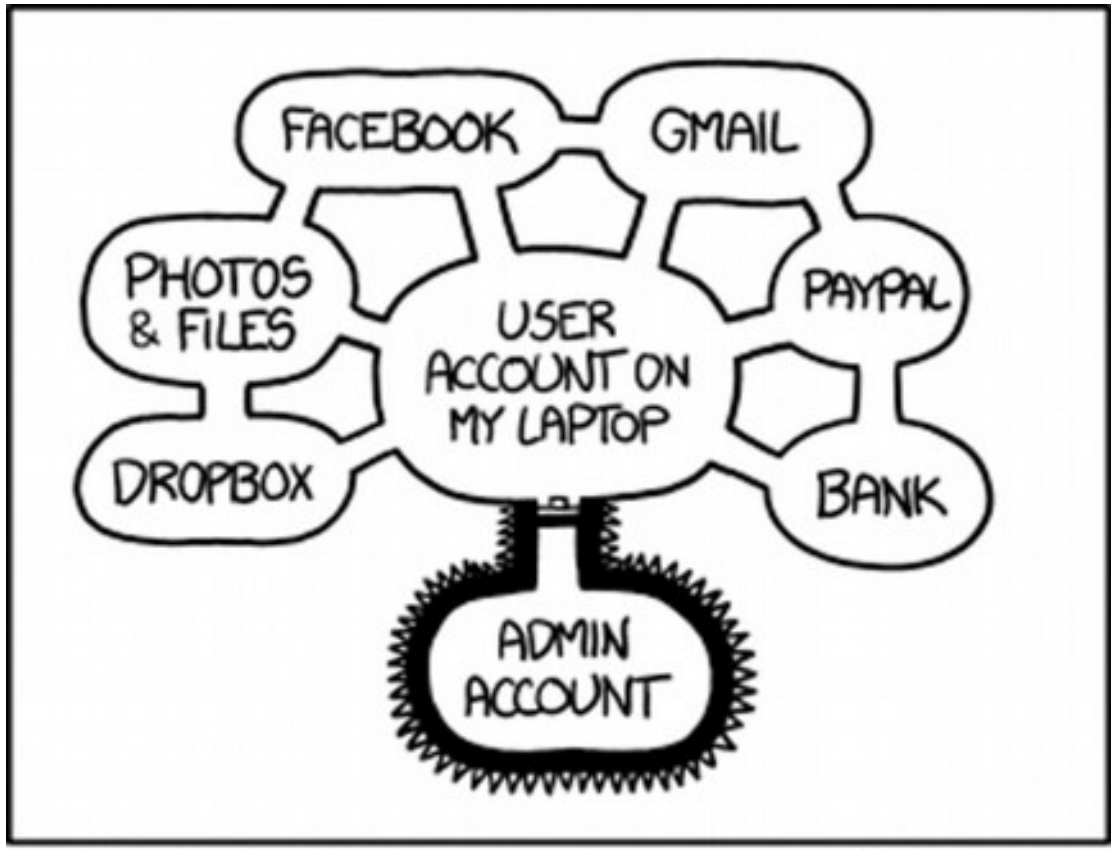
Segurança da Informação em Órgãos Públicos

Marcelo Caiado, M.Sc., CISSP, GCFA, EnCE, GCIH
Chefe da Divisão de Segurança da Informação
Procuradoria Geral da República
marcelobc@mpf.mp.br



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

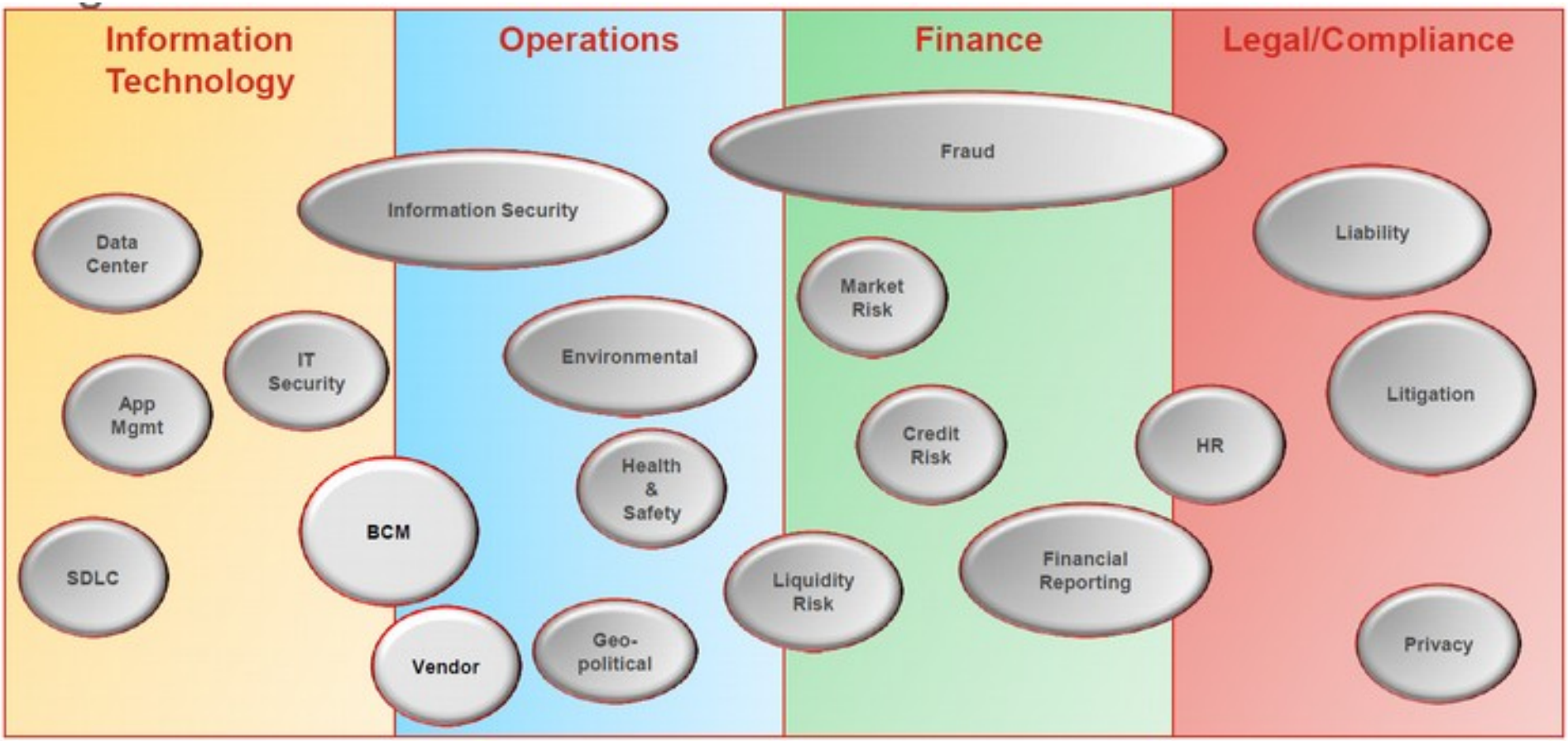
ALÉM DOS LOGINS: OUTROS PROD
VENDIDOS NO MERCADO NEGRO

http://www.tecmundo.com.br/privacidade/80767-brasilexposed-crise-seguranca-internet-brasileira.htm

Enfrentando questões organizacionais e culturais

- Entenda a visibilidade da área de Tecnologia da Informação
- Compreenda a espinha dorsal, conhecendo o histórico da empresa e seus procedimentos
- Aborde os aspectos corporativos, além dos tecnológicos

Enfrentando questões organizacionais e culturais



Fonte: RSA

Enfrentando questões organizacionais e culturais

- Procure "vender" a área de segurança => estatísticas e cases

O surgimento de plataformas de cibercrime, como um serviço, é um dos principais motiv
preocupação para a Atos.

À medida que cresce o número de pessoas e dispositivos conectados, aumentam também as vulnerabilidad dos SI. A Atos identificou quais são sete áreas de segurança da informa merecedoras de maior atenção:

1 – **Factor humano**: as pessoas continuarão a ser um dos principais de ataques, e uma boa campanha d sensibilização poderá reduzir em 80 riscos de ataques. A protecção dos dispositivos em que as pessoas trabalham irá diminuir o perigo.

2 – **Ameaças internas**: têm a ver muitas vezes com má gestão, colocando em risco a confidencialidade de muitas informações importantes. A prevenção contra fugas de informação gestão dos direitos digitais (quem pode fazer o quê, como e quando fazê-lo e em que condições ajudam as organizações a reduzir tais riscos.

3 – **Segurança industrial**: gradualmente o mundo industrial e a informática estão a convergir, à medida que as organizações tratam de optimizar a sua gestão e obter informação valiosa de ambientes industriais ou de infra-estruturas críticas, que em algum momento da sua evolução n activaram os requisitos de segurança que se exigem a um ambiente conectado. As empresas que gerem infra- estruturas críticas começam a estar conscientes destas novas ameaças, que vão desde a sabotagem à manipulação de informação de controlo e à fraude.

http://www.computerworld.com.pt/2015/06/08/sete-areas-criticas-de-seguranca/

HOME SEARCH **The New York Times**

The Opinion Pages | OP-ED CONTRIBUTOR

Edward Snowden: The World Says No to Surveillance

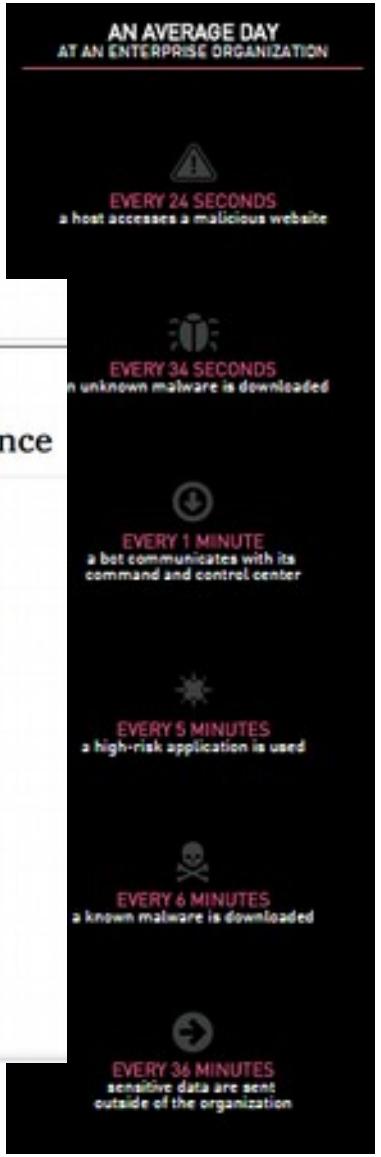
By EDWARD J. SNOWDEN JUNE 4, 2015

Adam Maida

MOSCOW — TWO years ago today, three journalists and I worked nervously in a Hong Kong hotel room, waiting to see how the world would react to the revelation that the National Security Agency had been making records of nearly every phone call in the United States. In the days that followed, those journalists and others published documents revealing that democratic governments had been monitoring the private activities of ordinary citizens who had done nothing wrong.

Within days, the United States government responded by bringing charges against me under World War

http://www.nytimes.com/2015/06/05/opinion/edward-snowden-the-world-says-no-to-surveillance.html?_r=0



http://www.checkpoint.com/resources/2015securityreport/

“O que não pode ser medido,

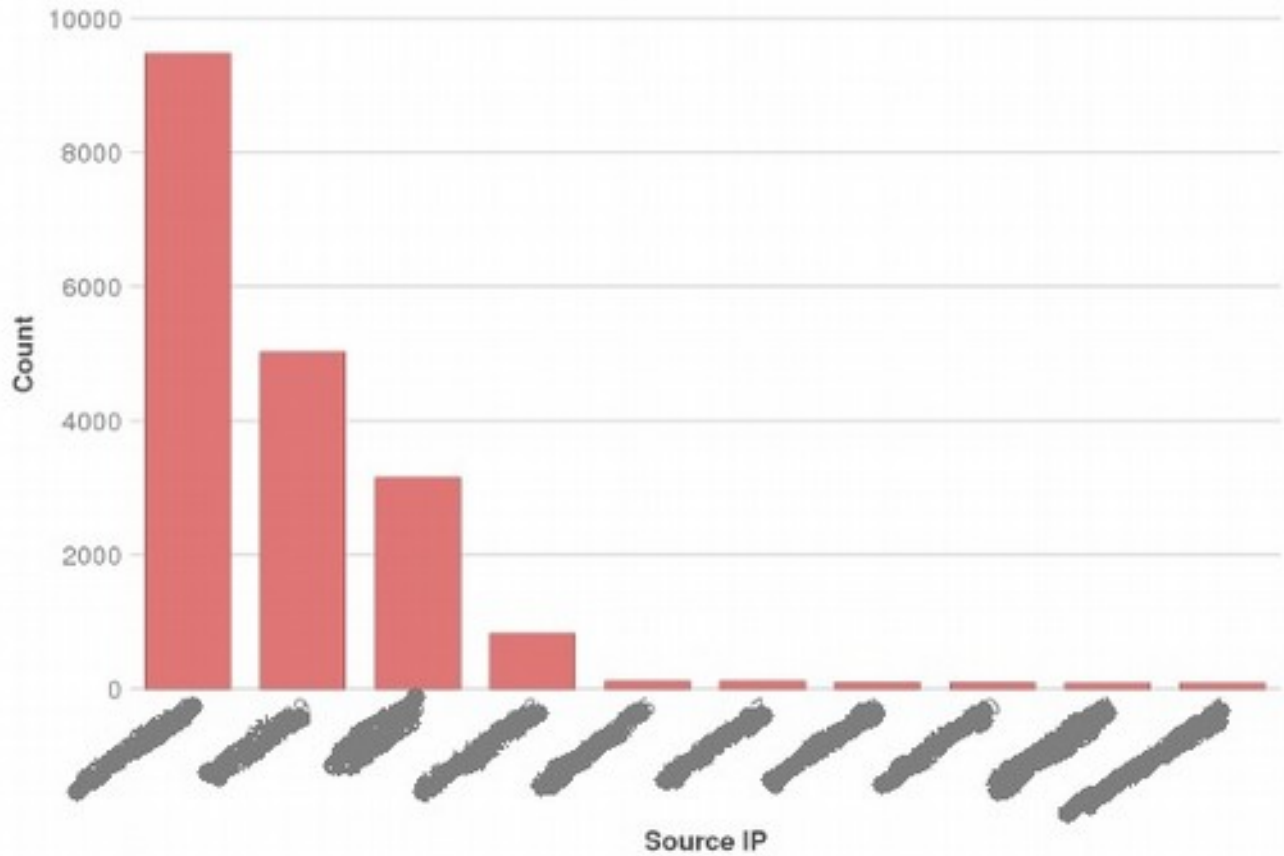
não pode ser gerenciado.”

William Edwards Deming

Prepare sua segurança

Malware Intrusions - Top 10

Time Window: *2015-05-01 07:00:00 - 2015-06-01 07:00:00*



Source IP	Count
[redacted]	9,481
[redacted]	5,026
[redacted]	3,163
[redacted]	824
[redacted]	120
[redacted]	118
[redacted]	101
[redacted]	96
[redacted]	91
[redacted]	87

Prepare sua segurança

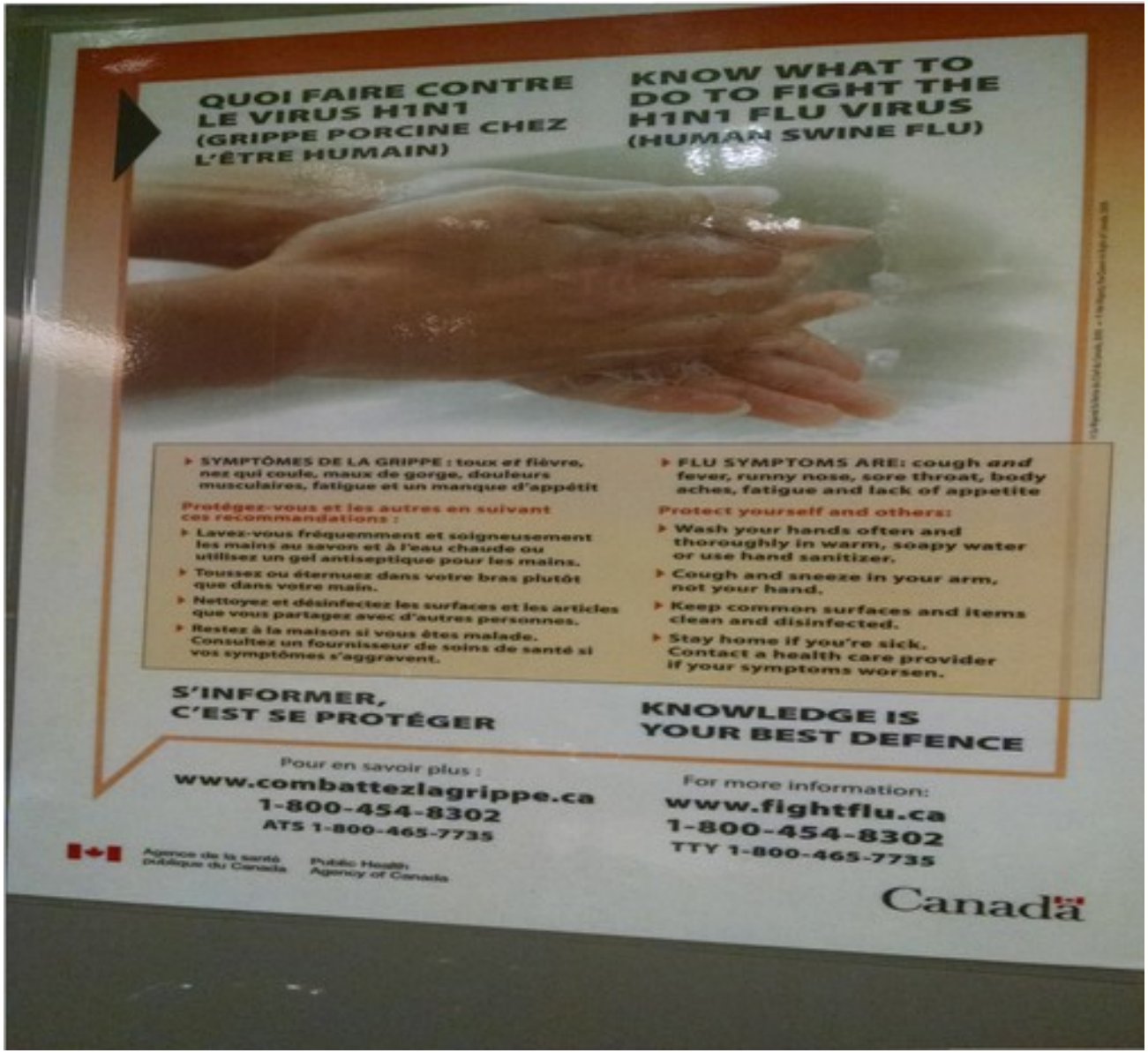
- Possua um time ou equipe de Resposta a Incidentes (treinado e equipado)
- Observe a “Teoria do pato”
- Proporcione canais fáceis de notificação de incidentes
  - RFC 2142 => Mailbox Names

MAILBOX	AREA	USAGE
ABUSE	Customer Relations	Inappropriate public behaviour
NOC	Network Operations	Network infrastructure
SECURITY	Network Security	Security bulletins or queries

Prepare sua segurança

- Conscientize e eduque seus usuários

Prepare sua segurança



Prepare sua segurança

Prepare sua segurança

- Conscientize e eduque seus usuários

> Comer chocolate todo dia pode ajudar a emagrecer, diz estudo http://t.co/jVTrrXTGnk pic.twitter.com/Dn53pXaQbZ
>
> — Folha de S.Paulo (@folha) April 7, 2015

> http://t.co/hq88J8gwDl – A notícia do seu dia: estudo diz que comer chocolate diariamente pode ajudar a emagrecer pic.twitter.com/1f0lJr3nA9
>
> — Portal Virgula (@portalvirgula) April 8, 2015

Prepare sua segurança

- Conscientize e eduque seus usuários

CIÊNCIA

É terrivelmente fácil enganar milhões de pessoas com pesquisas científicas fajutas

Por Renan Lopes
3 de junho de 2015 às 9:26

COMPARTILHE 23357 0

Você deve ter lido alguma coisa sobre a suposta dieta que trazia resultados mais rápidos ao incluir chocolate no cardápio. As matérias sobre a tal dieta se baseavam em uma pesquisa do Instituto de Dieta e Saúde (Institute of Diet and Health) e eram de autoria do médico alemão e diretor do instituto Johannes Bohannon. Ela foi publicada por revistas científicas e divulgada mundialmente em sites, revistas e programas de TV. E ela não passou de uma grande mentira.

Johannes Bohannon e o Instituto de Dieta e Saúde não passam de invenções do jornalista John Bohannon. Ele criou o site do instituto e publicou o estudo para expor como é fácil divulgar um estudo científico duvidoso.

>>> Revistas científicas aceitam artigo "escrito" por Maggie Simpson
>>> 120 artigos foram criados em "gerador de lero-lero" e ninguém percebeu

O estudo

O jornalista explica no io9 que a pesquisa foi encomendada por um canal de televisão alemão. Uma equipe do canal produzia um documentário sobre a ciência fajuta da indústria da dieta, que transformam ciência ruim, barata e duvidosa em grandes manchetes em jornais. E, tirando os resultados, tudo foi feito como uma pesquisa de verdade: com médicos, um profissional de estatística e objetos de pesquisa — pessoas dispostas a participar da dieta.

Os sujeitos participantes da pesquisa — 5 homens e 11 mulheres, de 19 a 67 anos — receberam 150 euros cada e foram informados que o estudo fazia parte de um documentário sobre dietas e nada mais.

A escolha do chocolate amargo veio do médico responsável pelos exames clínicos da pesquisa. Gunther Frank, clínico geral e autor de um livro contra a pseudociência por trás de dietas, explica: "Chocolate amargo tem gosto ruim, e por isso as pessoas acham que ele faz bem", diz. "É como uma religião".

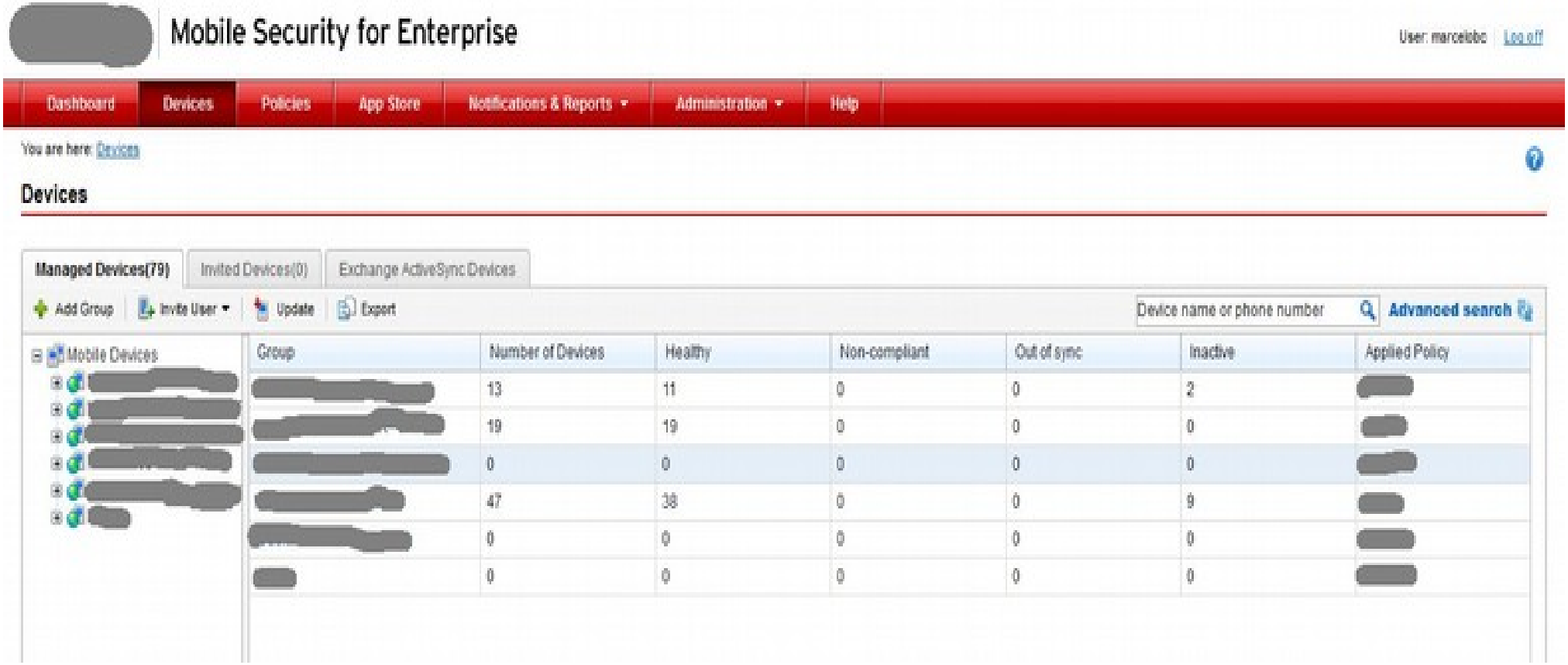
Depois de uma bateria de exames, o clínico separou os participantes em três grupos distintos: o primeiro em uma dieta de baixa caloria, o segundo na mesma dieta de baixa caloria mais a inclusão de 40 g de chocolate por dia e o terceiro grupo continuou com os mesmos hábitos alimentares que já mantinham. Cada indivíduo se pesou diariamente por 21 dias consecutivos e foi submetido a um questionário e mais uma bateria de exames ao final do experimento.

E o resultado? O terceiro grupo manteve ou teve mudanças insignificantes no peso, enquanto cada indivíduo do segundo e do primeiro grupo emagreceram cerca de 2.5 kg, com o segundo grupo, o que incluía chocolate na dieta, perdendo peso 10% mais rápido e com melhores resultados nos exames de colesterol que o primeiro.

http://gizmodo.uol.com.br/pesquisas-fajutas-midia/

Prepare sua segurança

- Mantenha sua segurança compatível com a tecnologia atual



Prepare sua segurança

- Realize provas de conceito

Infected Host IP	Severity	Infection	Callback	Last Malware	Last seen at (BRT)	Host Name
[redacted]	critical	0	282	Bot.Conficker.D	04/04/14 10:42:00	
[redacted]	critical	0	138	Trojan.Downloader.Small	04/11/14 12:17:23	
[redacted]	minor	0	1	FEDNSTestEvent.DNS	04/01/14 16:30:25	
[redacted]	minor	0	1	FEDNSTestEvent.DNS	04/01/14 16:30:25	
[redacted]	critical	0	1	Trojan.Spy.Banker.ACN	04/04/14 11:48:43	

The call backs were going to the following unique destination addresses: 55

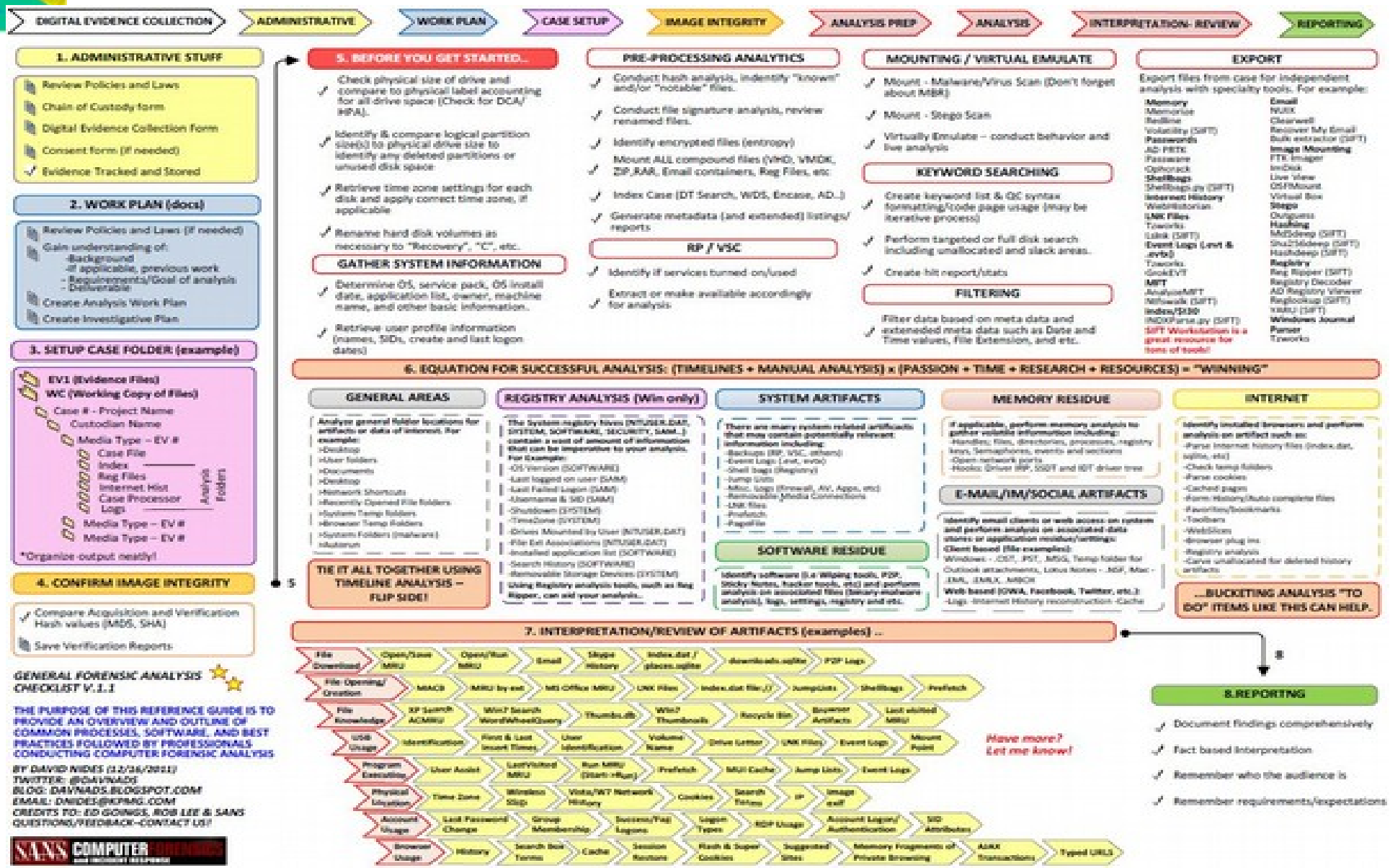
When resolved, the destination address of the CnC servers pointed to the following major geo-locations areas around the world.

AU (1)	AZ (1)	BE (1)	BR (1)
CA (2)	CN (4)	CO (1)	CR (1)
DE (1)	EG (1)	EU (1)	FI (1)
FR (1)	GB (3)	JP (4)	KR (1)
MX (1)	PL (1)	RU (2)	US (24)
Other (2)			

Respondendo a um incidente

- Preocupe-se com a cadeia de custódia
  - Cuidado especial com a síndrome do faz-tudo (a.k.a. Teoria do Pato)
- Realize o devido engajamento Jurídico
- Notifique a alta administração em casos mais graves
  - Lista de contatos
- Possua um manual de procedimentos com responsabilidades bem definidas

Respondendo a um incidente



Recursos Humanos

- Teoria dos dois Fatores (Herzberg)
  - A satisfação no cargo é função do conteúdo ou atividades desafiadoras e estimulantes do cargo, são os chamados "fatores motivacionais";
  - A insatisfação no cargo é função do ambiente, da supervisão, dos colegas e do contexto geral do cargo, enriquecimento do cargo (ampliar as responsabilidades) são os chamados "fatores higiênicos".

Recursos Humanos

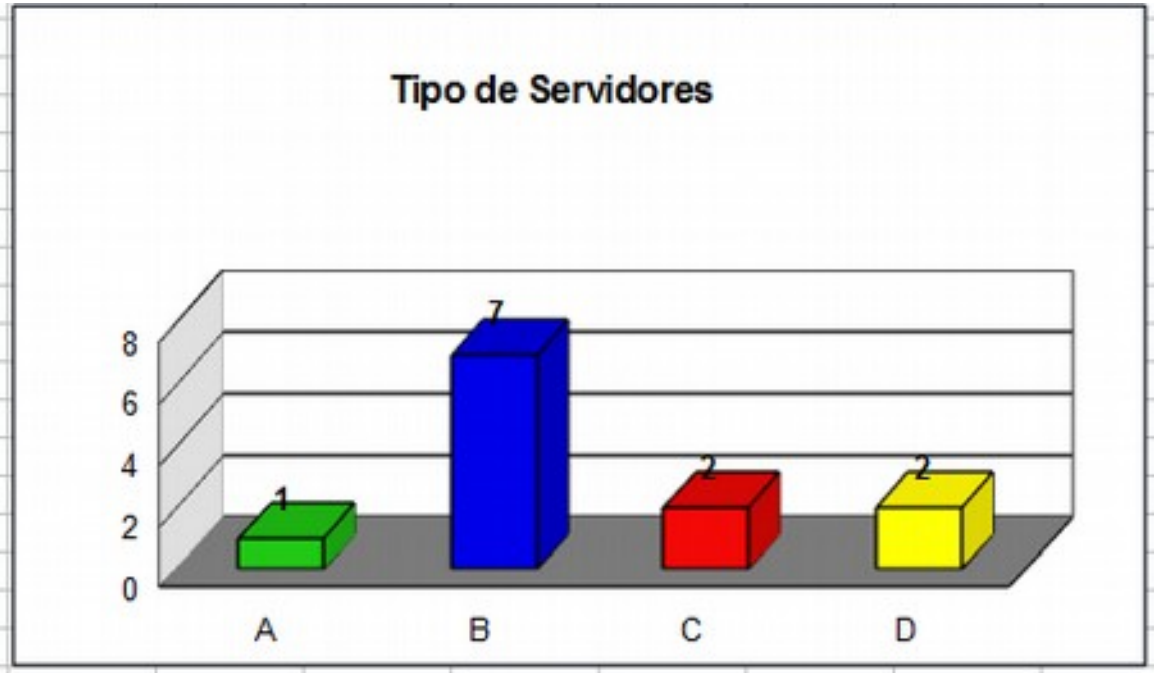
- Teoria dos dois Fatores (Herzberg)

Quadro Estatístico dos Tipos de Servidores

Tipo	Frequência	Porcentagem
A	1	8%
B	7	58%
C	2	17%
D	2	17%
Total	12	100%

TIPO	Motivação e Higiene
A	Satisfeito e Insatisfeito
B	Satisfeito e Não Insatisfeito
C	Não Satisfeito e Insatisfeito
D	Não Satisfeito e Não Insatisfeito

Fatores	Satisfeito	Não Satisfeito	
Insatisfeito	1	2	3
Não Insatis	7	2	9
	8	4	12



Recursos Humanos

- Líderes eficazes são capazes de engajar o seu time de diversas formas:
  I. Articulam uma visão de forma a enfatizar os valores de seu público alvo;
  II. Criam um ambiente de união segurança;
  III. Envolvem as pessoas no processo de decisão sobre como a visão compartilhada vai ser alcançada;
  IV. Apoiam os esforços dos funcionários em compreender a visão, disponibilizando *coaching*, dando *feedback* e sendo um modelo exemplar;
  V. Reconhecem e premiam o sucesso.

Recursos Humanos

- Líderes eficazes reconhecem as diferenças e utilizam diferentes estilos

Recursos Humanos

- Grandes líderes possuem um elevado grau de Inteligência Emocional:
  - Autoconsciência: a habilidade para reconhecer e compreender seu estado de espírito, suas emoções e seus ímpetos, assim como seus efeitos sobre outras pessoas.
  - Autocontrole: a habilidade para controlar ou redirecionar impulsos e ânimos disruptivos, evitar julgamentos e pensar antes de agir.
  - Motivação: a habilidade para perseguir metas com energia e perseverança, por motivos que vão além do dinheiro ou do status.
  - Empatia: a habilidade para compreender a estrutura emocional das pessoas.
  - Habilidade social: a habilidade para gerenciar relações, criar redes de relacionamentos e encontrar um denominador comum.

Recursos Humanos

- Invista em servidores que demostram comprometimento
  - (ISC)2 – www.isc2.org
  - SANS Institute – www.sans.org
  - Certificações de fabricantes
  - Norma Complementar nº 17/IN01/DSIC/GSIPR
    - Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).

Mandamentos do Gestor de SEGINFO

1. Participarás junto com sua equipe em atividades de prospecção de tecnologias;
2. Implementarás demandas de segurança com requisitos de conformidade, privacidade e coorporativos;
3. Monitorarás todos seus ativos de segurança, como NGFW, IDS/IPS, SIEM, DLP, antivírus, etc;
4. Estarás atento aos desafios diários como sites maliciosos, vulnerabilidades, zero days, espionagem, crime organizado, funcionários insatisfeitos, script kiddies, hacktivistas, etc;

Mandamentos do Gestor de SEGINFO

5. Trabalharás ativamente para que a cultura seja da resposta a incidentes, e não da resposta <u>após</u> incidentes;
6. Engajarás a alta administração;
7. Indicarás as tecnologias de segurança adequadas e aplicarás os devidos processos;
8. Não descuidarás da capacitação de sua equipe;
9. Protegerás seus ambientes físico, móvel e virtual;
10. Atuarás sempre de forma ética.

Cânones do Código de Ética do (ISC)[2]

I. Proteger a sociedade, o bem comum, necessária confiança mútua e confiança do público, e a infra-estrutura.
II. Agir honradamente, honestamente, de forma justa, com responsabilidade e dentro da lei.
III. Fornecer serviço diligente e competente para a alta administração.
IV. Avançar e proteger a profissão.

Concluindo (1)

Release of the Reports on the Terrorist Attack of October 22, 2014

Ottawa, Wednesday, June 3, 2015 – Today, the Royal Canadian Mounted Police (RCMP), the House of Commons and the Senate released four reports examining the terrorist attack on Parliament Hill on October 22, 2014.

These four reports were requested by the Speaker of the House of Commons and the RCMP in order to provide clarity regarding the events of Oct. 22, to review all actions taken by security forces, and to provide suggestions on a way forward towards improving security within the parliamentary precinct.

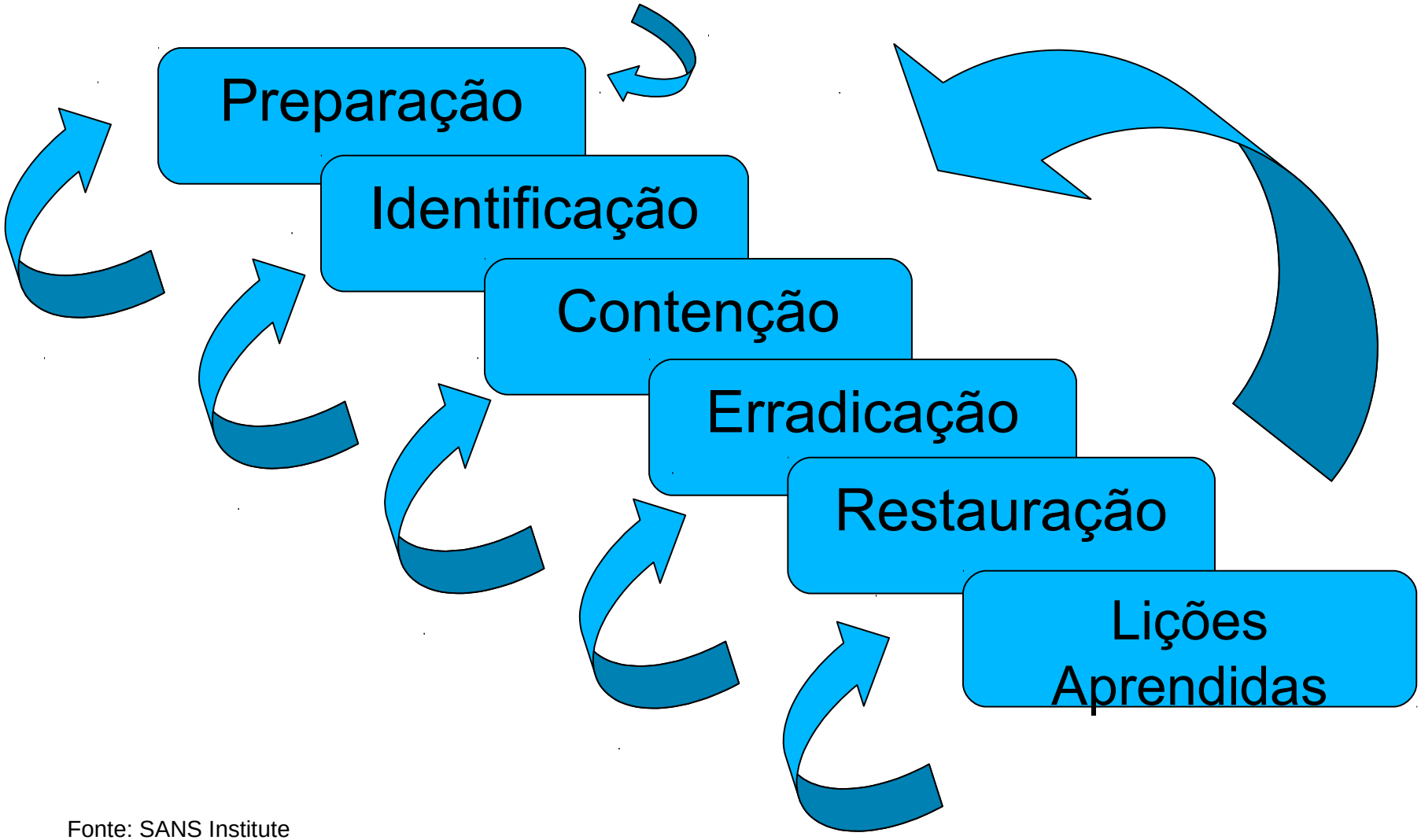
Two of the reports were conducted by the Ontario Provincial Police (OPP): the *Independent Investigation by the Ontario Provincial Police into the Death of Michael Zehaf-Bibeau*, further to the request of the Speaker of the House of Commons and the Royal Canadian Mounted Police; and the *Independent Investigation by the Ontario Provincial Police into the RCMP Security Posture on Parliament Hill*.

These two investigations included a detailed forensic analysis as well as a thorough account of the events, based on extensive interviews conducted with many witnesses.

The areas examined in the investigation into the RCMP's security posture included: the RCMP's security posture on the grounds of Parliament Hill at the time of the incident, including compliance with Standard Operating Procedures; and the RCMP's initial incident response, including actions of RCMP officers, operational communications and compliance with the Operational Preparedness Plan. From this report came 66 recommendations. Some of the recommendations have already been implemented while some will take additional analysis and consultation with our partners.

Also released today are the *RCMP's After Action Review* and the *House of Commons Incident Response Summary*. Information in the two OPP reports and the RCMP'S After Action Review has been redacted in order to protect personal privacy and the Parliament

Concluindo (2)



Fonte: SANS Institute

Para Reflexão

SEGURANÇA CIBERNÉTICA NO BRASIL

UM MANIFESTO POR MUDANÇAS

Para ajudar a aumentar a conscientização sobre segurança cibernética e sobre os riscos enfrentados, aqui está uma lista de cinco perguntas-chave para seus executivos:

Os riscos cibernéticos são levados em conta no processo global de planejamento corporativo?

Sabe quantos incidentes de segurança você sofreu no ano passado e a causa destes incidentes?

Quanto que uma falha de cibersegurança custaria para sua organização?

Você tem educado e treinado seus funcionários para reconhecer e responder à questão?

Você tem uma estratégia de segurança cibernética que está alinhada com sua estratégia de negócios, e ela é atualizada de acordo com as necessidades em evolução?

Juntos podemos rever leis, influenciar positivamente nossa economia e proteger o Brasil

www.cyber-manifesto.org
@cyber_manifesto

Links úteis

- DFIR
  http://dfir.com.br
- HTCIA Brasilia
  http://www.facebook.com/HTCIABrasilia
- CERT.br
  http://www.cert.br/docs/whitepapers/notificacoes
- DSIC
  http://dsic.planalto.gov.br/documentos/publicacoes
- SANS Institute Blogs
  http://www.sans.org/security-resources/blogs

Perguntas