COGEF
Comissão de Gestão Fazendária

COGEF/TI
Abril/2022

Estratégias de Governança e Segurança

Lindenberg Naffah Ferreira
SEF/MG

FAZENDA MINAS GERAIS GOVERNO DIFERENTE. ESTADO EFICIENTE.

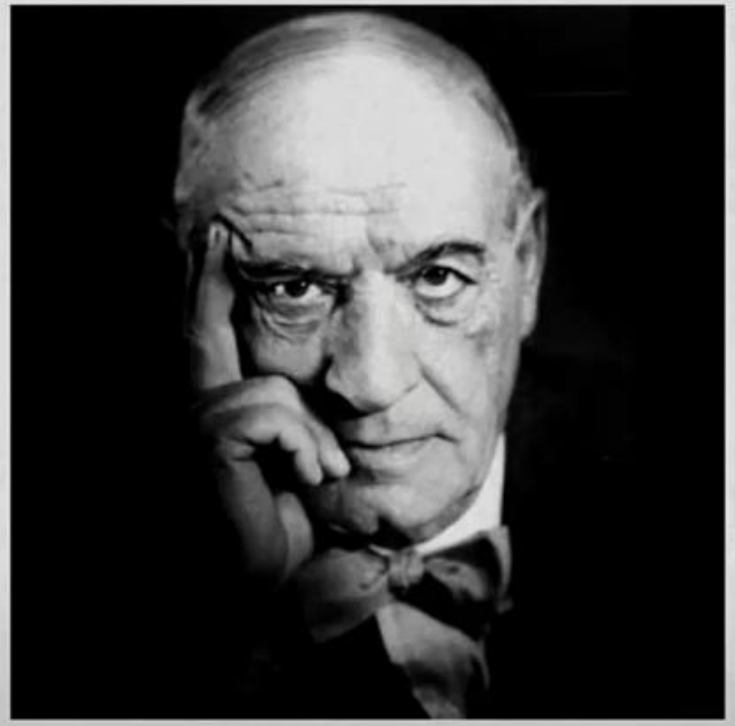
Roteiro


Contexto + Princípios
Inserção Institucional
Comitês de Segurança e Similares
Contratação de Consultoria e Serviços
Conclusões

SEF
Secretaria de Estado de Fazenda
de Minas Gerais

Contexto + Princípios

Secretaria de Estado de Fazenda de Minas Gerais



"EU SOU EU E MINHA CIRCUNSTÂNCIA, E SE NÃO SALVO A ELA, NÃO ME SALVO A MIM" ORTEGA Y GASSET

Invasão a órgãos públicos

Tribunal Superior Eleitoral

CONSELHO NACIONAL DE JUSTIÇA

CGU

1ª REGIÃO

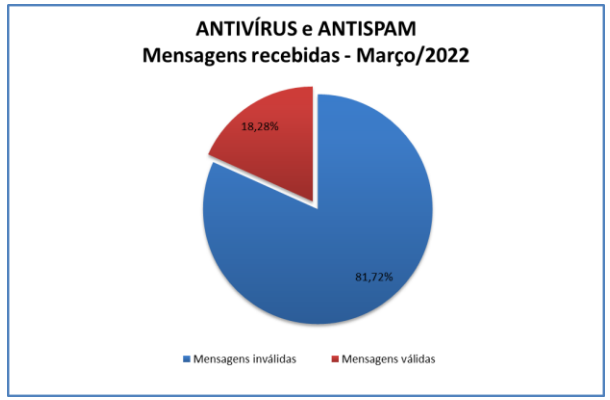
STJ SUPERIOR TRIBUNAL DE JUSTIÇA

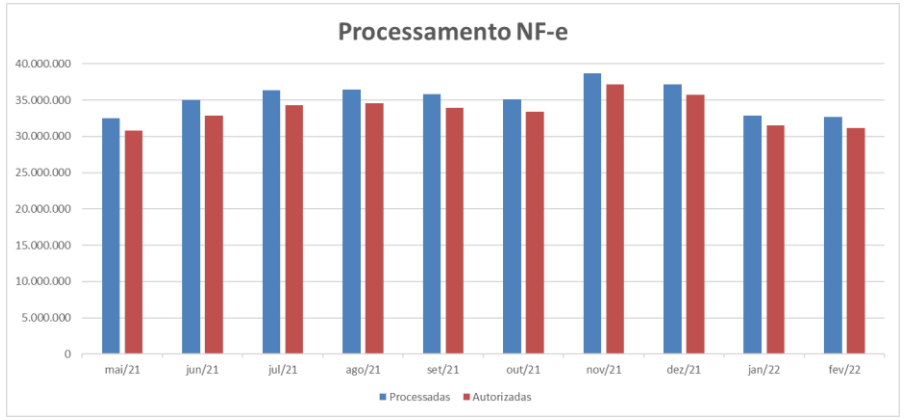
MinSAÚDE

https://g1.globo.com/economia/tecnologia/noticia/2021/12/14/alem-da-saude-cgu-prf-e-ifpr-tambem-confirmaram-invasao-por-grupo-hacker.ghtml
https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2020/11/28/brasil-vira-alvo-de-ataques-hackers.htm
https://www.cnnbrasil.com.br/nacional/pf-aponta-que-ataque-hacker-atingiu-ministerios-e-mais-de-20-de-orgaos-do-governo/
https://www.istoedinheiro.com.br/orgaos-do-governo-sofrem-novo-ataque-de-hackers-diz-gsi/
https://economia.uol.com.br/noticias/redacao/2021/08/15/tesouro-nacional-ataque-hacker-ransomware-virus.htm

Porque investir em Segurança da Informação

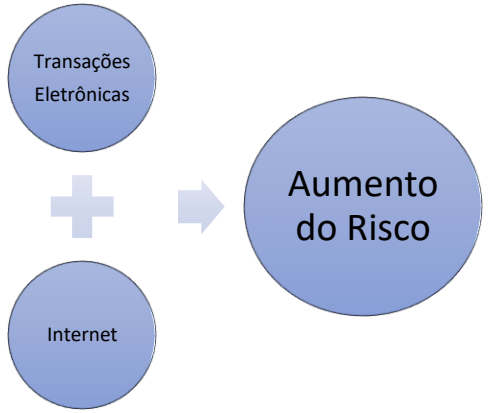
Descrição	Mensagens	Mensagens
Total de Mensagens inválidas (Filtro de Reputação, Filtro de Conteúdo, Recipiente Inválido, Spam e Vírus detectado, Mensagem de Marketing e mídia social)	81,72 %	1.321.367
Mensagens válidas	18,28 %	295.563
Total de Mensagens	100,00 %	1.616.930





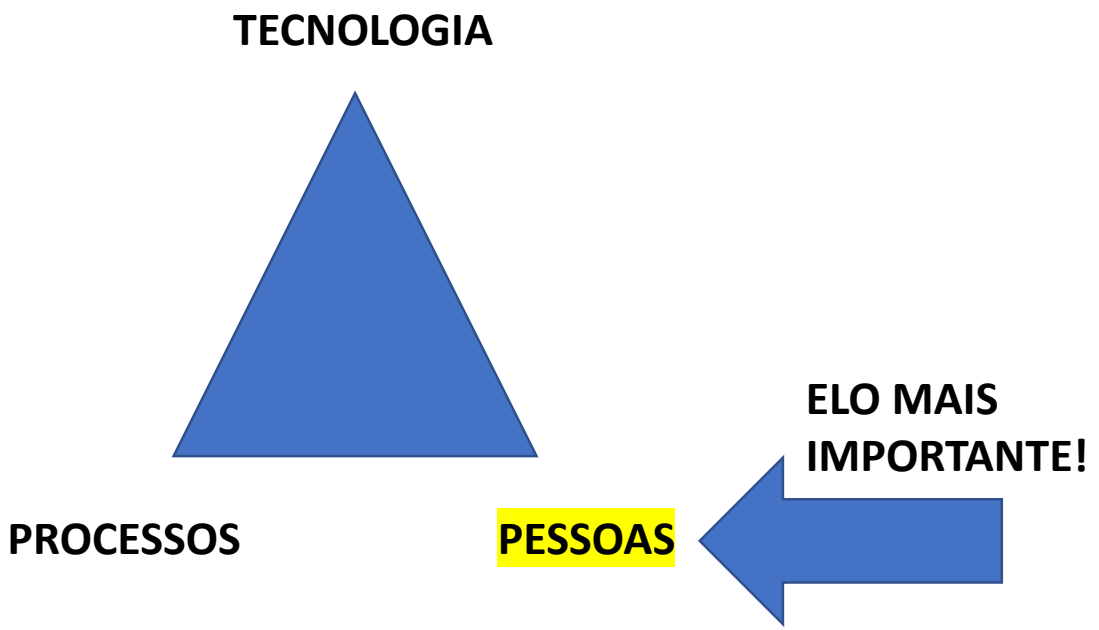
Autorizações de NFC-e em MG em dezembro de 2021=

256.050.969



TECNOLOGIA NÃO É TUDO!

- **SEGURANÇA DA INFORMAÇÃO NÃO ENVOLVE APENAS TECNOLOGIA!**



TECNOLOGIA NÃO É TUDO!

- Simplificar processos pode reduzir custos e torná-los mais seguros, diminuindo o número de pontos de falha.
- A economia gerada com a revisão de processos pode ser muito maior do que aquela alcançada com o aumento da eficiência da área de tecnologia.

CUIDADO COM OS ACUMULADORES DIGITAIS!

- **GUARDAR LIXO NÃO É BOA PRÁTICA: VOCÊ NÃO TEM O QUE PRECISA E GUARDA AQUILO DE QUE NÃO PRECISA.**
- **TÃO IMPORTANTE QUANTO A POLÍTICA DE BACKUP É A POLÍTICA DE EXPURGO DE DADOS.**

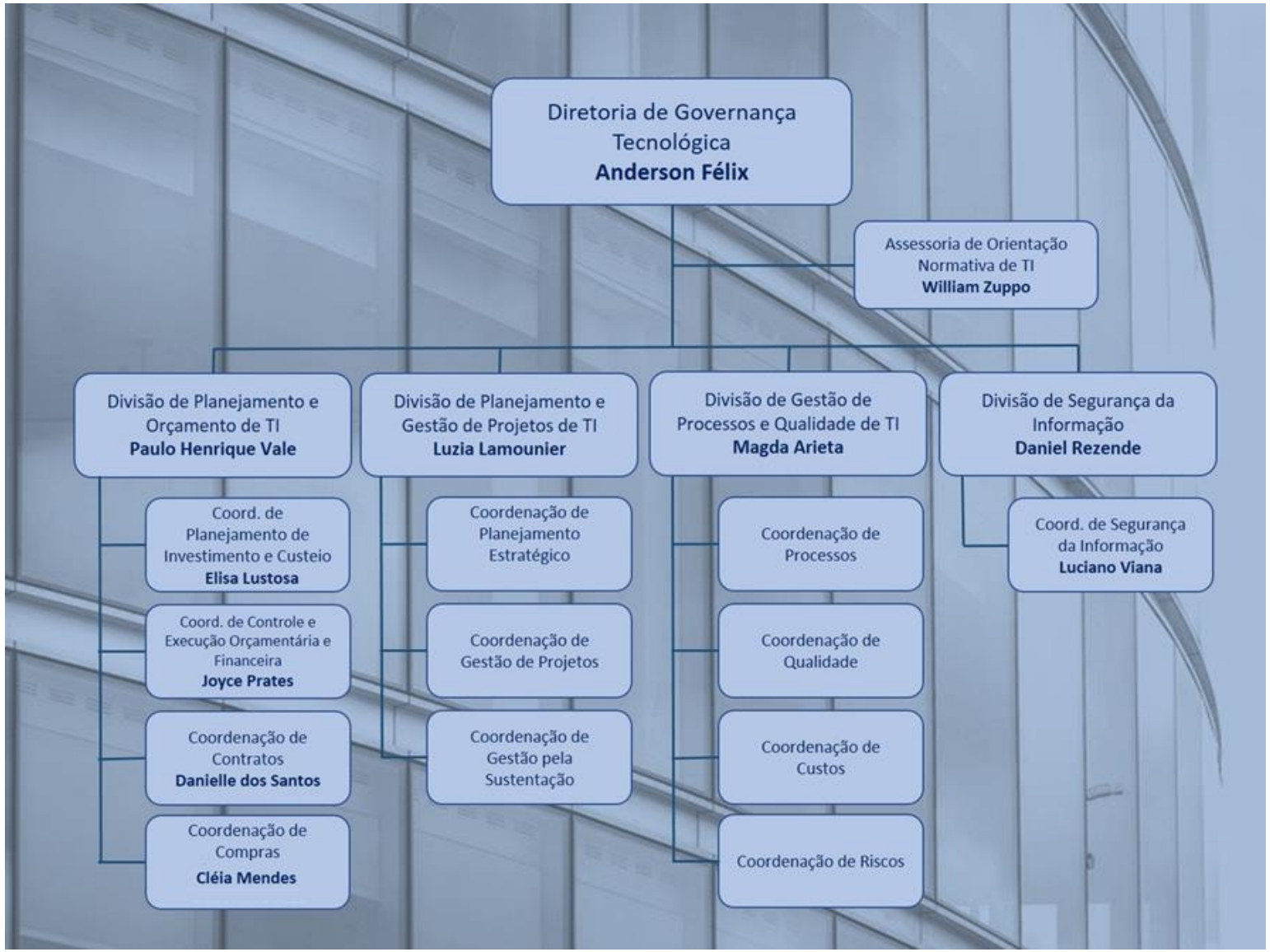
SEF
Secretaria de Estado de Fazenda
de Minas Gerais

Inserção Institucional

EXEMPLO DE ORGANOGRAMA (SEF-MG)

Secretaria de Estado de Fazenda

EXEMPLO DE ORGANOGRAMA (SEF-MG)



EQUIPE GOVERNANÇA

Magda Arieta

Anderson Félix

EQUIPE GOVERNANÇA

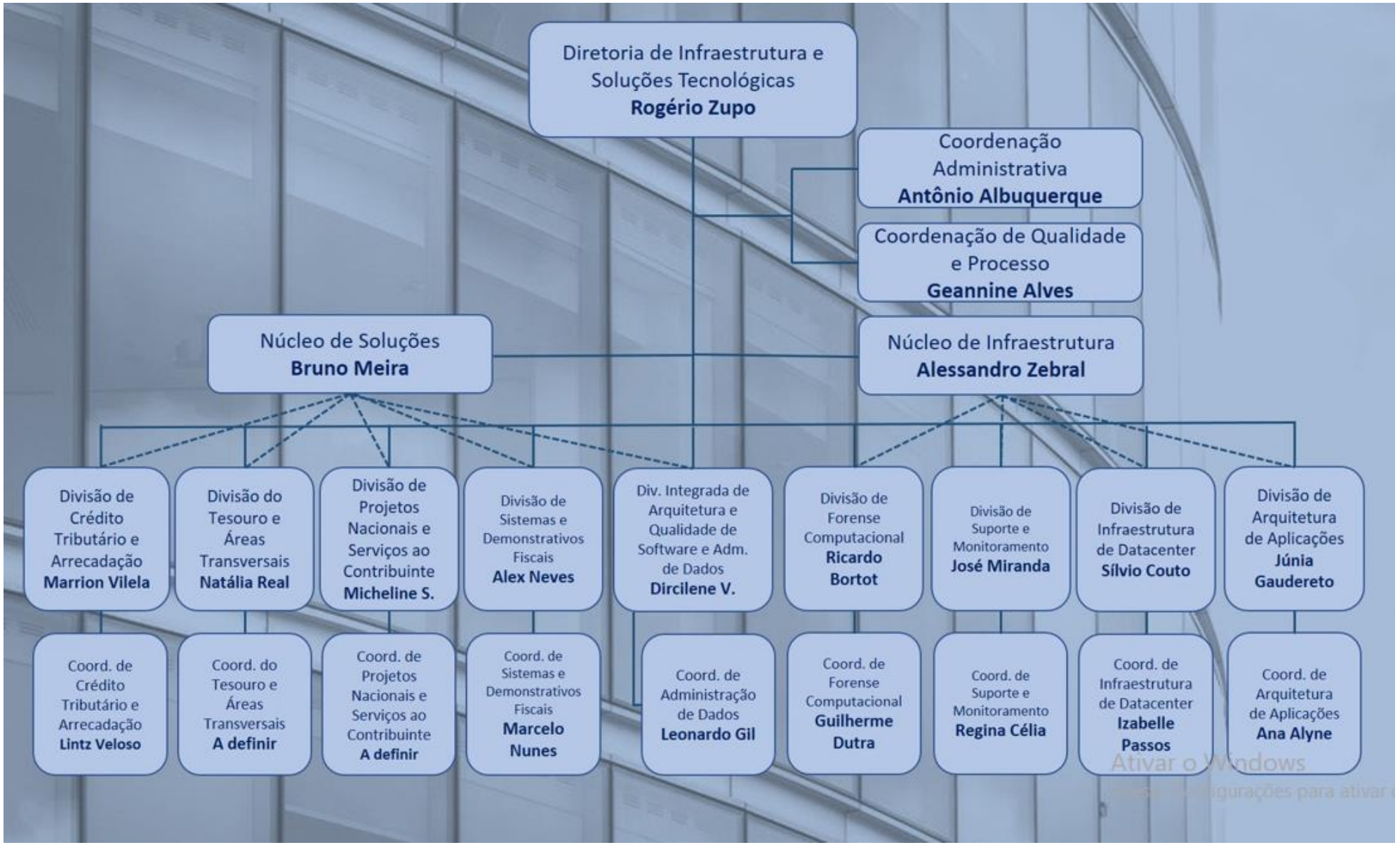
Daniel Rezende

Luciano Viana

Secretaria de Estado de Fazenda

EQUIPE GOVERNANÇA

EXEMPLO DE ORGANOGRAMA (SEF-MG)



EQUIPE INFRAESTRUTURA E SOLUÇÕES

Rogério Zupo

Alessandro Zebral

Inserção institucional da área de segurança da informação

- Dentro ou fora da TI?
- Depende...
- Aspectos a serem considerados:

1. Aspectos legais/regulamentares

- DENTRO OU FORA DA TI?
- DEPENDE...
- ASPECTOS A SEREM CONSIDERADOS:

2. FLUXO DE TRABALHO E CAPACIDADE DE EXECUTÁ-LO

- DENTRO OU FORA DA TI?
- DEPENDE...
- ASPECTOS A SEREM CONSIDERADOS:

3. INFLUÊNCIA E AUTORIDADE

SEF
Secretaria de Estado de Fazenda
de Minas Gerais

Comitês de Segurança e Similares

Modelo de Governança

Item	Ativos	Perfil de Risco - Vulnerabilidade	Descrição do risco associado	Proprietário do Risco	P	I	R	P.I.R.	Situação	Estratégia de Resposta
	A	B	C	D	E	F	G	H	I	J
5										

Item	Ativos	Perfil de Risco - Vulnerabilidade	Resposta ao Risco	Ação de Contingência e Controles	Situação Atual / Observações
	A	B	K	L	M
5					

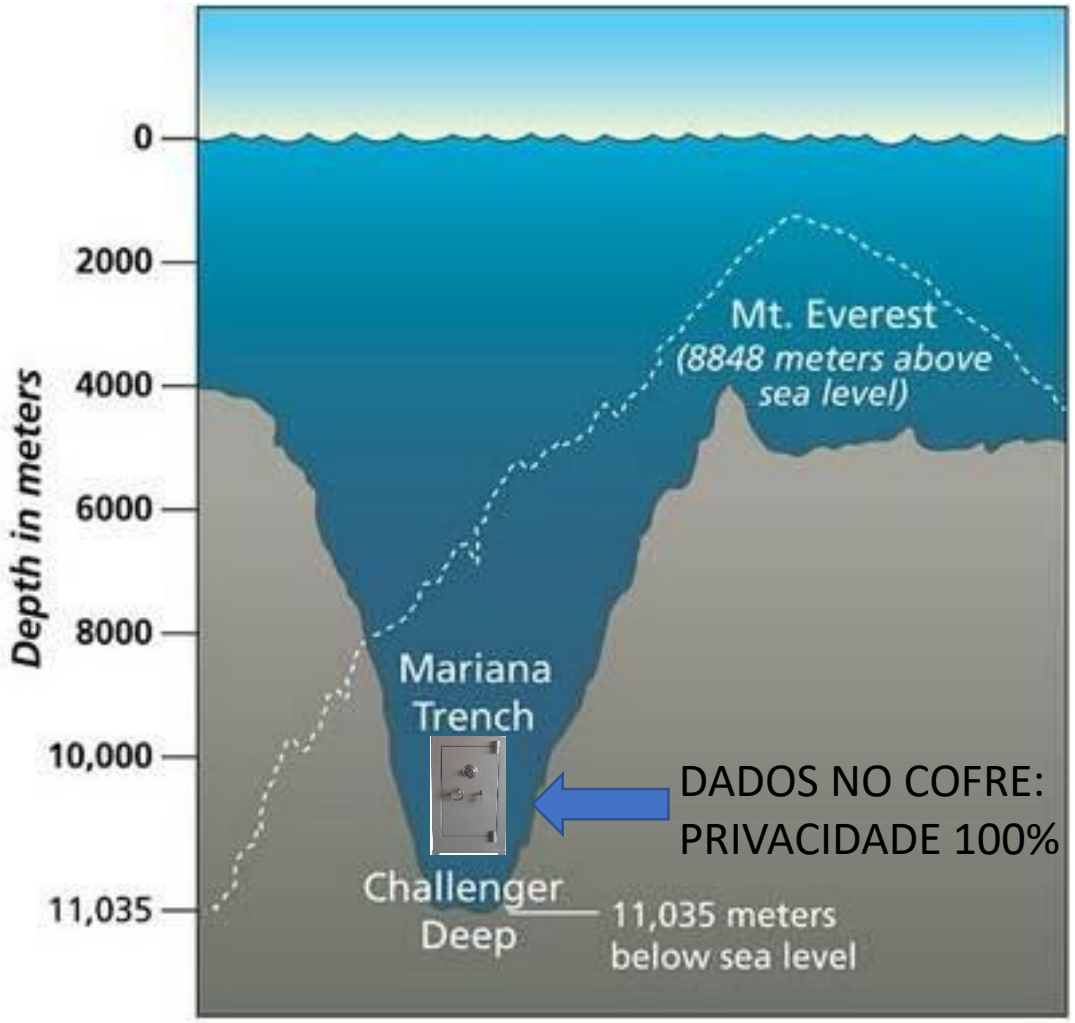
Faixas PIR
Probabilidade x Impacto x Relevância

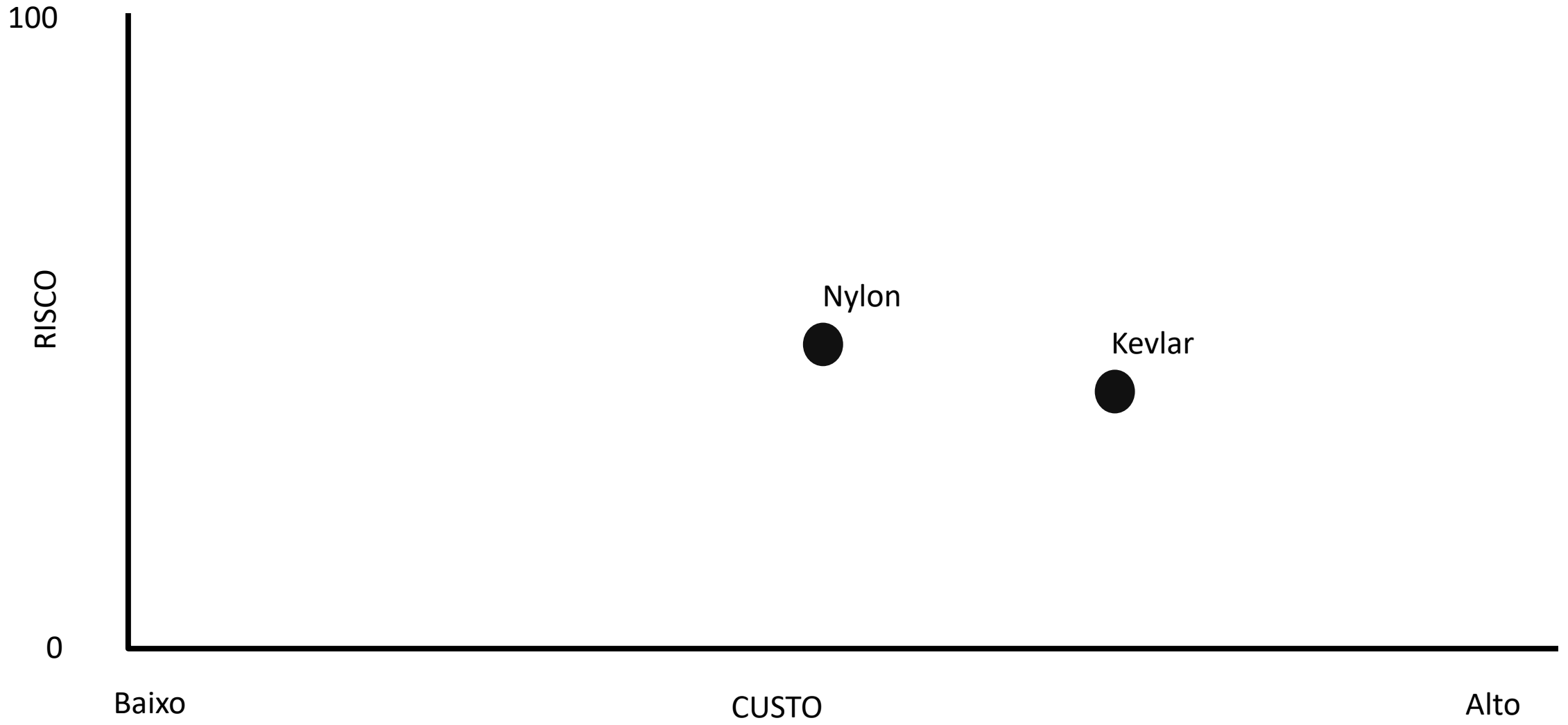
<60
=60
>60

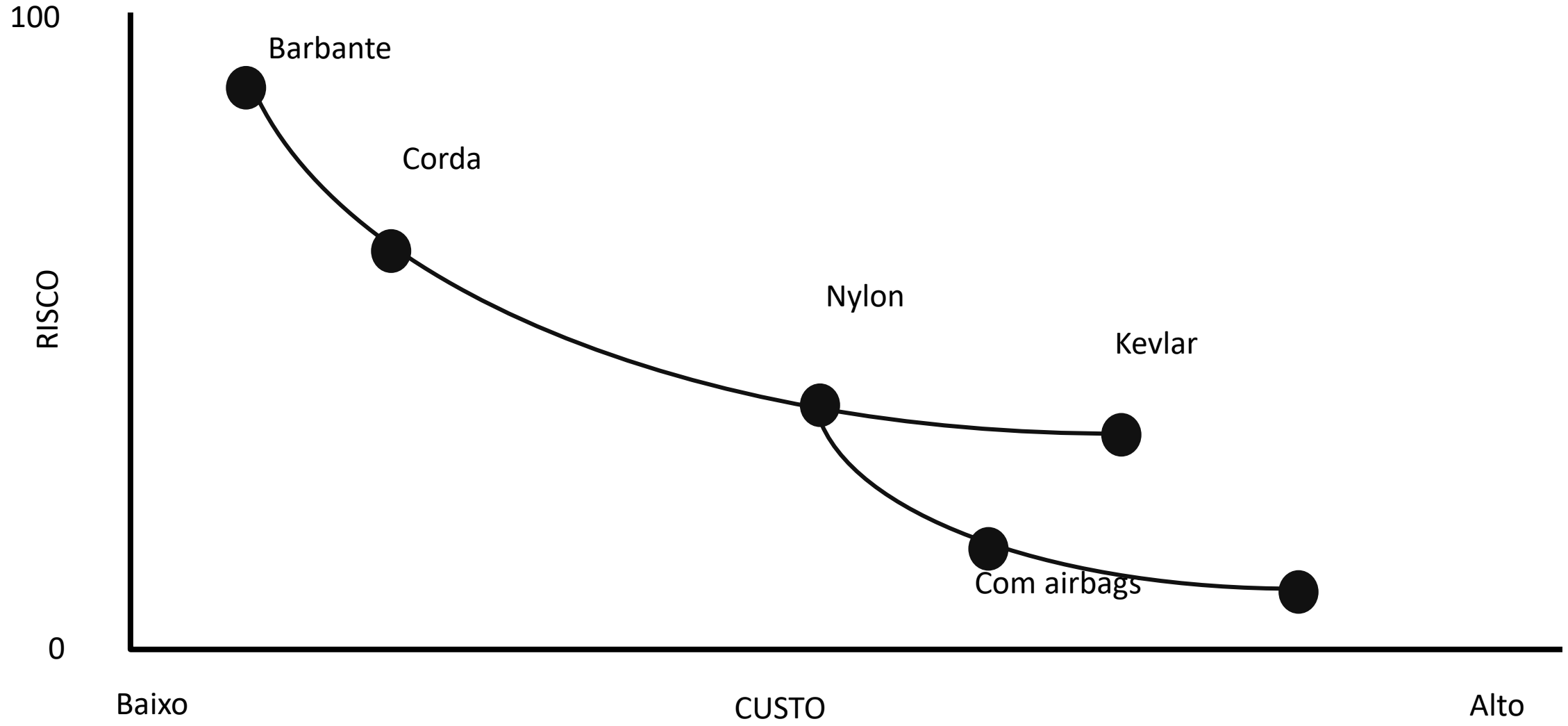
Nível	PIR	Valores possíveis para o PIR
Muito baixo	São riscos aceitáveis	1,2,3,4,5,6
Baixo	São riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos	8, 9, 10, 12, 15, 16
Médio	São riscos que podem ser acetáveis após revisão e confirmação dos gestores dos ativos.	18,20 ,24, 25, 27, 30
Alto	São riscos inaceitáveis e os gestores dos ativos são orientados para pelo menos mitigá-los.	32, 36, 40, 45, 48, 50
Muito Alto	São riscos inaceitáveis, e os gestores dos ativos devem ser orientados que os eliminem.	**60**, 64, 75, 80, 100, 125

É inviável eliminar todos os riscos!

NÃO É POSSÍVEL OBTER 100% DE CONFIDENCIALIDADE SEM SACRIFICAR A DISPONIBILIDADE DOS DADOS.

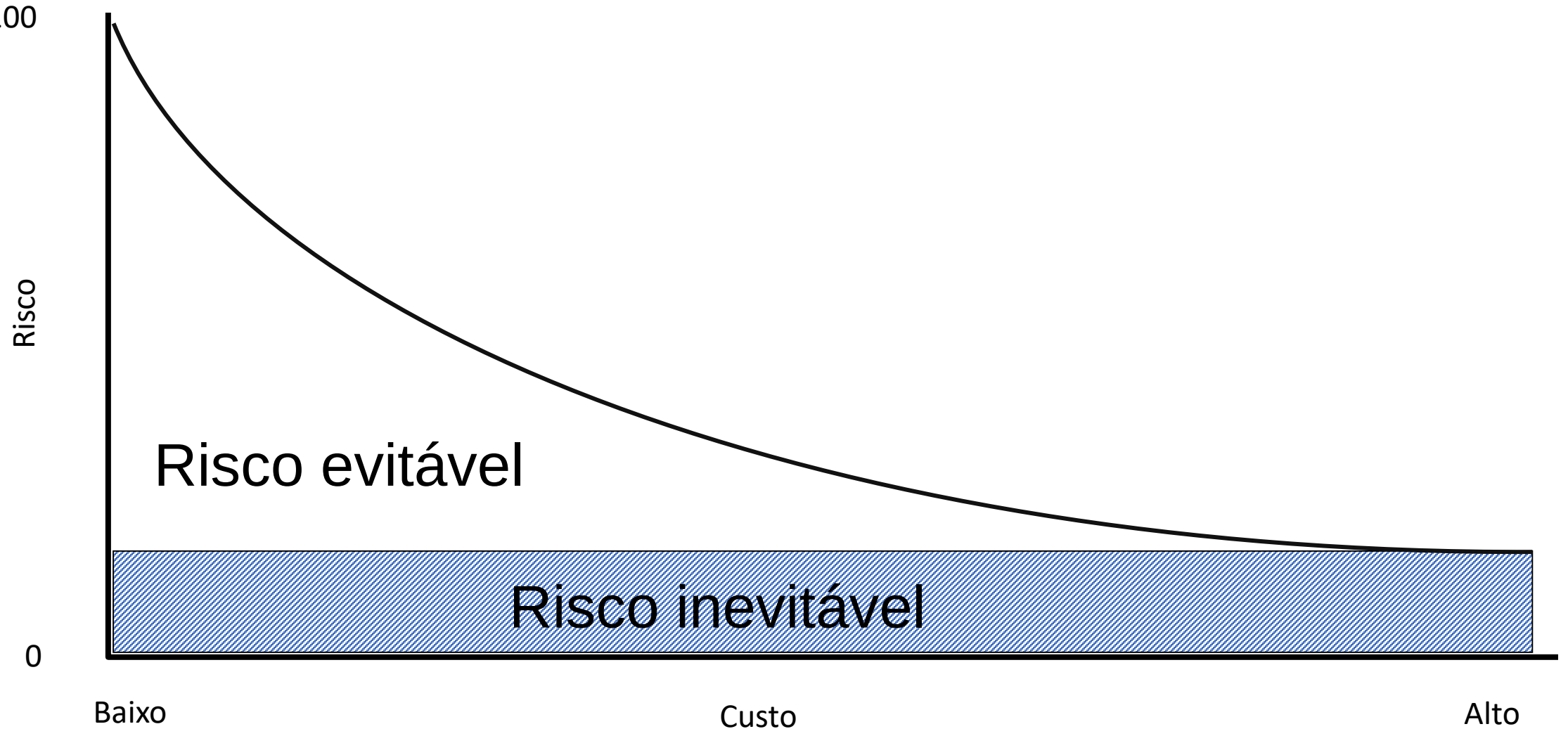



100
RISCO
0
Nylon
Kevlar
Baixo
CUSTO
Alto


100
RISCO
0
Barbante
Corda
Nylon
Kevlar
Com airbags
Baixo
CUSTO
Alto

Em tempo: essa era a realidade em 2015. O custo de gerência de endpoint caiu muito desde então.

Gerenciando Risco



Secretaria de Estado de Fazenda

“Relatórios que dizem que algo não aconteceu são sempre interessantes para mim porque, como sabemos, há coisas que sabemos que sabemos. Também existem coisas que sabemos que não sabemos, ou seja, sabemos que existem algumas coisas que não sabemos. Mas também há as que não sabemos que não sabemos. E se olharmos ao longo da história do nosso país e de outros países livres, é a última categoria que tende a ser a mais difícil.” Donald Rumsfeld

Secretaria de Estado de Fazenda

Secretaria de Estado de Fazenda

Secretaria de Estado de Fazenda

- O departamento de rede quer comprar uma nova placa de interface WAN para atualizar seus roteadores Cisco 1760
- Eles recomendam a placa WIC-1DSU-T1-V2O, cujo preço de varejo sugerido pela Cisco é de cerca de US $ 1.000
- A recomendação é aprovada e o pedido de peças vai para o departamento de compras
- O departamento de compras, sabendo que dinheiro não cai do céu, vai pesquisar os preços na Internet
- Vamos ver o que eles descobriram....

Secretaria de Estado de Fazenda

Cisco WIC-1DSU-T1 Card

1-Port T1/Fractional T1 DSU/CSU WAN Interface Card ...

Condition: **Certified Pre-Owned**

UC Part #: 213262

Availability: **In Stock - Ready to ship**

Be the first to write a review

Actual item may differ from photo shown. UsedCisco.com does not sell or include licensed software of any kind. All products are tested and updated with the latest manufacturer's firmware.

EXTEND YOUR WARRANTY

1 Year Warranty	Free
2 Year Warranty	$10.00
3 Year Warranty	$20.00

PRODUCT PRICING

List Price:	~~$1,000.00~~
You Save:	$900.01 (90%)
Today's Price:	$99.99

QTY: 1 Add To Cart

ADD-ONS

No accessories available.

Add To Cart

Secretaria de Estado de Fazenda

Google WIC-1DSU-T1-V2 Sign in

Web Images Maps Shopping More

Electronics
Audio
Computers & Devices
Photo & Optics
TV & Video
More

Bernards, NJ
Change

Show only
In stock nearby
New items

Price
Up to $100
$100 – $250
$250 – $600
Over $600
$ to
$ Go

Category
Bridges & Routers
Modems

Sort: Default View: Grid My Shortlists

Merchant links are sponsored

Cisco Module **WIC-1DSU-T1-V2**
$25.00 from Triton Datacom Online

Cisco 1-Port **T1** CSU/DSU Card, **WIC-1DSU-T1-V2**, NEW
$229.95 from CablesAndKits.com

Genuine Cisco Systems **Wic-1dsu-t1-v2** Interface Card For Router **T1** ...
$18.99 used from eBay - citirom

Cisco **WIC-1DSU-T1-V2** - Cisco **T1** DSU/CSU WAN Interface Card
$20.00 from CPU Medics

Cisco Systems Cisco 1841 Router - with Cisco **T1** DSU/CSU WAN ...
$699.85 from 10+ stores

Cisco - 1.5 Mbps DSU/CSU - PC
$94.14 from 25+ stores

Genuine Cisco **Wic-1dsu-t1-v2** Warranty 50 Available
$15.50 used from eBay - certlabkits

WIC-1DSU-56K Cisco Systems One Port 4-wire 56/64 CSU/DSU WAN Interfac
$64.64 from 10+ stores


"DIRTY" WELDING
CLEAN WELDING
WIC-1DSU-T1
V1
www.andovercg.com
COLOR WRONG
FONT WRONG
BAR CODE LOW
TIGHT
COPPER
TWISTS
SPACED
COPPER
TWISTS
JACK CLOSE TO CARD
JACK STICKS OUT BY 1/16 -1/32 INCH
SHINY SCREWS
COUNTERFEIT
DULL SCREWS
GENUINE

SEF
Secretaria de Estado de Fazenda de Minas Gerais

Contratação de consultoria e serviços

O caso da SEF/MG – 2005 até hoje

Secretaria de Estado de Fazenda

Fase 1 – 2005/2006 – Principais produtos

Diagnosticar:

- A situação de segurança da informação da SEF/MG
- Índice de risco da organização
- Ações emergenciais
- Gap Analisys em relação à ISO/IEC 17799 (hoje ISO/IEC 27.001)

Definir:

- Política de Segurança da Informação
- Plano Diretor de Segurança da Informação
- Plano de Continuidade de Negócios
- Plano de Ação da Campanha de Divulgação
- Metodologia de Gestão de Riscos

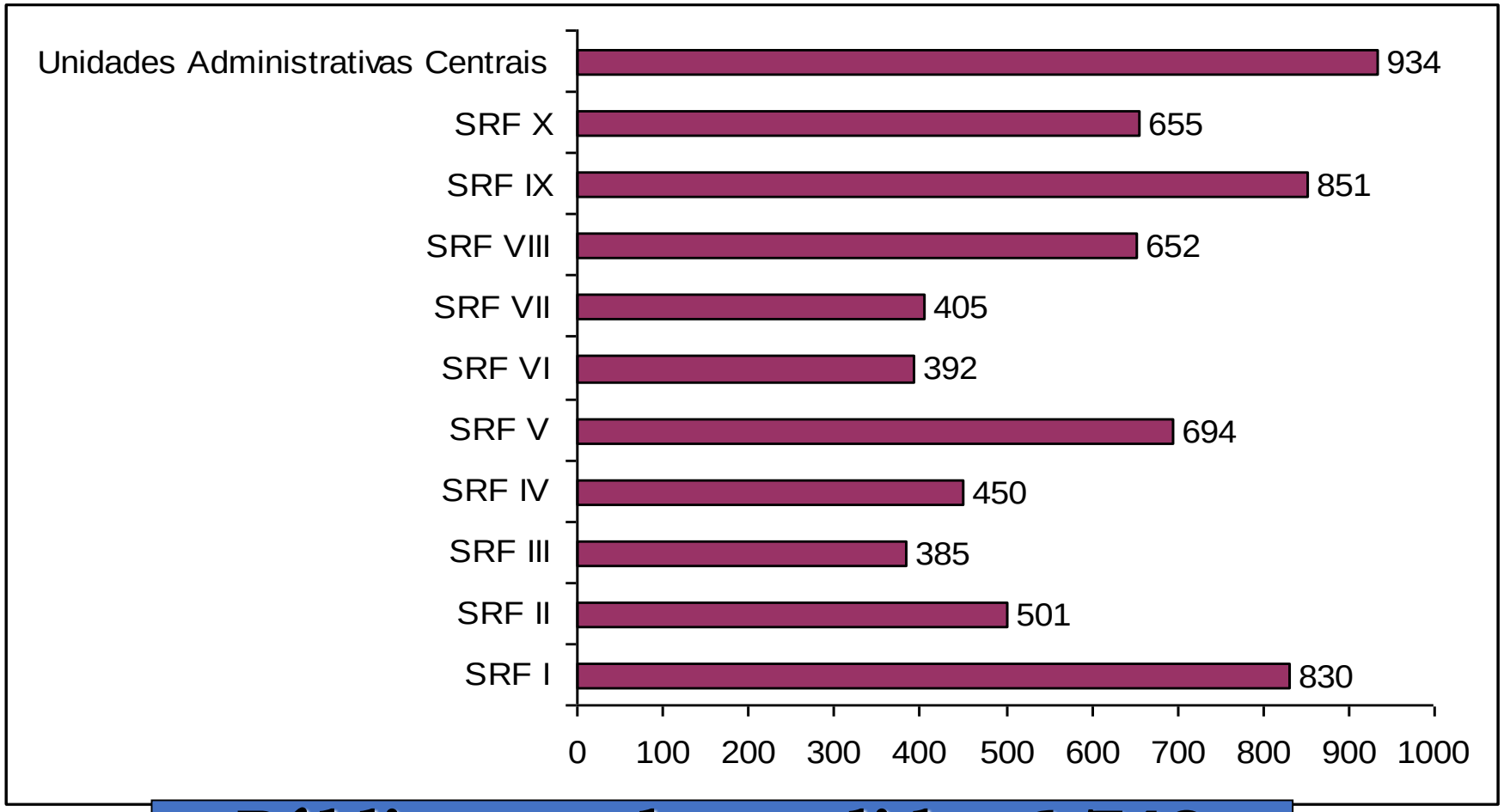
Implementar:

- Capacitação dos responsáveis pela área de SI
- Ferramenta de Gestão de Riscos
- Programa de Sensibilização dos Servidores da SEF/MG

1ª Campanha de sensibilização/divulgação

Convencer

Público atendido pela Campanha de Divulgação - Fase I



Público total atendido: 6.749

Peças publicitárias criadas em 2006

Bloco

Calendário 2007

Mouse Pad

Cartaz

O caso da SEF/MG – 2005 até hoje

Fase 2 – 2007/2008 – Principais produtos

Seção I – Análise de riscos

- Atualização de ferramenta de gestão de riscos
- Análise de riscos
- Implementação de segurança dos Ativos da Rede
- Testes de invasão, análise de risco da aplicação NF-e e do ambiente de desenvolvimento

Seção II – NBR ISO/IEC 17799:2005

- Estruturação da Gerência de Segurança da Informação
- Análise e especificação da segurança da informação
- Especificação de segurança dos requisitos da política de segurança
- Classificação da Informação

Seção III – Educação e Conscientização

- Campanha de Divulgação da Politica de Segurança da Informação
- Certificação de Security Officer
- E-learning – Auto-treinamento em Segurança da Informação para Colaboradores

Abertura da Campanha de Segurança 2007/2008

Peça teatral

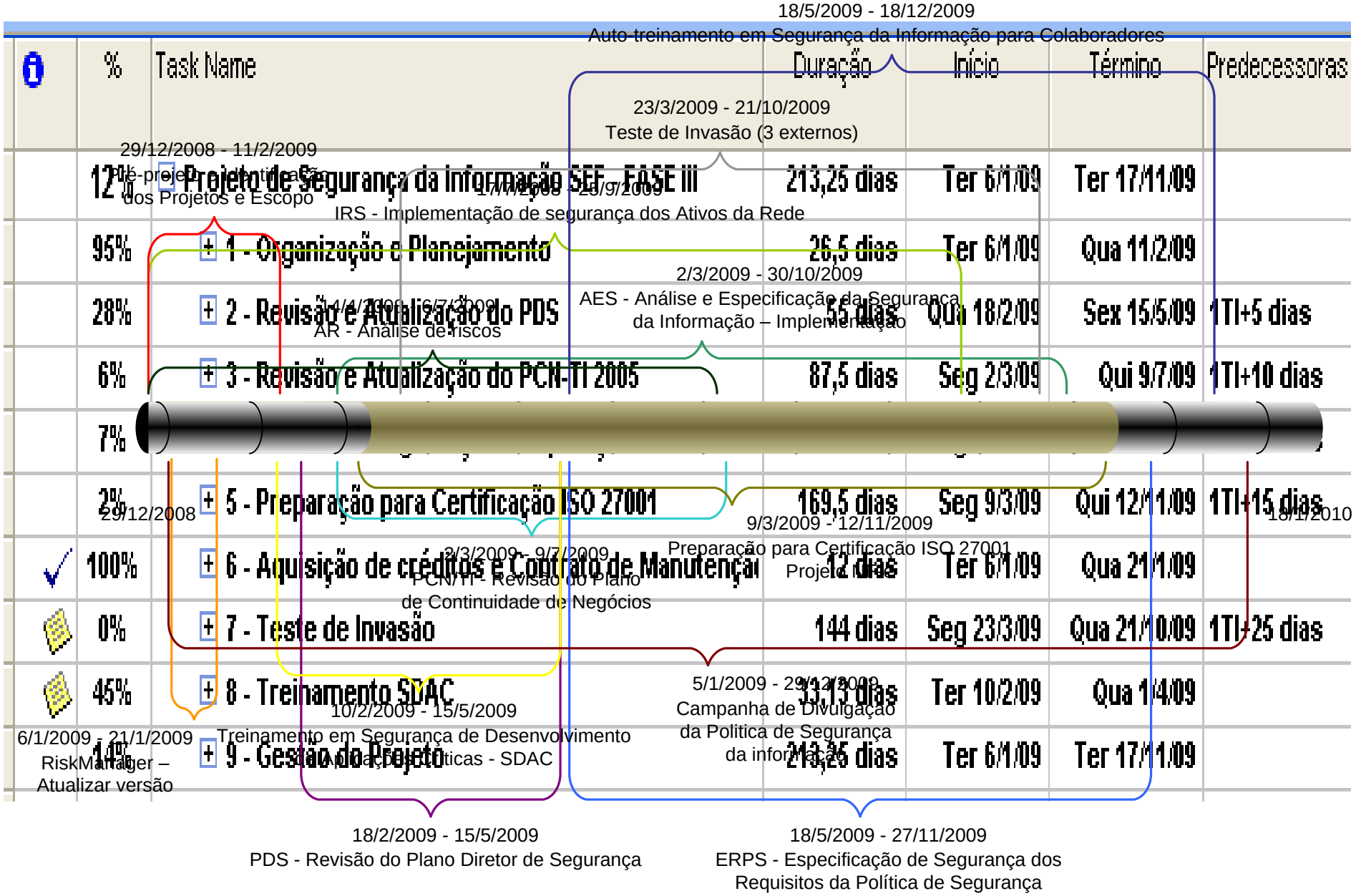
Peças publicitárias criadas em 2007/2008

Cartilha

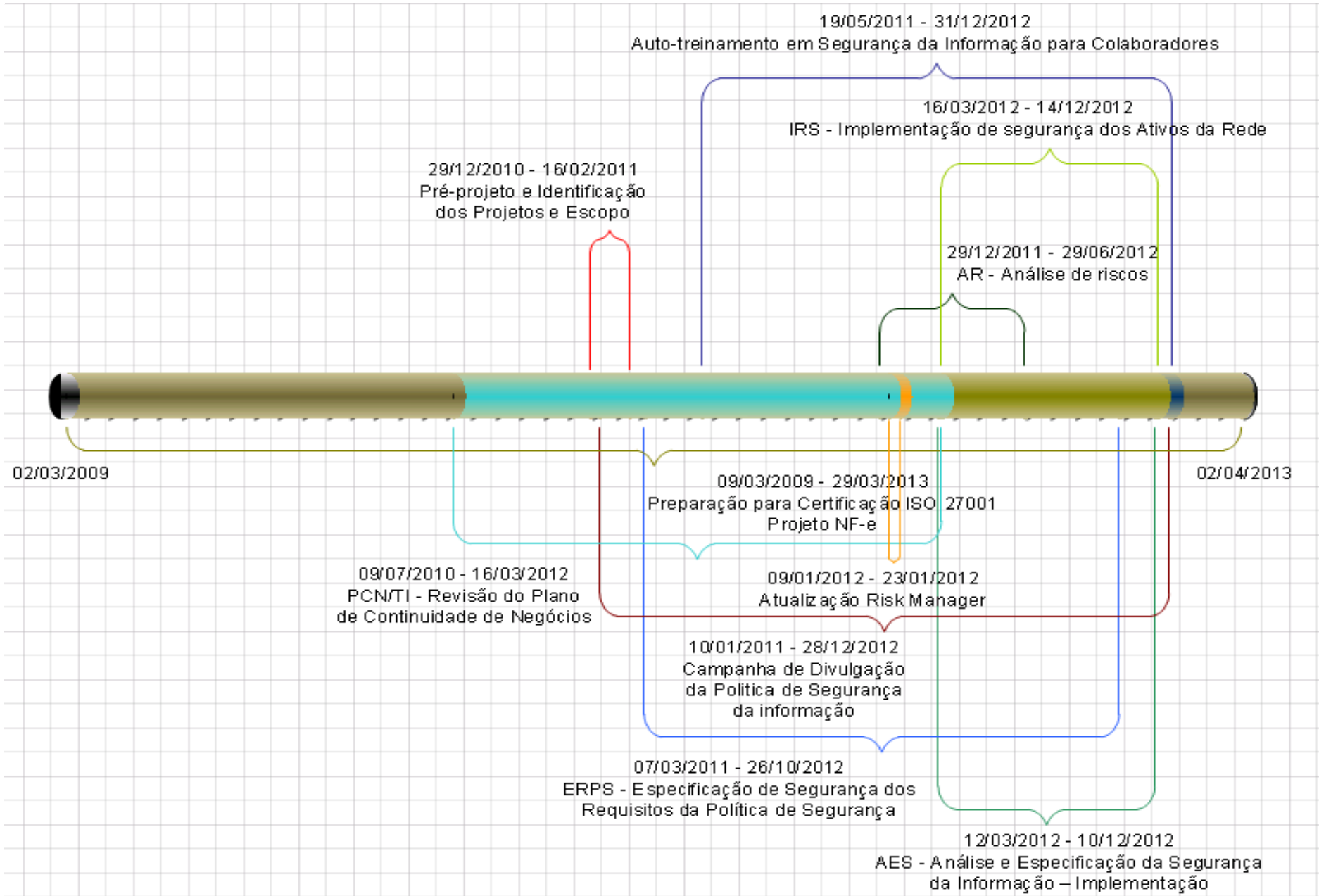
Calendário 2008

Cartazes

Cronograma do Projeto



Cronograma do Projeto



SERVIÇOS DE SEGURANÇA CONTRATADOS DE FORMA REGULAR HOJE

- Testes de invasão
- Atualização de ferramenta de gestão de riscos
- Certificação ISO 27.001 do ambiente de autorização de NF-e

Certificação ISO 27.001 – autorização de NF-e em produção

Benefícios Fundamentais da implementação da ISO 27001

Conformidade

Redução de Despesas

Vantagem de Mercado

Aprimoramento da Organização

A certificação pode demonstrar o explicitamente o compromisso do estado de Minas Gerais com:

Cidadãos (público em geral) e empreendedores que estão estabelecidos em Minas Gerais e

àqueles que pretendem se estabelecer no estado de Minas Gerais no futuro próximo;

Certificação ISO 27.001 – autorização de NF-e em produção

Benefícios

Gestão de Risco - Aumento no nível de Segurança da Informação

Implementação de normas

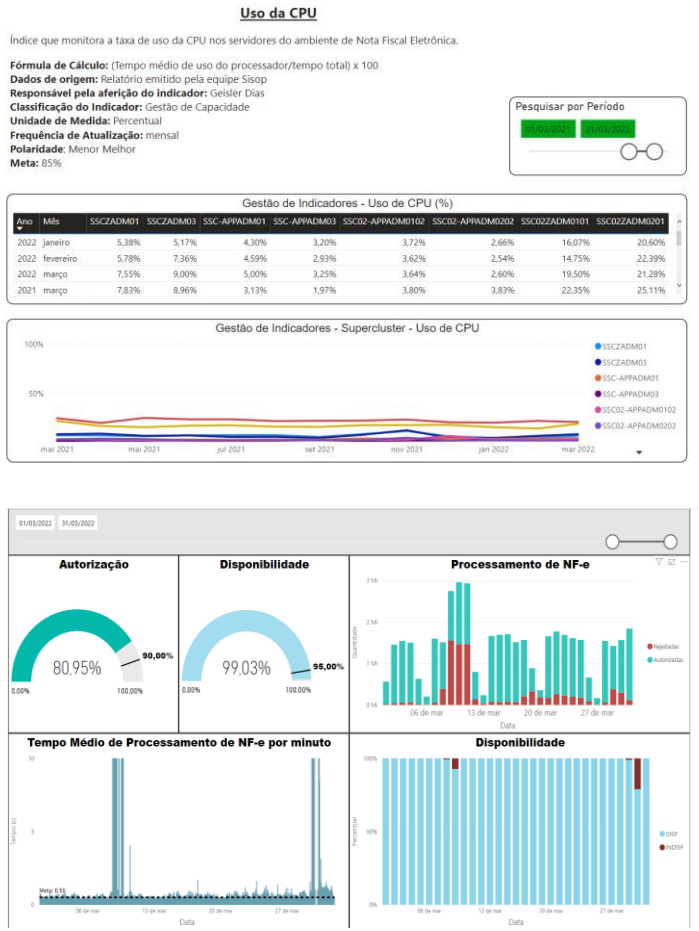
- Anexo A – Norma ISO 27001:2013
  - 95 Controles Implementados
  - 19 Controles Não aplicáveis
- Política da Segurança e Regulamentos
  - 345 Controles implementados
- Regulamentos e Procedimentos
  - 1534 Controles Implementados

Certificação ISO 27.001 – autorização de NF-e em produção

Benefícios

Gestão de Indicadores

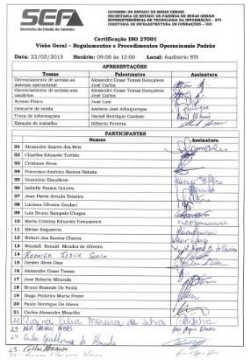
- Análise de Risco
- Número de Não conformidades em aberto
- Número de Incidentes
- Uso da CPU
- Uso da Memória
- Uso De Espaço em Disco
- Disponibilidade de Rede
- Capacidade da rede elétrica para a sala cofre
- Capacidade do No-Break
- Disponibilidade dos servidores de NF-e
- Tempo Médio de Processamento
- Processamento do NF-e
- Processamento do NF-e no ambiente de contingência
- ERPS – Especificação dos Requisitos da Política de Segurança da Informação



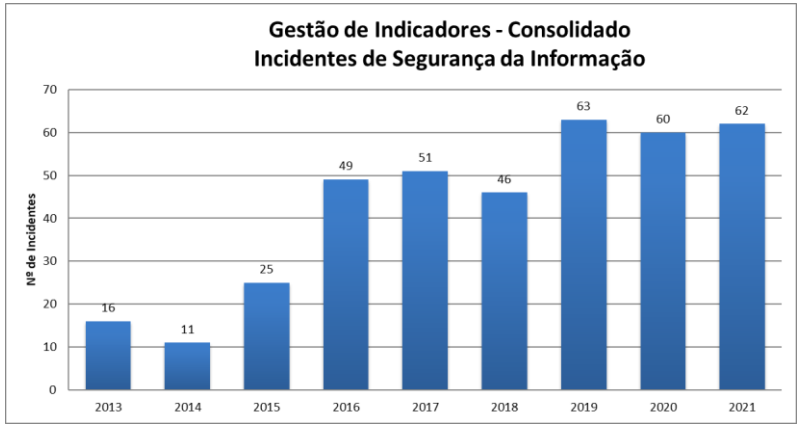
Certificação ISO 27.001 – autorização de NF-e em produção

Benefícios

Treinamento e Conscientização



Identificação e tratamento de Incidentes



Outras Ações

- Testes de Invasão
- Construção da Sala-cofre
- Modelo de Estação Segura

SEF
Secretaria de Estado de Fazenda
de Minas Gerais

Conclusões

CONCLUSÕES

- Levar em conta pessoas e processos, não apenas tecnologia.
- Avaliar a sua realidade local antes de definir a quem a segurança da informação deve ficar vinculada.
- Avaliar a necessidade de criar um comitê específico para segurança da informação.
- Usar estruturas multiníveis para comitês (comitês propositivos/executivos e deliberativo[s]).
- Contratar serviços especializados (testes de invasão, preparação para certificação, auditoria de certificação etc.) e avaliar a possibilidade de executar por conta própria outras atividades estratégicas, como planejamento de segurança, elaboração de política de segurança, sensibilização em segurança etc. Uma consultoria ou empresa de aconselhamento poderá rever o trabalho ou poderá ser contratada para estruturar a equipe e a função segurança da informação na organização.

COGEF
Comissão de Gestão Fazendária

COGEF/TI
Abril/2022

Obrigado!

Lindenberg Naffah Ferreira
lindenberg.naffah@fazenda.mg.gov.br
SEF/MG

FAZENDA MINAS GERAIS GOVERNO DIFERENTE. ESTADO EFICIENTE.