Conscientização de SI – estamos sendo efetivos?

Realização nic.br

Pininga

12/2023

Quem sou eu?

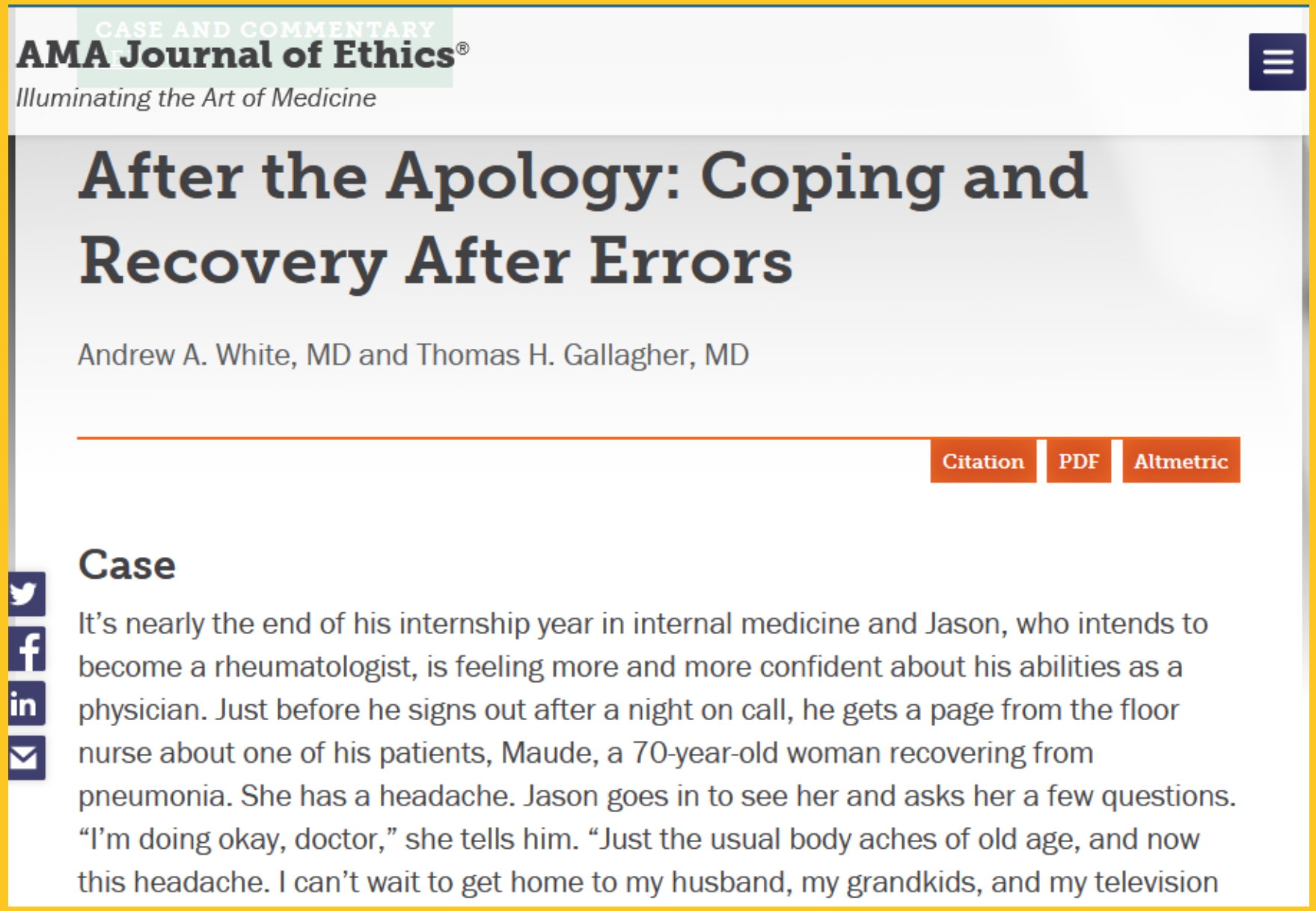
- José Edmir **Pininga** Duque
- Formação Ciência da Computação – UNICAP, Pós graduação Segurança da informação - UNIRIO
- Evangelizador de SI
- SI da Alpargatas – 15 anos
- Professor – Faculdade Impacta de Tecnologia / IBTA
- Palestrante/Consultor

https://www.linkedin.com/in/jos%C3%A9-edmir-pininga-duque-8564491/

Orgulho.

Tudo mundo é capaz.

Todos erramos.



CASE AND COMMENTARY

AMA Journal of Ethics®

Illuminating the Art of Medicine

After the Apology: Coping and Recovery After Errors

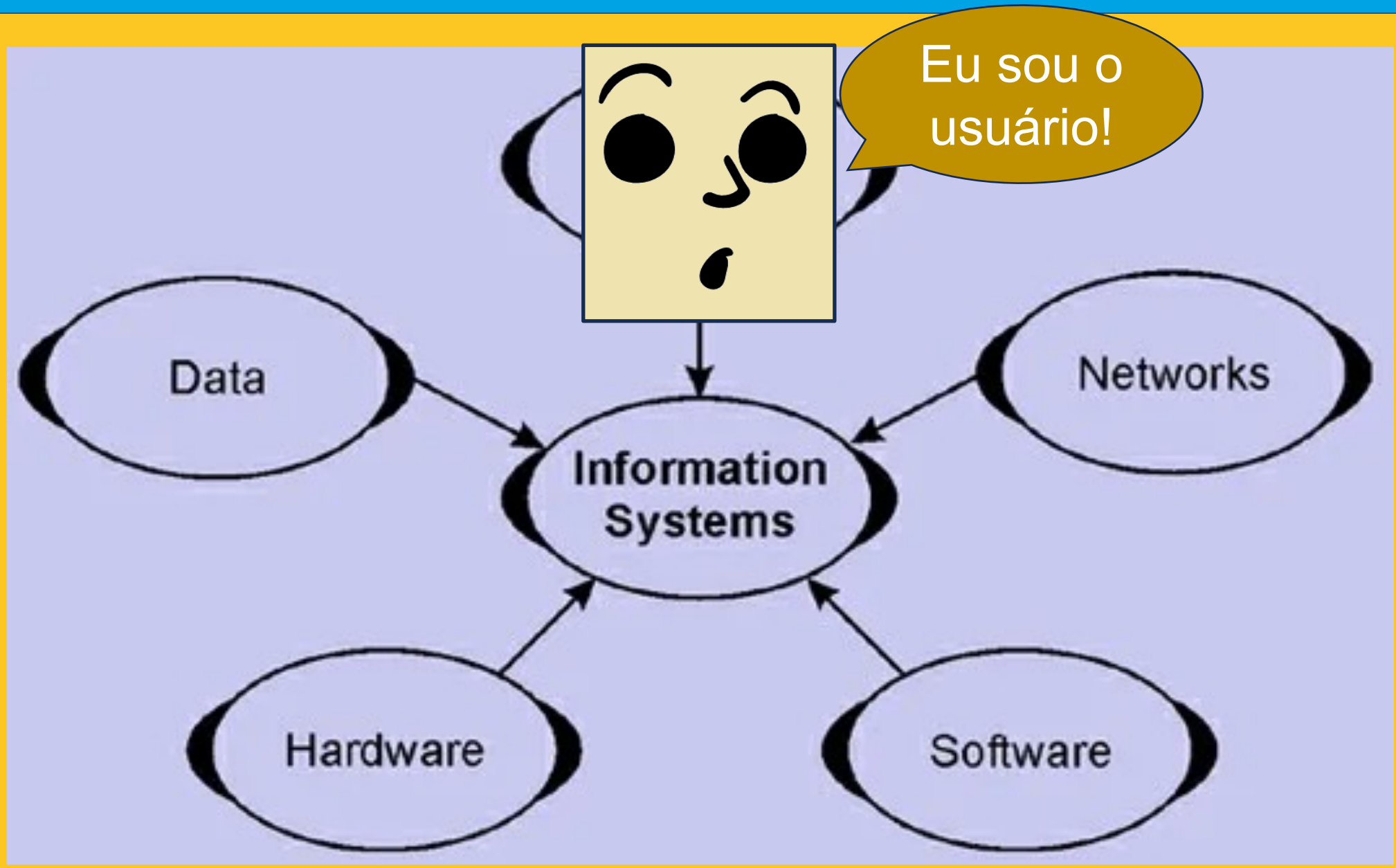
Andrew A. White, MD and Thomas H. Gallagher, MD

Citation PDF Altmetric

Case

It's nearly the end of his internship year in internal medicine and Jason, who intends to become a rheumatologist, is feeling more and more confident about his abilities as a physician. Just before he signs out after a night on call, he gets a page from the floor nurse about one of his patients, Maude, a 70-year-old woman recovering from pneumonia. She has a headache. Jason goes in to see her and asks her a few questions. "I'm doing okay, doctor," she tells him. "Just the usual body aches of old age, and now this headache. I can't wait to get home to my husband, my grandkids, and my television

Este também é um item de avaliação.



Esta vulnerabilidade continuará sendo explorada.

Phil Muncaster
UK / EMEA News Reporter, Infosecurity Magazine
Email Phil Follow @philmuncaster

The volume of data breach incidents reported to the UK's watchdog over the past two years increased 75% as organizations geared up for the new data protection regime, according to a new FOI request.

Risk management firm Kroll also found that human error accounted for the vast majority (88%) of incidents reported to the Information Commissioner's Office (ICO) over the past year: 2124 reports versus just 292 cases that were down to deliberate cyber-attacks.

Of these, data emailed to the wrong recipient (447) topped the list, followed by data posted/faxed to the incorrect recipient (441), loss/theft of paperwork (438), failure to redact data (256) and data left in an insecure location (164).

Reflexões 01 – Seja orgulhoso, mas seja “consciente”.

01 Há quanto tempo falamos em conscientização de SI?

02 Se os usuários seguem as regras de RH, porque não seguem as regras de TI/SI?

03 Existe uma estratégia?

Usuário do metrô x casa da avó

Vejamos ...

- Sua empresa tem política clara sobre CLASSIFICAÇÃO DA INFORMAÇÃO?
- Sua empresa tem política clara sobre USO NÃO AUTORIZADO?
- Sua empresa tem política clara sobre SEGURANÇA EM VIAGEM? Uso de Wifi e redes públicas, por exemplo.

Isso não será um Mito?

- Só porque as pessoas estão cientes de um problema não significa que elas agirão de acordo com sua consciência.
- Todo mundo sabe que fast food não é a escolha mais saudável, mas ainda assim muitas pessoas comem.

Precisamos de pessoas CONSCIENTES ou COMPROMETIDAS?

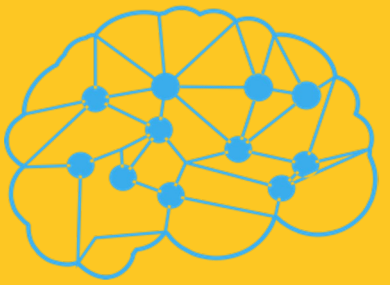
Segurança x Cultura!?!

Segurança perfeita não existe.

O objetivo ao estabelecer um programa de conscientização de segurança é reduzir o risco influenciando as ações do usuário.

Cultura (organizacional) da empresa!

Ainda pensando no usuário.

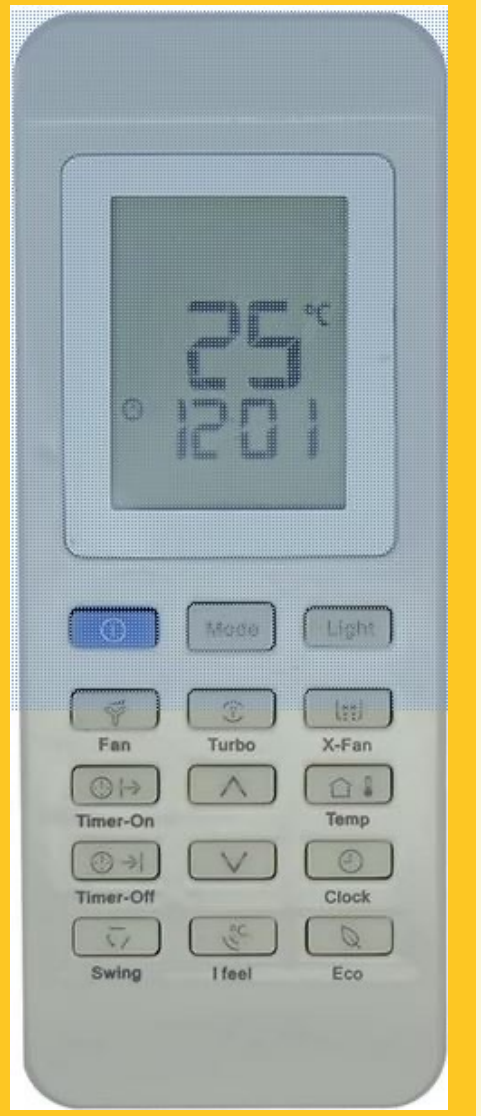


UX.

Será que todo usuário é igual?

Estamos dando ênfase no usuário ou na tarefa?

Ainda pensando no usuário.



CHIHUAHUA SYNDROME

MESSY, UNVALIDATED HAND-ENTERED DATA

DOG DATABASE

Breeds ↑	
BOXER	118,726
BULLDOG	109,215
CHE HUA HUA	2
CHE-HUA-HUA	16
CHE-WAWA	3
CHEE-HUA-HUA	14
CHEEHUAHUA	25
CHEHUAHUA	1032
CHEHAHA	458
CHEHAWA	1
CHIHAHA	67
CHIHUA HUA	65,421
CHIHUAWA	17
CHIWAWA	13,098
CHIEHUAUA	362

Segurança não é gozação!

Abuso sexual x segurança da informação

A punição está sendo JUSTA?

Qual a punição para quem foi o causador (reincidente) do vírus que contaminou a estação de trabalho ou pior, a rede?

Ao usuário ou à ferramenta/processo que não funcionou?

Reflexões 02 – Reveja seus conceitos/processos.

- Não espere a perfeição como resultado de um programa de conscientização dos usuários.
- Mantenha as ferramentas de proteção atualizadas e reveja os processos de segurança contra ações maliciosas visando os usuários.
- Lembre-se que “não coloque o dedo na tomada” tem um efeito sedutor.

Qual o objetivo da conscientização?

- Para os treinamentos, basta assinar a lista de presença?
- Para a auditoria, basta evidenciar que existe um sistema de conscientização?
- Será fácil descrever e **justificar** as métricas usadas atualmente?

- Qual o(s) OBJETIVO(S) do seu programa de conscientização?

Reflexão 03 – Qual critério usar?

- Um usuário atrasado para uma reunião crítica com um cliente, mesmo sabendo que proteger o espaço de trabalho é importante, ele chegará ainda mais tarde à reunião para proteger seu computador e bloquear documentos confidenciais?

- Como ele determina qual ação correta tem prioridade?

A calçada da segurança!

The end

Muito obrigado!

Pininga

pininga@gmail.com