Centro de Informática e Sistemas

Paulo Crispim

pcrispim@ipt.pt

Incidentes@IPT no Campus do Politécnico de Tomar

ipt

Instituto Politécnico de Tomar

Problemas

- Dar resposta aos incidentes
  e Procedimentos lentos
- Diminuição de passwords caçadas (?)
- Diminuição dos equipamentos comprometidos no acesso (?)
- Servidores comprometidos
- Incapacidade de saber quem usa, o que usa, quando usa e usa durante quanto tempo.

Enquadramento (Sistemas)

- Plataformas Windows 2003, 2008 e 2012
- Plataformas Centos e Debian
- Alojamentos em websitepanel/MSPcontrol e ISPConfig3

- Existe “em datacenter” servidores geridos por, e para as engenharias
- Existe geridos pelo CIS servidores “em datacenter” para apoio aos docentes, estudantes e IPT.
- Temos servidores soltos na Engenharias

Problemas (sem atualizações)

- Windows 2008 com sintoma de doublepulsar

https://www.tenable.com/pvs-plugins/700059

Evidência:

[193.137.5.2XY] DOUBLEPULSAR SMB IMPLANT DETECTED!!! XOR Key: 0x886b8a5b

Informações complementares:

NI:I.RGEL.102-1.2xy

IP:193.137.5.2xy

MAC: 84:2b:2b:77:4d:9b

Bastidor: I0

Switch: BlocoI_rack_I0

Porta do switch: 1

Tomada (passivo): I-102-1 (significa, sala I102 tomada 1)

Resolução da vulnerabilidade:

https://support.microsoft.com/pt-pt/help/4013078/title (disponível no Windows update)

Problemas (zero-day)

- 19/04/2017-10:59 > introdução do ms40b.exe
- 19/04/2017-12:54 > introdução do w3wp.exe
- 11/05/2017-8:07 > introdução do ms29.exe
- 4/06/2017-9:10 > w3svc overflow, dcom overflow, introdução do bash.exe
- 14/06/2017-5:33 > w3svc overflow, dcom overflow, introdução do bash32.exe
- 25/06/2017-11:33 > w3svc overflow, dcom overflow, introdução do node32.exe
- 02/07/2017- 13:58:40 > w3svc overflow, dcom overflow, introdução do node.exe
- 08/07/2017-12:37:47 > w3svc overflow, dcom overflow, introdução do node.exe

- domingo, 9 de Julho de 2017 > instalação de WindowsServer2003-KB3197835-x86-custom-ENU.exe,
- compilado a 2016/10/07 e lançado a 13/06/2017 para corrigir a vulnerabilidade WebDAV remote code execution vulnerability (CVE-2017-7269)

Problemas (password)

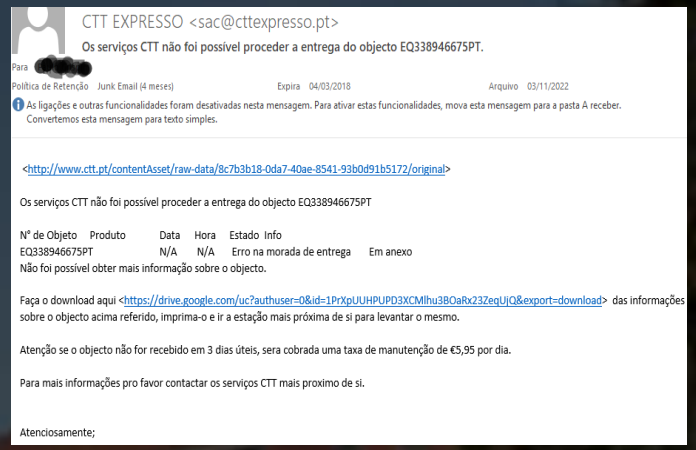
- Instalação do office 365 em múltiplas máquinas
  - As mesmas credenciais vagueiam …

- Uso do mesmo acesso em múltiplos dispositivos que podem não ser controlados pelo mesmo individuo
  - 11/06/2017,17:10:41,4,"xxxxxxx@ipt.pt",,"000B8640AFA0","C83870C6D1CA",,"194.210.240.98“
  - 11/07/2017,09:30:39,4,"xxxxxxx@ipt.pt",,"000B8640AFA0","EC9BF33C8969",,"194.210.240.206“ (desde 2jun2016)

Troca de password a 9 de novembro

  - 11/06/2017,17:10:34,4,"xxxxxxx@ipt.pt",,"000B8640AFA0","2C0E3DBEBB41",,"194.210.241.5“
  - 11/06/2017,18:28:02,4,"xxxxxxx@ipt.pt",,"000B8640AFA0","A8C83A03F71D",,"194.210.240.176"

Problema (spam)



CTT EXPRESSO <sac@cttexpresso.pt>

Os serviços CTT não foi possivel proceder a entrega do objecto EQ338946675PT.

Para [redacted]

Política de Retenção Junk Email (4 meses) Expira 04/03/2018 Arquivo 03/11/2022

As ligações e outras funcionalidades foram desativadas nesta mensagem. Para ativar estas funcionalidades, mova esta mensagem para a pasta A receber. Convertemos esta mensagem para texto simples.

<http://www.ctt.pt/contentAsset/raw-data/8c7b3b18-0da7-40ae-8541-93b0d91b5172/original>

Os serviços CTT não foi possível proceder a entrega do objecto EQ338946675PT

Nº de Objeto	Produto	Data	Hora	Estado	Info
EQ338946675PT		N/A	N/A	Erro na morada de entrega	Em anexo

Não foi possível obter mais informação sobre o objecto.

Faça o download aqui <https://drive.google.com/uc?authuser=0&id=1PrXpUUHPUPD3XCMlhu3BOaRx23ZeqUjQ&export=download> das informações sobre o objecto acima referido, imprima-o e ir a estação mais próxima de si para levantar o mesmo.

Atenção se o objecto não for recebido em 3 dias úteis, sera cobrada uma taxa de manutenção de €5,95 por dia.

Para mais informações pro favor contactar os serviços CTT mais proximo de si.

Atenciosamente;

- Phishing

(encomendas UPS, FedEx, ctt, dhl…)

(bancos BPI, BCP, Montepio, NB…)

- Utilização massiva da mesma password

(usam a mesma password para tudo e gravam-na no browser)

Problema (acesso indevido a alojamento)

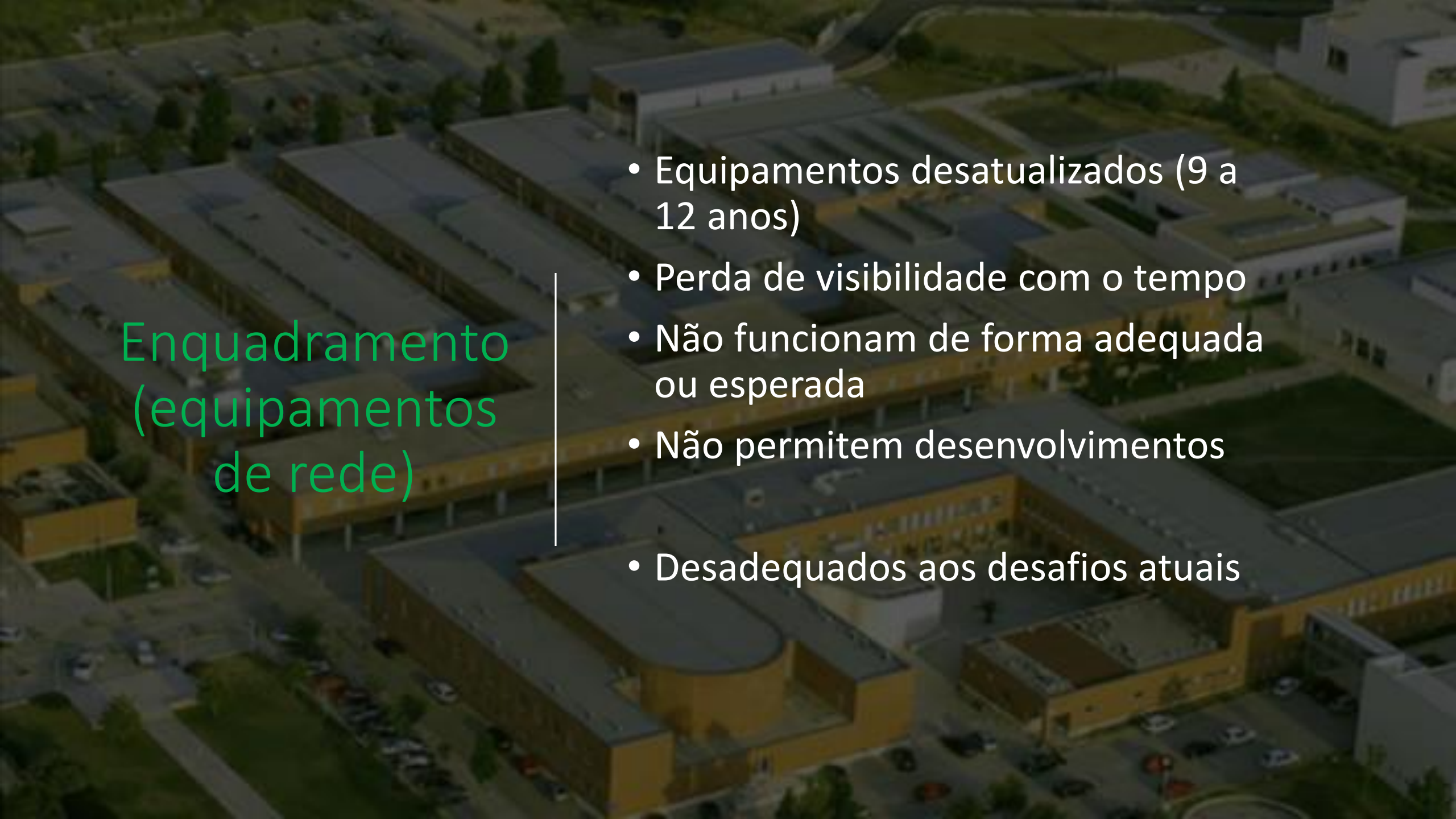
- Acesso ilegítimo ao email (consequência do problema de SPAM)
- Acesso ilegítimo ao alojamento (usamos MSPControl e ISPConfig3)

Problema (infeção local)

- Utilizador com dispositivo infetado com ransomware

Não “usa” anti-vírus
Não “usa” anti-malware
Não “usa” anti-ransomware (?)
(Por vezes as informações são confusas)
Consome www
Consome email
Consome pastas partilhadas e sincronizadas em serviços externos
Consome mensagens instantâneas
Deseja ligar-se à rede

(se o restauro estiver ativo pudemos ajuda-lo)



Enquadramento (equipamentos de rede)

- Equipamentos desatualizados (9 a 12 anos)
- Perda de visibilidade com o tempo
- Não funcionam de forma adequada ou esperada
- Não permitem desenvolvimentos
- Desadequados aos desafios atuais

Problema (DHCP ilegítimos e uso de IP de forma ilegítima)

- DHCP Snooping

O objectivo é prevenir que sejam colocados em qualquer ponto da rede dhcp’s não autorizados.

- Ip source guard

Evitar que sejam usados IP não entregues pela estrutura de forma dinâmica ou estática

- Notificação de novos MACaddress ou expirados

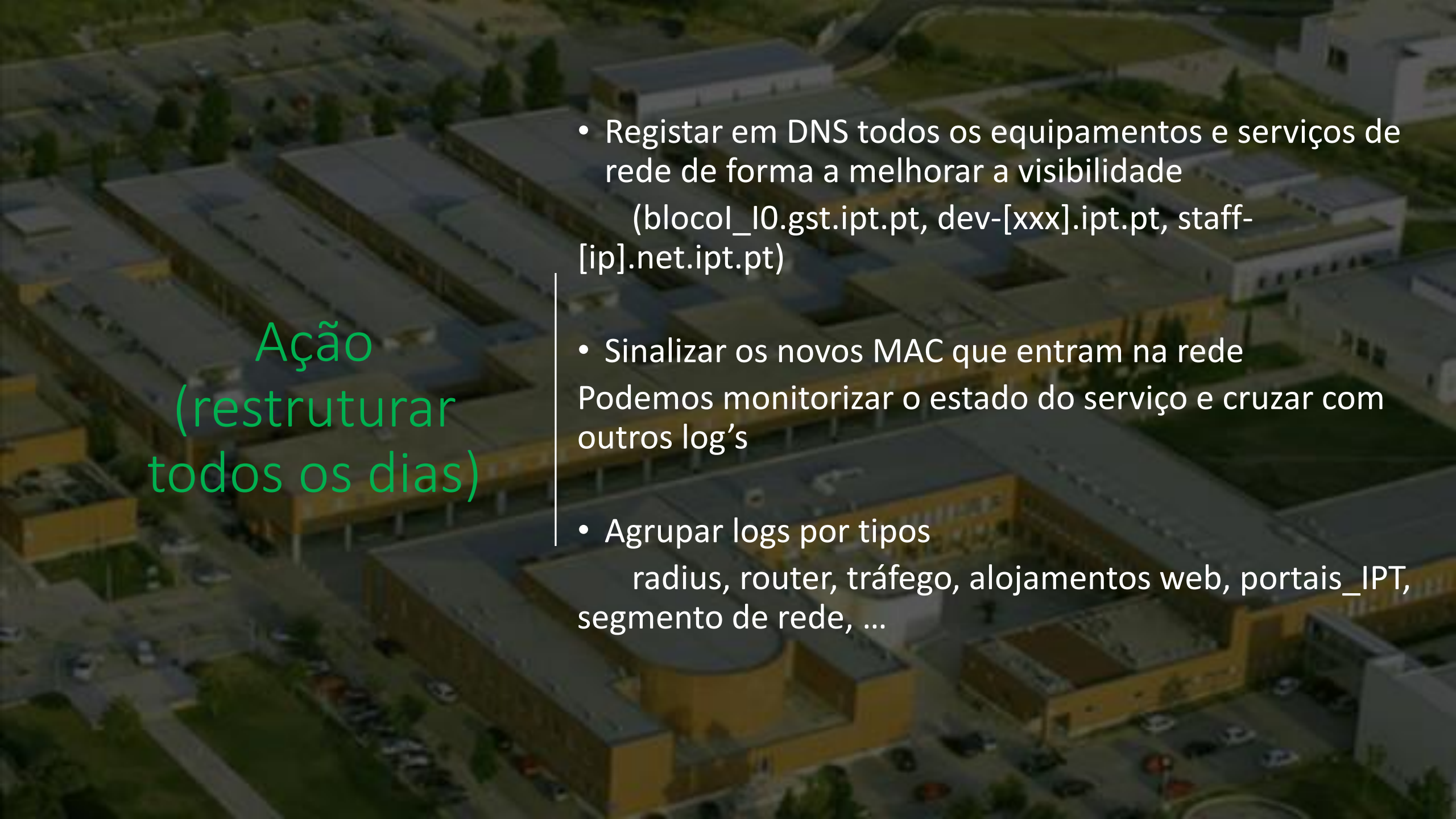
Estar atento ao dinamismo dos MAC para que quando for necessário, existir, para se poder investigar

Ação (restruturar todos os dias)

- Organizar e simplificar
  Cadastrar (muito pouco deve ficar ao acaso ou deve ser por tentativa)
  Quanto mais se pretende automatizar melhor deverá ser o cadastro
  Procurar estar atento ao detalhe

- Segmentar por tipos de utilização o mais possível
  _BlocoNN_rack_NNNXXX, _caboXXX, _radioXXX, _NATInf, _NATEletro, _adm, _salasXXX

- Autenticar por 802.1x (user e maquina) ou por MAC
  utilizar os registos que ficam no radius para cruzar com informação
  do registo de outros log's



Ação (restruturar todos os dias)

- Registar em DNS todos os equipamentos e serviços de rede de forma a melhorar a visibilidade

  (blocoI_I0.gst.ipt.pt, dev-[xxx].ipt.pt, staff-[ip].net.ipt.pt)

- Sinalizar os novos MAC que entram na rede

Podemos monitorizar o estado do serviço e cruzar com outros log's

- Agrupar logs por tipos

  radius, router, tráfego, alojamentos web, portais_IPT, segmento de rede, …

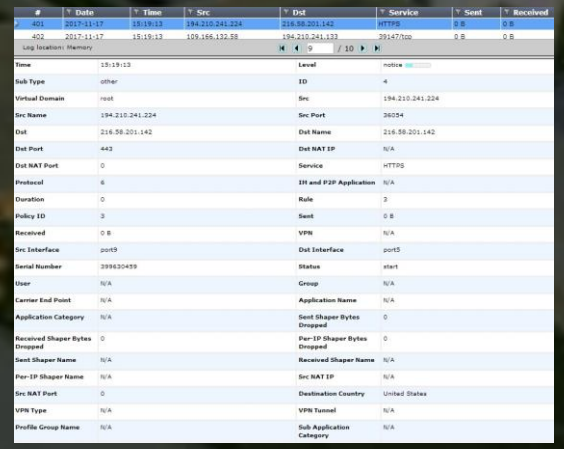
Ação (restruturar todos os dias)

- Interpretar a informação recebida
- Estabelecer modelos para as operações diárias
- Automatizar q.b. o mais possível

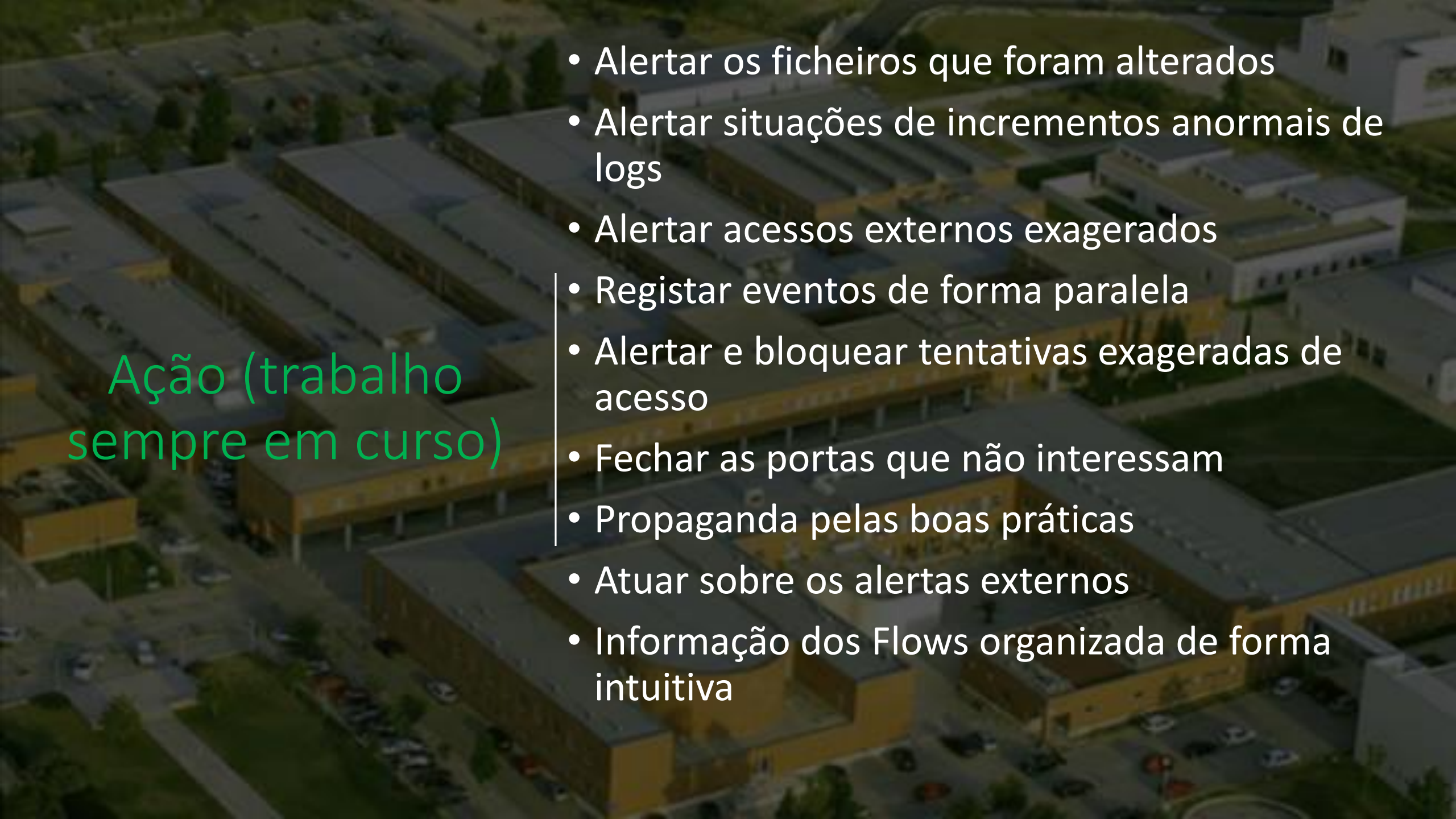
  python,

  perl,

  PS, Shell



- Usar uma rede de gestão (NAT para o exterior)
- Favorecer as operações fora de banda (em estrutura à parte)
- Registar as ligações e perceber os consumos



Ação (trabalho sempre em curso)

- Alertar os ficheiros que foram alterados
- Alertar situações de incrementos anormais de logs
- Alertar acessos externos exagerados
- Registar eventos de forma paralela
- Alertar e bloquear tentativas exageradas de acesso
- Fechar as portas que não interessam
- Propaganda pelas boas práticas
- Atuar sobre os alertas externos
- Informação dos Flows organizada de forma intuitiva

incidentes@IPT

Torna-se difícil passar uma mensagem de boas práticas que seja clara e fácil para todos os utilizadores.

Por vezes gostamos de partir para as grandes coisas porque admitir que as pequenas falharam é frustrante.

ipt
Instituto
Politécnico
de Tomar