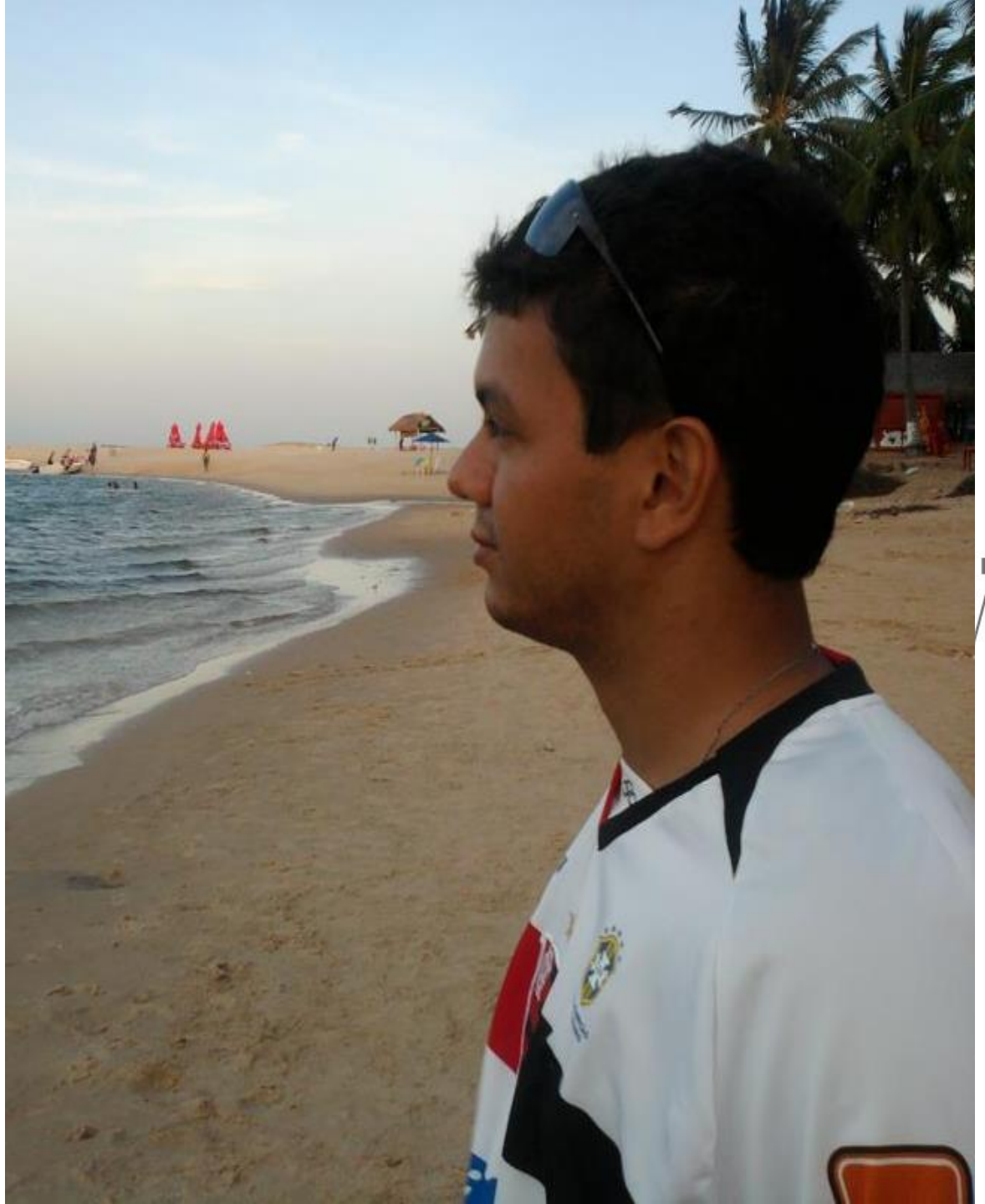
A importância da conscientização em ambientes corporativos para evitar prejuízos com ransomware

Yuri Alexandro
CAIS/RNP

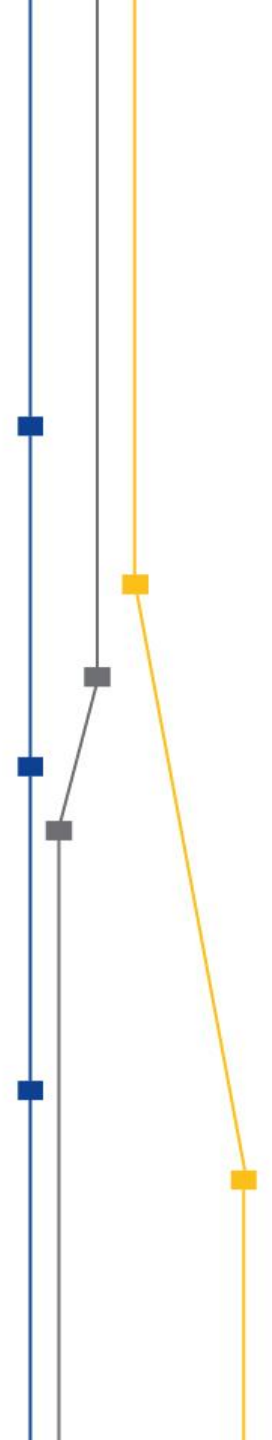
RNP
MINISTÉRIO DA DEFESA
MINISTÉRIO DA CULTURA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
BRASIL GOVERNO FEDERAL

Yuri Alexandro

- Não é AleSSandro, nem AleCHandro
- Analista de Sistemas desde 2007
- Especialista em Segurança da Informação desde 2010
- Certificado Modulo Security Officer desde 2011
- Soteropolitano com orgulho desde sempre
- Flamenguista desde vidas passadas



AWARENESS



“Ato ou efeito de (se) conscientizar.”

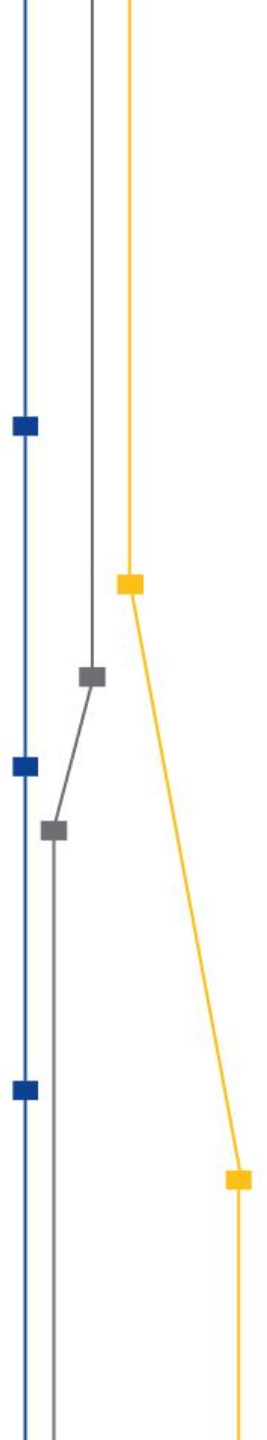
Dicionário do Aurélio

“É ato de se tornar consciente, esclarecido sobre algo.”

Wikipedia.org

“Ação de tomar conhecimento de algo, sendo que a partir de então, hábitos e atitudes poderão ser alterados para que possam se ajustar à nova realidade conhecida.”

significados.com.br



Relatório do TCU de Perfil de Governança de TIC Ciclo de 2014*

	Não adota	Adota parcial/integral
Organização realiza, de forma periódica, ações de conscientização, educação e treinamento em segurança da informação para seus colaboradores.	**63%**	**37%**

*Ciclo de 2016 em curso

Mais de **70%** dos incidentes de segurança da informação que causam prejuízos financeiros para organizações envolvem *insiders*.

Fonte: Gartners Group,2016

U$ 683 mil

média anual de perda financeira com ataques cibernéticos em empresas que não investem em conscientização segurança da informação.

U$ 162 mil

é o prejuízo anual ocasionado por incidentes de segurança em empresas que investiram nesse tipo de ação.

Fonte: Pricewaterhouse Coopers

POLÍTICAS DE SEGURANÇA, NORMAS E PROCEDIMENTOS

POLÍTICA, FERRAMENTAS, NORMAS E PROCEDIMENTOS

FERRAMENTAS PESSOAS

PONTO IMPORTANTE Nº 1

ISO 27002

7.2.2 Conscientização, educação e treinamento em segurança da informação

Controle

Convém que todos os funcionários da organização e, onde pertinente, partes externas devem recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

PONTO IMPORTANTE Nº 2

Considerar os níveis de funções dentro da Organização

NÍVEL GERENCIAL

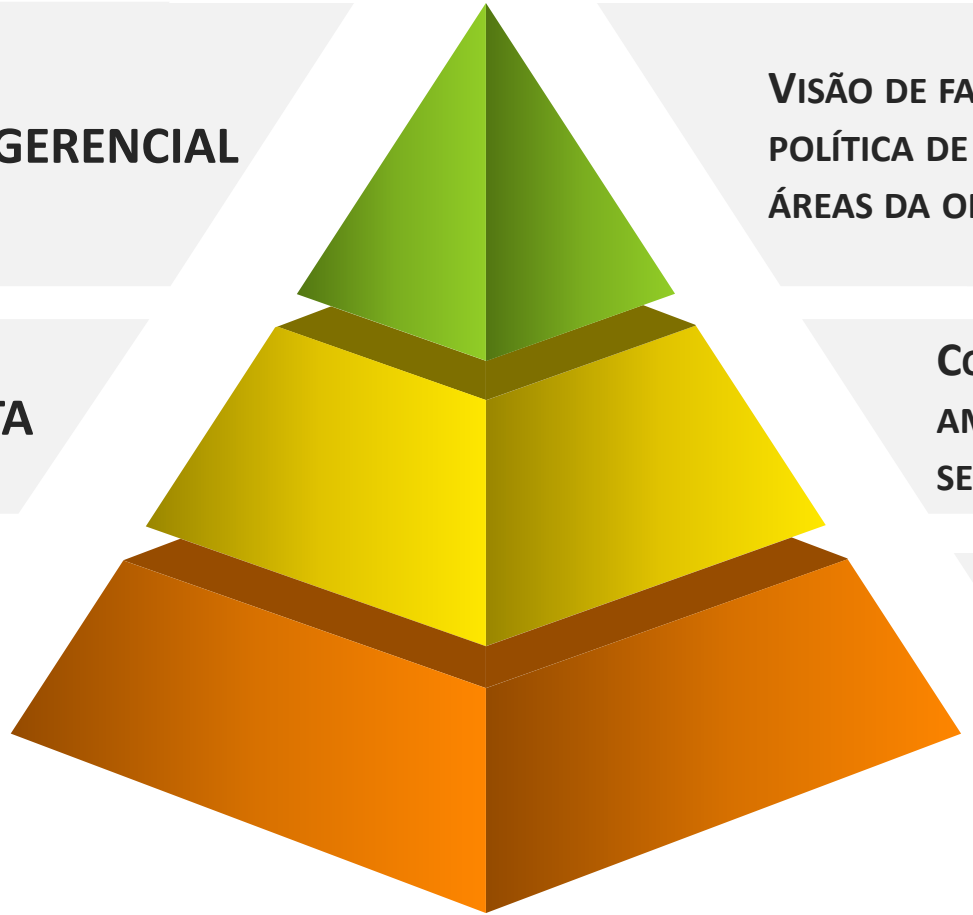
VISÃO DE FATORES DE RISCO E DA POLÍTICA DE SEGURANÇA ENTRE AS ÁREAS DA ORGANIZAÇÃO

NÍVEL DE ESPECIALISTA

CONSTRUIR E MANTER O AMBIENTE COMPUTACIONAL SEGURO NA ORGANIZAÇÃO

NÍVEL PESSOAL

RECONHECER E EVITAR AMEAÇAS



PONTO IMPORTANTE Nº 3

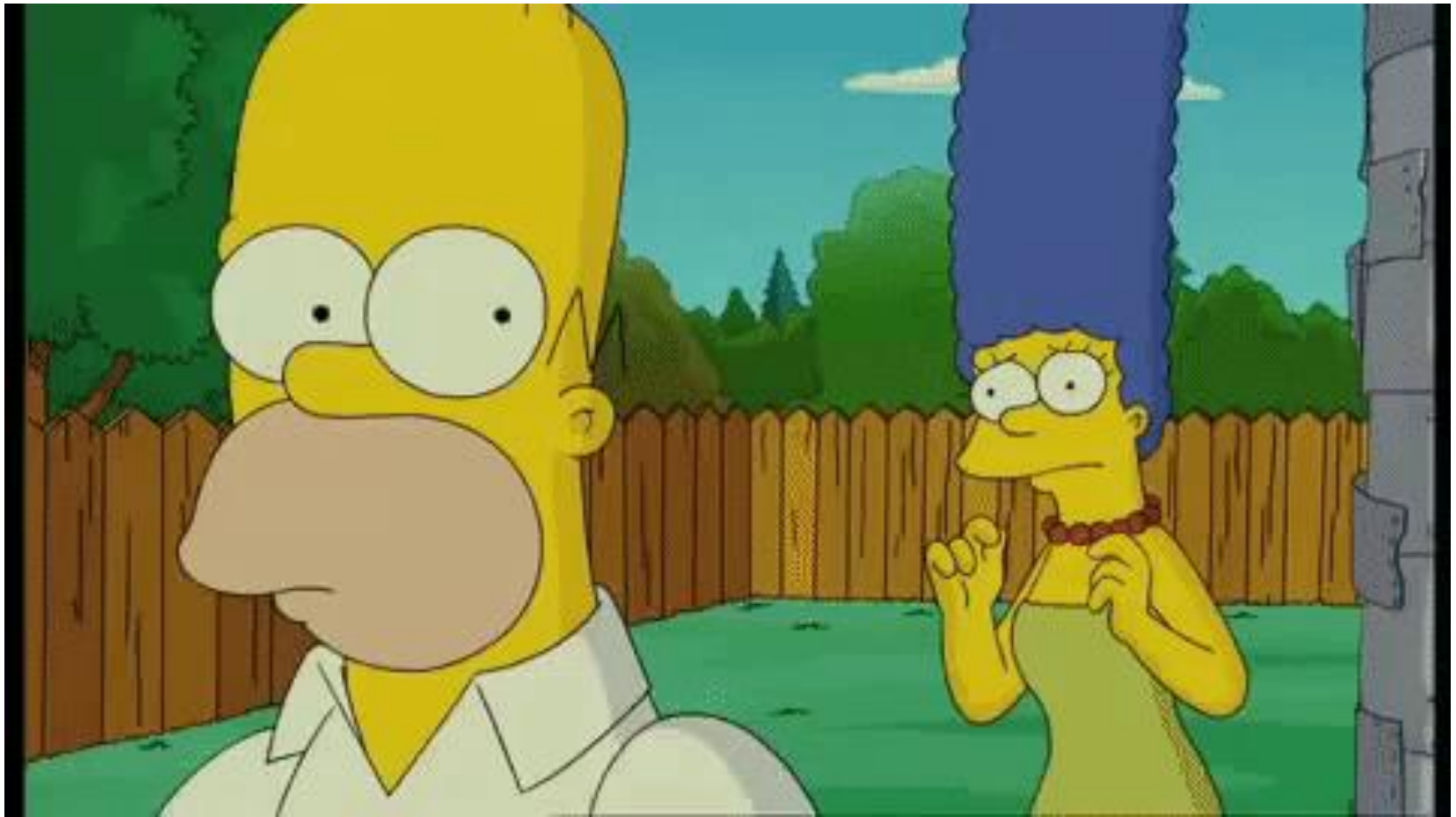
Ter uma equipe responsável pela conscientização, formada por pessoas de diferentes áreas da organização

PONTO IMPORTANTE Nº 4

A conscientização deve respeitar a cultura organizacional

PONTO IMPORTANTE Nº 5

Conscientização é MAIS que SÓ palestra!



PONTO IMPORTANTE Nº 6

Conscientizar NÃO é colocar medo nas pessoas!

PONTO IMPORTANTE Nº 7

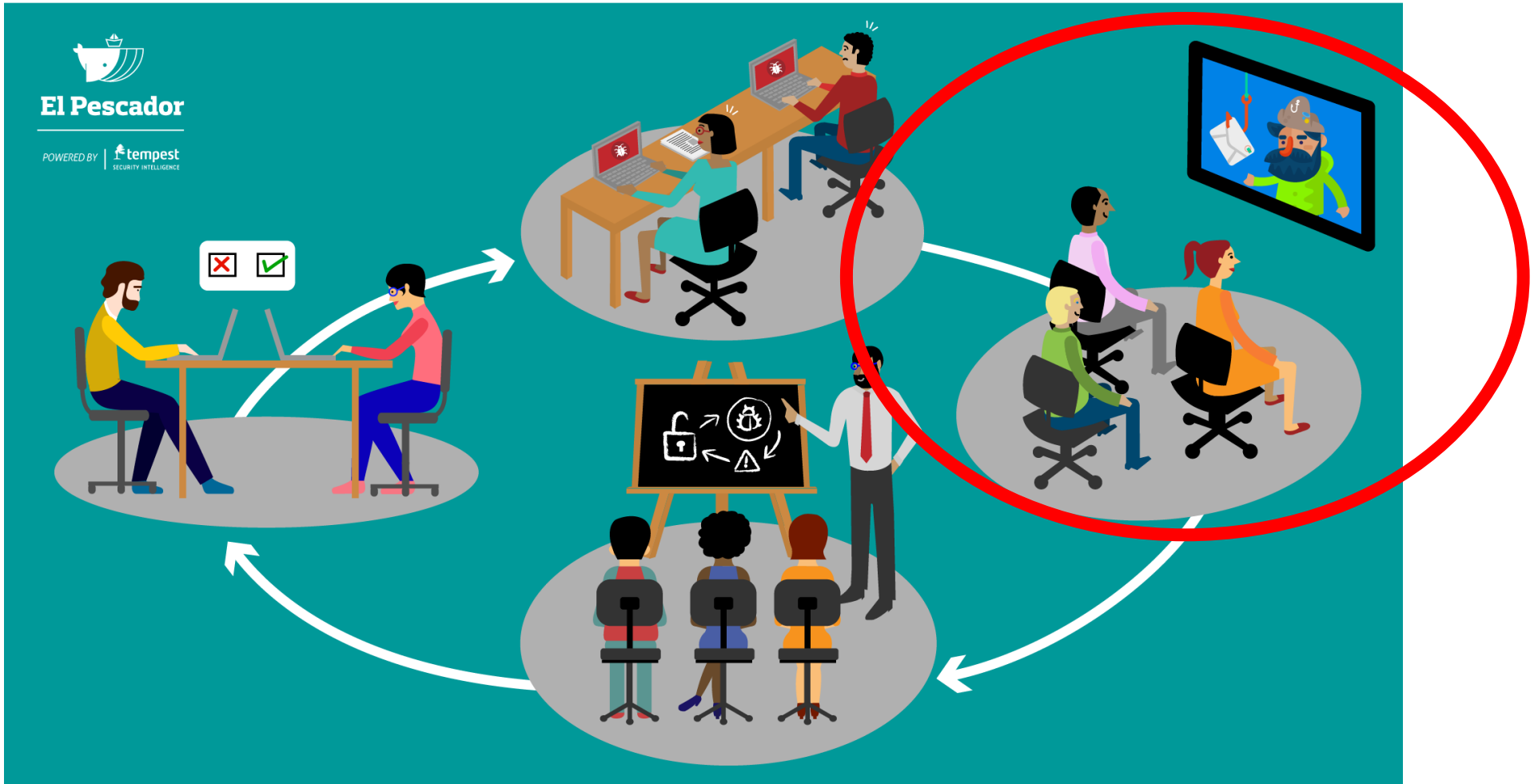
Trabalhar com o conceito de CICLO EDUCATIVO

PONTO IMPORTANTE Nº 7

Trabalhar com o conceito de CICLO EDUCATIVO: AVALIAR

PONTO IMPORTANTE Nº 7

Trabalhar com o conceito de CICLO EDUCATIVO: EDUCAR



PONTO IMPORTANTE Nº 7

Trabalhar com o conceito de CICLO EDUCATIVO: REFORÇAR

PONTO IMPORTANTE Nº 7

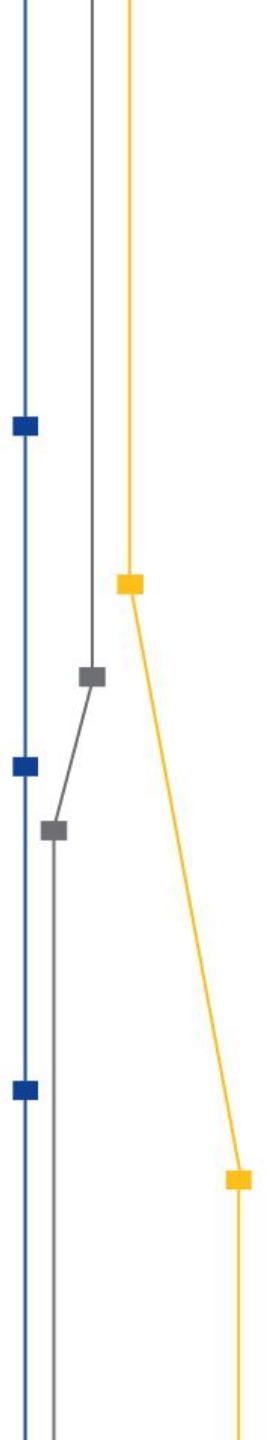
Trabalhar com o conceito de CICLO EDUCATIVO: MEDIR

PONTO IMPORTANTE Nº 8

Estabelecer metas e incentivos para os colaboradores da organização

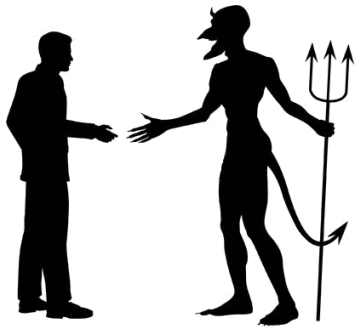
COMO TRABALHAR A CONSCIENTIZAÇÃO PARA EVITAR PREJUÍZOS COM O RANSOMWARE?

IDENTIFICAR OS VETORES



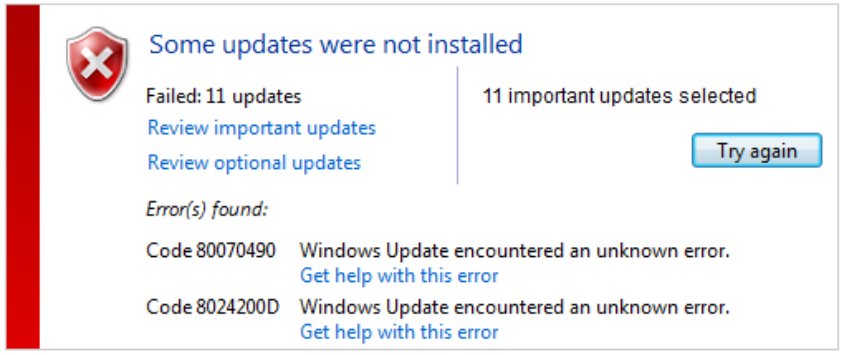
IDENTIFICAR OS VETORES

phishing

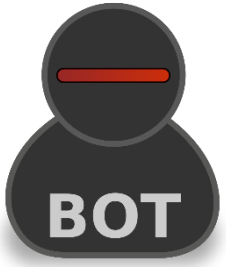


engenharia social

sites maliciosos



sistemas desatualizados

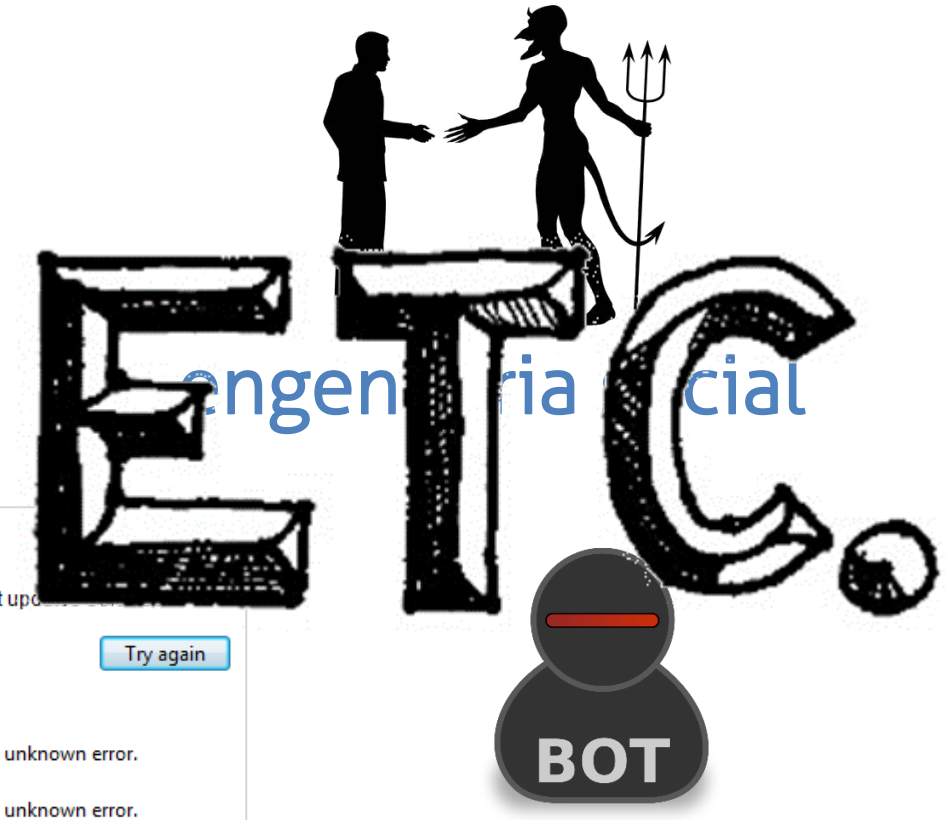


botnets

softwares piratas

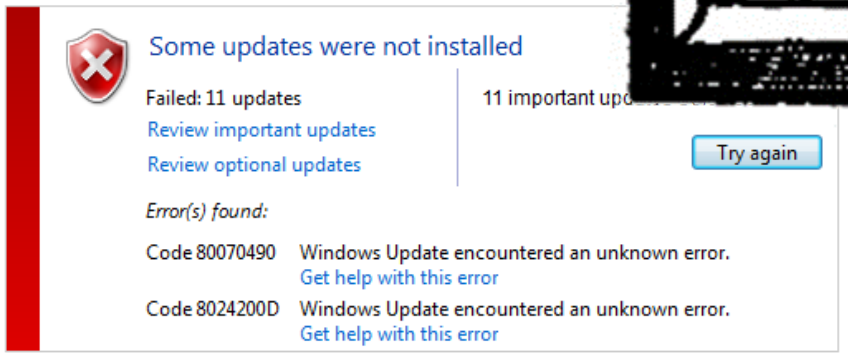
IDENTIFICAR OS VETORES

phishing



engenharia social

sites maliciosos

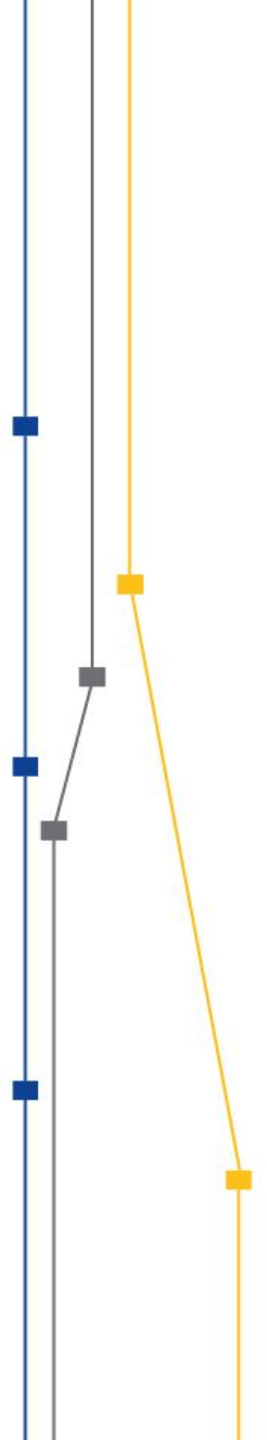


sistemas desatualizados

botnets

softwares piratas

ESCOLHER OS MÉTODOS



ESCOLHER OS MÉTODOS

Palestras

Webinar - Backup - O básico cada vez mais essencial

Seminários online / webinars

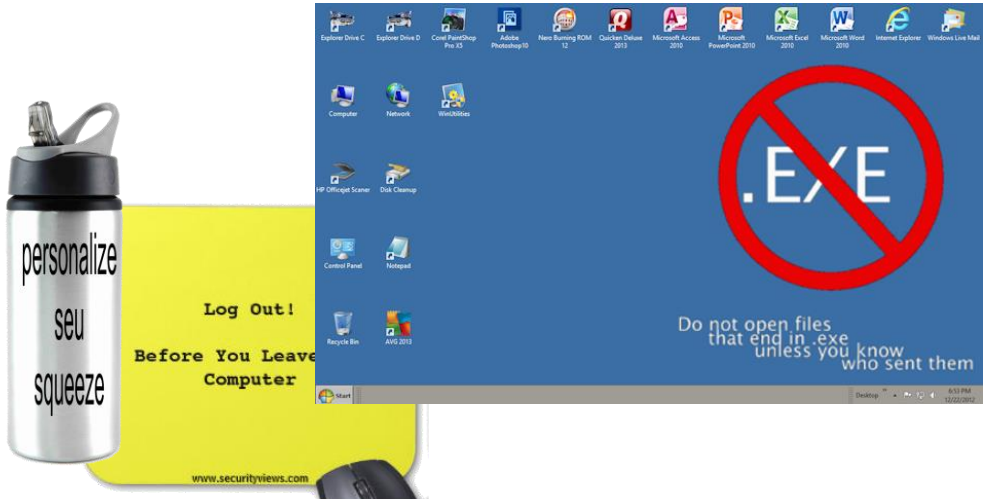
ESCOLHER OS MÉTODOS

Mailing list

Cartilhas

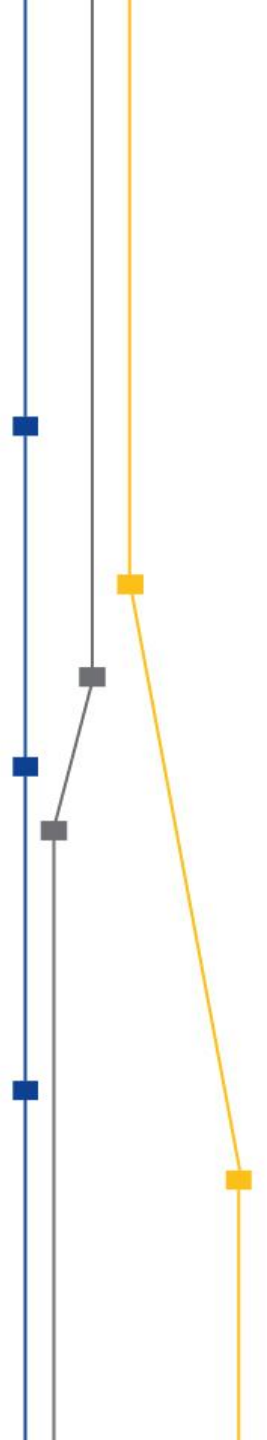
ESCOLHER OS MÉTODOS

Gamification



Wallpapers e outros materiais

CONSCIENTIZAR PARA...



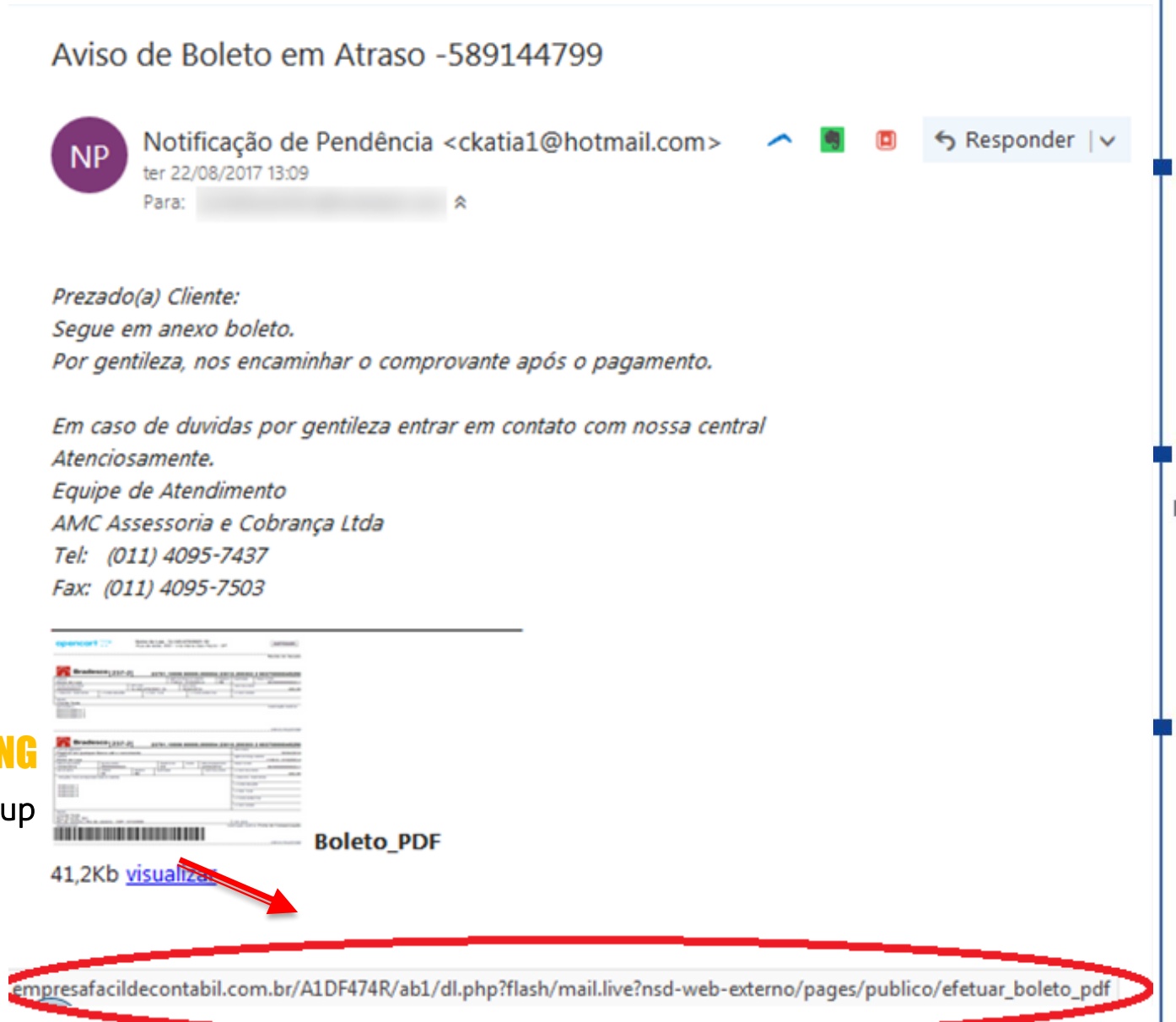
CONSCIENTIZAR PARA...

Identificar mensagens, sites e e-mails maliciosos

95%

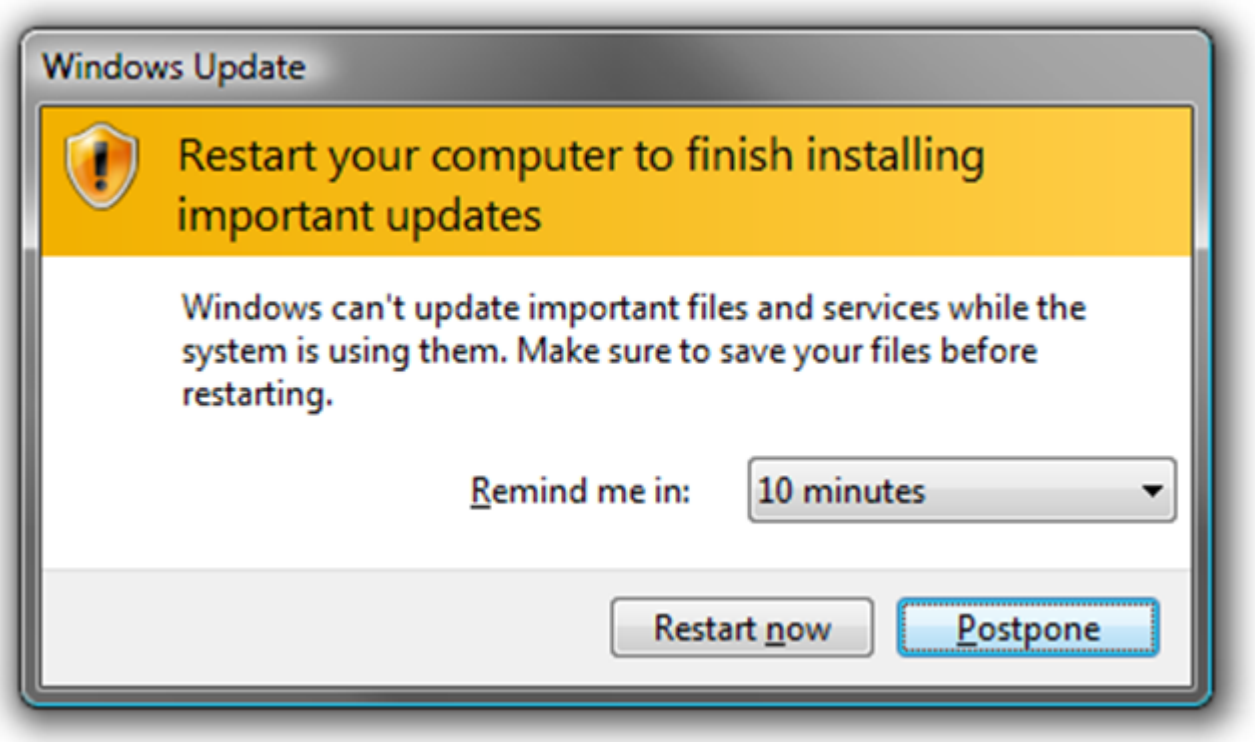
DAS AMEAÇAS DIGITAIS COMEÇAM POR PHISHING

Fonte: Gartners Group



CONSCIENTIZAR PARA...

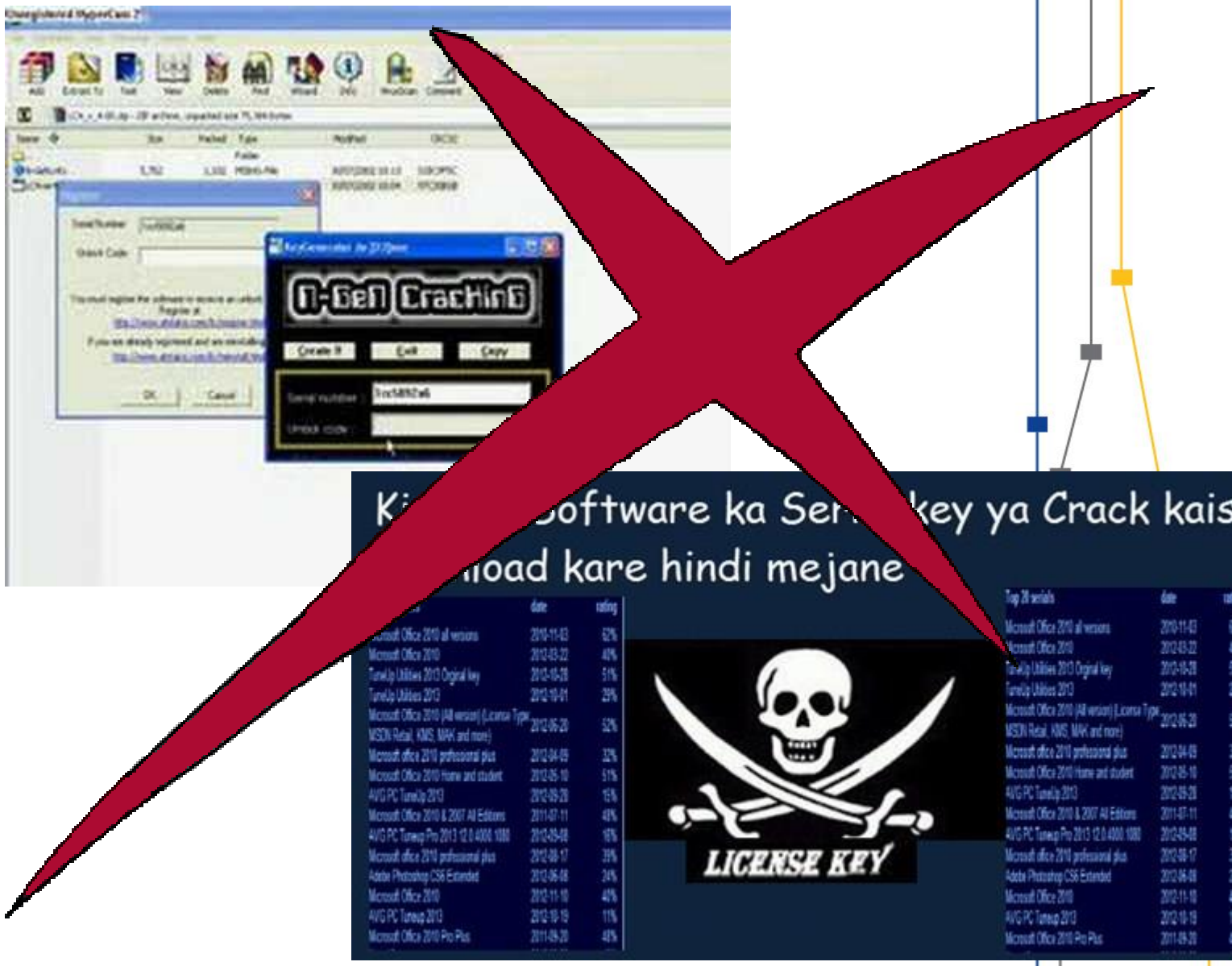
Reiniciar o computador para aplicar as atualizações do sistema



COMPUTADOR SEM REINICIAR = COMPUTADOR DESATUALIZADO

CONSCIENTIZAR PARA...

Não fazer download de arquivos ou softwares que "quebram" licenças de outros softwares.



CONSCIENTIZAR PARA...

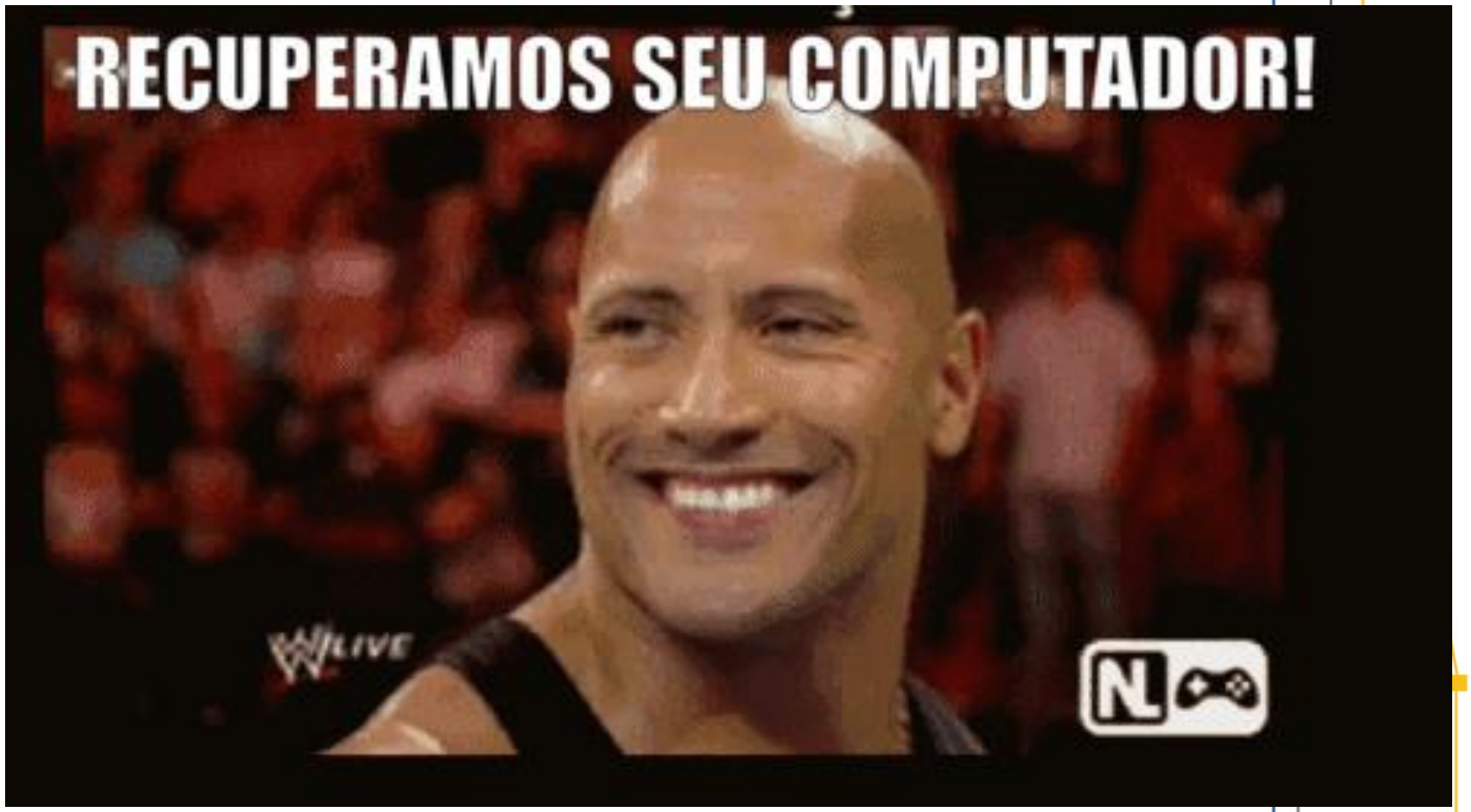
Não usar mídias removíveis de origem desconhecida

CONSCIENTIZAR PARA...

Bloquear sempre o computador quando se ausentar.

CONSCIENTIZAR PARA...

Realizar cópias de segurança dos dados corporativos periodicamente



CONSCIENTIZAR PARA...

Reportar à equipe de segurança qualquer problema ou desconfiança

CONSCIENTIZAR PARA...

Não pagar o resgate!

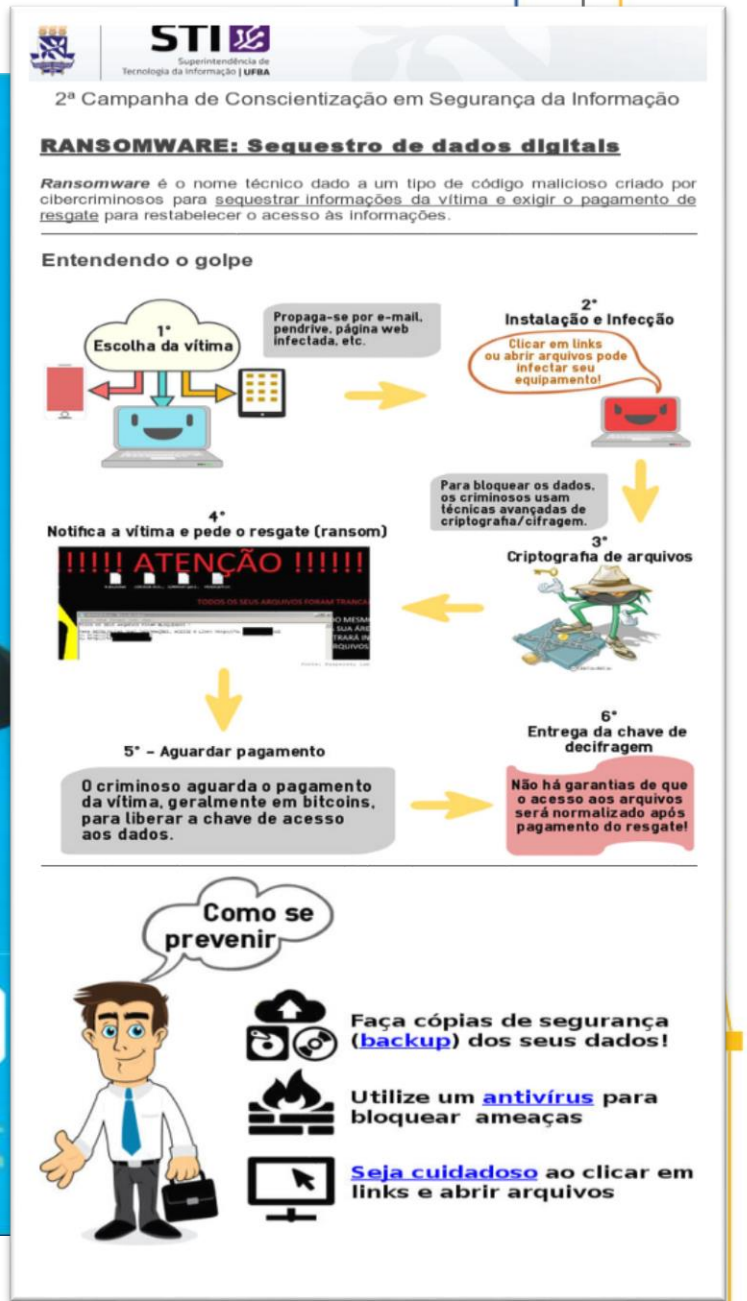
BYOD

Instruir o colaborador a ter o hábito de uso seguro da tecnologia também em casa.

CASE

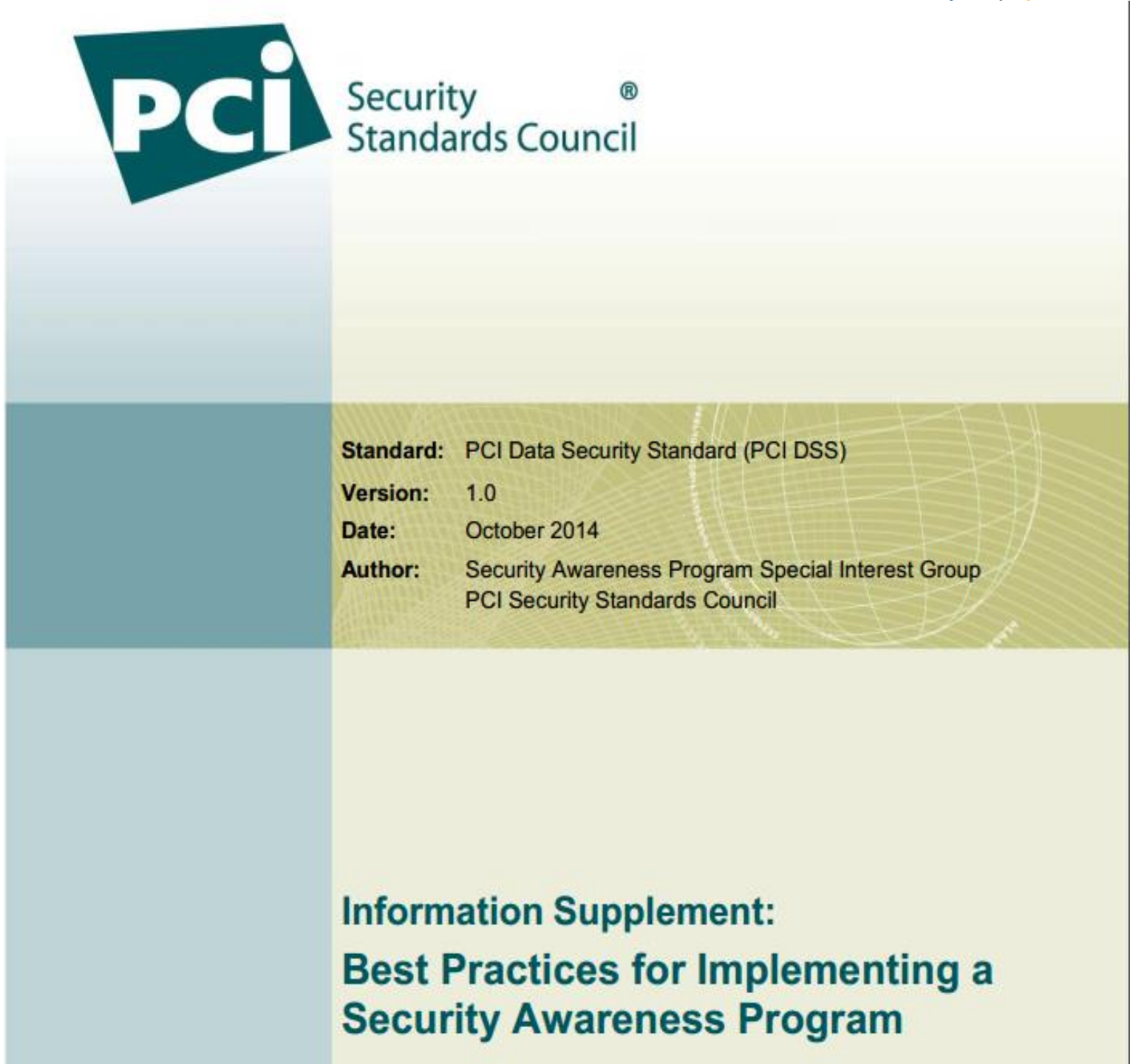
Universidade Federal da Bahia

- Produção de conteúdo informativo, com linguagem simples
- Produção e distribuição de cartilhas
- Divulgação/comunicação realizada por e-mail
- Realização do EnSI, evento anual voltado para palestras de conscientização
- Nenhum registro de *ransomware* nos últimos grandes ataques.



REFERÊNCIA

http://bit.ly/infosecawereness



Perguntas?

RNP

MINISTÉRIO DA DEFESA

MINISTÉRIO DA CULTURA

MINISTÉRIO DA SAÚDE

MINISTÉRIO DA EDUCAÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES

BRASIL GOVERNO FEDERAL