Contrainteligência Cibernética - Uma abordagem prática para redes corporativas.

Colóquio Técnico de 2015 CTIRGov

Felipe Cavalcanti

1º Trimestre 2013

2.1 – Distribuição de notificações de incidentes por *status* e mês de criação

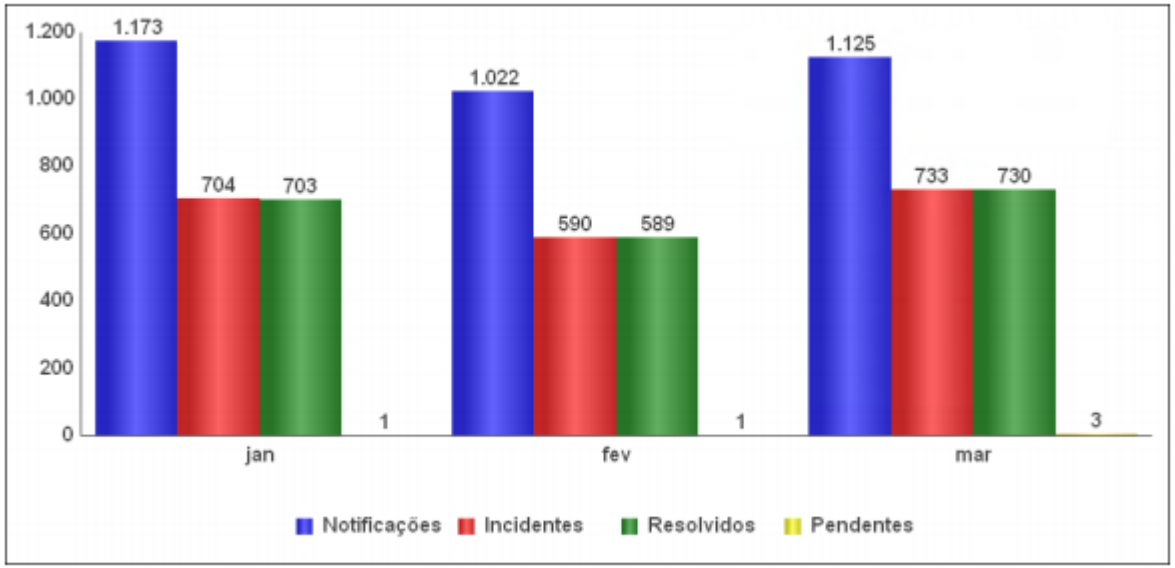


Gráfico 1 – Distribuição de notificações por *status* e mês de criação

Fonte: http://www.ctir.gov.br/arquivos/estatisticas/2013/Estatisticas_CTIR_Gov_1o_Trimestre_2013.pdf

1º Trimestre 2014

2.1 – Distribuição de notificações de incidentes por *status* e mês de criação

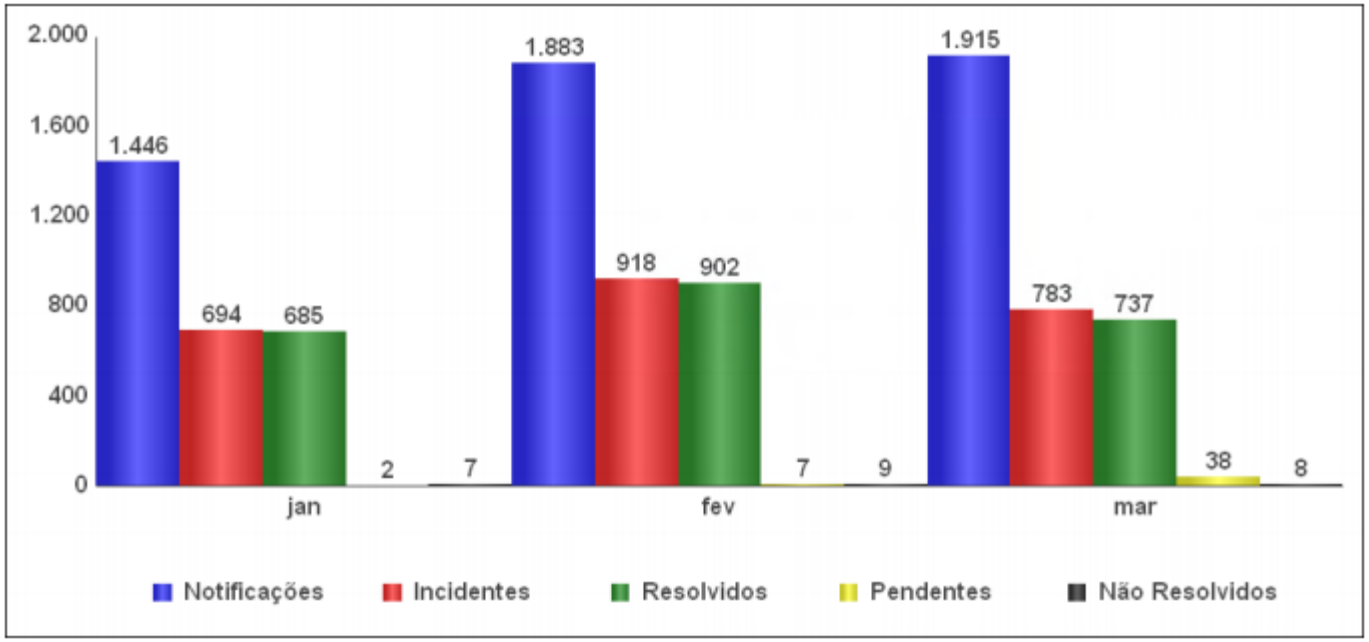


Gráfico 1 – Distribuição de notificações por *status* e mês de criação

Fonte: http://www.ctir.gov.br/arquivos/estatisticas/2014/Estatisticas_CTIR_Gov_1o_Trimestre_2014.pdf

1º Trimestre 2015

2.1 – Distribuição de notificações de incidentes por *status* e mês de criação

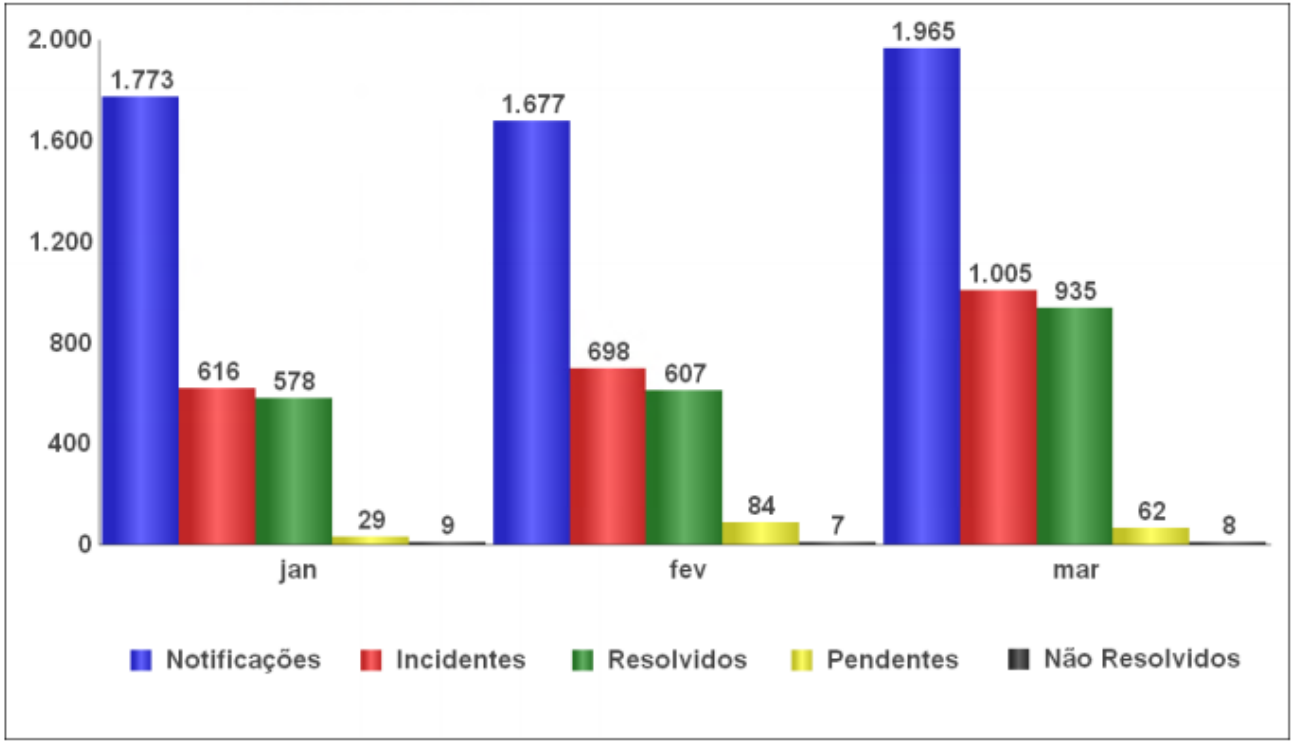
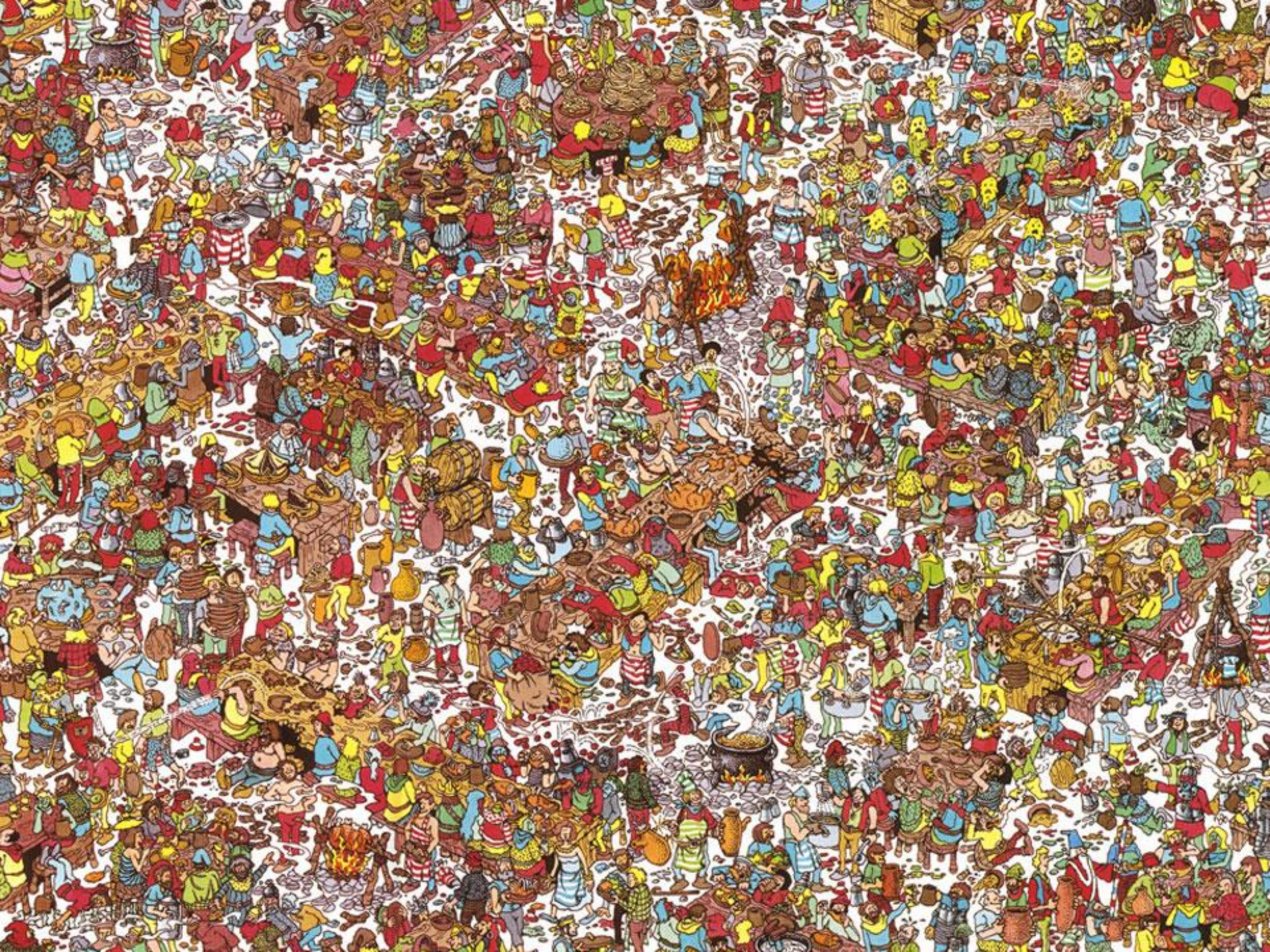


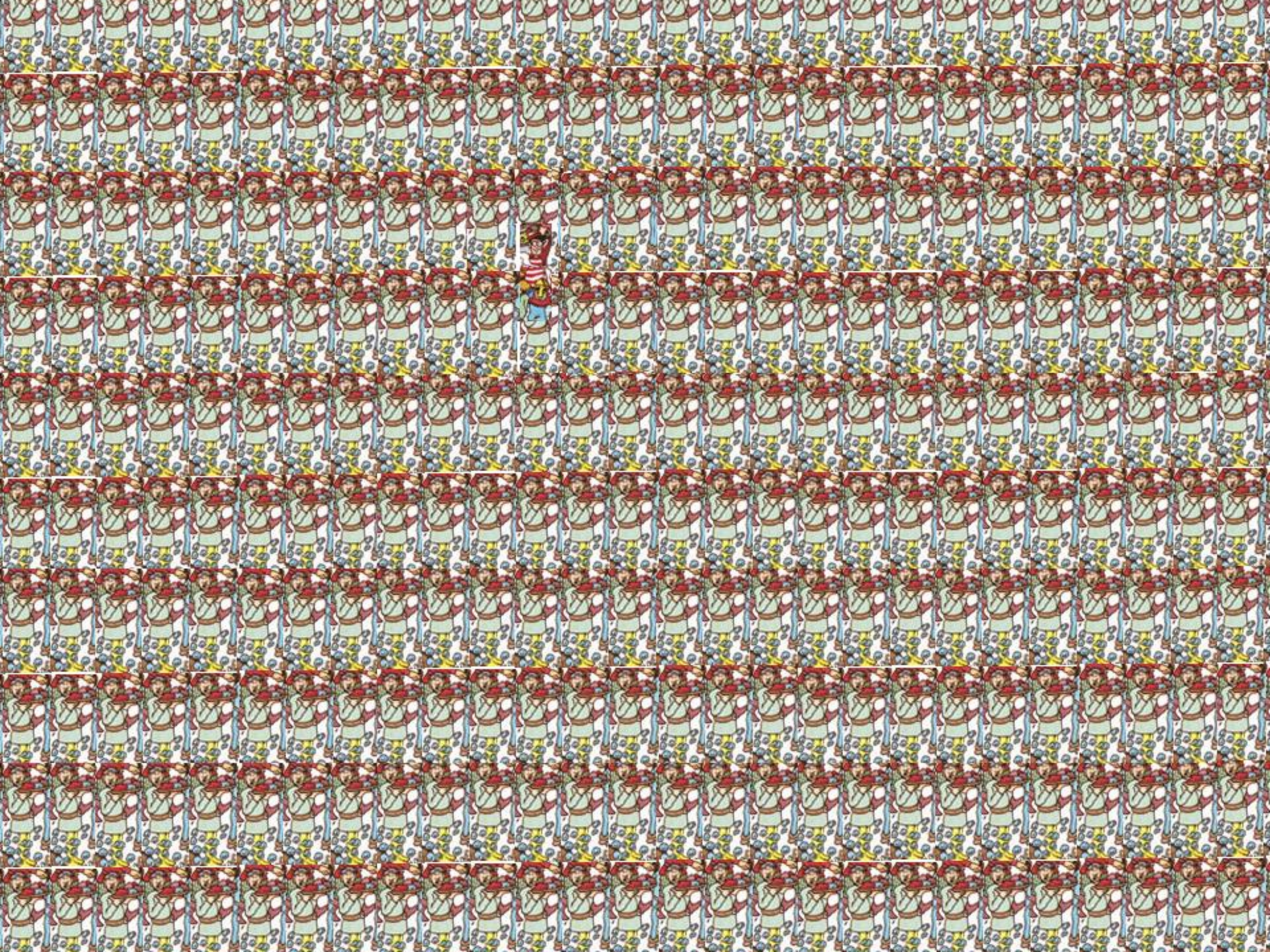
Gráfico 1 – Distribuição de notificações por *status* e mês de criação

Fonte: http://www.ctir.gov.br/arquivos/estatisticas/2015/Estatisticas_CTIR_Gov_1o_Trimestre_2015.pdf

Slide em branco 1. Não remover.



Slide em branco 2. Não remover.



AGENDA

Estratégias:

1. Prevenção para Estações de Trabalho.
2. Acesso à Internet.
3. Prevenção de Perda de Dados.
4. Detecção e Reação.

Handbook for Computer Security Incident Response Teams (CSIRTs)

Carnegie Mellon - Dezembro de 1998

2. Assuntos Básicos
2.3 Serviços de CTIR
2.3.2 Descrição dos Serviços
2.3.2.1 Serviços Reativos
2.3.2.2 **Serviços Proativos**

Norma Complementar n°08/IN01/DSIC/GSIPR

Serviços da ETIR:

7.3.6 Avaliação de segurança - Este serviço consiste em efetuar uma análise detalhada da infraestrutura de segurança em redes de computadores da organização com base em requisitos da própria organização ou em melhores práticas de mercado [...]

1. Prevenção para Estações de Trabalho

Sistema Operacional – Padrão único.

Objetivos:

i. Comportamento previsível;
ii. Controle das estações de trabalho;
iii. Dificuldade elevada para adulterar o padrão;
iv. Baixo risco de comprometimento devido ao acesso físico a estação de trabalho;

1. Prevenção para Estações de Trabalho

I. Inicialização por PXE (Rede);

II. Configuração da BIOS;

   I. "*Boot*" apenas por PXE ou HD;

   II. Habilitar *Trusted Platform Module* (TPM);

   III. Definir senha (aleatória);

III. Instalação do S.O.

   I. Criar partições;

   II. Entrega do S.O. / *Drivers*;

1. Prevenção para Estações de Trabalho

IV. Instalação de Aplicativos;

I. Antivírus;

II. Navegadores;

III. Produtividade;

V. Atualização Centralizada;

IV. Sistema Operacional;

V. Aplicativos (Navegadores, Flash, Java);

1. Prevenção para Estações de Trabalho

VI. Lista segura (*whitelist*) de aplicativos;

I. Diretórios de instalação (RX);

II. Assinatura Digital;

VII. Aplicação de políticas;

I. Regras de *Firewall*;

II. “Remoção” da conta *Admin* local;

III. Inclusão em grupos (estação de trabalho);

Olho na Norma

N° 07/IN01/DSIC/GSIPR

6.1.3.Utilizar conta de acesso no perfil de administrador somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

1. Prevenção para Estações de Trabalho

VIII. Criptografia de disco;

I. Armazenamento da chave no *TPM*;

II. Nenhuma interatividade;

IX. Controle de acesso à rede;

I. Certificado digital;

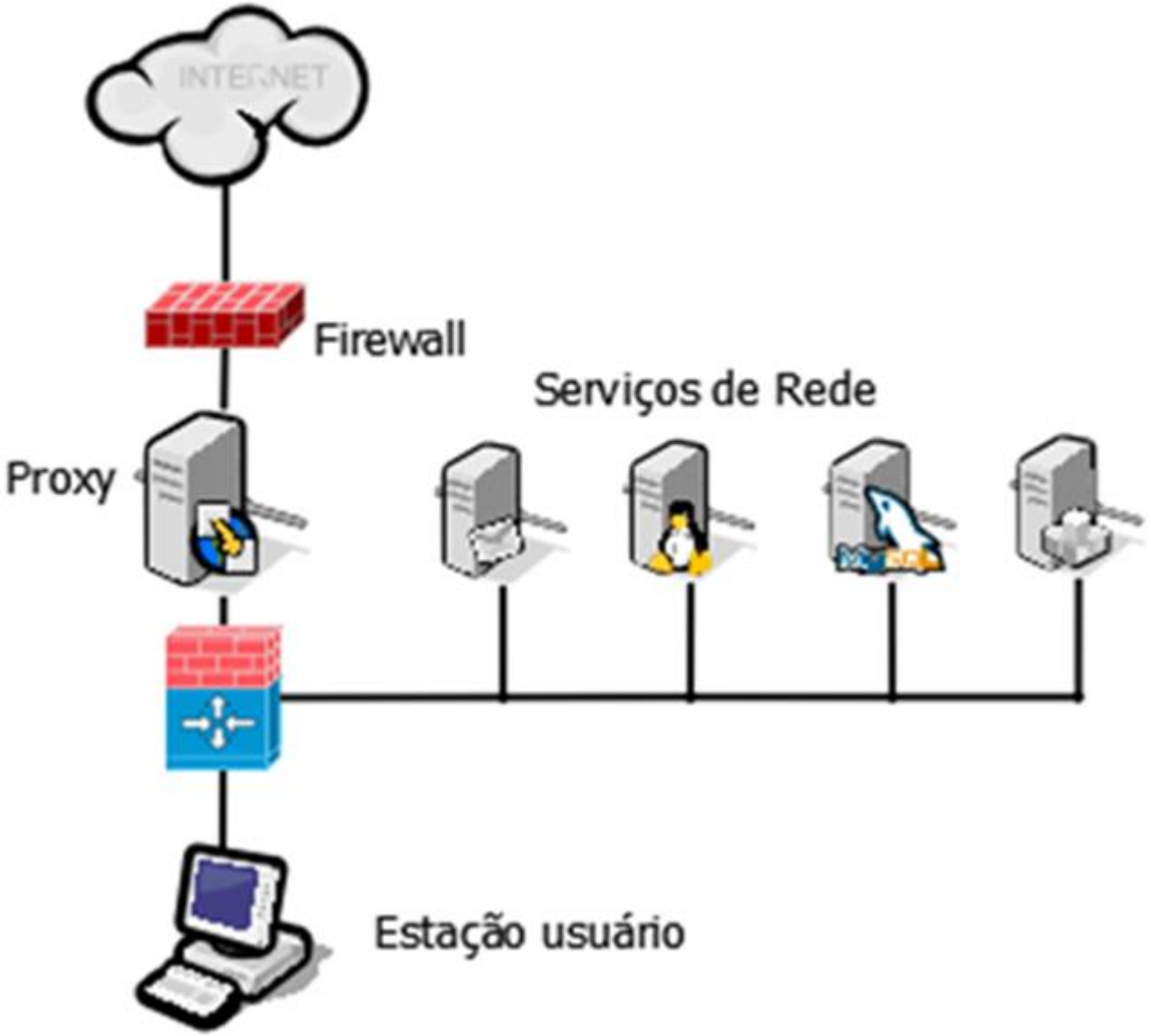
II. Switches com 802.1X EAP-TLS;

Olho na Norma

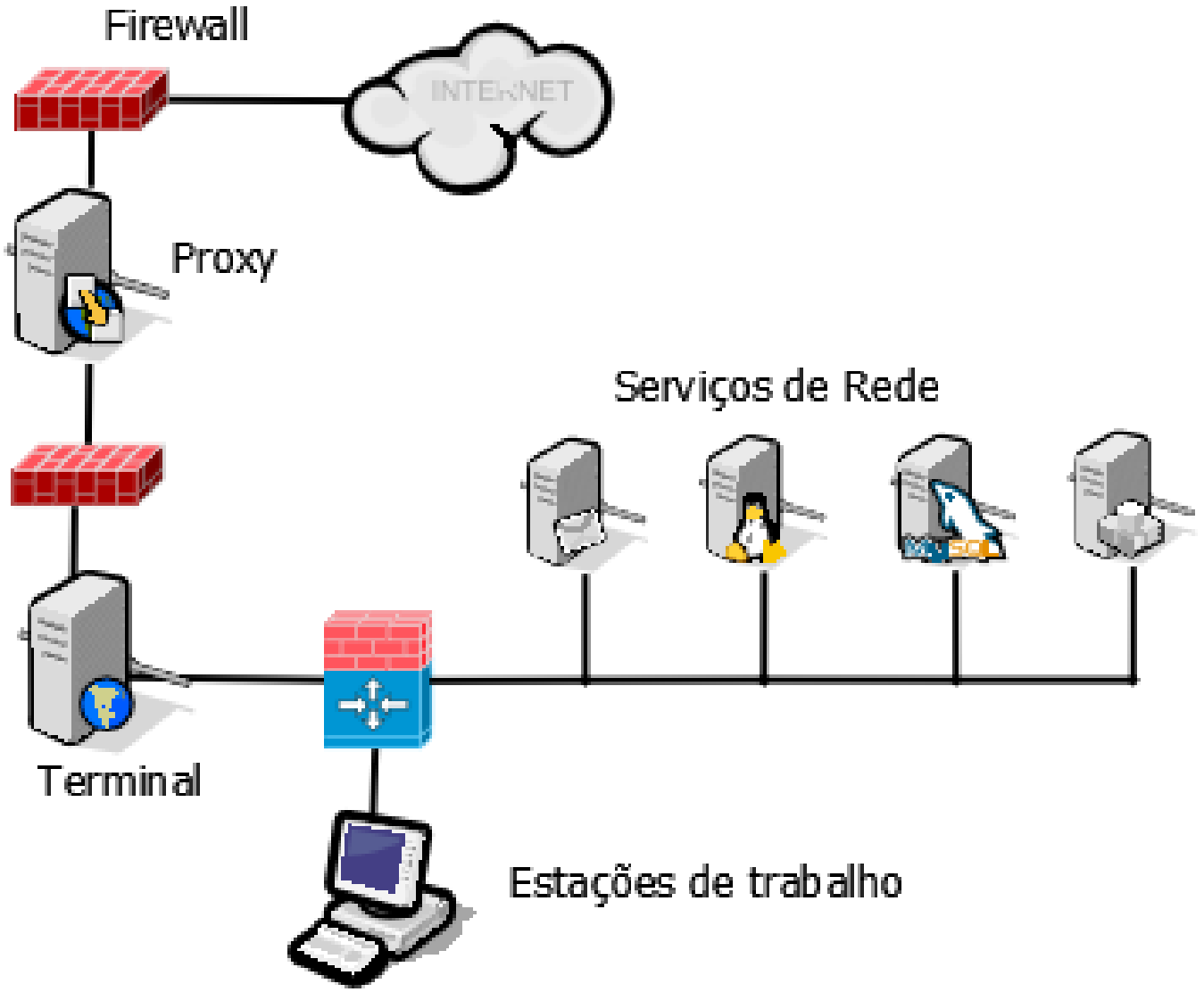
N° 07/IN01/DSIC/GSIPR

6.2.4. Utilizar mecanismos automáticos para inibir que equipamentos externos se conectem na rede corporativa de computadores.

MODELO DE REDE CONVENCIONAL
"ACESSO A INTERNET POR PROXY"



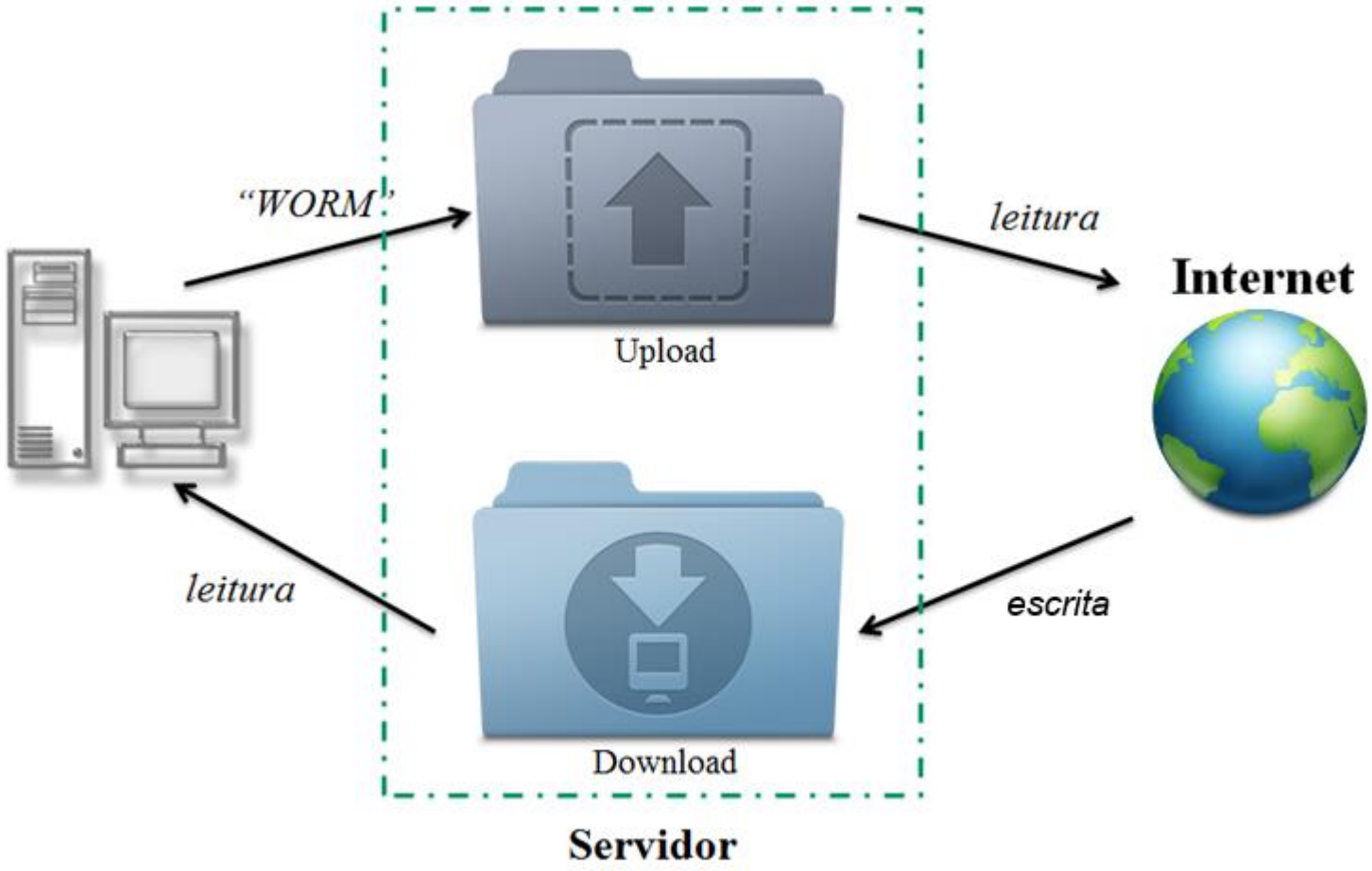
"ACESSO A INTERNET POR TERMINAL"



2. Acesso à Internet

- Vantagens:
  - Isolamento do acesso;
    - Contenção do *malware*: acesso limitado aos recursos;
    - Tráfego previsível em cada segmento;
  - Dificuldade de comunicação com *Comando e Controle* na infecção interna;
  - Fortalecimento dos servidores de Terminal;
    - SELINUX, EMET, HIDS, bloqueio de aplicativos;
  - Atualização de navegadores e *plug-ins*;
    - Menor tempo no Terminal;
    - Mais controlada nas estações de trabalho;

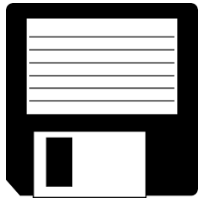
2. Acesso à Internet



3. Prevenção de Perda de Dados

- Bloquear:
  - Mídias Removíveis: USB, CD-ROM, Floppy;
  - Bluetooth;
  - Celular: ancoragem e mídia;
  - Impressoras locais.






3. Prevenção de Perda de Dados

- Porta RJ-45
  - Regra de firewall local (2 perfis):
    - Rede corporativa – Acesso;
    - Rede Pública – Bloqueio;
- Acesso à Internet por Terminal

3. Prevenção de Perda de Dados

- Criptografia completa do disco rígido.
- Armazenamento de chave no *TPM*. 
- Previne tentativas de vazamento através de:
  - Extração física do disco rígido;
  - Inicialização por S.O. paralelo.

Olho na Norma

N° 12/IN01/DSIC/GSIPR

5.1.2 Agentes públicos com dispositivos móveis corporativos [...] e) É recomendada a adoção de mecanismos que garantam a proteção e sigilo dos dados armazenados nos dispositivos em casos de extravio;

4. Detecção e Reação

I. Monitorar:
   a.) Estações de Trabalho;
   b.) Rede;

Monitoração de riscos residuais (desconhecidos ou assumidos) para detectar ameaças que eventualmente evadam as camadas de prevenção.

4. Detecção e Reação

Quais dados coletar?

- Integridade do sistema:
  - Alteração em disco e/ou em memória (*Ebury, Careto, Poweliks*).

Olho na Norma

N° 21/IN01/DSIC/GSIPR

6.5 Devem-se acompanhar os sistemas e redes de comunicação de dados, registrando-se os eventos de segurança elencados abaixo, sem prejuízo de outros considerados relevantes: [...]

f) Acesso ou modificação de arquivos ou sistemas considerados críticos[...]

4. Detecção e Reação

Quais dados coletar?

- Persistência:
  - Alteração de chaves de inicialização no registro*;*
  - Criação de serviços (*Stuxnet, Uroburos, Careto*);
- Processos (ativos na memória):
  - Caminho completo no disco;
  - Portas de comunicação;
  - Memória corresponde à imagem de disco?

4. Detecção e Reação

Quais dados coletar?

- Anomalias de fluxo;
- Anomalias de tráfego DNS;
- Anomalias de HTTP:
  - *User-Agent*;
  - *Referer*;
  - Chamadas direto para IP;
  - Envio de dados (*POST*);
  - Relação de entrada e saída;

4. Detecção e Reação

Reação

- Triagem
- Investigação
- Contenção
- Análise
- Recuperação

ENISA
https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management/at_download/fullReport

SANS
http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NIST 800-61
http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Olho na Norma

N° 05/IN01/DSIC/GSIPR

10.5 A ETIR poderá usar as melhores práticas de mercado[...]

4. Detecção e Reação

- Dados relevantes:
  - *IOCs*;
  - *Domínios/IPS*;
  - *Modus Operandi*;
- Compartilhamento de Conhecimento Situacional.

Olho na Norma

N° 02/IN01/DSIC/GSIPR

3.4 (“Act – A”) Agir - É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações aperfeiçoará as ações de segurança da informação e comunicações, baseando-se no monitoramento realizado na fase anterior.[...]