CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Democlydes Carvalho
Analista de Incidentes

5º Fórum Brasileiro de CSIRTs
23 de setembro de 2016

5º Fórum Brasileiro de CSIRTs
23 de setembro de 2016

Atuação do CTIR Gov na coordenação das atividades de tratamento de incidentes na APF no Período dos Jogos Olímpicos e Paralímpicos Rio2016.

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

http://www.ctir.gov.br

CTIRGov

Democlydes Carvalho
Analista de Incidentes

Objetivo

Apresentar a visão do CTIR Gov sobre os incidentes ocorridos, desafios e lições aprendidas no Período dos Jogos Olímpicos e Paralímpicos Rio2016.

Sumário

- CTIR GOV
- Metodologia de Gestão de Incidentes
- Jogos Olímpicos
- Conclusões

CTIR GOV

AMBIENTAÇÃO

CTIR GOV
Ambientação

GSI/PR

DSIC

CTIR Gov

LEI Nº 10.683, DE 28 DE MAIO DE 2003.

CAPÍTULO I
DA PRESIDÊNCIA DA REPÚBLICA
Seção I
Da Estrutura

Art. 1º A Presidência da República é constituída, essencialmente:

VI - pelo Gabinete de Segurança Institucional;

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

IV - coordenar as atividades de inteligência federal e de segurança da informação;

DECRETO Nº 5.772, DE 8 DE MAIO DE 2006. (revogado)
DECRETO Nº 6.931, DE 11 DE AGOSTO DE 2009. (revogado)
DECRETO Nº 7.411, DE 29 DE DEZEMBRO DE 2010. (revogado)

DECRETO Nº 8.100, DE 4 DE SETEMBRO DE 2013

Aprova a Estrutura Regimental
Cargos e Funções

CAPÍTULO III
DAS COMPETÊNCIAS DOS ÓRGÃOS
Seção I

Art. 6º Ao Departamento de Segurança da Informação e Comunicações compete:

III - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;

CTIR GOV
Ambientação

DSIC

CTIR Gov

GABINETE DE SEGURANÇA INSTITUCIONAL

PORTARIA Nº 13, DE 4 DE AGOSTO DE 2006

Art. 1º Aprovar o Regimento Interno do Gabinete de Segurança Institucional da Presidência da República, na forma do anexo a esta Portaria.

Art 39. À Coordenação-Geral de Tratamento de Incidentes de Redes compete:

I - operar e manter o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov;

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

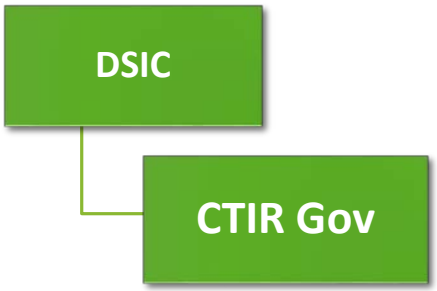
III - apoiar órgãos e entidades da administração pública federal nas atividades de tratamento de incidentes de segurança em redes de computadores;

IV - monitorar e analisar tecnicamente os incidentes de segurança nas redes de computadores da administração pública federal;

V - implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança nas redes de computadores da administração pública federal; e

VI - apoiar, incentivar e contribuir no âmbito da administração pública federal para a capacitação no tratamento de incidentes de segurança em redes de computadores.

CTIR GOV
Ambientação



- ✓ **Centro de Coordenação Nacional**
- ✓ **Comunidade de Tratamento de Incidentes do CTIR Gov**
  - APF direta e indireta
  - excepcionalmente, Estados e Municípios
  - “gov.br”, “jus.br”, “leg.br”, “mil.br”, “mp.br” e outros.

GABINETE DE SEGURANÇA INSTITUCIONAL

PORTARIA Nº 13, DE 4 DE AGOSTO DE 2006

Art. 1º Aprovar o Regimento Interno do Gabinete de Segurança Institucional da Presidência da República, na forma do anexo a esta Portaria.

Art 39. À Coordenação-Geral de Tratamento de Incidentes de Redes compete:

I - operar e manter o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov;

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

III - apoiar órgãos e entidades da administração pública federal nas atividades de tratamento de incidentes de segurança em redes de computadores;

IV - monitorar e analisar tecnicamente os incidentes de segurança nas redes de computadores da administração pública federal;

V - implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança nas redes de computadores da administração pública federal; e

VI - apoiar, incentivar e contribuir no âmbito da administração pública federal para a capacitação no tratamento de incidentes de segurança em redes de computadores.

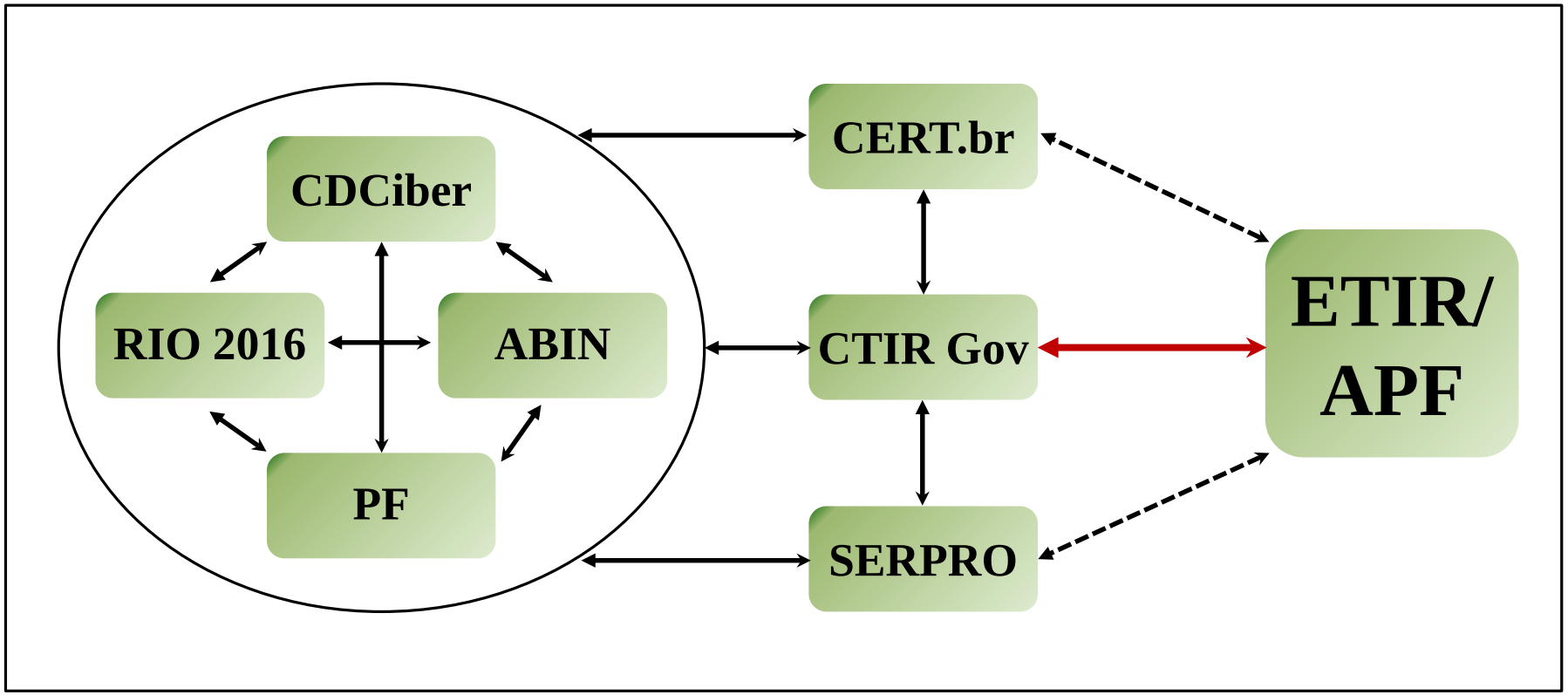
Metodologia de Gestão de Incidentes

NOTIFICAÇÕES

Metodologia de Gestão de Incidentes

NOTIFICAÇÕES

Ligações



Metodologia de Gestão de Incidentes

NOTIFICAÇÕES

Relacionamento entre Gestão de Incidentes, Tratamento de Incidentes e Resposta a Incidentes

Fonte: Adaptado do CERT-CC

Metodologia de Gestão de Incidentes

A Equipe

Dias não úteis e dias úteis (após às 19:00 hs)

Dias Úteis (08:00 às 19:00 hs)

Matriz de comunicação

- ✓ Sobreaviso
- ✓ INOC-DBA
- ✓ Telefones fixos

NOME	FUNÇÃO
Cel Ex Arthur Pereira Sabbat	Coordenador
Maj Ex Alexandre José Ribeiro	Assessor Técnico Militar
Maj Ex Democlydes Divino Pereira de Carvalho	Assessor Técnico Militar
Cap Ex Wagner Barp Meyer	Assessor Técnico Militar
1º Sgt Ex Alexandre Santos da Silva	Assistente Militar
Maurício Leite Ferreira da Silva	Assistente Técnico
José Carlos Soares de Azevedo	Assistente Técnico

Jogos Olímpicos

INCIDENTES [RIO2016]

2014 FIFA WORLD CUP Brasil

Jogos Olímpicos

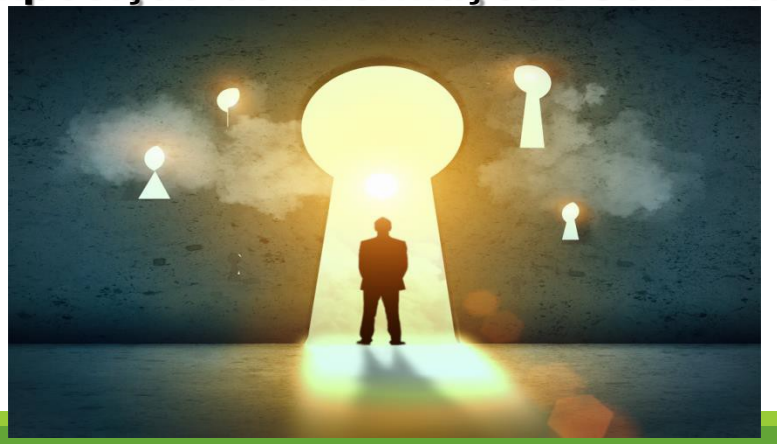
Ameaças

Ataques de Negação de Serviço

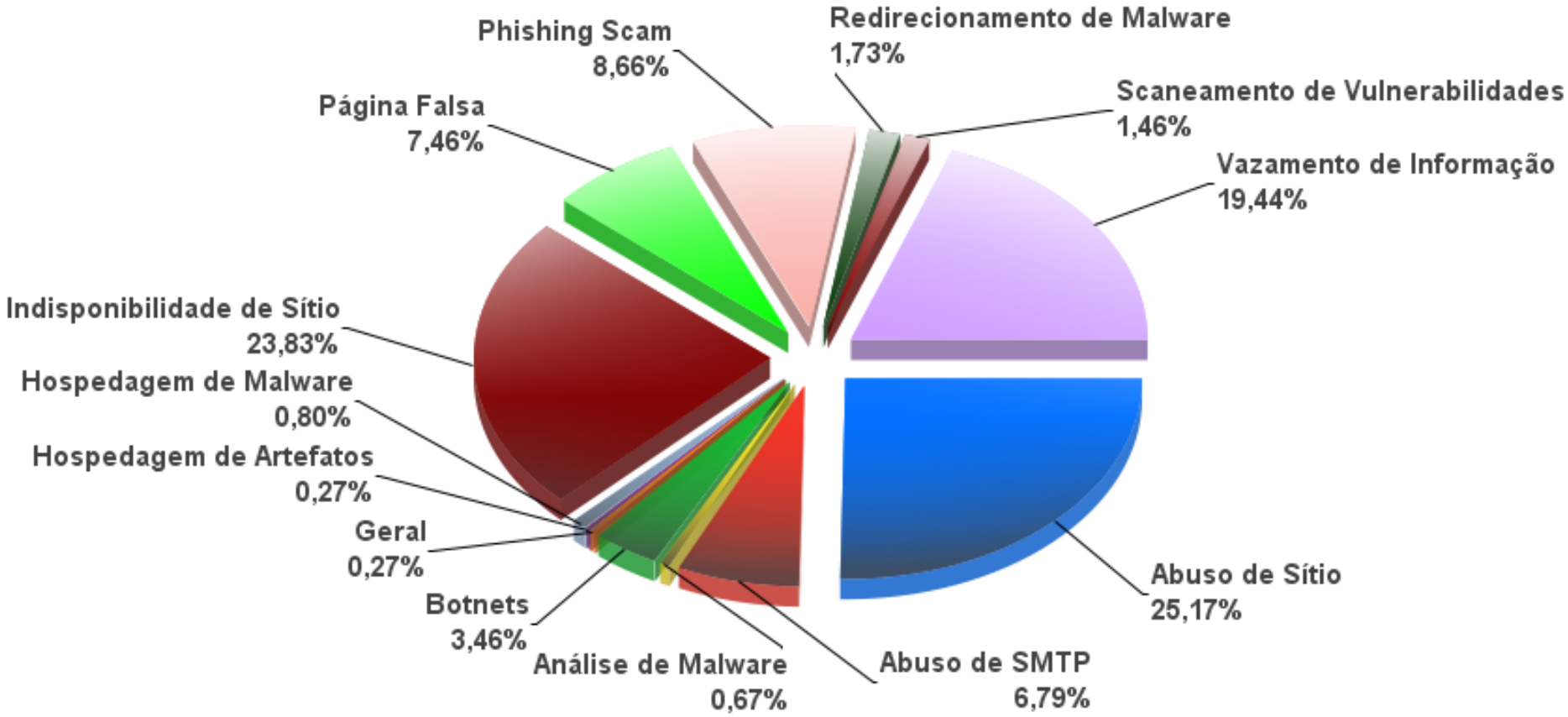
Abuso de Sítios

Ataques de Engenharia Social

Exposição de Informações Sensíveis



Jogos Olímpicos
Incidentes

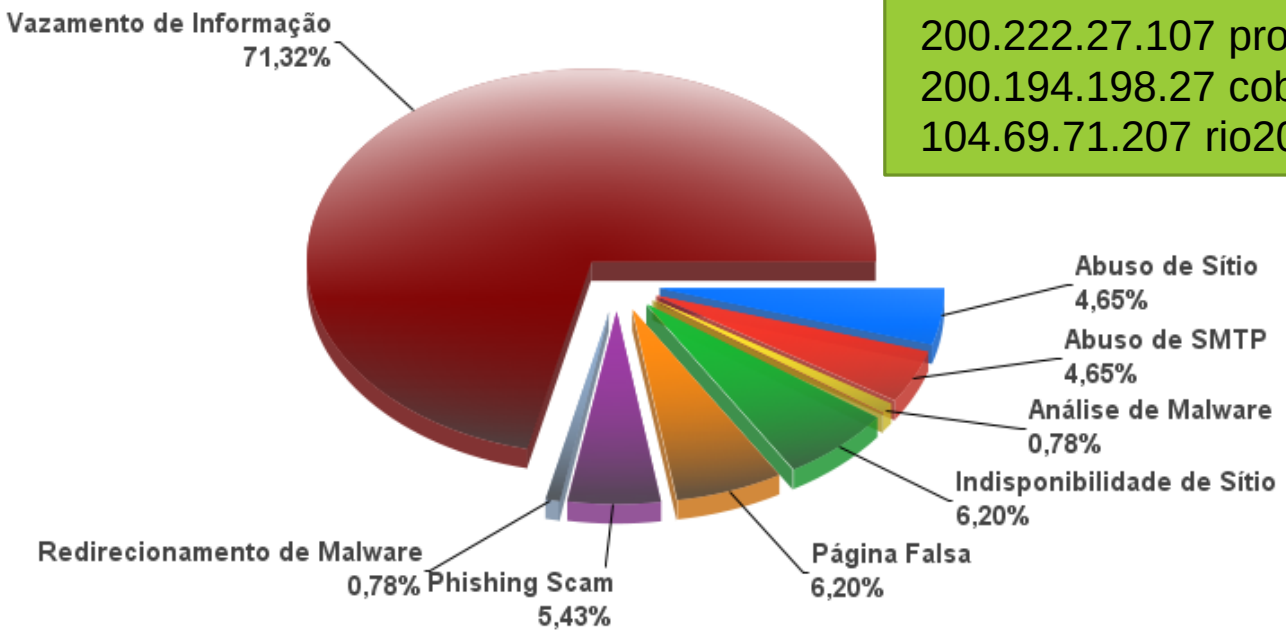


751 Incidentes de 05 a 21 de agosto de 2016

Jogos Olímpicos
Incidentes

- 05/08/2016 (ABERTURA)

Ferramenta “Anonymous DDoS” com alvo para:
200.198.193.122 www.esporte.gov.br
200.198.193.123 www.serpro.gov.br
200.222.27.107 proderj.rj.gov.br
200.194.198.27 cob.org.br
104.69.71.207 rio2016.com



http://pastebin.com/iSHY3qBx
Vazamento de informações de vulnerabilidades *.rj.gov.br
http://www.megafileupload.com/buvP/opolympddos.rar
Update de ferramenta de DDoS direcionada a domínios *.rj.gov.br e *.brasil2016.gov.br
https://www.cyberguerrilla.org/blog/database-of-gestaorecursos-cpb-org-br/
Informações que podiam ser usadas para ataque ao site principal “www.cpb.org.br”

Jogos Olímpicos
Incidentes

- 06/08/2016

Jogos Olímpicos Incidentes

- **Servidor NTP mal configurado**

```
[redacted]$ ntpdc -n -c monlist 2[redacted]6
remote address               port local address      count m ver code avgint  lstint
===============================================================================
200.[redacted]                123 2[redacted]6          401 4 4      0    847     104
200.[redacted]                123 2[redacted]6          405 4 4      0    839     138
192.168.[redacted]          46755 192.168.[redacted]    650 3 4    180    520     167
200.[redacted]                123 2[redacted]6          403 4 4      0    843     201
200.[redacted]                123 2[redacted]6          404 4 4      0    841     463
201.[redacted]                123 2[redacted]6          387 4 4      0    878     471
192.168.[redacted]          35424 192.168.[redacted]    613 3 4    180    553     575
200.[redacted]                123 2[redacted]6          402 4 4      0    845     847
192.168.[redacted]          50381 192.168.[redacted]    674 3 4    180    502     913
200.[redacted]                123 2[redacted]6          379 4 4      0    896     973
192.168.[redacted]          49519 192.168.[redacted]    606 3 4    180    559     978
192.168.[redacted]          51290 192.168.[redacted]    625 3 4    180    542    1064
192.168.[redacted]          40918 192.168.[redacted]    752 3 4    180    451    1210
200.[redacted]                123 2[redacted]6          301 4 4      0   1129    1266
192.168.[redacted]          38743 192.168.[redacted]    596 3 4    180    569    1353
180.[redacted]              60187 2[redacted]6            1 3 4      0 164445  164445

[redacted]$ ntpq -c rv 2[redacted]6
assID=0 status=0615 leap_none, sync_ntp, 1 event, event_clock_reset,
version="ntpd 4.2.6p5@1.2349-o Sat May 12 09:07:18 UTC 2012 (1)",
processor="i686", system="Linux/3.14.12", leap=00, stratum=2,
precision=-21, rootdelay=46.114, rootdisp=56.983, refid=2[redacted]6,
reftime=db8bc656.01628b28  Tue, Sep 20 2016 14:29:42.005,
clock=db8bc9b0.267eb4d8  Tue, Sep 20 2016 14:44:00.150, peer=34491,
tc=10, mintc=3, offset=-0.250, frequency=21.606, sys_jitter=0.926,
clk_jitter=0.385, clk_wander=0.028
```

Jogos Olímpicos
Incidentes

- **DNS Recursivo Aberto**

(servidor DNS mal configurado).

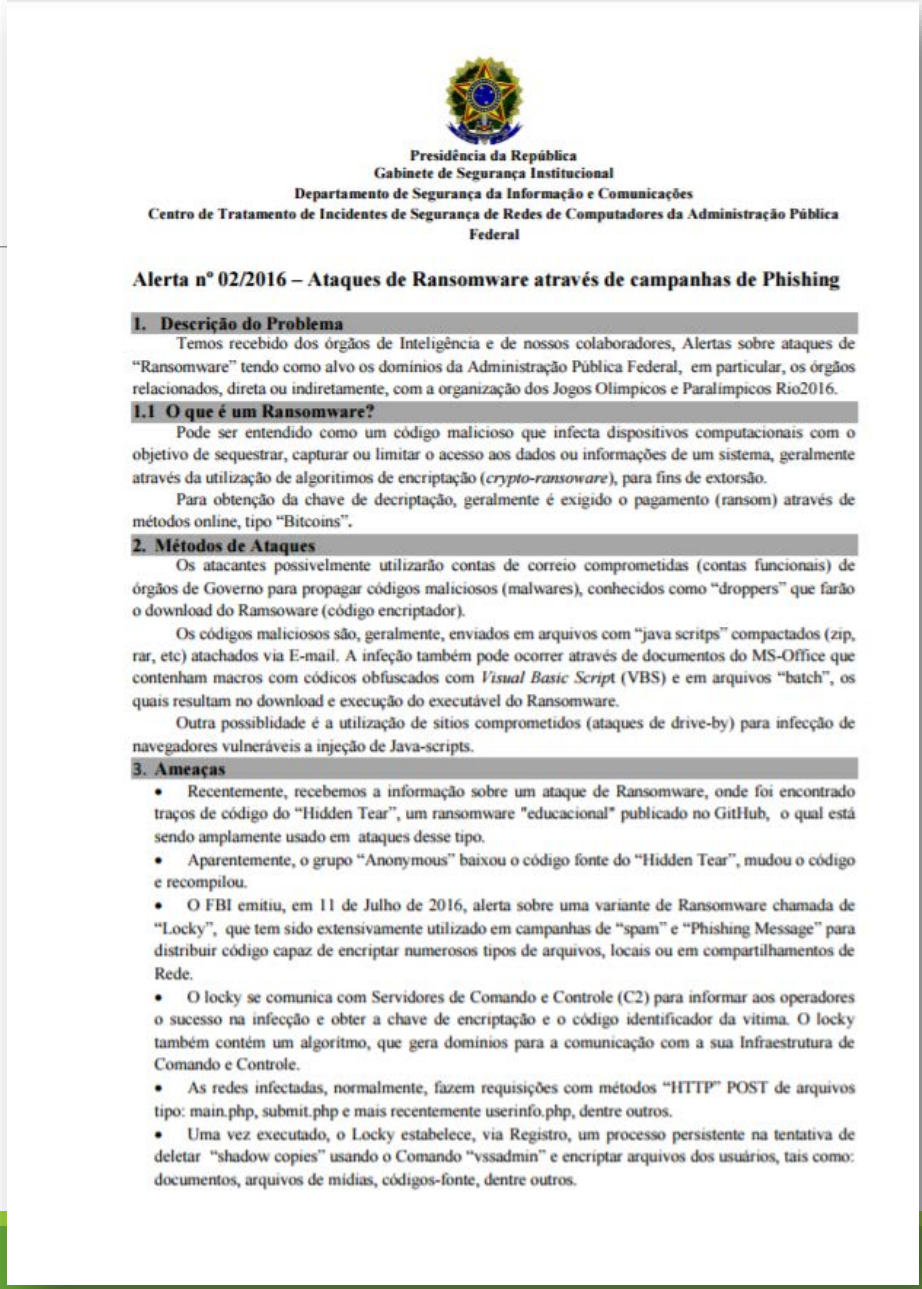
Para amplificar ataques de negação de serviço

```
[redacted]$ dig @1[redacted]3 www.google.com A

; <<>> DiG 9.8.4-P2 <<>> @1[redacted]3 www.google.com A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39620
;; flags: qr rd ra; QUERY: 1, ANSWER: 16, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         97      IN      A       200.195.190.123
www.google.com.         97      IN      A       200.195.190.113
www.google.com.         97      IN      A       200.195.190.94
www.google.com.         97      IN      A       200.195.190.88
www.google.com.         97      IN      A       200.195.190.104
www.google.com.         97      IN      A       200.195.190.98
www.google.com.         97      IN      A       200.195.190.84
www.google.com.         97      IN      A       200.195.190.119
www.google.com.         97      IN      A       200.195.190.109
www.google.com.         97      IN      A       200.195.190.103
www.google.com.         97      IN      A       200.195.190.108
www.google.com.         97      IN      A       200.195.190.93
www.google.com.         97      IN      A       200.195.190.118
www.google.com.         97      IN      A       200.195.190.99
www.google.com.         97      IN      A       200.195.190.89
www.google.com.         97      IN      A       200.195.190.114

;; AUTHORITY SECTION:
google.com.             75634   IN      NS      ns1.google.com.
google.com.             75634   IN      NS      ns3.google.com.
google.com.             75634   IN      NS      ns2.google.com.
google.com.             75634   IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         248446  IN      A       216.239.32.10
ns3.google.com.         248439  IN      A       216.239.36.10
ns2.google.com.         248446  IN      A       216.239.34.10
ns4.google.com.         248446  IN      A       216.239.38.10

;; Query time: 43 msec
;; SERVER: 1[redacted]3#53(1[redacted]3)
;; WHEN: Tue Sep 20 14:18:16 2016
;; MSG SIZE  rcvd: 424
```

Jogos Olímpicos
Alertas

Alerta nº 02/2016 – Ataques de *Ransomware* através de campanhas de *Phishing*

"Temos recebido dos órgãos de Inteligência e de nossos colaboradores, Alertas sobre ataques de "Ransomware" tendo como alvo os domínios da Administração Pública Federal, em particular, os órgãos relacionados, direta ou indiretamente, com a organização dos Jogos Olímpicos e Paralímpicos Rio2016."



Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal

Alerta nº 02/2016 – Ataques de Ransomware através de campanhas de Phishing

1. Descrição do Problema

Temos recebido dos órgãos de Inteligência e de nossos colaboradores, Alertas sobre ataques de "Ransomware" tendo como alvo os domínios da Administração Pública Federal, em particular, os órgãos relacionados, direta ou indiretamente, com a organização dos Jogos Olímpicos e Paralímpicos Rio2016.

1.1 O que é um Ransomware?

Pode ser entendido como um código malicioso que infecta dispositivos computacionais com o objetivo de sequestrar, capturar ou limitar o acesso aos dados ou informações de um sistema, geralmente através da utilização de algoritimos de encriptação (*crypto-ransoware*), para fins de extorsão.

Para obtenção da chave de decriptação, geralmente é exigido o pagamento (ransom) através de métodos online, tipo "Bitcoins".

2. Métodos de Ataques

Os atacantes possivelmente utilizarão contas de correio comprometidas (contas funcionais) de órgãos de Governo para propagar códigos maliciosos (malwares), conhecidos como "droppers" que farão o download do Ramsoware (código encriptador).

Os códigos maliciosos são, geralmente, enviados em arquivos com "java scritps" compactados (zip, rar, etc) atachados via E-mail. A infeção também pode ocorrer através de documentos do MS-Office que contenham macros com códicos obfuscados com *Visual Basic Script* (VBS) e em arquivos "batch", os quais resultam no download e execução do executável do Ransomware.

Outra possiblidade é a utilização de sítios comprometidos (ataques de drive-by) para infecção de navegadores vulneráveis a injeção de Java-scripts.

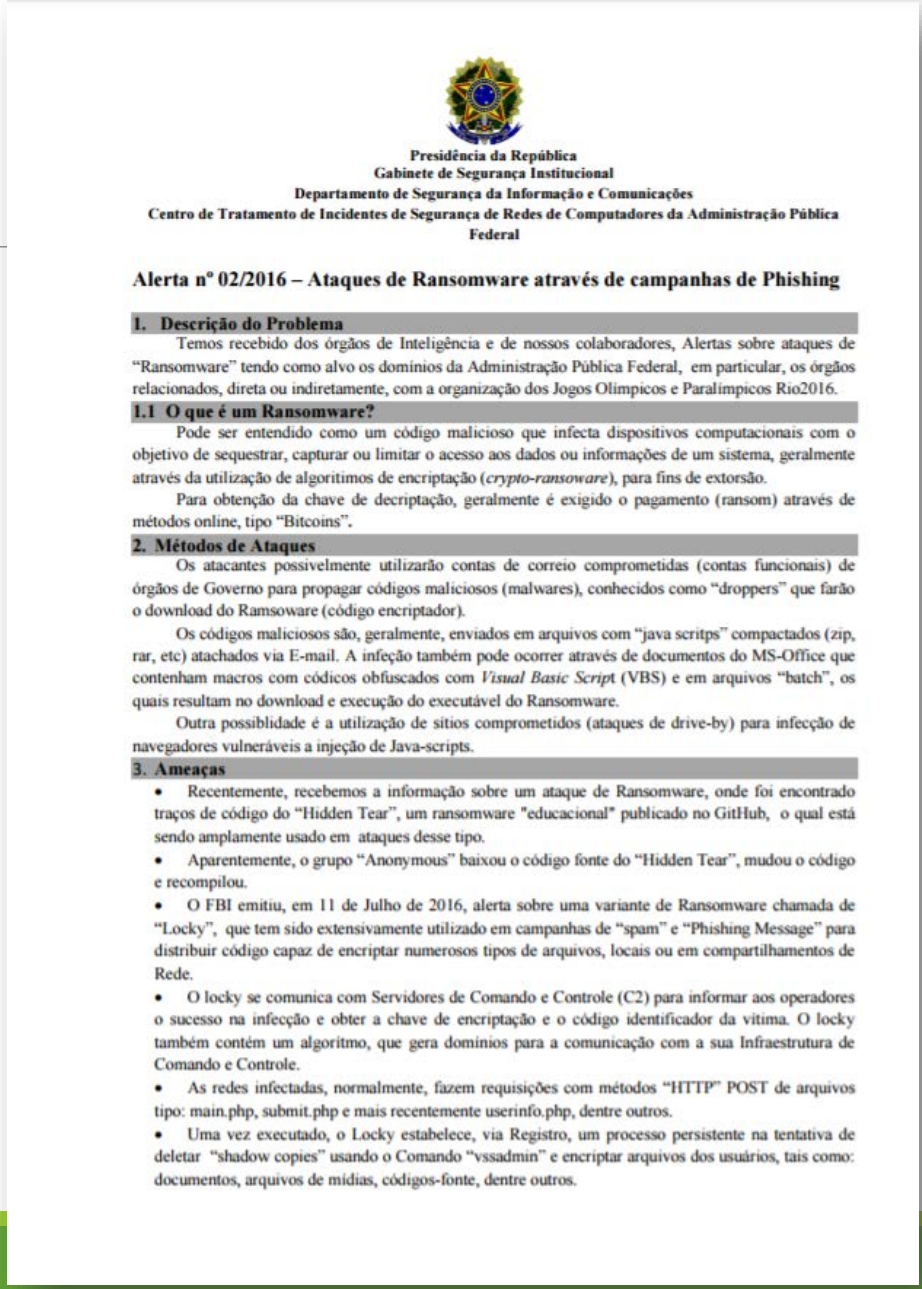
3. Ameaças

- Recentemente, recebemos a informação sobre um ataque de Ransomware, onde foi encontrado traços de código do "Hidden Tear", um ransomware "educacional" publicado no GitHub, o qual está sendo amplamente usado em ataques desse tipo.
- Aparentemente, o grupo "Anonymous" baixou o código fonte do "Hidden Tear", mudou o código e recompilou.
- O FBI emitiu, em 11 de Julho de 2016, alerta sobre uma variante de Ransomware chamada de "Locky", que tem sido extensivamente utilizado em campanhas de "spam" e "Phishing Message" para distribuir código capaz de encriptar numerosos tipos de arquivos, locais ou em compartilhamentos de Rede.
- O locky se comunica com Servidores de Comando e Controle (C2) para informar aos operadores o sucesso na infecção e obter a chave de encriptação e o código identificador da vítima. O locky também contém um algoritmo, que gera domínios para a comunicação com a sua Infraestrutura de Comando e Controle.
- As redes infectadas, normalmente, fazem requisições com métodos "HTTP" POST de arquivos tipo: main.php, submit.php e mais recentemente userinfo.php, dentre outros.
- Uma vez executado, o Locky estabelece, via Registro, um processo persistente na tentativa de deletar "shadow copies" usando o Comando "vssadmin" e encriptar arquivos dos usuários, tais como: documentos, arquivos de mídias, códigos-fonte, dentre outros.

Jogos Olímpicos
Alertas

Alerta nº 03/2016 – Distribuição de Ferramentas para Exploração de Vulnerabilidades em Equipamentos Cisco, Fortinet e WatchGuard

"Em 13 de agosto de 2016, um grupo intitulado Shadow Brokers disponibilizou um grupo de ferramentas para exploração de vulnerabilidades em equipamentos Cisco, Fortinet e WatchGuard. As ferramentas incluem ferramentas de exploração, de varredura e de estabelecimento de conexão e documentação.."



Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal

Alerta nº 02/2016 – Ataques de Ransomware através de campanhas de Phishing

1. Descrição do Problema

Temos recebido dos órgãos de Inteligência e de nossos colaboradores, Alertas sobre ataques de "Ransomware" tendo como alvo os domínios da Administração Pública Federal, em particular, os órgãos relacionados, direta ou indiretamente, com a organização dos Jogos Olímpicos e Paralímpicos Rio2016.

1.1 O que é um Ransomware?

Pode ser entendido como um código malicioso que infecta dispositivos computacionais com o objetivo de sequestrar, capturar ou limitar o acesso aos dados ou informações de um sistema, geralmente através da utilização de algoritimos de encriptação (*crypto-ransoware*), para fins de extorsão.

Para obtenção da chave de decriptação, geralmente é exigido o pagamento (ransom) através de métodos online, tipo "Bitcoins".

2. Métodos de Ataques

Os atacantes possivelmente utilizarão contas de correio comprometidas (contas funcionais) de órgãos de Governo para propagar códigos maliciosos (malwares), conhecidos como "droppers" que farão o download do Ramsoware (código encriptador).

Os códigos maliciosos são, geralmente, enviados em arquivos com "java scritps" compactados (zip, rar, etc) atachados via E-mail. A infeção também pode ocorrer através de documentos do MS-Office que contenham macros com códicos obfuscados com *Visual Basic Script* (VBS) e em arquivos "batch", os quais resultam no download e execução do executável do Ransomware.

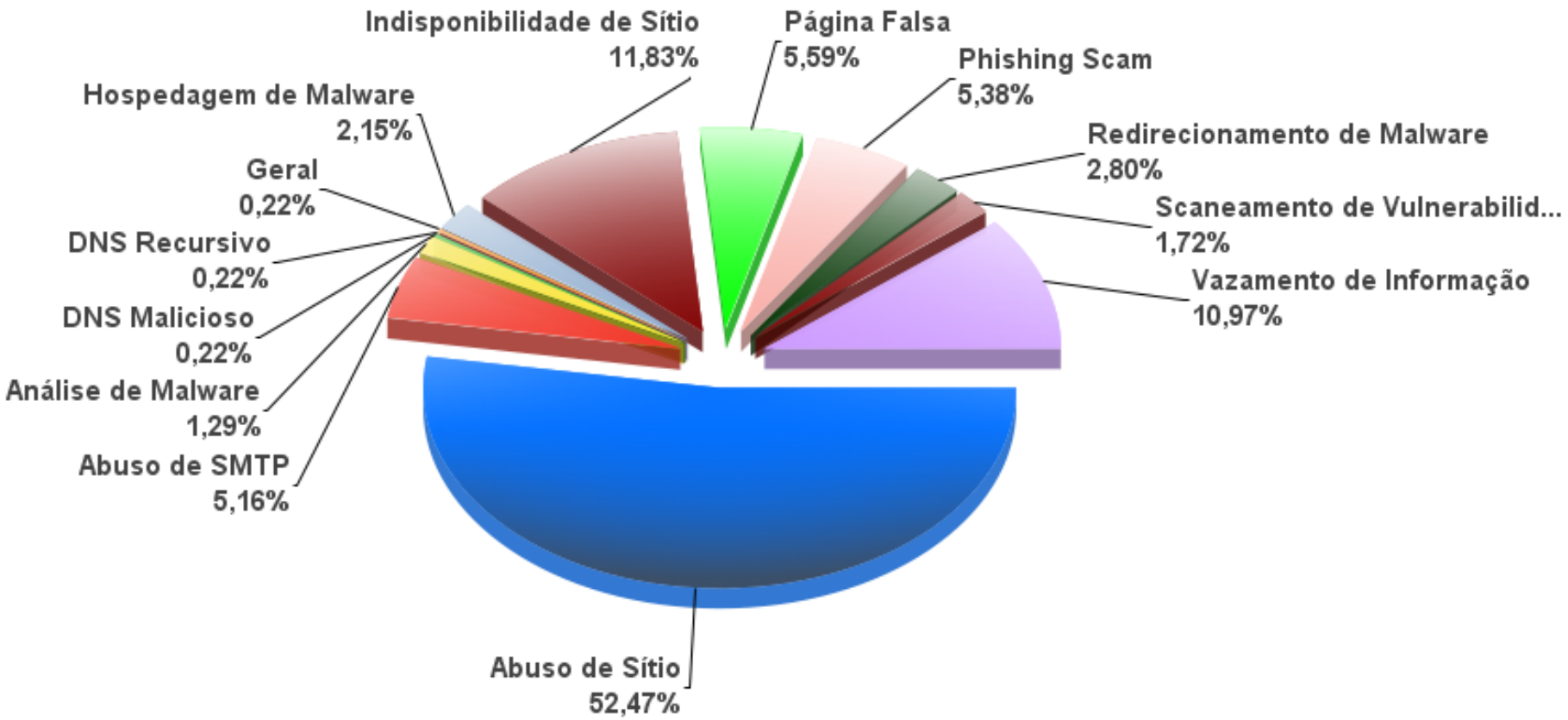
Outra possiblidade é a utilização de sítios comprometidos (ataques de drive-by) para infecção de navegadores vulneráveis a injeção de Java-scripts.

3. Ameaças

- Recentemente, recebemos a informação sobre um ataque de Ransomware, onde foi encontrado traços de código do "Hidden Tear", um ransomware "educacional" publicado no GitHub, o qual está sendo amplamente usado em ataques desse tipo.
- Aparentemente, o grupo "Anonymous" baixou o código fonte do "Hidden Tear", mudou o código e recompilou.
- O FBI emitiu, em 11 de Julho de 2016, alerta sobre uma variante de Ransomware chamada de "Locky", que tem sido extensivamente utilizado em campanhas de "spam" e "Phishing Message" para distribuir código capaz de encriptar numerosos tipos de arquivos, locais ou em compartilhamentos de Rede.
- O locky se comunica com Servidores de Comando e Controle (C2) para informar aos operadores o sucesso na infecção e obter a chave de encriptação e o código identificador da vítima. O locky também contém um algoritmo, que gera domínios para a comunicação com a sua Infraestrutura de Comando e Controle.
- As redes infectadas, normalmente, fazem requisições com métodos "HTTP" POST de arquivos tipo: main.php, submit.php e mais recentemente userinfo.php, dentre outros.
- Uma vez executado, o Locky estabelece, via Registro, um processo persistente na tentativa de deletar "shadow copies" usando o Comando "vssadmin" e encriptar arquivos dos usuários, tais como: documentos, arquivos de mídias, códigos-fonte, dentre outros.

Jogos Olímpicos
Incidentes

Jogos Paralímpicos



Tickets Gerados

2a Notificacao - Leaks - [RIO2016]-Sensible Information Exposure [ghostbin.com|52.91.215.199]
[RIO2016] Intel: Facebook
[abuse@cdciber.eb.mil.br: [CDCiber #12080] [RIO2016] Alerta sobre poss?vel manifesto de grupo hacker]
[CDCiber #12077] [RIO2016] Possível reprodução não autorizada de página - www.brasil2016.gov.br
[Rio2016} ENC: Report of DDoS attacks
[CDCiber #12080] [RIO2016] Alerta sobre possível manifesto de grupo hacker
[RIO2016]-Sensible Information Exposure [ghostbin.com|52.91.215.199]
[RIO2016] - Possivel comprometimento (marinha.mil.br)
[RIO2016] Domínio envolvido em campanha maliciosa contra Rio2016
[RIO2016] Vazamento de informacoes sensiveis (https://cidadao.sp.gov.br)
[RIO2016] Vazamento de informacoes sensiveis (https://saopaulo.sp.gov.br)
[RIO2016] Vazamento de informacoes sensiveis (senado.leg.br)
[RIO2016] Database exposed (obs.tv)
[RIO2016] Database exposed (tas-cas.org)
[CDCiber #12989] [RIO2016] Possível indisponibilidade de sítio - http://www.brasilia.df.gov.br/
[CDCiber #12248] [RIO2016] Possível desfiguração de sítio - www.ipea.gov.br (Instituto de Pesquisa Econômica Aplicada)
[RIO2016] Vazamento de informacoes sensiveis (zerobin.net/?1be)
[RIO2016] Vazamento de informacoes sensiveis de jus.br (http://pastebin.com/MDFFNNyJ)
[RIO2016] Atualizacao de alvos DOS
[RIO2016] Ataque DoS em curso contra: http://www.brasil2016.gov.br/
[RIO2016] Avisos sobre os ataques DoS as empreiteiras: http://pastebin.com/raw/2DvKm0SK
[RIO2016] brasil2016.gov.br - outros ataques
[RIO2016] Vulnerabilidade em website (camara.rj.gov.br)
[CDCiber #12989] [RIO2016] Possível indisponibilidade de sítio - http://www.brasilia.df.gov.br/
[RIO2016] Vazamento de informacoes sensiveis (https://ghostbin.com/paste/mt42t)

Conclusões

Conclusões
Óbices

COMO AS AMEAÇAS SÃO VISTAS

Para os países desenvolvidos

- Espionagem
- Sabotagem
- Terrorismo
- Roubo

Para os países em desenvolvimento

- Fraudes bancárias
- Vazamento de dados

Conclusões
Óbices

- Falta de Respostas por parte dos responsáveis;
- Alguns dias com dois na Triagem;
- Reformulação na APF (troca de Governo)
- Falta um melhor desenvolvimento nas atividades de inteligência.
- Recompletamento de Pessoal
  - Dificuldade em “garimpar” profissionais que atendam ao perfil;
  - Seleção deve atender requisitos técnicos e comportamentais;
  - Complexidade na formação de profissionais da equipe; e
  - Manutenção do conhecimento adquirido (rotatividade).

Conclusões
Aspectos Positivos

- Integração das equipes
- Instituições e pessoas continuam bem integradas;
- Percepção das potencialidades de cada time.
- Preparação técnica – aprendizado (oportunidade)
- Conhecimentos nivelados;
- Metodologias semelhantes.
- Proatividade
- Todas as equipes foram além dos trabalhos inicialmente previstos;

Referências

DSIC/GSIPR. _____. *Norma Complementar nº 03/IN01/DSIC/GSIPR*: Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Diário Oficial da República Federativa do Brasil. Brasília, DF, 03 Jul 2009, nº 125 - Seção 1**.** Brasília, 2009a.

DSIC/GSIPR. _____. *Norma Complementar nº 04/IN01/DSIC/GSIPR*: Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. Diário Oficial da República Federativa do Brasil. Brasília, DF, 17 Ago 2009, nº 156 - Seção 1**.** Brasília, 2009b.

DSIC/GSIPR. _____. *Norma Complementar nº 05/IN01/DSIC/GSIPR*: Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Diário Oficial da República Federativa do Brasil. Brasília, DF, 17 Ago 2009, nº 156 - Seção 1**.** Brasília, 2009c.

DSIC/GSIPR. _____. *Norma Complementar nº 06/IN01/DSIC/GSIPR*: Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Diário Oficial da República Federativa do Brasil. Brasília, DF, 23 Nov 2009, nº 223 - Seção 1**.** Brasília, 2009d.

DSIC/GSIPR. _____. *Norma Complementar nº 07/IN01/DSIC/GSIPR*: Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Diário Oficial da República Federativa do Brasil. Brasília, DF, 07 Mai 2010, nº 86 - Seção 1**.** Brasília, 2010a.

OBRIGADO!

Democlydes Carvalho – democlydes@gmail.com

http://www.ctir.gov.br

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

cgtir@planalto.gov.br (assuntos diversos)

INOC-DBA: **10954*810**