

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

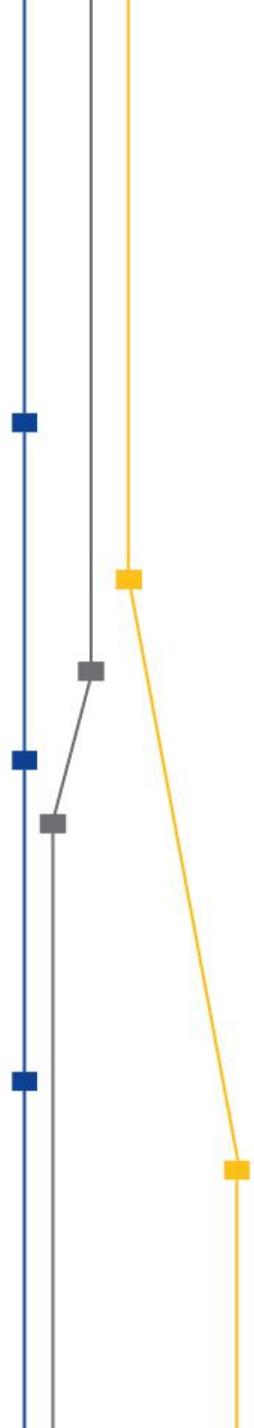
Yuri Alexandro  
CAIS/RNP

# 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.”

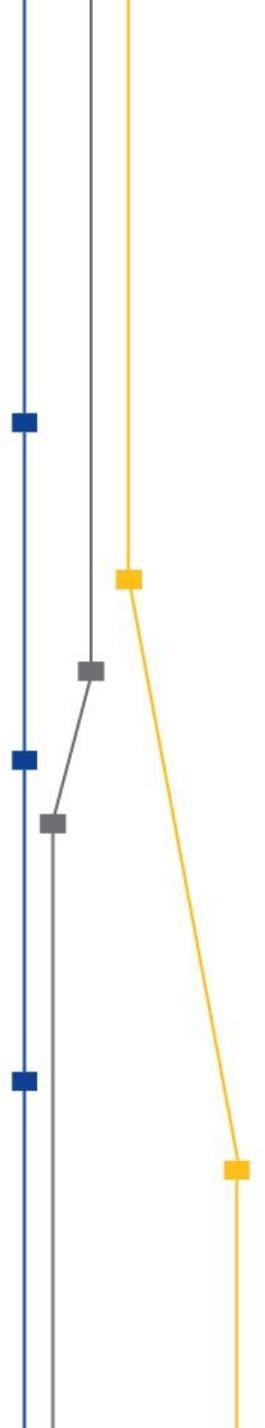
Dicionário do Aurélio

“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.”

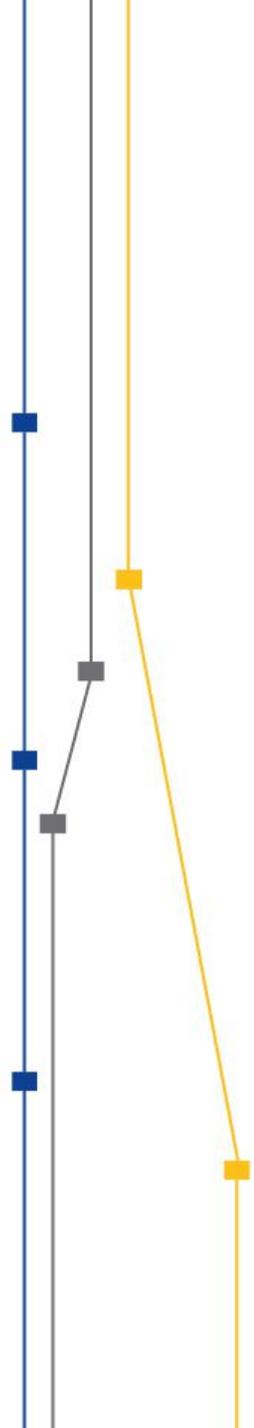
significados.com.br



## 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.	<b>63%</b>	<b>37%</b>

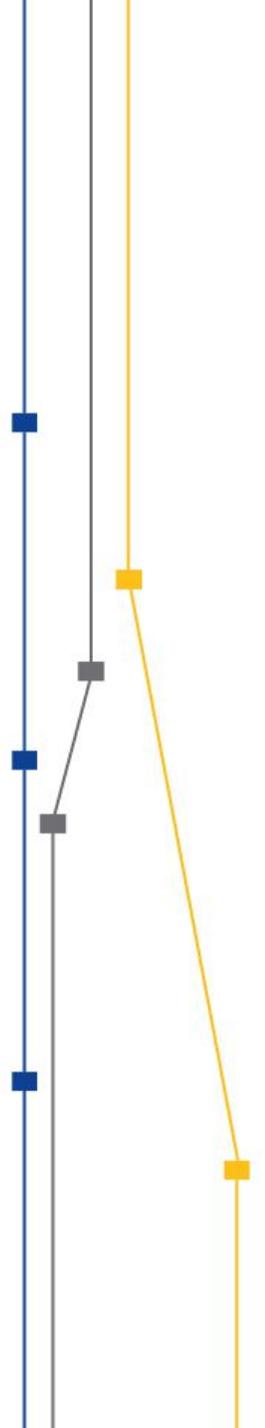
\*Ciclo de 2016 em curso





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

Fonte: Gartners Group,2016



# US\$ 683 mil

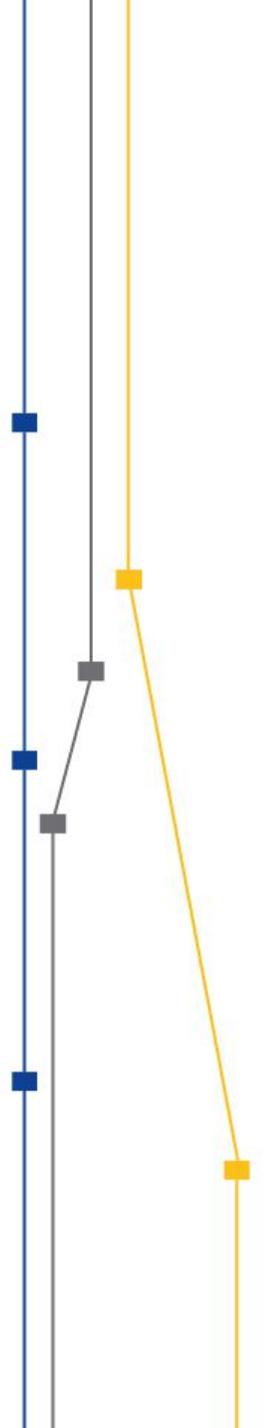
média anual de perda financeira com ataques cibernéticos em empresas que não investem em conscientização segurança da informação.



# US\$ 162 mil

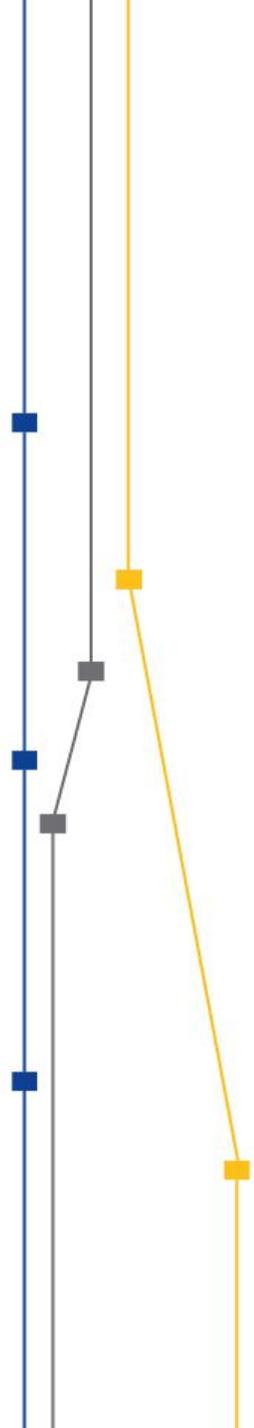
é o prejuízo anual ocasionado por incidentes de segurança em empresas que investiram nesse tipo de ação.

Fonte: Pricewaterhouse Coopers



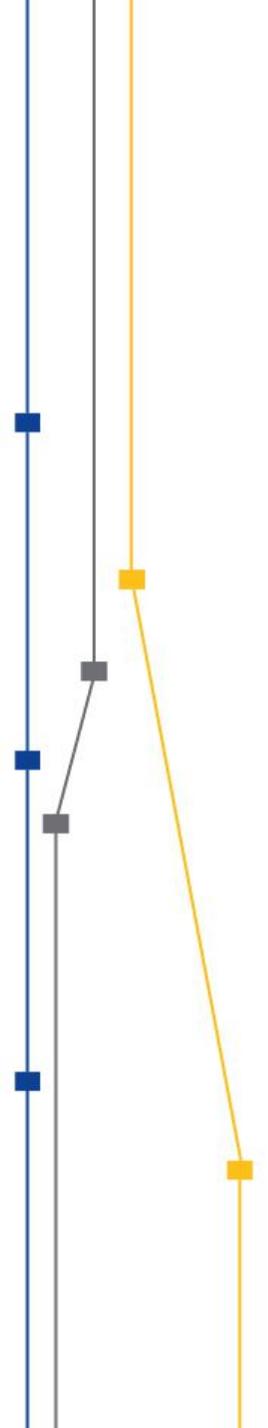


**POLÍTICAS DE SEGURANÇA,  
NORMAS E PROCEDIMENTOS**



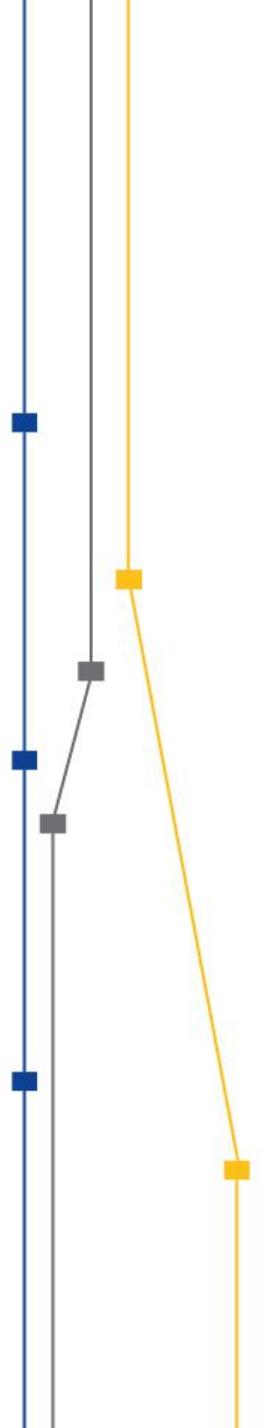


**POLÍTICA, FERRAMENTAS,  
NORMAS E PROCEDIMENTOS**





# FERRAMENTAS PESSOAS



# PONTO IMPORTANTE Nº 1



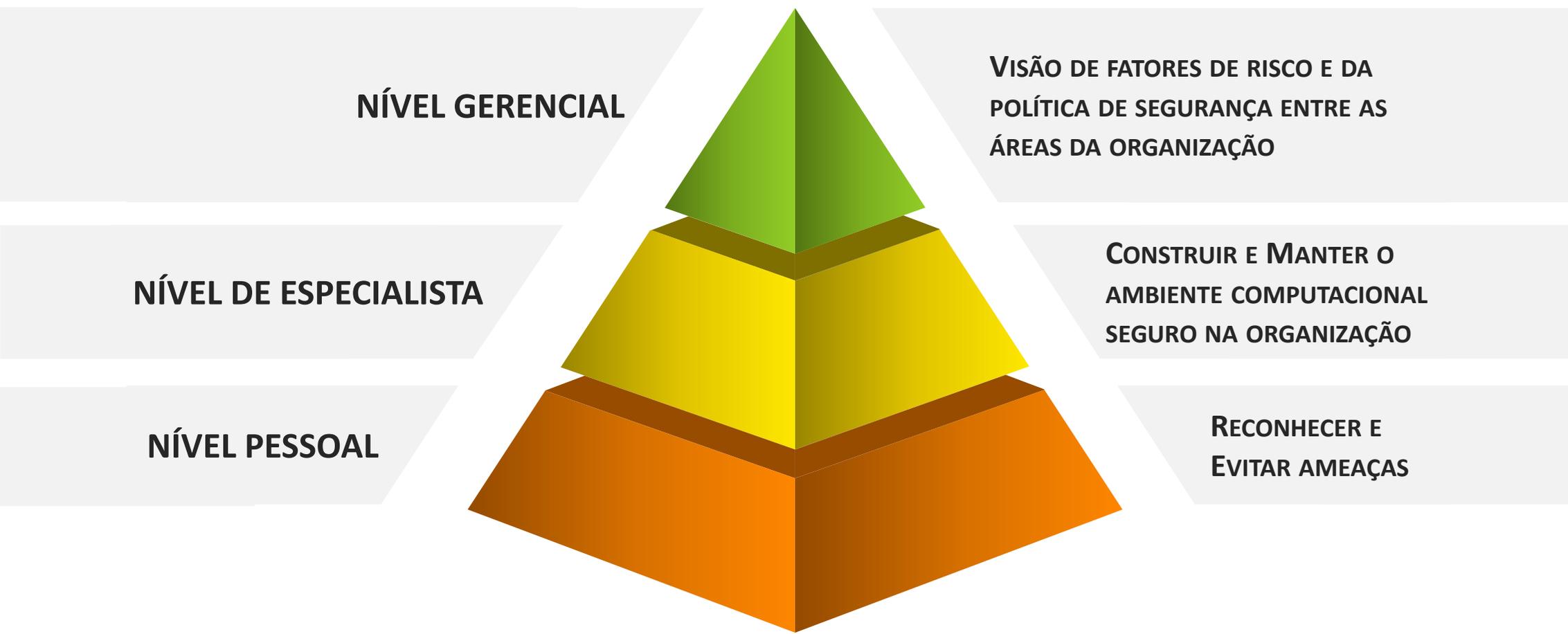
## 7.2.2 Conscientização, educação e treinamento em segurança da informação

### Controle

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

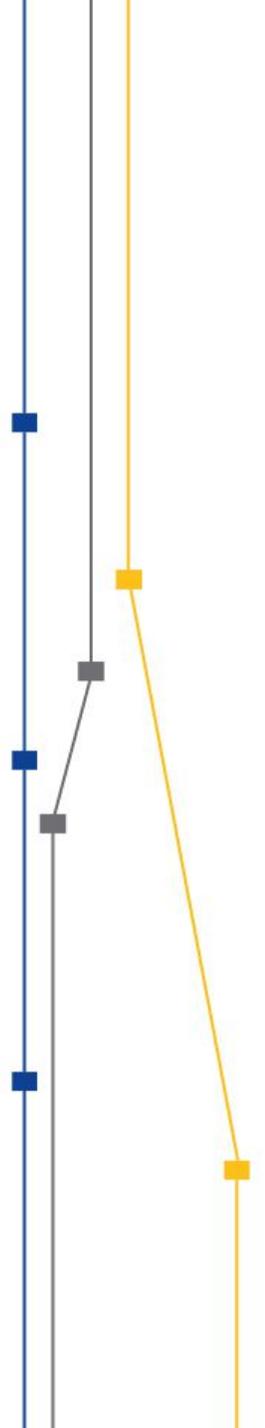
# PONTO IMPORTANTE Nº 2

Considerar os níveis de funções dentro da Organização



## PONTO IMPORTANTE Nº 3

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



# PONTO IMPORTANTE Nº 4

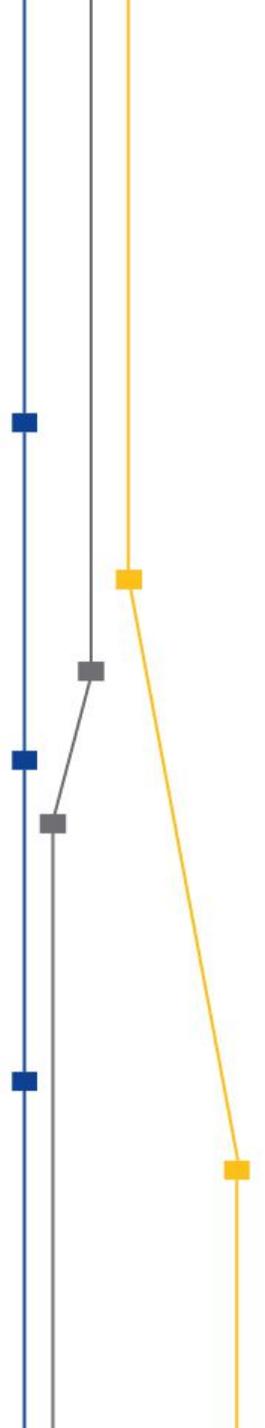
A conscientização deve respeitar a cultura organizacional



A hand holding a yellow marker with a red cap, pointing towards a word cloud of organizational culture terms. The words are arranged in a circular pattern around the central text 'ORGANIZATIONAL CULTURE'. The words include: unique, cognitive, employee, task, result, meaning, success, satisfaction, symbols, type, high, values, cultural, behavior, leadership, society, belief, external, problems, collective, company, growth, expertise, social, result, knowledge, management, deepest, feedback, status, stories, organizational, outlasting, important, interpersonal.

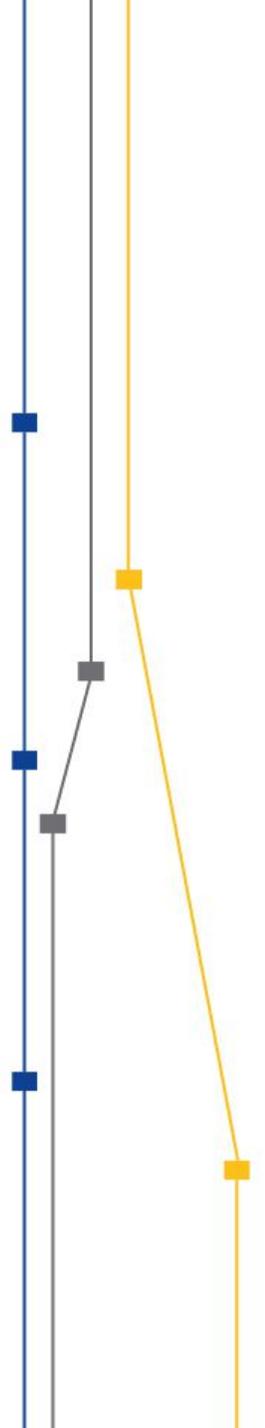
# PONTO IMPORTANTE Nº 5

Conscientização é MAIS que SÓ palestra!



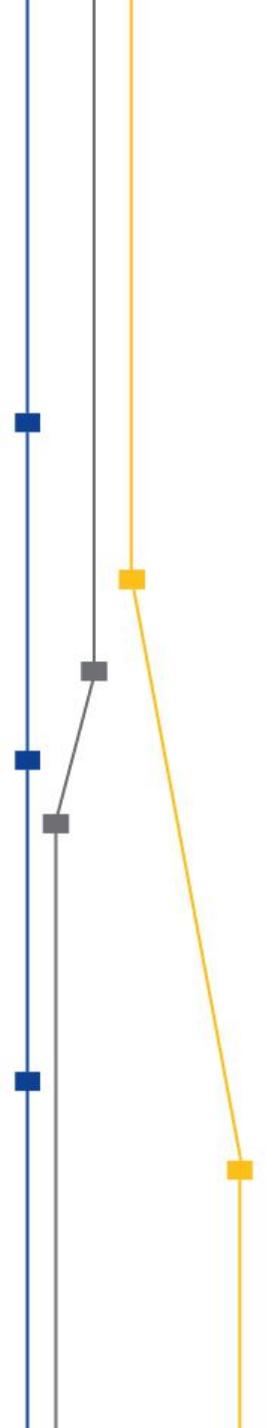
# PONTO IMPORTANTE Nº 6

Conscientizar NÃO é colocar medo nas pessoas!



# PONTO IMPORTANTE Nº 7

## Trabalhar com o conceito de CICLO EDUCATIVO



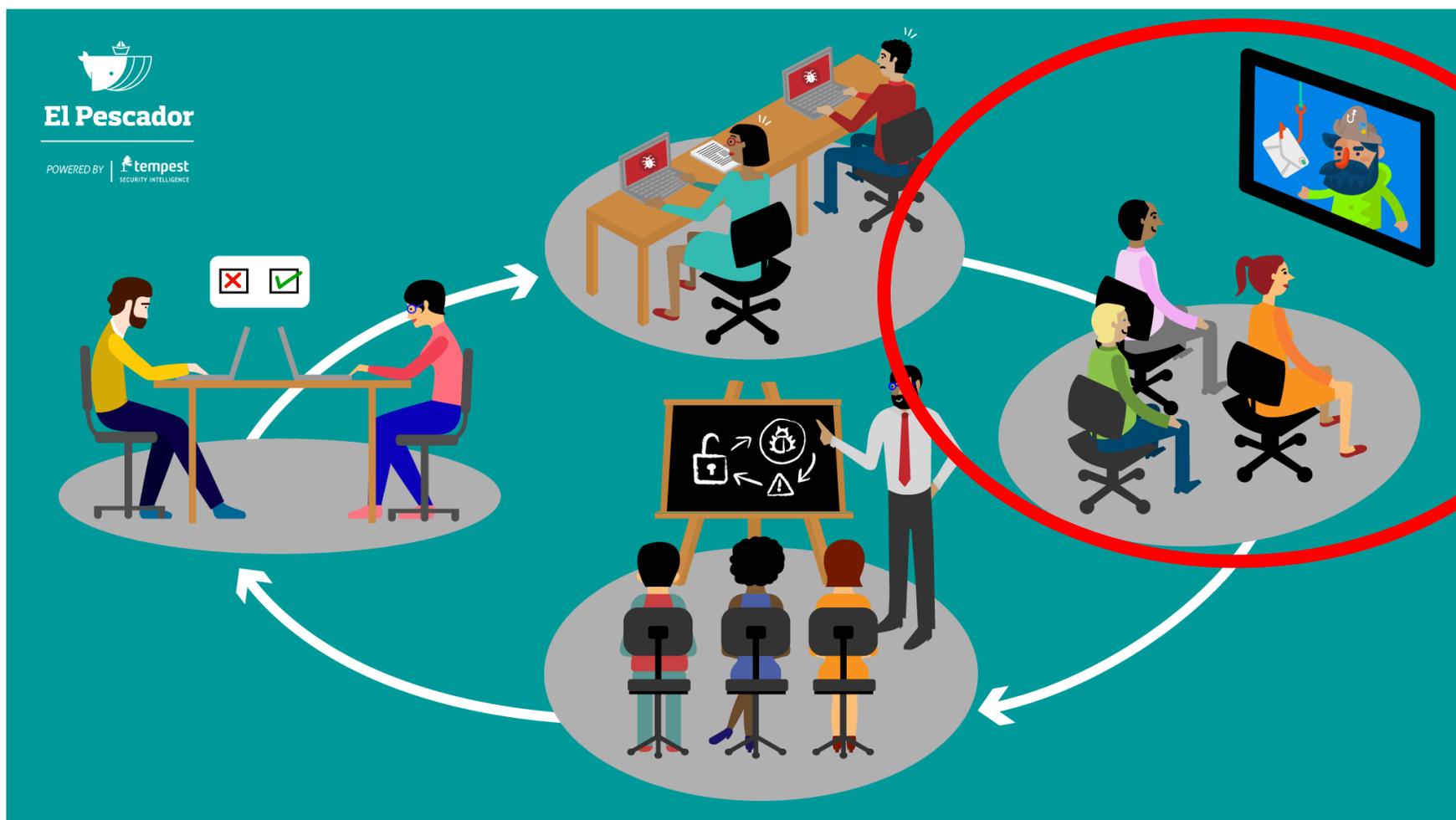
# PONTO IMPORTANTE Nº 7

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



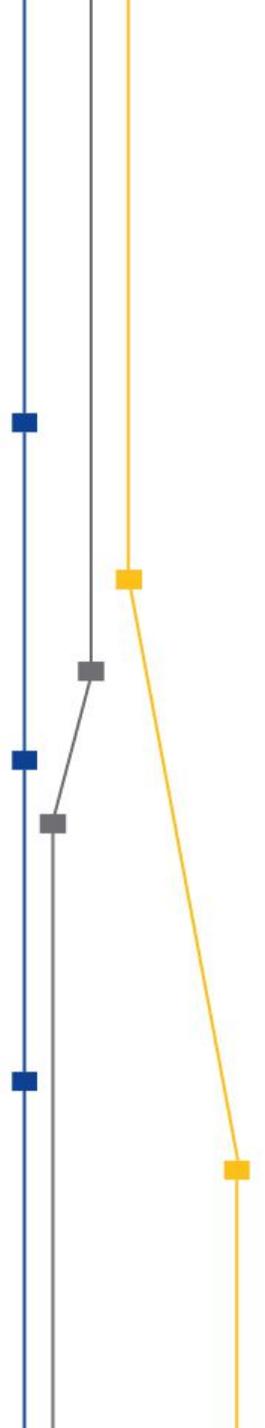
# PONTO IMPORTANTE Nº 7

Trabalhar com o conceito de CICLO EDUCATIVO: MEDIR



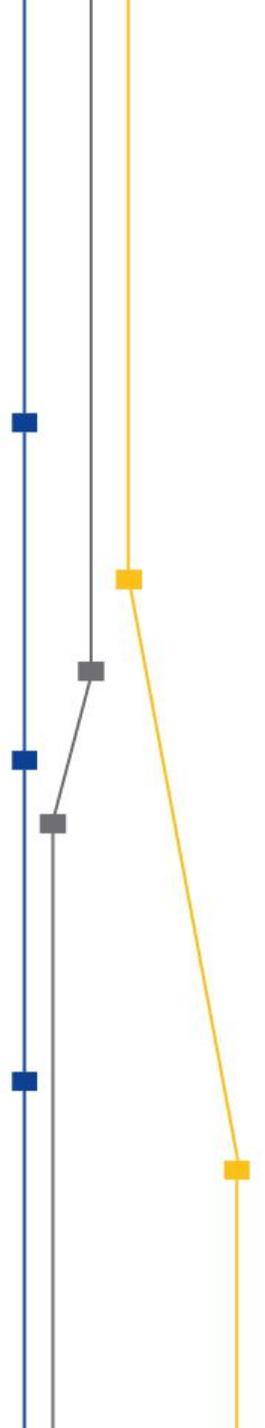
# PONTO IMPORTANTE Nº 8

Estabelecer metas e incentivos para os colaboradores da organização

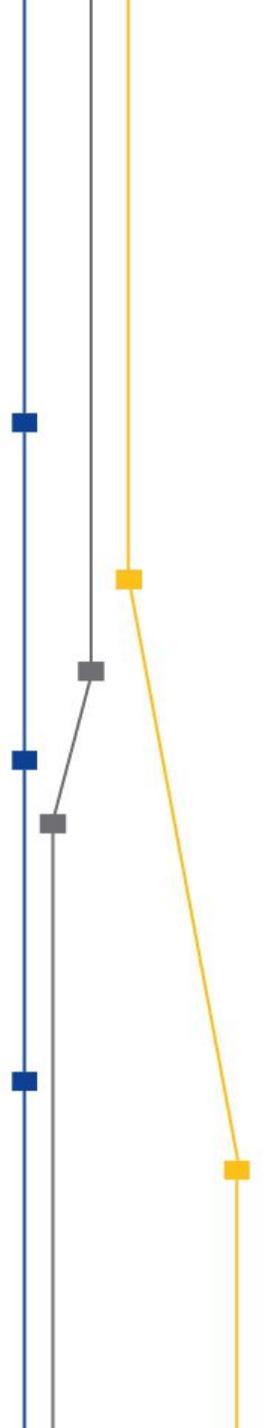




# COMO TRABALHAR A CONSCIENTIZAÇÃO PARA EVITAR PREJUÍZOS COM O *RANSOMWARE?*



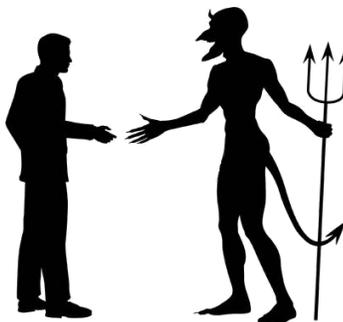
# IDENTIFICAR OS VETORES



# IDENTIFICAR OS VETORES



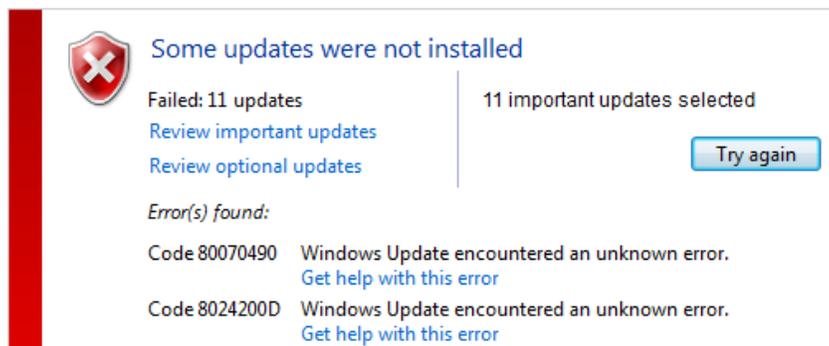
*phishing*



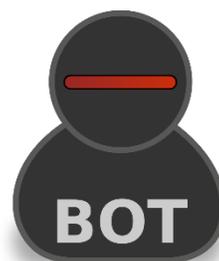
*engenharia social*



*sites maliciosos*



*sistemas desatualizados*



*botnets*



*softwares piratas*

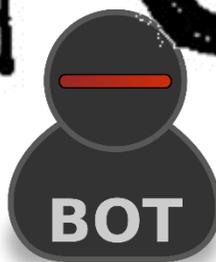
# IDENTIFICAR OS VETORES



phishing



engenheiro(a) técnico(a)

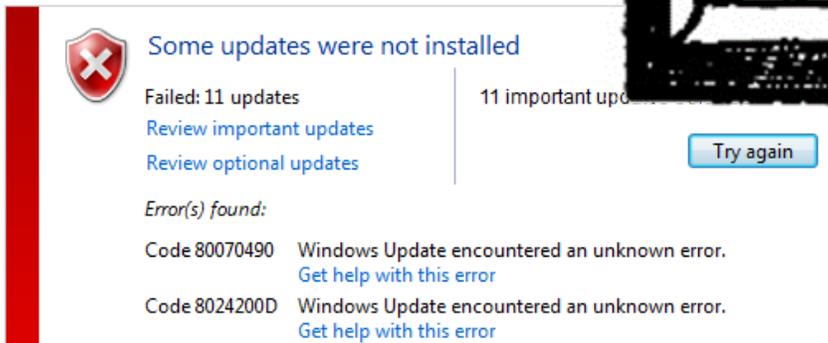


BOT

botnets



sites maliciosos

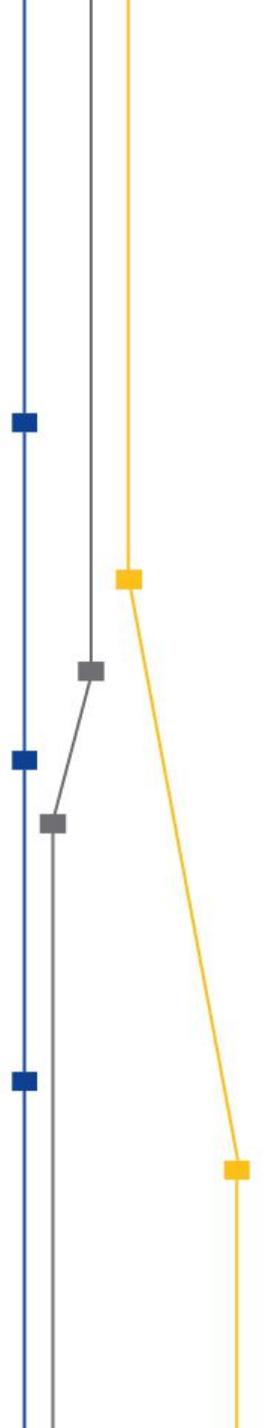


sistemas desatualizados



softwares piratas

# ESCOLHER OS MÉTODOS



# ESCOLHER OS MÉTODOS

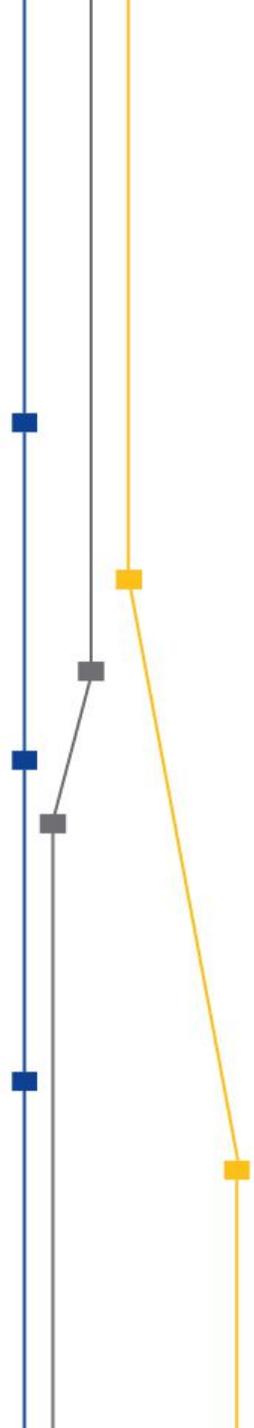


## Palestras

*Webinar - Backup - O básico cada vez mais essencial*



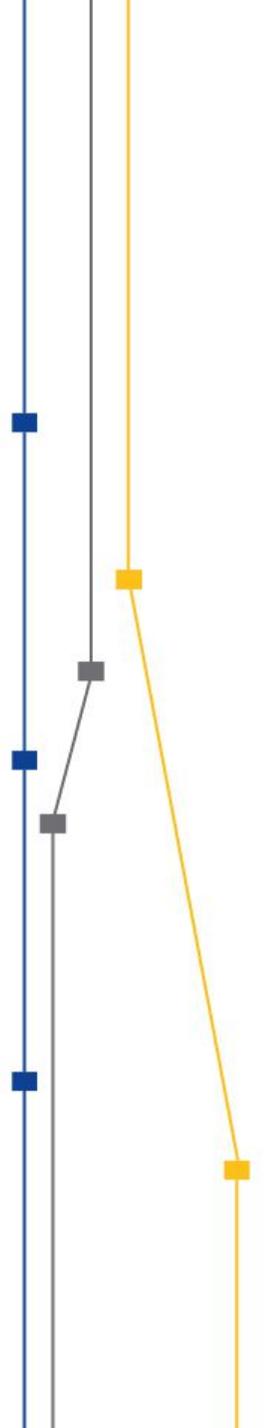
## Seminários online / webinars



# ESCOLHER OS MÉTODOS

Mailing list

Cartilhas



# ESCOLHER OS MÉTODOS



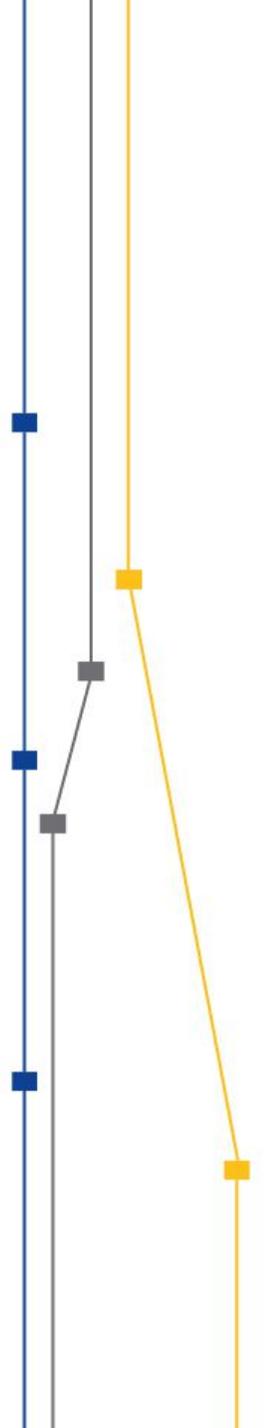
## Gamification



## 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

Aviso de Boleto em Atraso -589144799



Notificação de Pendência <ckatia1@hotmail.com>

ter 22/08/2017 13:09

Para: [Redacted]



Responder | v

Prezado(a) Cliente:

Segue em anexo boleto.

Por gentileza, nos encaminhar o comprovante após o pagamento.

Em caso de duvidas por gentileza entrar em contato com nossa central  
Atenciosamente.

Equipe de Atendimento

AMC Assessoria e Cobrança Ltda

Tel: (011) 4095-7437

Fax: (011) 4095-7503



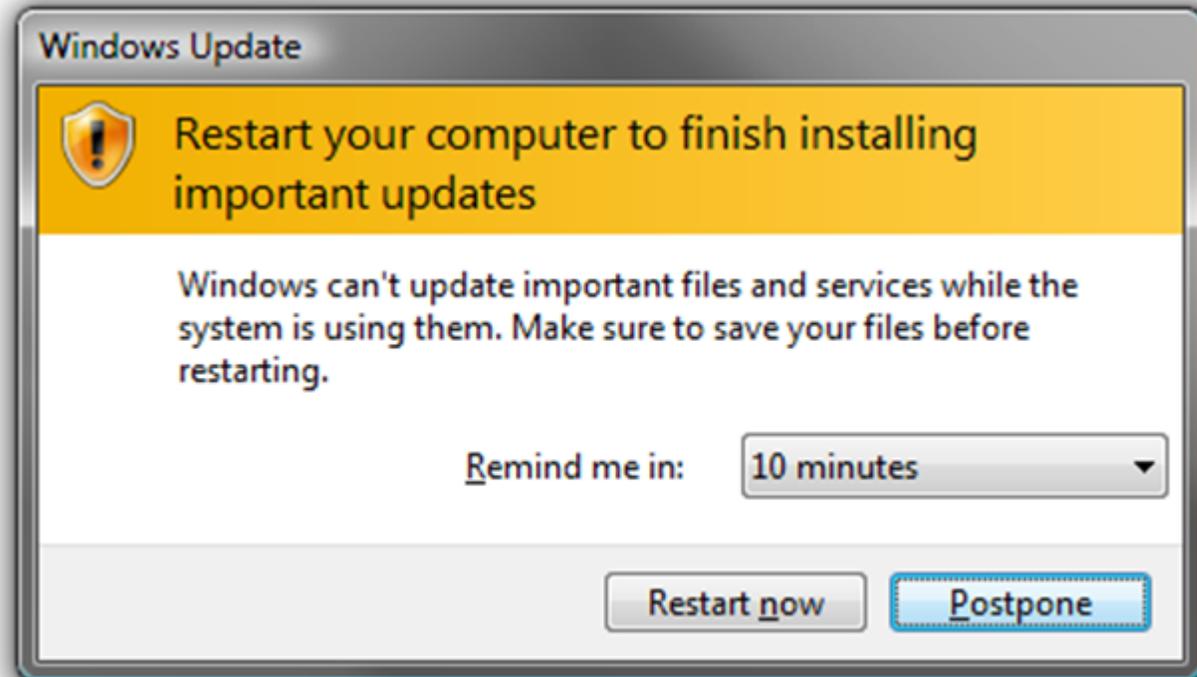
Boleto\_PDF

41,2Kb [visualize](#)

[empresafacildecontabil.com.br/A1DF474R/ab1/dl.php?flash/mail.live?nsd-web-externo/pages/publico/efetuar\\_boleto\\_pdf](http://empresafacildecontabil.com.br/A1DF474R/ab1/dl.php?flash/mail.live?nsd-web-externo/pages/publico/efetuar_boleto_pdf)

# 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.*



KeyCracker Software ka Serial key ya Crack kaise download kare hindi me jane

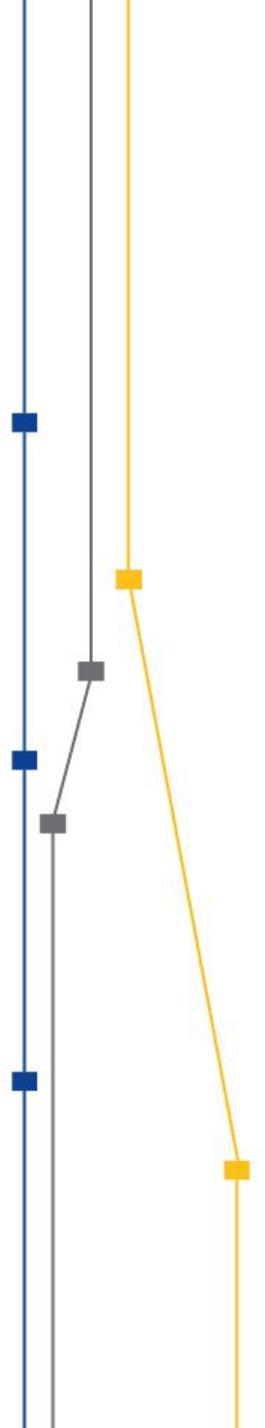
Software	date	rating
Microsoft Office 2010 all versions	2010-11-03	62%
Microsoft Office 2010	2012-03-22	49%
TurnUp Utilities 2013 Original key	2012-10-28	51%
TurnUp Utilities 2013	2012-10-01	29%
Microsoft Office 2010 (All versions) (License Type: MSDN Retail, KMS, MAK and more)	2012-06-20	52%
Microsoft office 2010 professional plus	2012-04-09	32%
Microsoft Office 2010 Home and student	2012-05-10	51%
AVG PC TuneUp 2013	2012-09-20	15%
Microsoft Office 2010 & 2007 All Editions	2011-07-11	48%
AVG PC Tuneup Pro 2013 (2.0.4000.1000)	2012-05-04	16%
Microsoft office 2010 professional plus	2012-08-17	39%
Adobe Photoshop CS6 Extended	2012-06-08	24%
Microsoft Office 2010	2012-11-10	46%
AVG PC Tuneup 2013	2012-10-19	11%
Microsoft Office 2010 Pro Plus	2011-09-20	48%



Top 20 serials	date	rating
Microsoft Office 2010 all versions	2010-11-03	62%
Microsoft Office 2010	2012-03-22	49%
TurnUp Utilities 2013 Original key	2012-10-28	51%
TurnUp Utilities 2013	2012-10-01	29%
Microsoft Office 2010 (All versions) (License Type: MSDN Retail, KMS, MAK and more)	2012-06-20	52%
Microsoft office 2010 professional plus	2012-04-09	32%
Microsoft Office 2010 Home and student	2012-05-10	51%
AVG PC TuneUp 2013	2012-09-20	15%
Microsoft Office 2010 & 2007 All Editions	2011-07-11	48%
AVG PC Tuneup Pro 2013 (2.0.4000.1000)	2012-05-04	16%
Microsoft office 2010 professional plus	2012-08-17	39%
Adobe Photoshop CS6 Extended	2012-06-08	24%
Microsoft Office 2010	2012-11-10	46%
AVG PC Tuneup 2013	2012-10-19	11%
Microsoft Office 2010 Pro Plus	2011-09-20	48%

# CONSCIENTIZAR PARA...

*Não usar mídias removíveis  
de origem desconhecida*



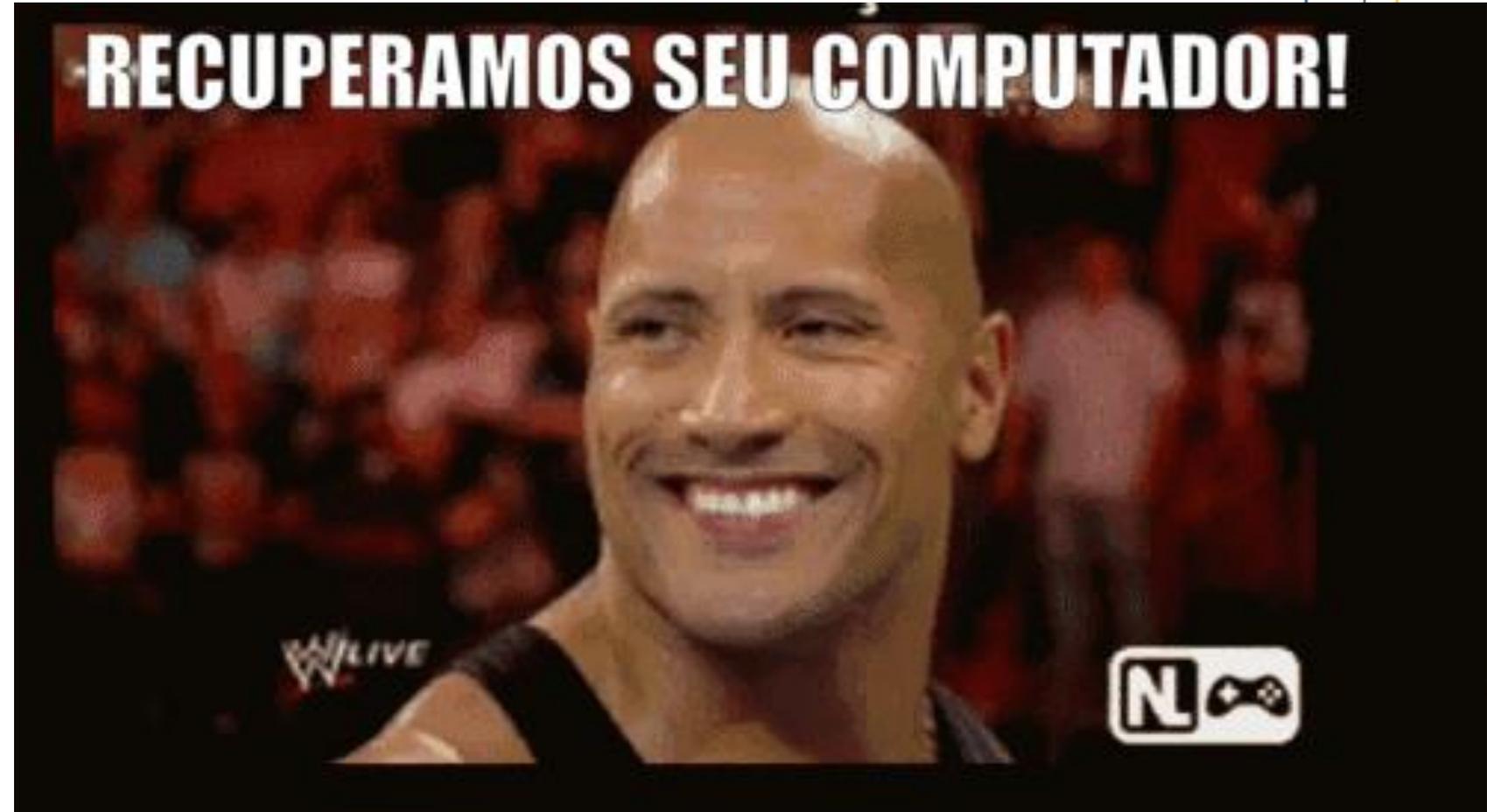
# CONSCIENTIZAR PARA...

*Bloquear sempre o computador quando se ausentar.*



# CONSCIENTIZAR PARA...

*Realizar cópias de  
segurança dos dados  
corporativos  
periodicamente*



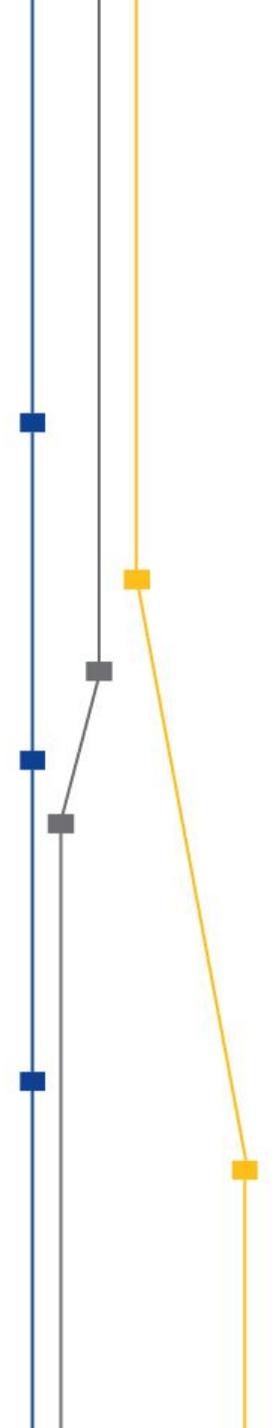
# CONSCIENTIZAR PARA...

*Reportar à equipe de segurança qualquer problema ou desconfiância*



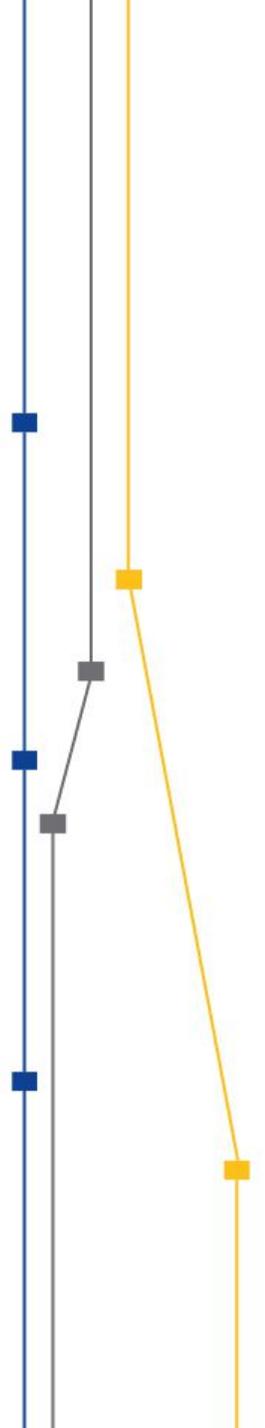
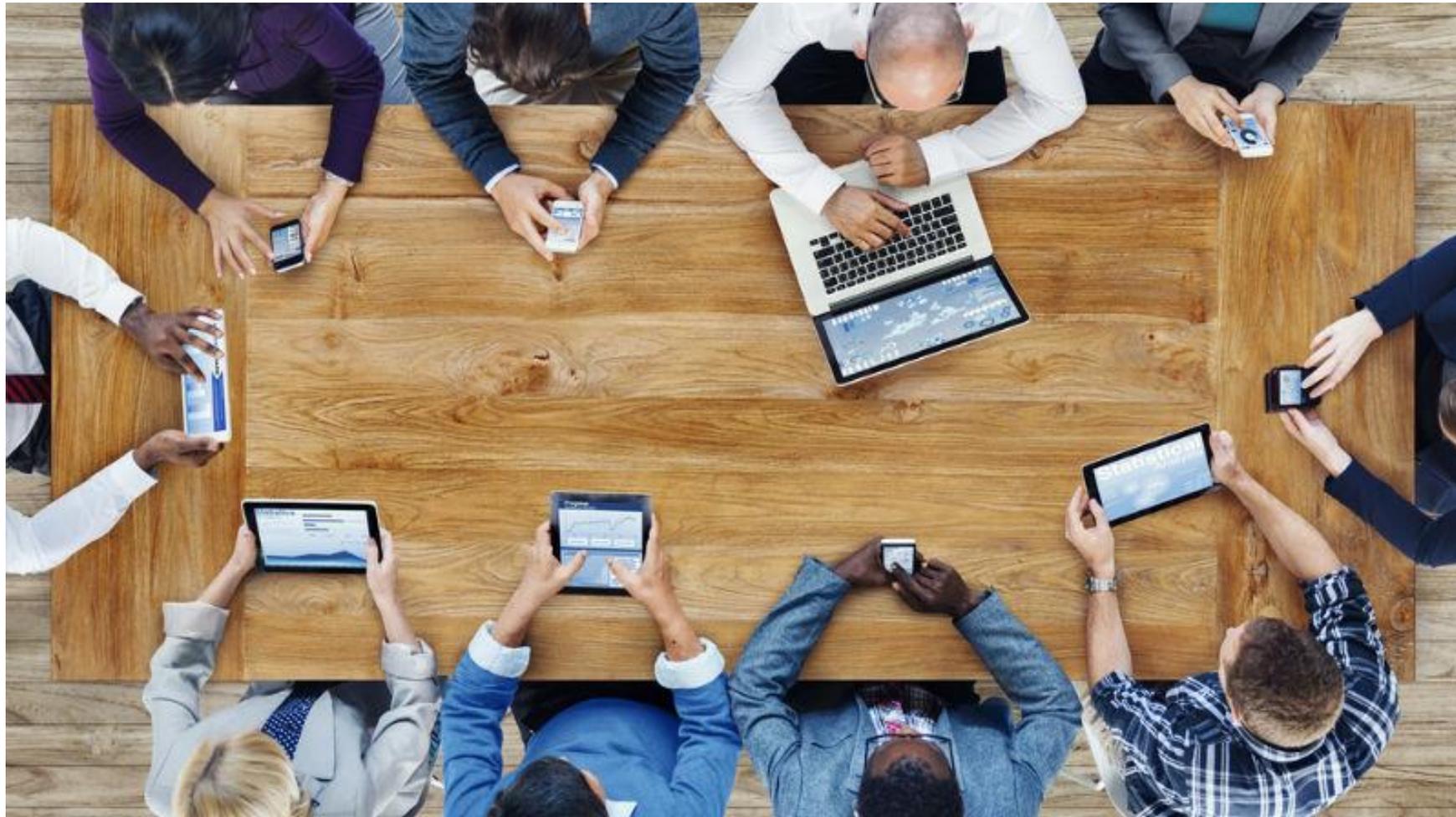
# CONSCIENTIZAR PARA...

*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.



**STI**  
Superintendência de Tecnologia da Informação | UFBA

2ª Campanha de Conscientização em Segurança da Informação

**RANSOMWARE: Sequestro de dados digitais**

*Ransomware* é o nome técnico dado a um tipo de código malicioso criado por cibercriminosos para sequestrar informações da vítima e exigir o pagamento de resgate para restabelecer o acesso às informações.

**Entendendo o golpe**

1º **Escolha da vítima**  
Propaga-se por e-mail, pendrive, página web infectada, etc.

2º **Instalação e Infecção**  
Clicar em links ou abrir arquivos pode infectar seu equipamento!

3º **Criptografia de arquivos**  
Para bloquear os dados, os criminosos usam técnicas avançadas de criptografia/cifragem.

4º **Notifica a vítima e pede o resgate (ransom)**  
!!!! ATENÇÃO !!!!!  
TODOS OS MEUS ARQUIVOS FORAM TRANCADOS  
SEMPRE QUE TENTAR ABRI-LOS, O MESMO MENSAGEM SE REPETIRÁ PARA INFORMAR O SEU STATUS.

5º - **Aguardar pagamento**  
O criminoso aguarda o pagamento da vítima, geralmente em bitcoins, para liberar a chave de acesso aos dados.

6º **Entrega da chave de decifragem**  
Não há garantias de que o acesso aos arquivos será normalizado após pagamento do resgate!

**Como se prevenir**

- Faça cópias de segurança (**backup**) dos seus dados!
- Utilize um **antivírus** para bloquear ameaças
- Seja cuidadoso** ao clicar em links e abrir arquivos



Security  
Standards Council®

# REFERÊNCIA

<http://bit.ly/infosecawereness>

**Standard:** PCI Data Security Standard (PCI DSS)

**Version:** 1.0

**Date:** October 2014

**Author:** Security Awareness Program Special Interest Group  
PCI Security Standards Council

**Information Supplement:  
Best Practices for Implementing a  
Security Awareness Program**

# PERGUNTAS?



**Yuri Alexandre**  
Analista de Segurança - Security Analyst

yuri.ferreira@rnp.br

Rede Nacional de Ensino e Pesquisa  
Prédio Embrapa / Unicamp  
Av. André Tosello, 209  
Cidade Universitária Zeferino Vaz  
13083-886 Campinas São Paulo Brasil  
+55 (19) 3787-3300  
+55 (11) 98011-7414 cel  
www.rnp.br



MINISTÉRIO DA  
**DEFESA**

MINISTÉRIO DA  
**CULTURA**

MINISTÉRIO DA  
**SAÚDE**

MINISTÉRIO DA  
**EDUCAÇÃO**

MINISTÉRIO DA  
**CIÊNCIA, TECNOLOGIA,  
INOVAÇÕES E COMUNICAÇÕES**

