



Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Redes do Governo

ESTATÍSTICAS DE INCIDENTES DE REDE NO GOVERNO – 1º TRIMESTRE/2017

1. Apresentação

As informações estatísticas publicadas neste documento referem-se ao período de janeiro a março de 2017 e apresentam algumas considerações sobre o trabalho de detecção, análise e resposta a incidentes de segurança de rede de computadores desenvolvido pelo Centro de Tratamento de Incidentes de Redes do Governo – CTIR Gov, em comparação com o 4º trimestre de 2016.

Para fins de análise, o CTIR Gov considera: (a) **Notificações:** eventos detectados e/ou reportados a este centro, pelo endereço ctir@ctir.gov.br, incluindo os considerados como não incidentes, *spams*, falso-positivos, reiterações de incidentes já tratados e outras correspondências relacionadas à atividade de tratamento de incidentes de rede; (b) **Incidentes:** são as notificações que, após processo de triagem, são caracterizados como evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, conforme NC 05/IN01/DSIC/GSIPR; (c) **Resolvidos:** incidentes finalizados com tratamento realizado com sucesso; (d) **Pendentes:** incidentes que aguardam ação de terceiros para resolução; (e) **Não Resolvidos:** incidentes que após prazo estabelecido não obtiveram sucesso na resolução.

Fila	4º trimestre 2016	1º trimestre 2017
Abuso de Sítio	786	823
Abuso de SMTP	366	132
Análise de Malware	73	23
Botnets	9	12
DNS Malicioso	1	11
DNS Recursivo	0	90
FREAK - Factoring RSA Export Keys	0	278
Geral	22	40
Hospedagem de Artefatos	6	1
Hospedagem de Malware	71	76
Indisponibilidade de Sítio	432	583
NTP	1	27
Página Falsa	217	119
Phishing Scam	466	185
Redirecionamento de Malware	83	149
Scaneamento de Vulnerabilidades	23	27
Vazamento de Informação	676	229
SNMP	58	22
Violação de Direitos Autorais	0	1

Tabela 1 – Variação da quantidade de incidentes por categoria

2.3 – Subtipos da categoria Abuso de Sítios

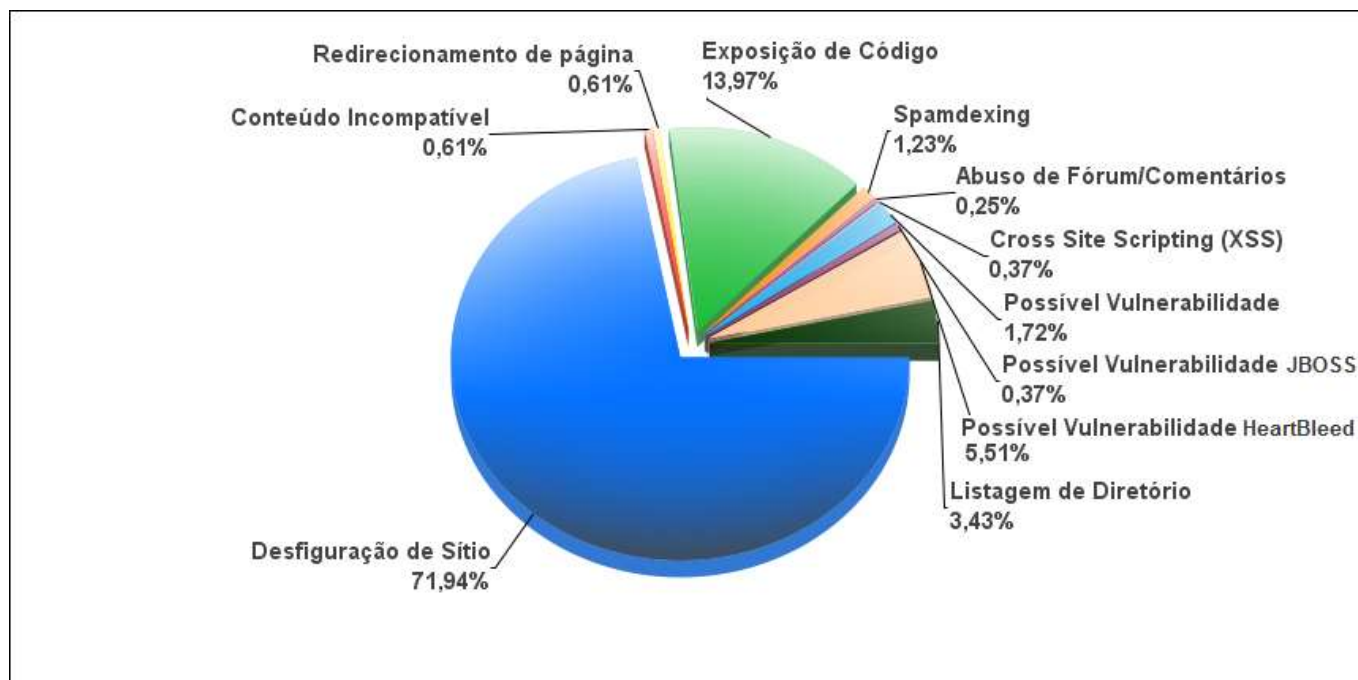


Gráfico 3 – Subtipos da categoria Abuso de Sítios

O Gráfico n° 3, acima, apresenta, em relação ao trimestre anterior, diminuição no subtipo “Desfiguração de Sítio” (71,94%), e um aumento significativo no subtipo “Exposição de Código” (13,97%).

2.4 – Distribuição de notificações de Abuso de Sítios por UF

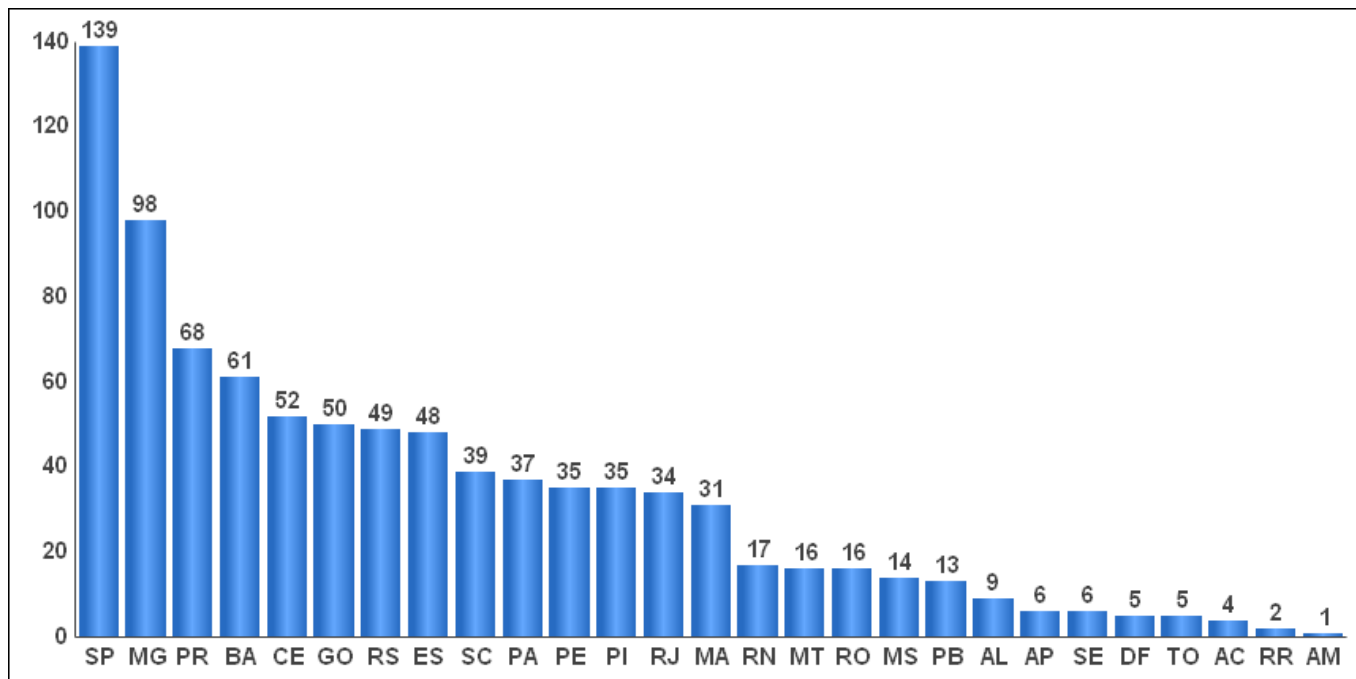


Gráfico 4 – Distribuição de notificações de Abuso de Sítios por UF

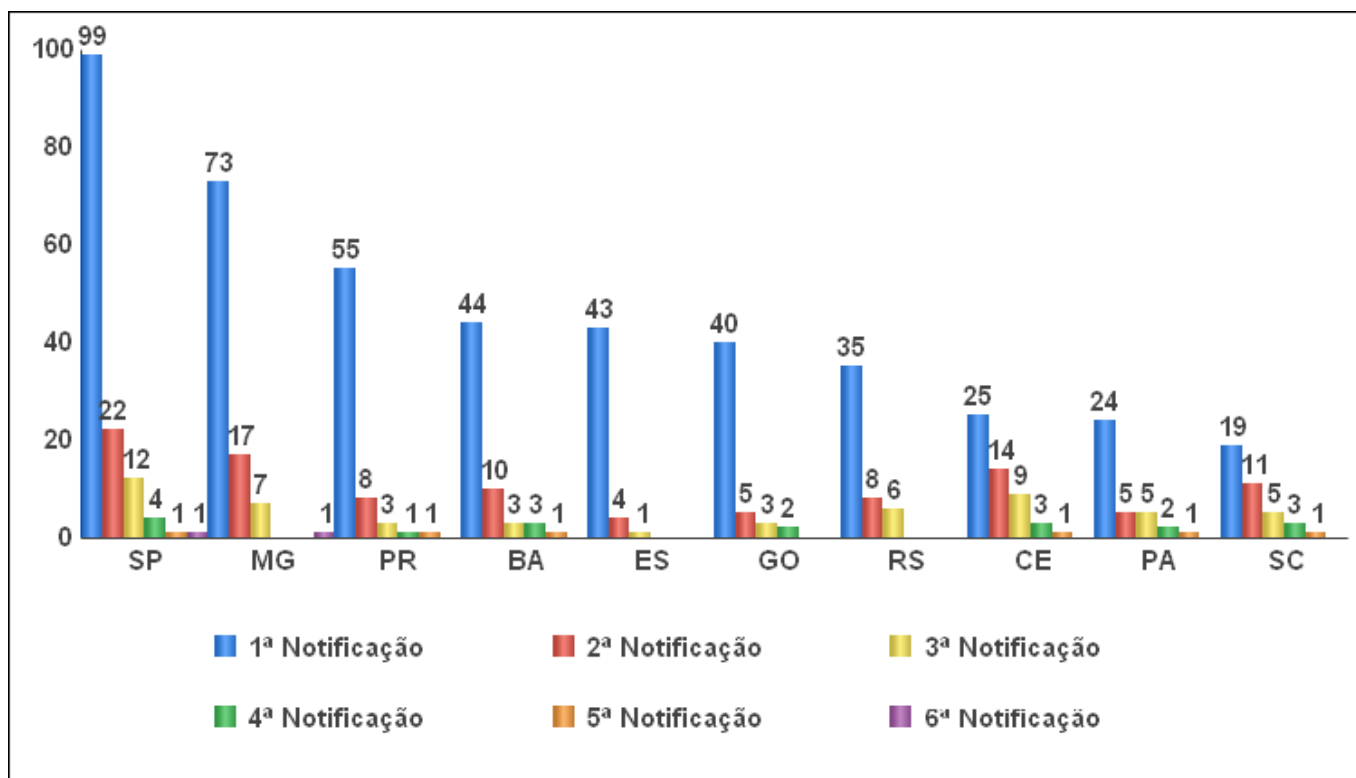


Gráfico 5 – Distribuição de renotificações de Abuso de Sítios por UF

O Gráfico nº 4 detalha a distribuição de notificações referentes à categoria de “Abusos de Sítios”, pelas unidades da federação (UF), enquanto o Gráfico nº 5 apresenta as dez unidades da federação com maior registro de incidentes desta categoria notificados, bem como as respectivas reiterações necessárias para resolução dos incidentes.

Na análise dos dados colhidos para este item, foi observado o aumento de incidentes de Abusos de Sítios e renotificações no Estado de São Paulo, levando-o a ocupar o primeiro lugar na estatística do número de notificações de Abuso de Sítios por UF neste primeiro trimestre de 2017.

2.5 – Domínios de hospedagem ou redirecionamento de *Malwares*

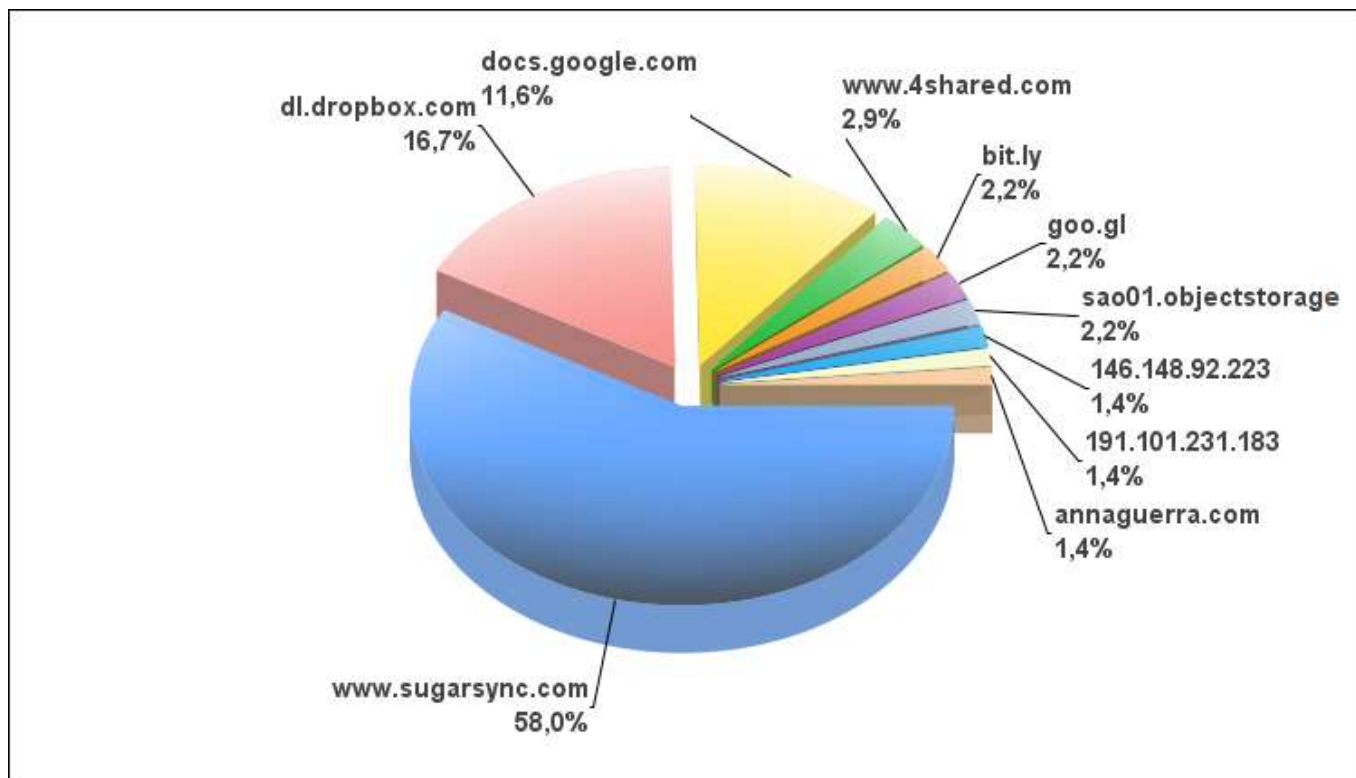


Gráfico 6 – Distribuição de domínios de hospedagem/redirecionamento de *Malwares*

No Gráfico nº 6, é possível observar os dez domínios de maior ocorrência na hospedagem ou redirecionamento de “*Malware*”.

Neste 1º trimestre de 2017 destacam-se os domínios “sugarsync.com” (58,0%), dl.dropbox (16,7%) e “docs.google” (11,6%) entre os domínios com mais notificações de hospedagem/redirecionamento de *Malwares*.

O CTIR Gov recomenda aos órgãos do Governo que não possuam necessidade de relacionamento institucional com os domínios listados, que adotem medidas julgadas cabíveis, alinhadas à Política de Segurança da Informação e Comunicações da instituição e que avaliem a necessidade do acesso ou a conveniência de bloquear as conexões aos domínios relacionados.

2.6 – Países destinatários das notificações de incidentes

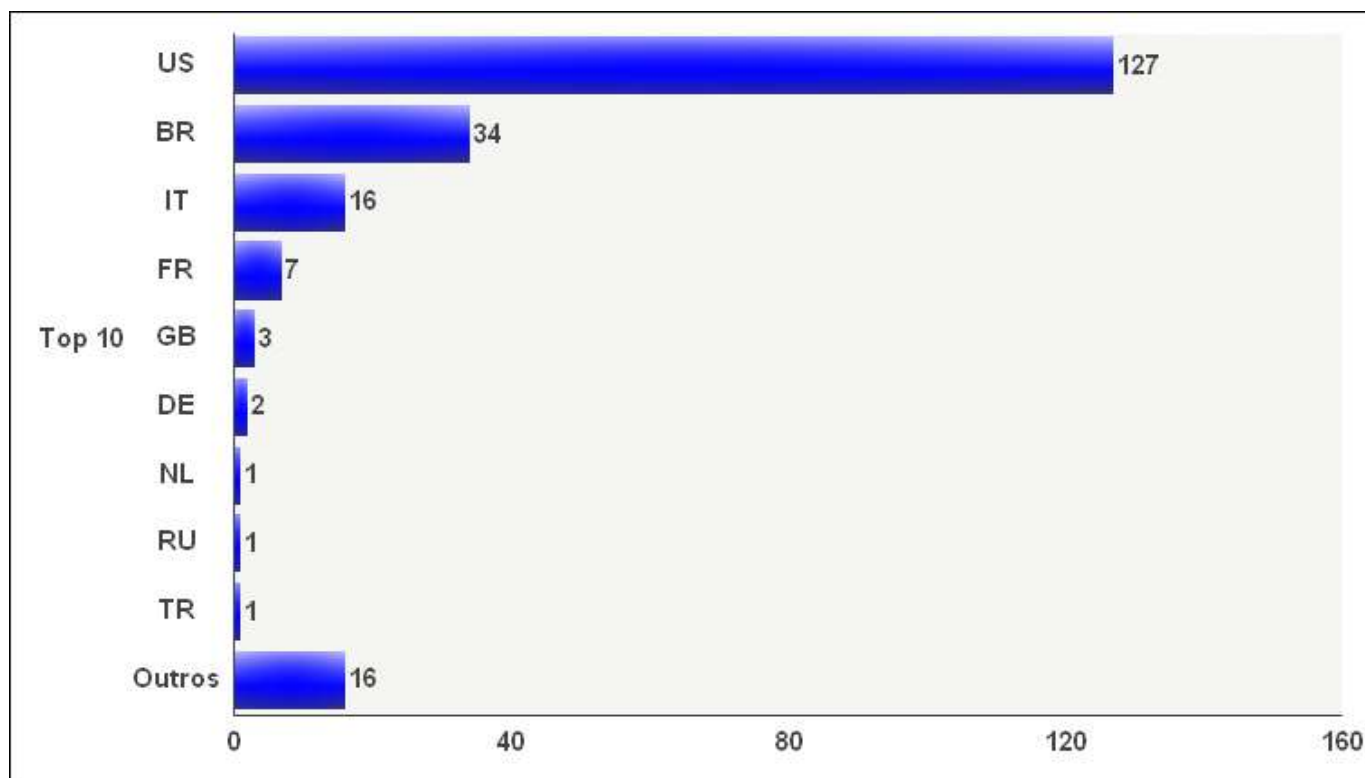


Gráfico 7 – Países destinatários das notificações de incidentes

O Gráfico nº 7 apresenta os dez países com maior número de notificações de incidentes tratados pelo CTIR Gov. De modo geral, observa-se que os Estados Unidos da América, Brasil, Itália e França se destacam quanto aos países destinatários das notificações de incidentes.

2.7 – Tempo de resolução dos Incidentes

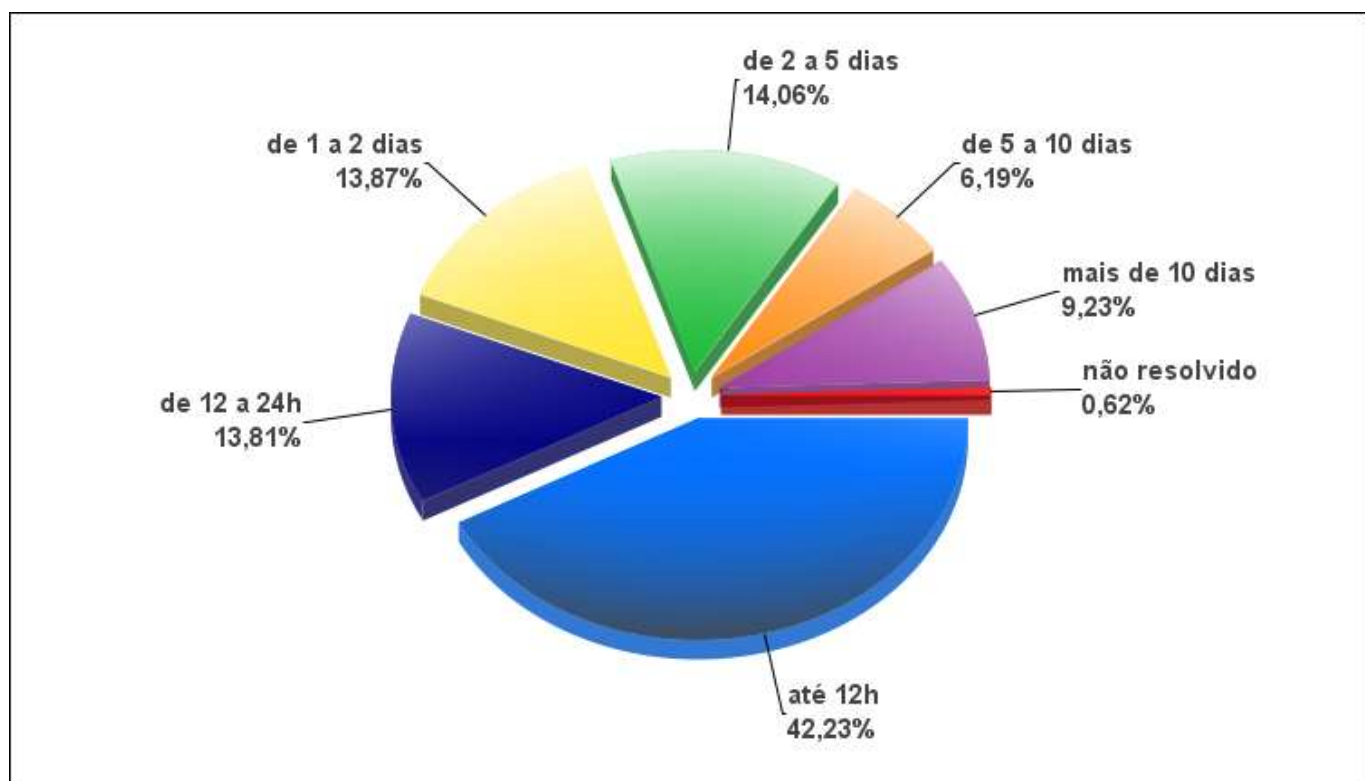


Gráfico 8 – Tempo de resolução

Com base nos dados do Gráfico nº 8, observa-se que 56,04% dos incidentes foram solucionados

nas primeiras vinte e quatro horas, sendo que 42,23%, nas primeiras 12 horas após a notificação. Ressalta-se que o “tempo de resolução” é o tempo necessário para a solução de Incidentes reportados pelo CTIR Gov, de modo que este gráfico basicamente reflete as ações de terceiros.

3. Conclusão

O CTIR Gov recebe notificações de incidentes de segurança dos órgãos afetados e de entidades parceiras, do Brasil e do Exterior, além dos detectados através de seus mecanismos de busca em fontes abertas.

Os números apresentados englobam incidentes de segurança relacionados às organizações e instituições do Governo Federal, Estadual e Municipal.

Tais números, apesar de não representarem a totalidade dos incidentes de segurança, podem ser considerados como uma amostra qualitativa e quantitativa das principais ameaças, e servir como base para orientar ações proativas e os investimentos necessários ao fortalecimento da segurança das redes do governo.

Vale destacar que o CTIR Gov trabalha de forma colaborativa com as equipes de segurança dos Órgãos da Administração Pública, e em parceria com o CDCiber, CERT.br e empresas especializadas em segurança. De modo que o presente relatório é fruto desse trabalho colaborativo, sendo, portanto, de fundamental importância que os órgãos e entidades públicas informem ao CTIR Gov os incidentes ocorridos em suas respectivas redes, para que melhor se apresente à sociedade, o cenário de ameaças que afetam a segurança das redes e dos recursos computacionais das diversas organizações que compõe a Administração Pública Brasileira.

Brasília-DF, Abril de 2017.

CTIR Gov/DSIC/CM/PR
www.ctir.gov.br