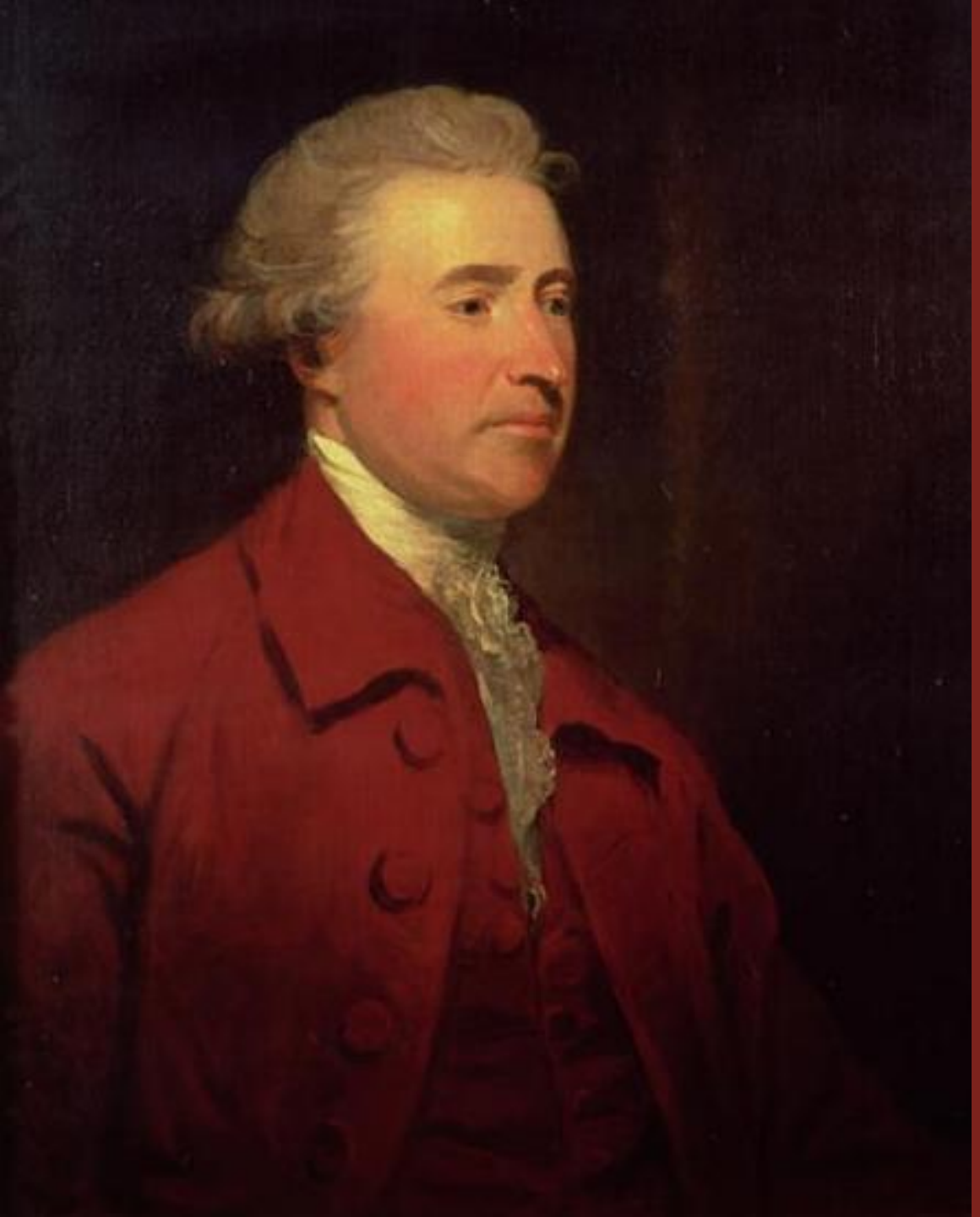
Gestão de Riscos e 3 Linhas de Defesa

(Oficina para gestores do MS)

Teams, out-nov/20



“A única coisa necessária para o triunfo do mal é que os homens bons não façam nada”

Edmund Burke,

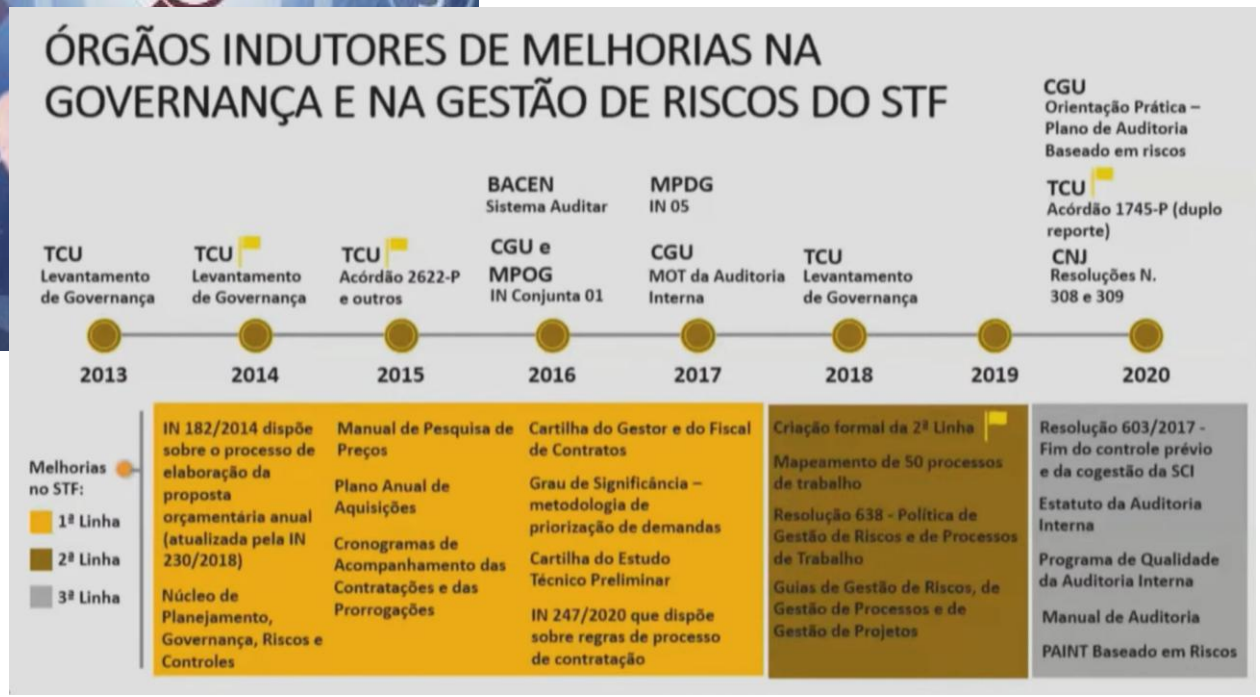
estadista e filósofo britânico.

CAN YOU SOLVE THE BRIDGE RIDDLE?

*Cada grupo ou naipe de instrumentos tem um **solista** ou **chefe** que é o protagonista dos solos e da liderança desse grupo.*

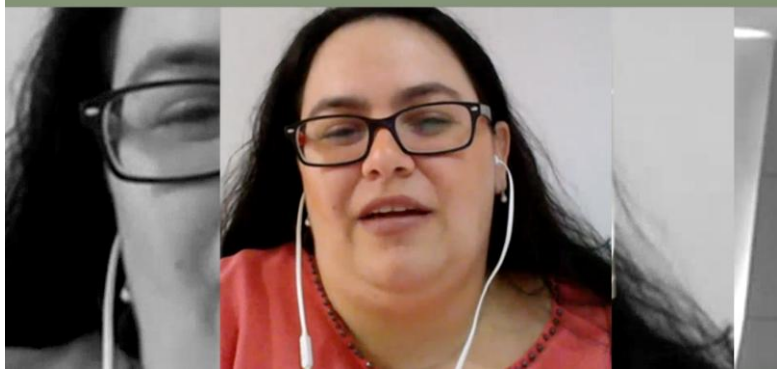
É possível?


ciclo:
Integração dos Controles
Gestão de Riscos –
experiências e avaliações
15 de setembro
às 10h

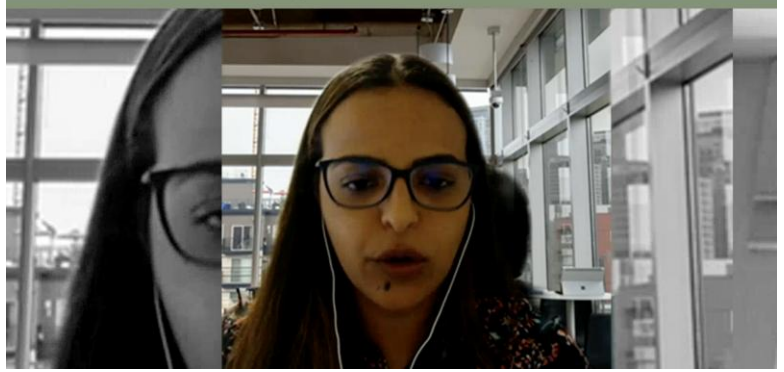

ÓRGÃOS INDUTORES DE MELHORIAS NA GOVERNANÇA E NA GESTÃO DE RISCOS DO STF
TCU
Levantamento de Governança
2013
TCU
Levantamento de Governança
2014
TCU
Acórdão 2622-P e outros
2015
BACEN
Sistema Auditar
CGU e MPOG
IN Conjunta 01
2016
MPDG
IN 05
CGU
MOT da Auditoria Interna
2017
TCU
Levantamento de Governança
2018
2019
CGU
Orientação Prática – Plano de Auditoria Baseado em riscos
TCU
Acórdão 1745-P (duplo reporte)
CNJ
Resoluções N. 308 e 309
2020
Melhorias no STF:
1ª Linha
2ª Linha
3ª Linha
IN 182/2014 dispõe sobre o processo de elaboração da proposta orçamentária anual (atualizada pela IN 230/2018)
Núcleo de Planejamento, Governança, Riscos e Controles
Manual de Pesquisa de Preços
Plano Anual de Aquisições
Cronogramas de Acompanhamento das Contratações e das Prorrogações
Cartilha do Gestor e do Fiscal de Contratos
Grau de Significância – metodologia de priorização de demandas
Cartilha do Estudo Técnico Preliminar
IN 247/2020 que dispõe sobre regras de processo de contratação
Criação formal da 2ª Linha
Mapeamento de 50 processos de trabalho
Resolução 638 - Política de Gestão de Riscos e de Processos de Trabalho
Guias de Gestão de Riscos, de Gestão de Processos e de Gestão de Projetos
Resolução 603/2017 - Fim do controle prévio e da cogestão da SCI
Estatuto da Auditoria Interna
Programa de Qualidade da Auditoria Interna
Manual de Auditoria
PAINT Baseado em Riscos

É possível?

Janaina Nogueira
Projeto InformatizaAPS/MS

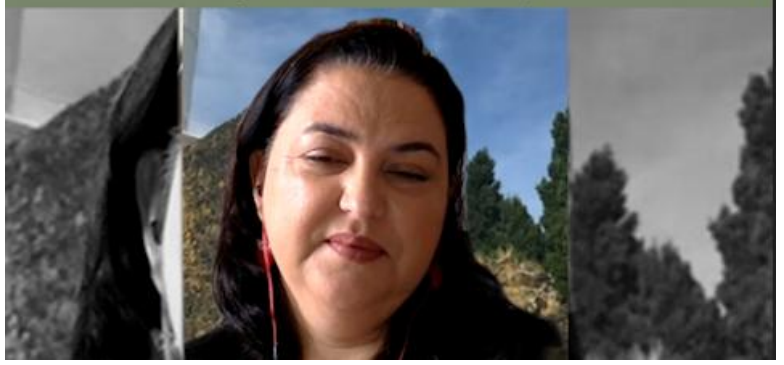


Juliana Zinander
Programa ConecteSUS/MS



Marcos Paulo
Projeto CArga de Dados da RNDS/MS

Patrícia Irigaray
Projeto Gestão de Riscos da ESD/MS

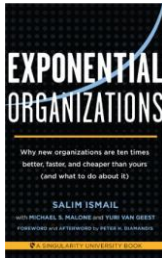


A jornada…

(1ª parte)

Um convite…

(2ª parte)



A jornada...

Participar onde sou parte interessada

Saber em qual linha de defesa estou

Ser dono dos seus riscos

Objetivos

Controles Internos

Riscos

O que eu ganho com isso?

Um norte...
Segurança...
Diminui a chance de ter problemas...
Produtos melhores...

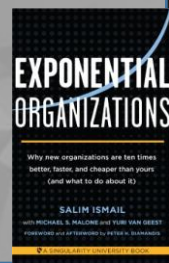
Imagem: Pixelstalk

Papel da 1ª linha de defesa:

Implementar controles para gerir os riscos de sua responsabilidade

Exemplos de atividades de controle típicos da 1ª linha de defesa:

Acompanhar, Monitorar, Conferir, Revisar (p.ex., emitir parecer)



MAPA DE RISCOS

MAPA DE RISCOS

Mapeamento de Riscos															
Macroprocesso	Identificação de Eventos de Riscos							Avaliação dos Riscos		Tratamento de Riscos					
	Causa	Evento Indesejado	Consequências	Categoria do Risco	Risco Inerente			Identificação dos Controles Existentes	Risco Residual	Resposta ao Risco	Controles Propostos	Unidade Responsável	Unidade Corresponsável	Responsável pela Implementação	
					I	P	NR	Descrição do Controle							
1. Implantação da RNDS em produção no Estado de Alagoas (Projeto Piloto)	- Arquitetura da RNDS não disponível em tempo suficiente para realização da carga; - Ausência dos modelos de referência da RNDS (FHIR); - Ausência do mapeamento e regras de negócio entre os modelos de referência e da RNDS; - Insuficiência de recursos computacionais para garantir o tempo necessário para realização da carga; - Complexidade de conversão entre os modelos (relacional vs. JSON FHIR); - Desalinhamento entre as áreas negociais (falha no gerenciamento do processo);	1.1 Ausência dos dados legados (Carga Inicial)	Cenário 1: Implantação da RNDS sem dados históricos: a) Menor valor de uso. b) Baixa adesão à RNDS (EAS conectados à RNDS, mas com baixa utilização); Cenário 2: Prorrogação do início em produção: a) perda de credibilidade do processo; b) desgaste dos atores envolvidos	Operacional	8	5	40	- Reuniões de alinhamento entre todas as equipes envolvidas; - Transferência de conhecimento entre as equipes interdependentes;e - Definição prévia da alocação de equipe e recursos computacionais dedicadas para a tarefa; - Controle semanal rigoroso da Carga inicial pela Diretoria	24,0	Mitigar		CGISD/DATASUS	CGSIO/DATASUS	Michael Diana (Ramal: 2058)	
	- Falha na implementação da arquitetura na nuvem; - Falhas estruturais impeditivas na arquitetura; - Não implementação de todos os componentes essenciais no prazo necessário.	1.2 RNDS Não disponível em produção.	EAS não conectados à RNDS; Dano à imagem do projeto.	Operacional	10	5	50	- Planejamento prévio do modelo de arquitetura MVP (SEI 25000.122188/2019-95); - Discussão com especialistas nacionais e internacionais sobre os componentes de arquitetura; - Bechmarking - Validação da estratégia de arquitetura com a NHS Digital; - Bechmarking com a Amazon; - Definição clara de papéis, responsabilidades e pontos de convergência entre as equipes (Documento de Visão); - Gerenciamento das interdependências do projeto; - Reforço do gerenciamento do projeto, para um acompanhamento mais efetivo de todos as eventuais questões arquiteturais encontradas durante o projeto - Processo incremental e gradual; - Realização de ambientes de imersão na arquitetura (Sala de Guerra); - Realização de testes de estresse por agente externo	27,8	Aceitar		CGSIO/DATASUS	CGISD/DATASUS	Henrique Nixon (Ramal: 2058)	
	- Indefinição do fluxo de habilitação à RNDS; - Não implementação do fluxo no Portal de Serviços de Interoperabilidade; - Documentação Técnica da RNDS para habilitação insuficiente/inexistente; - Ausência de Recursos Humanos para auxílio ao município	1.3 Indisponibilidade do processo de habilitação para os Estabelecimentos de Assistência à Saúde (EAS) se conectarem à RNDS	EAS não conectados à RNDS; Dano à imagem do projeto	Operacional	8	5	40	- Definição e disponibilização dos critérios técnicos para habilitação dos - - EAS no Portal RNDS (oito artefatos); - Disponibilização do Portal de Serviços de Interoperabilidade; - Detalhamento de uso e publicização da Documentação Técnica e Negociai - - Wiki; - Contratação de Bolsistas - Técnicos para RNDS (TED Fiocruz); - Planejamento da Contratação de Serviço de Suporte Técnico	27,2	Mitigar	Planejamento e Contratação de Serviço de Suporte Técnico	CGSIO/DATASUS	CGIED/DATASUS; CGISD/DATASUS	Henrique Nixon (Ramal: 2058)	
	- Indefinição da abordagem de Consentimento para a RNDS; - Desconhecimento da aplicabilidade da LGPD (vácuo legal); - Deficiência de comunicação que garanta o direito à informação do cidadão.	1.4 Não conformidade à Lei Geral de Proteção de Dados - LGPD	Dano à imagem do projeto; Ações judiciais contra o projeto	Legal	8	8	64	- Definição da Abordagem de Consentimento para RNDS com as áreas negociais e encaminhamento para apreciação da CONJURMS; - Elaboração do Termo de Consentimento; - Textos informativos ao cidadão no Portal Conecte SUS (Perfil Gestor, Cidadão e Profissional); - Instituição do Núcleo LGPD no âmbito do DATASUS para estudo e aplicabilidade da Lei - Demandar à ASCOM a elaboração de um Plano de Ação Comunicação do Conecte SUS que contemple a adequada informação ao cidadão (SEI 25000.182077/2019-38); - Acompanhar a execução do Plano de Ação de Comunicação do Conecte SUS executiva pela ASCOM	44,8	Mitigar		CGGOV/DATASUS	CGISD/DATASUS	Roberta Massa	
2. Ampliação do número de Equipes de Atenção Primária à Saúde informatizadas, após a se conectarem à RNDS (Projeto Piloto Informatiza APS)	- Comunicação deficiente do Ministério da Saúde sobre o programa e seus benefícios para o para os profissionais e para a população; - Articulação insuficiente com CONASS, CONASEMS e COSEMS para capilaridade do programa.	2.1 Baixa adesão dos gestores de Alagoas ao Informatiza APS por desconhecimento ou por não identificarem seus benefícios	Não atingir a meta de 75% de equipes informatizadas na APS nos municípios de Alagoas	Operacional	8	2	16	- Divulgação do programa e do Projeto Piloto para os gestores municipais, em agendas nos estados, associado ao novo financiamento da APS; - Encontros com representantes de CONASS, CONASEMS, COSEMS e gestores municipais para explicar o programa e seus benefícios, com ênfase para capilarizarem as informações para os gestores municipais;	6,4	Aceitar		CGISD/DATASUS	DESF/SAPS	Lucas Pedebos (Ramal:8838)	
	- Desconhecimento do gestor de como usar o recurso de custeio para informatizar seus estabelecimentos de saúde; - Licitação de um município não ser atrativa o suficiente para empresas de prestação de serviço; - Falta de conhecimento dos profissionais que conduzem o processo licitatório no município sobre os serviços que devem ser contratados a fim de tornar a unidade informatizada no tempo previsto pela Portaria 2.984/2019.	2.2 Municípios com dificuldades no processo licitatório e não conseguirem executar o recurso para informatização	Não atingir a meta de 75% de equipes informatizadas na APS; Município não conseguir executar o recurso de custeio para implantação no período de 6 meses, estabelecido na Portaria 2.984/2019; Município não conseguir fazer levantamento de toda infraestrutura necessária para o correto envio de dados por sistema de prontuário eletrônico.	Operacional (Risco Externo)	10	8	80	- Pactuação com a Secretaria Estadual de Saúde de Alagoas para realização de uma ata de registro de preços em parceria com o ITEC (Instituto de Tecnologia em Informática e Informação do Estado de Alagoas) para auxiliar os municípios com dificuldade nos processos licitatórios; - Disponibilização de exemplo de minuta de pregão (com especificações mínimas e Termo de Referência; minuta de contrato e instrumento de avaliação e roteiro de apresentação para prova de conceito - POC) para que o município adaptasse a sua necessidade; - Oficina de preparação para implantação do piloto - Programa Conecte SUS no estado de Alagoas; - Alinhamento Político e Estratégico para Implantação do Programa Conecte SUS (participação da Associação dos Municípios Alagoanos - AMA, de todos os municípios de AL e COSEMS/AL); - Capacitação para Instalação do PEC e-SUS APS - Alagoas (Capacitação de Implantadores); - Multirão para Implantação do PEC e-SUS APS em todos os municípios de Alagoas - Monitoramento semanal da evolução do número de equipes informatizadas - Elaboração e disponibilização da minuta de pregão para contratação em nível municipal e regional (com possibilidade de contratação centralizada /processo	48,0	Mitigar		DESF/SAPS	CGISD/DATASUS	Lucas Pedebos (Ramal:8838)	

Estabelecimento de Contexto | Mapa de Riscos | Cálculo do Risco Inerente | Cálculo do Risco Residual | Plano de Tratamento | Escala de Impacto (I) | Escala de Probabilidade (P)

Controle proporcional ao risco

Decreto-Lei 200/1967 (art. 14)
Decreto 83.936/1979 (“considerandos”)
Lei 13.460/2017, art. 5º, XI
Decreto 9.094/2017, art. 1º, V

A jornada…

Participar onde sou parte interessada

Saber em qual linha de defesa estou

Ser dono dos seus riscos

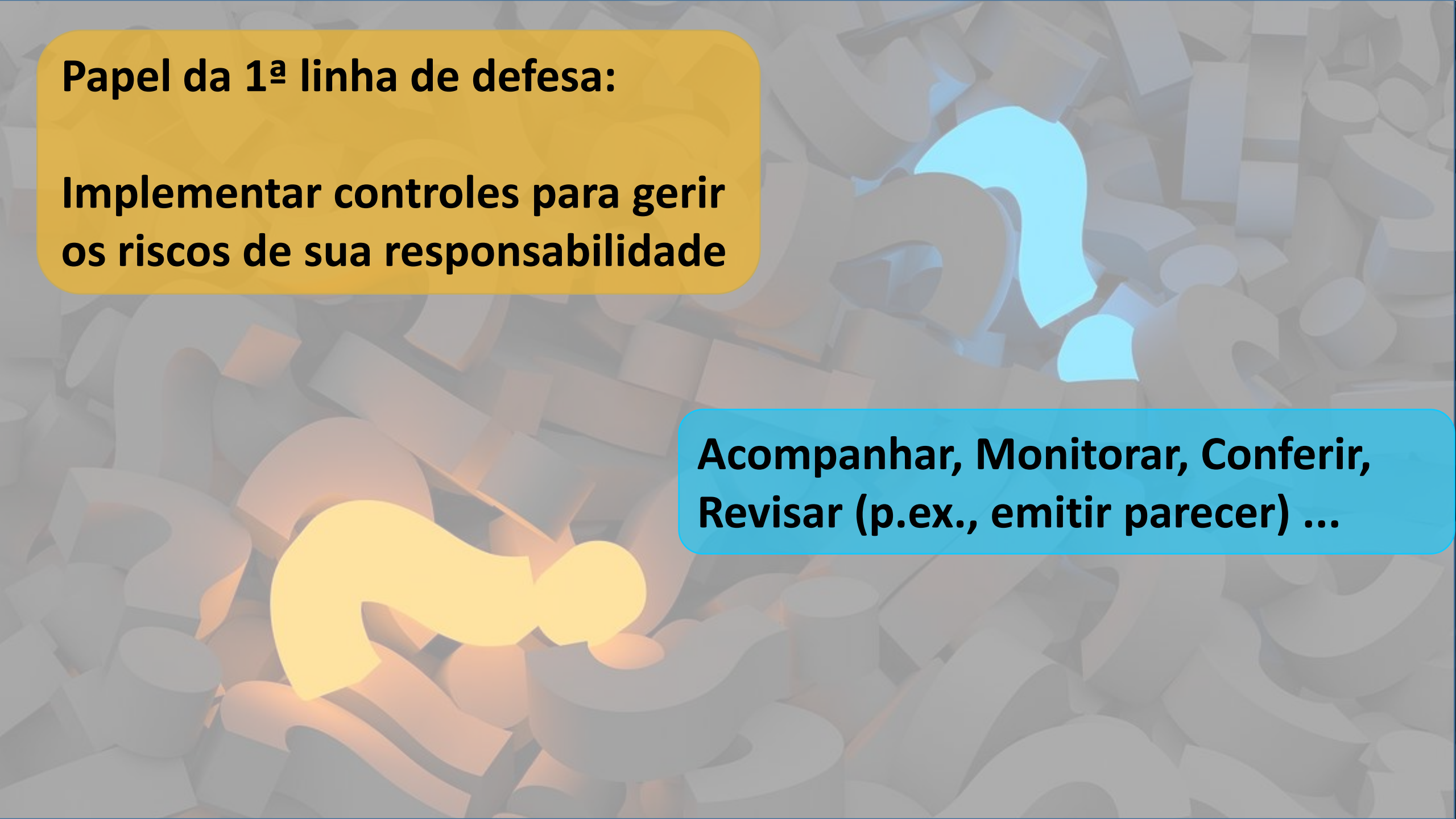
Modelo de Três Linhas de Defesa

Adaptação da *Guidance on the 8th EU Company Law Directive* da ECIIA/FERMA, artigo 41

Fonte: IIA

Papel da 1ª linha de defesa:

Implementar controles para gerir os riscos de sua responsabilidade



Acompanhar, Monitorar, Conferir, Revisar (p.ex., emitir parecer) ...

Papel da 2ª linha de defesa:

<u>supervisionar</u> GRC (Governança, Riscos e Controles)

Papel da 3ª. Linha de defesa:

<u>Avaliar</u> GRC (subsidiariamente, consultoria em GRC)

Imagem: https://pixabay.com/en/question-mark-pile-questions-symbol-2492009/

Instituto de Auditores Internos

(melhores práticas mundiais)

Referencial para Auditoria Interna Federal

(IN-SFC 3/2017)

Tribunal de Contas da União

Diversos Acórdãos (inclusive p/ MS)

O que pode ocorrer quando a 1ª linha de defesa não faz seu papel?

A) O risco não é gerido (2ª e 3ª linhas não têm recursos suficientes para fazer o papel da 1ª linha)

B) 2ª e 3ª linhas não exercem seu papel (supervisionar GRC, avaliar GRC)

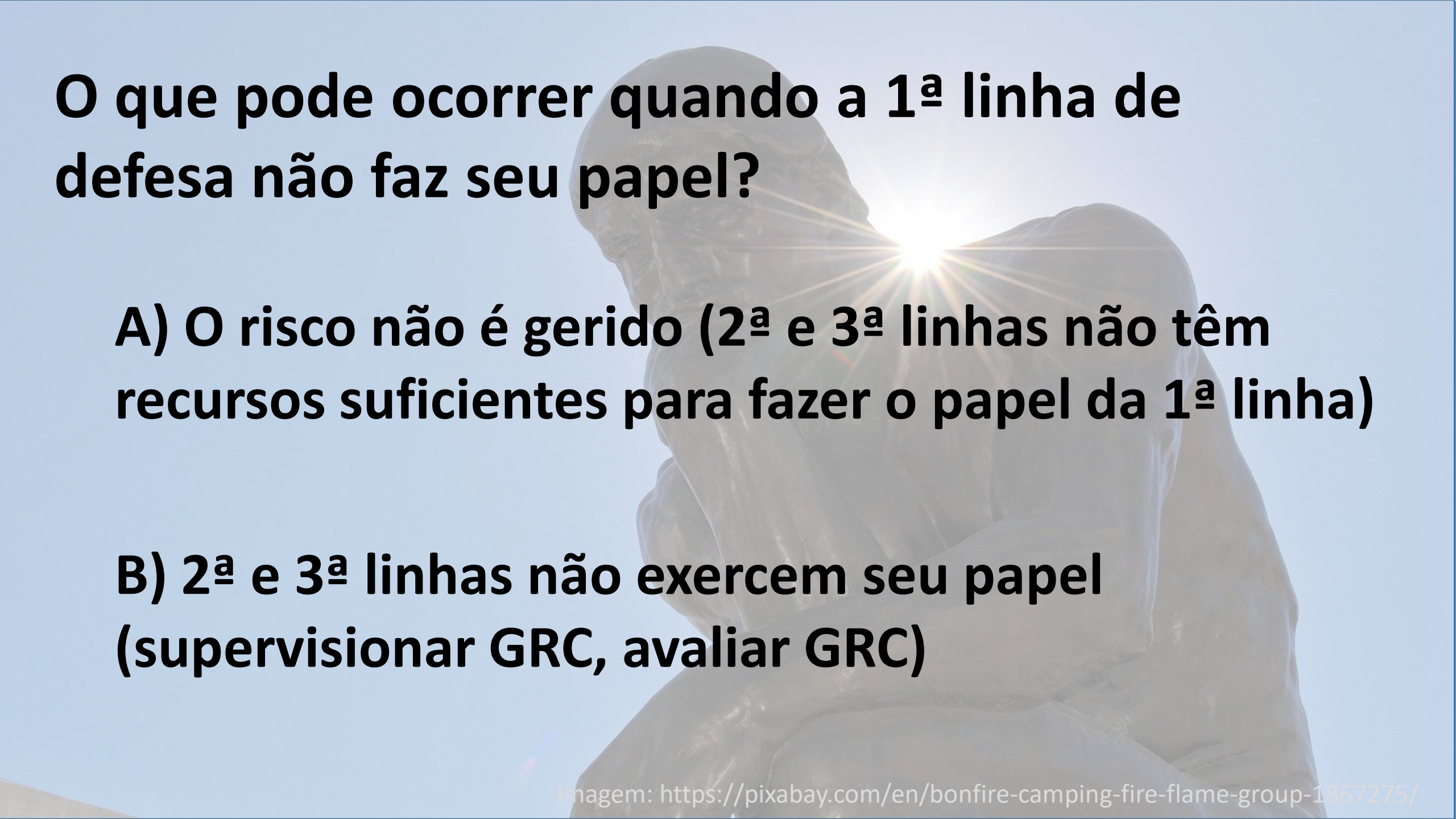


Imagem: https://pixabay.com/en/bonfire-camping-fire-flame-group-1867275/

A jornada...

Participar onde sou parte interessada

Saber em qual linha de defesa estou

Ser dono dos seus riscos

Por que uma auditoria de TI está preocupada com isso?

Porque “projetos de TI normalmente não são da TI” (para qual setor do MS são os projetos da ESD como, por exemplo, a RNDS?)

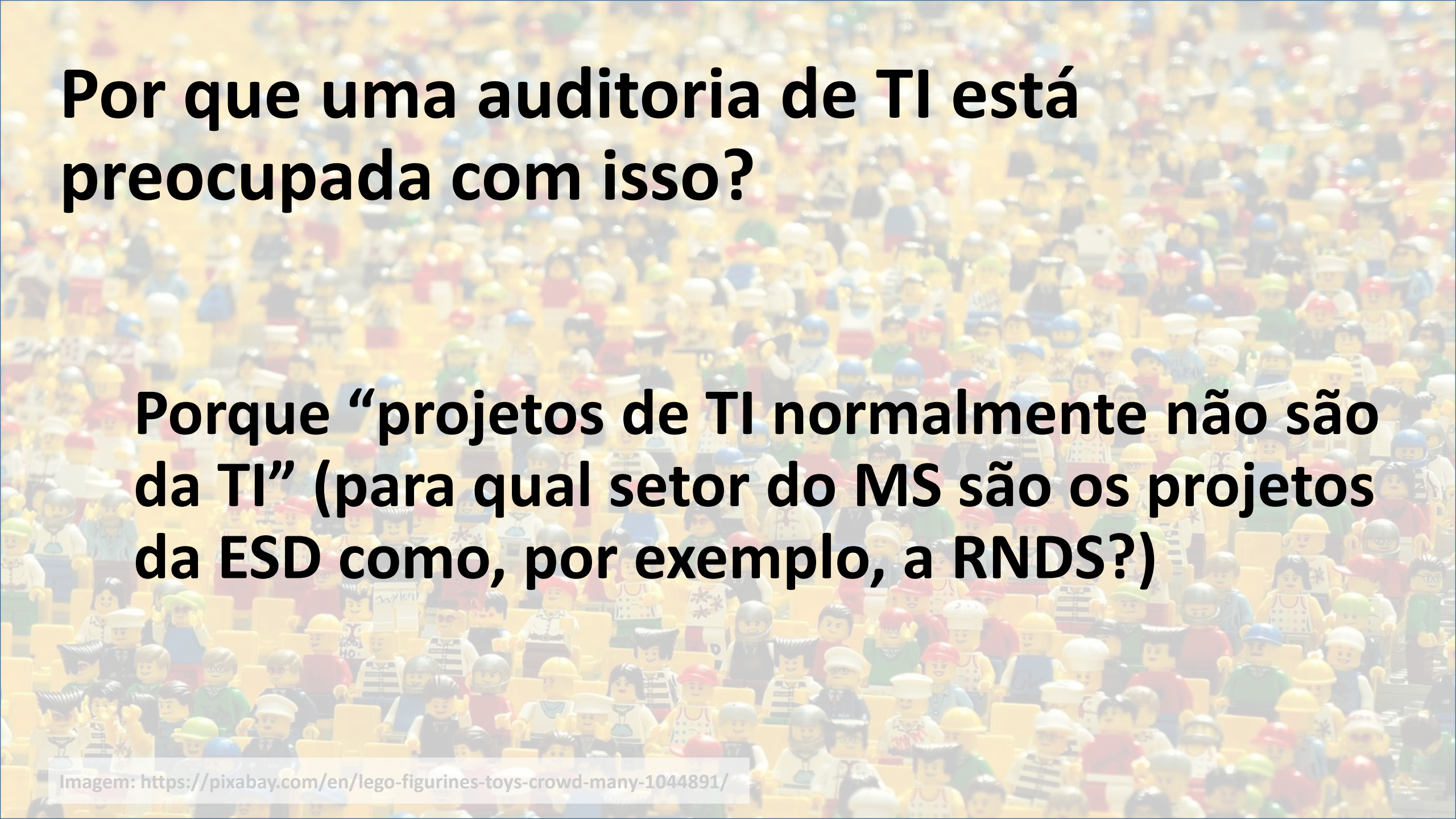


Imagem: https://pixabay.com/en/lego-figurines-toys-crowd-many-1044891/

O que fazer agora?

Imagem: Pixelstalk

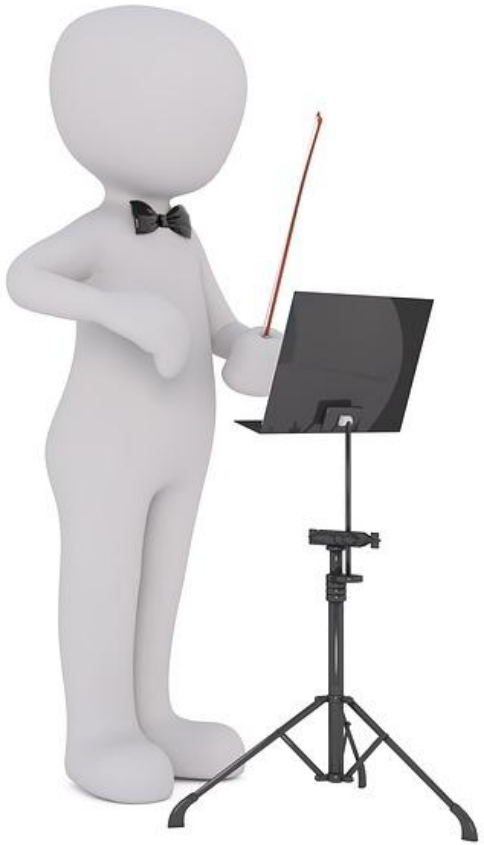
Percorrer a jornada…

Participar onde sou parte interessada

Saber em qual linha de defesa estou

Ser dono dos seus riscos

Tone of the Top



O que você pretende com as suas práticas?

Papel aceita tudo...

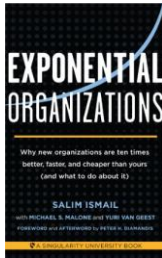
Imagem: Freeimages

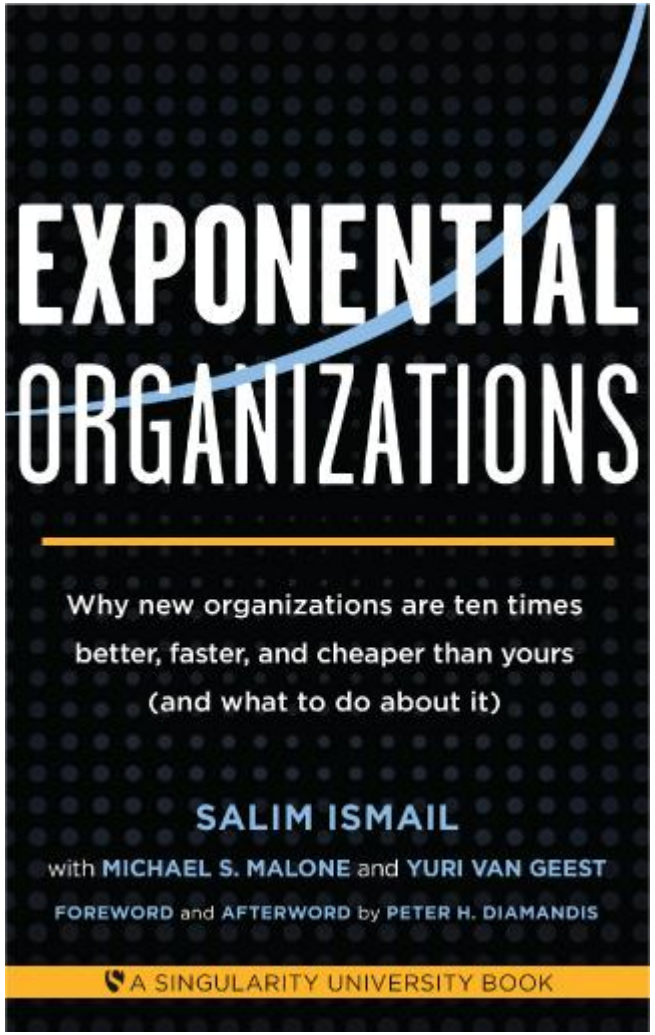
Controle proporcional ao risco

Decreto-Lei 200/1967 (art. 14)
Decreto 83.936/1979 (“considerandos”)
Lei 13.460/2017, art. 5º, XI
Decreto 9.094/2017, art. 1º, V

Um convite…

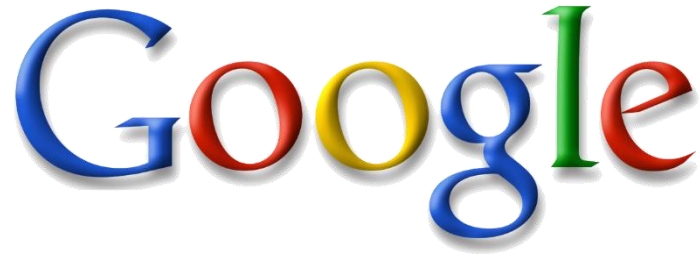
(2ª parte)





*"É aquela cujo impacto (ou resultado) é desproporcionalmente grande - pelo menos dez vezes maior - comparado aos seus pares, devido ao **uso de novas técnicas organizacionais** que alavancam as tecnologias aceleradas."*


amazon


Google


facebook


waze
OUTSMARTING TRAFFIC, TOGETHER


airbnb


UBER

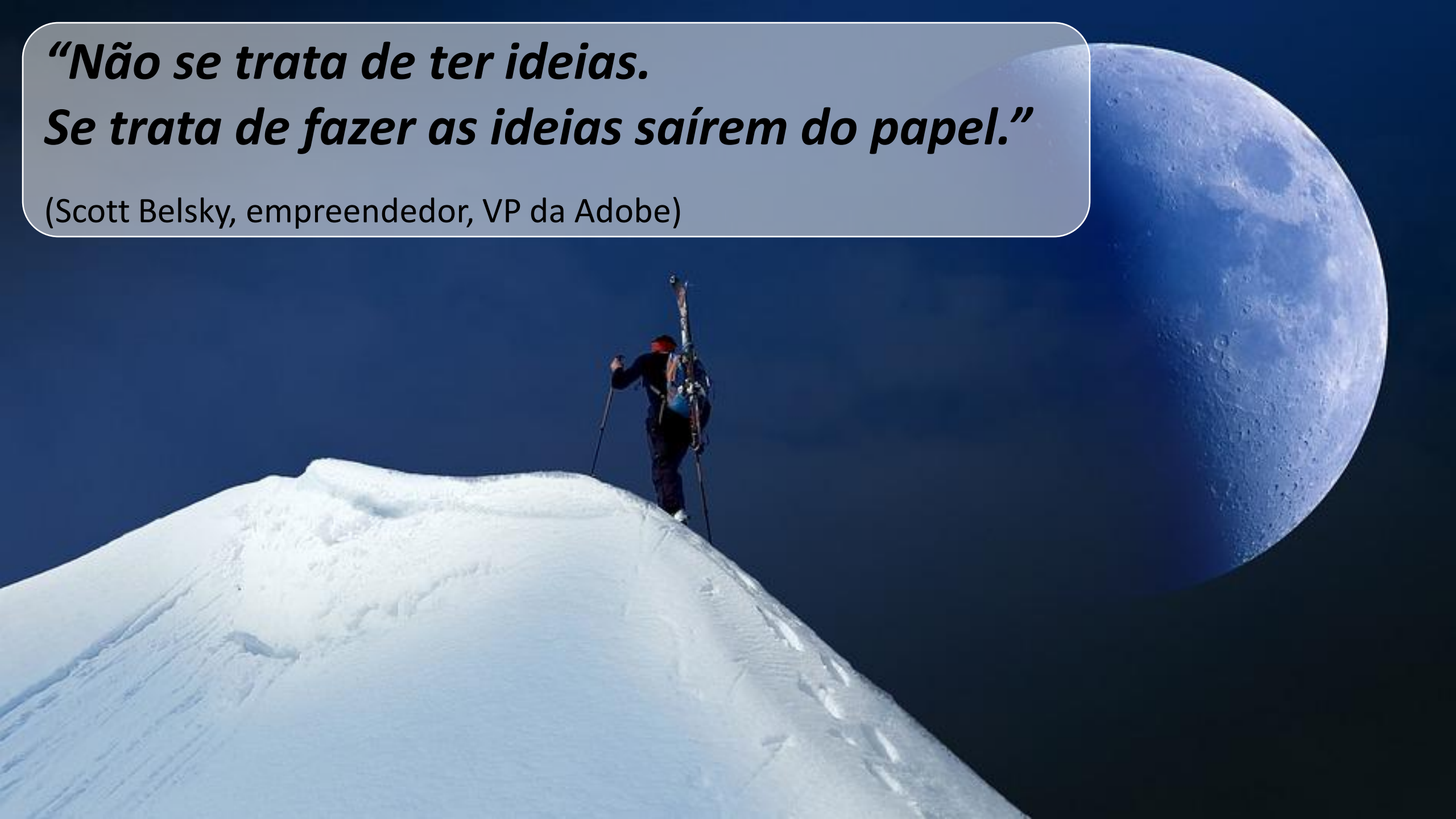

TESLA

Por que elas conseguem escalabilidade exponencial?

Algum aspecto do seu produto foi habilitado para a informação (e pela lei de Moore pode dobrar rapidamente)

Como é fácil fluir a informação, as principais funções de negócio podem ser executadas para fora da organização

Como fazer controle pensando assim?



“Não se trata de ter ideias.
Se trata de fazer as ideias saírem do papel.”

(Scott Belsky, empreendedor, VP da Adobe)

Faz sentido?

É possível?

Imagem: https://fotografia.folha.uol.com.br/galerias/44226-obras-de-nathan-sawaya