SI SERPRO**









Desafios

DESAFIOS, EXPECTATIVAS E PROJETOS

Desafios

- Falta da cultura de Segurança da Informação
- Crescimento e Complexidade das Redes de Governo (computadores, celulares, *IoT*)
- Processo Eleitoral de Outubro
- Segurança da Informação *é multistakeholder*
- Segurança da Informação é multidisciplinar

Expectativas e Projetos

- **Política Nacional de Segurança da Informação**
- **Acordos de Cooperação.**
- **GDPR e as leis de proteção de dados pessoais**
- **Projeto MISP**
- **Guardião Cibernético**
- **Plano Nacional de Gestão e Resposta a Incidentes de Redes**

Próximos Eventos

AGENDA 2018

Próximos Eventos

- Dia Internacional de Segurança em Informática - RNP
  - 30 de agosto de 2018
  - https://disi.rnp.br/sobre

- 7º Fórum Brasileiro de CSIRTs – CERT BR
  - 13 e 14 de setembro de 2018
  - https://www.cert.br/forum2018/

- Colóquio Técnico CTIR Gov / Cyberwomen Challenge - DSIC
  - Semana de 26 a 29 de novembro de 2018
  - https://www.ctir.gov.br/1coloquio2018.html

Obrigado aos Parceiros e Boa Oficina!

www.ctir.gov.br

ctir@ctir.gov.br (notificação de incidentes)

Sobreaviso: (61) 99995-7859

INOC-DBA: **10954*810**

cgtir@presidencia.gov.br (assuntos diversos)

@CtirGov

www.linkedin.com/company/ctirgov/

Coordenador Geral - Democlydes Carvalho
democlydes.carvalho@presidencia.gov.br

Para comunicação através de um canal seguro, por favor utilize a seguinte chave PGP:

PGP Key ID: 0xAFBEDFCF
Fingerprint: 1E57 8A38 4834 6F1B 76BB 98C4 953E EB94 AFBE DFCF
PGP Public Key : www.ctir.gov.br/arquivos/certificados/ctir2009.asc

ETIR-GOV mailing list
ETIR-GOV@listas.planalto.gov.br
https://www1.planalto.gov.br/mailman/listinfo/etir-gov

“Oficina “EQUIPES DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS – ETIR“ 2018

Brasília – 15 de agosto de 2018

CDCIBER

ENAP

RNP
REDE NACIONAL DE ENSINO E PESQUISA

CENTRO DE TRATAMENTO DE INCIDENTES DE REDES DO GOVERNO
CTIR Gov

GSI-PR
DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

CAIS Centro de Atendimento a Incidentes de Segurança

Coordenação-Geral de Gestão de Segurança da Informação