WTR
WORKSHOP
DE TECNOLOGIA DE REDES DO POP-ES
2022

Privacidade e a ponta do iceberg

Yuri Alexandro

13 JUL

PoP-ES
Ponto de Presença da RNP no Espírito Santo

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

#whoami

Yuri Alexandro

Analista de Sistemas

Especialista em Gestão de Segurança da Informação

IFBA, TJBA, UNEB, UFBA, CERT.Bahia e CAIS

Atualmente Coordenador de Privacidade – RNP

+20 anos na área de Tecnologia da Informação

+12 anos na área de Segurança da Informação

AGRADECIMENTOS

Privacidade

MICHAELIS | Português | Inglês | Espanhol | Alemão | Italiano | Francês

Dicionário Brasileiro da Língua Portuguesa

Sobre o dicionário | Como consultar | Noções gramaticais | Créditos

Português Brasileiro | Digite o termo desejado

privacidade

pri·va·ci·da·de

sf

Vida privada; intimidade, privatividade

ETIMOLOGIA

der do *ingl privacy+dade*, como *esp privacidad*.

PRIVACIDADE

LGPD

Lei Geral de Proteção de Dados Pessoais

Quando a gente lembra da LGPD...

MENU g1 DISTRITO FEDERAL BUSCAR

Netshoes terá de pagar R$ 500 mil por vazamento de dados de 2 milhões de clientes

Valor de indenização foi firmado em acordo com Ministério Público do DF. Incidente comprometeu dados pessoais de servidores da Presidência, da Polícia Federal e do STF.

Por G1 DF
05/02/2019 17h51 · Atualizado há 3 anos

Hackers conseguiram dados de quase 2 milhões de contas no site — Foto: Reprodução/Fantástico

Quando a gente lembra da LGPD...

MENU g1

MENU veja ASSINE BUSCAR

RADAR RADAR ECONÔMICO POLÍTICA ECONOMIA SAÚDE MUNDO CULTURA PLACAR

RADAR ECONÔMICO Por Josette Goulart

Análises e bastidores exclusivos sobre o mundo dos negócios e das finanças. Com Diego Gimenes.

Economia

Vazamento de chaves Pix liga o sinal de alerta do mercado para a Méliuz

VEJA Mercado: vazamento de 160 mil chaves revelado pelo Banco Central foi de empresa que pertence a Méliuz; XP vê notícia como negativa para a companhia

Por **Diego Gimenes** 26 jan 2022, 15h28

Quando a gente lembra da LGPD...

MENU g1

MENU

RADAR ECONÔM
Análises e bastidores exclusivos

Vazame

VEJA Mer

ESTADÃO

Saúde

Assine Estadão

Saúde

Nova falha do Ministério da Saúde expõe dados pessoais de mais de 200 milhões de brasileiros

Erro em sistema federal de registro de casos de covid permitiu acesso, durante seis meses, a informações pessoais de todos os brasileiros cadastrados no SUS e clientes de plano de saúde

Fabiana Cambricoli, O Estado de S.Paulo
02 de dezembro de 2020 | 05h00

Uma nova falha de segurança no sistema de notificações de covid-19 do Ministério da Saúde **deixou expostos na internet, por pelo menos seis meses, dados pessoais de mais de 200 milhões de brasileiros**. Não foram apenas pacientes com diagnóstico de covid que tiveram sua privacidade violada, como ocorreu em outro caso de exposição denunciado pelo **Estadão** na semana passada. Desta vez, ficaram abertas para consulta as informações pessoais de qualquer brasileiro cadastrado no SUS ou beneficiário de um plano de saúde.

LEIA TAMBÉM

Ministério da Saúde foi alertado em junho por ONG sobre outra exposição indevida de dados

DESTAQUES EM *SAÚDE*

SUS tem 30% de gasto ineficiente. Como melhorar o uso da verba na saúde pública?

ANS suspende temporariamente comercialização de 70 planos de saúde

Brasil registra 294 mortes e mais de 70 mil novos casos do coronavírus nas últimas 24 horas

Quando a gente lembra da LGPD...

MENU g1

MENU

RADAR ECONÔM
Análises e bastidores exclusivos

Vazame

VEJA Mer

ESTADÃO

Saúde

Nova falha
pessoais de

Erro em sistema federal de re
brasileiros cadastrados no SU

Fabiana Cambricoli, O Estado de
02 de dezembro de 2020 | 05h00

Uma nova falha de segurança
Saúde **deixou expostos na**
pessoais de mais de 200
diagnóstico de covid que tive
exposição denunciado pelo E
consulta as informações pess
beneficiário de um plano de

LEIA TAMBÉM

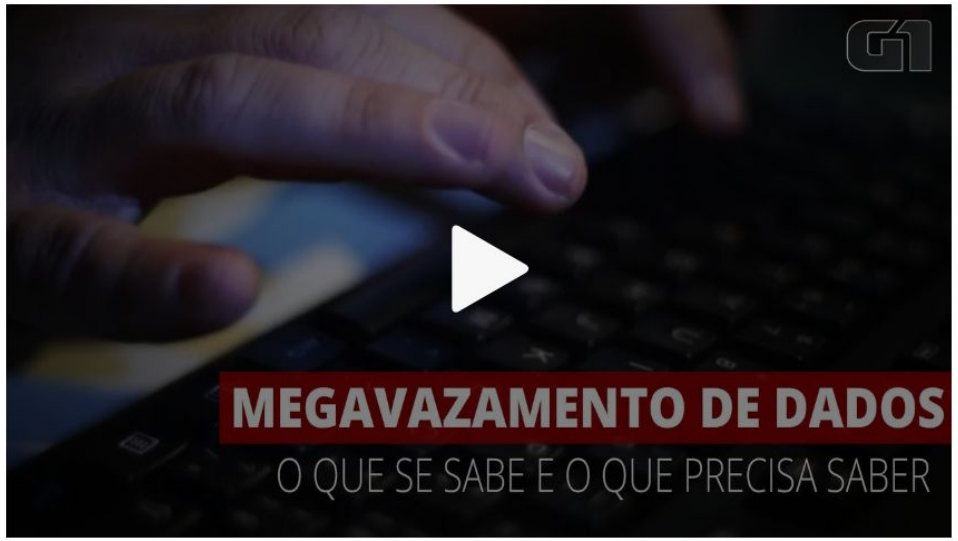
Ministério da
indevida de da

MENU g1 ECONOMIA BUSCAR

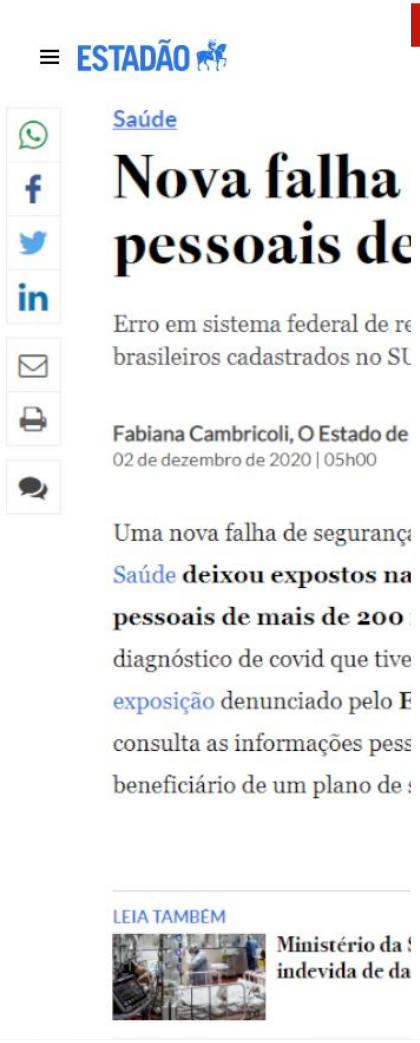
Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber

Número é maior do que a população do país, estimada em 212 milhões, porque inclui dados de falecidos. Informações expostas incluem CPF, nome, sexo e data de nascimento, além de uma tabela com dados de veículos e uma lista com CNPJs. Origem dos dados ainda é desconhecida.

Por G1
28/01/2021 18h34 · Atualizado há um ano



Quando a gente lembra da LGPD...



Todo ~~acidente~~ **incidente** é causado por uma **corrente** de eventos interligados.

A ponta do iceberg

...os dados pessoais vazados não eram tão necessários assim para o objetivo do processo?

...os dados pessoais pudessem ser estruturados de outra forma na base de dados?

...os fornecedores da cadeia de suprimento não cumpriram os requisitos de proteção dos dados?

Princípios de tratamento de dados pessoais

01 **Finalidade** especificada e informada explicitamente ao titular

02 **Adequação** à finalidade previamente acordada e divulgada

03 **Necessidade** do tratamento, limitado ao uso de dados essenciais para alcançar a finalidade inicial

04 **Acesso livre**, fácil e gratuito das pessoas à forma como seus dados são tratados

05 **Qualidade dos dados**, deixando-os exatos e atualizados, segundo a real necessidade no tratamento

06 **Transparência**, ao titular, com informações claras e acessíveis sobre o tratamento e seus responsáveis

07 **Segurança** para coibir situações acidentais ou ilícitas como invasão, destruição, perda, difusão

08 **Prevenção** contra danos ao titular e a demais envolvidos

09 **Não discriminação**, ou seja, não permitir atos ilícitos ou abusivos

10 **Responsabilização** do agente, obrigado a demonstrar a eficácia das medidas adotadas

Hipóteses de tratamento de dados pessoais

Consentimento

Cumprimento da Obrigação Legal

Execução de Políticas Públicas

Estudos por Órgão de Pesquisa

Execução de Contrato/ Diligências Pré contratuais

Exercício Regular de Direitos

Proteção da Vida

Tutela da Saúde

Interesses Legítimos do Controlador/ Terceiro

Proteção ao Crédito

WTR
WORKSHOP
DE TECNOLOGIA DE REDES DO POP-ES
2022

Boas práticas e governança

Seção II
Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

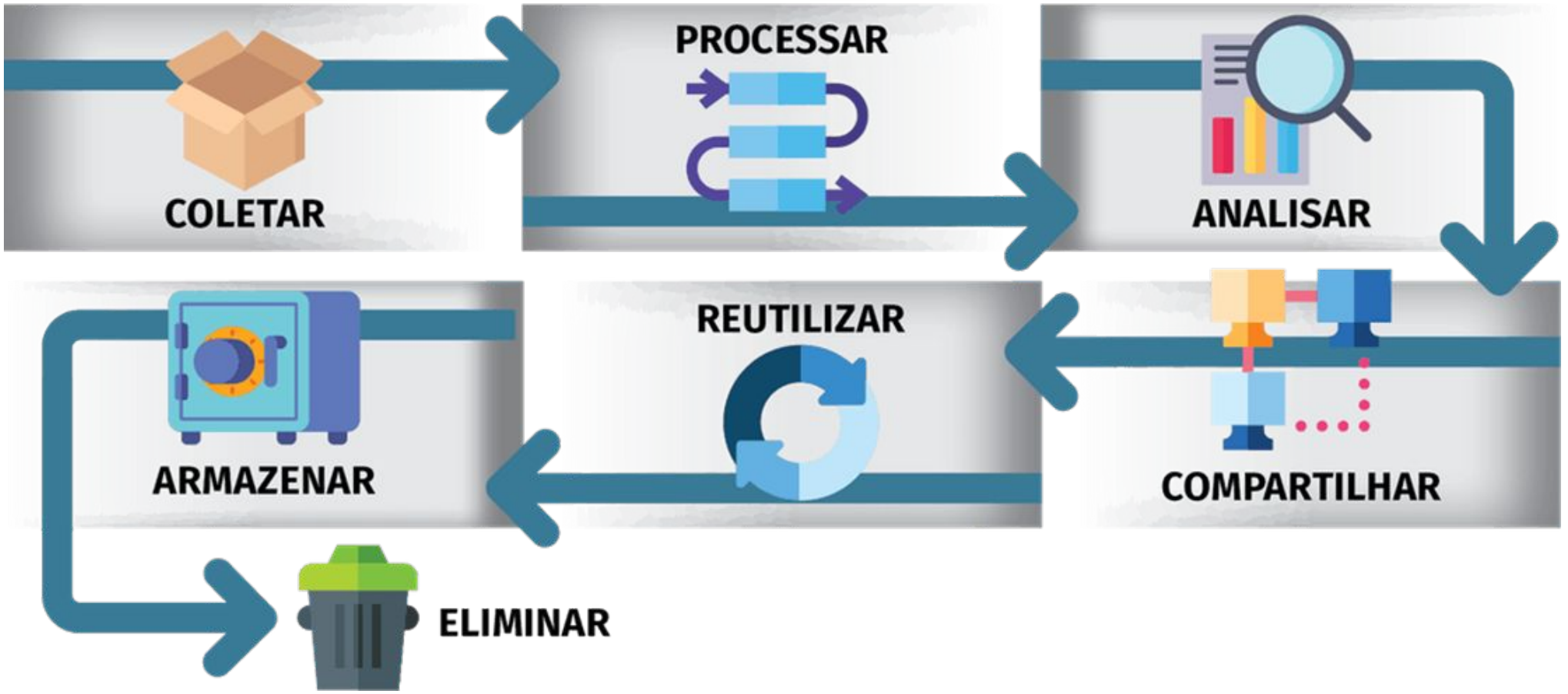
II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

NÃO É UMA RESPONSABILIDADE SÓ DA TI.

Ciclo de vida dos dados pessoais



Step 1 - Quem participa e responsabilidades

Alta gestão

Comitê de privacidade

Responsáveis locais

Encarregado pelo Tratamento de dados pessoais

Segurança cibernética

Step 2 – Mapeamento de dados e riscos

Mapeamento de Dados

Quais dados pessoais são tratados?

Qual o fluxo dos dados?

Qual a finalidade e hipótese de tratamento?

Qual o end-of-life dos dados?

Caracterização dos dados

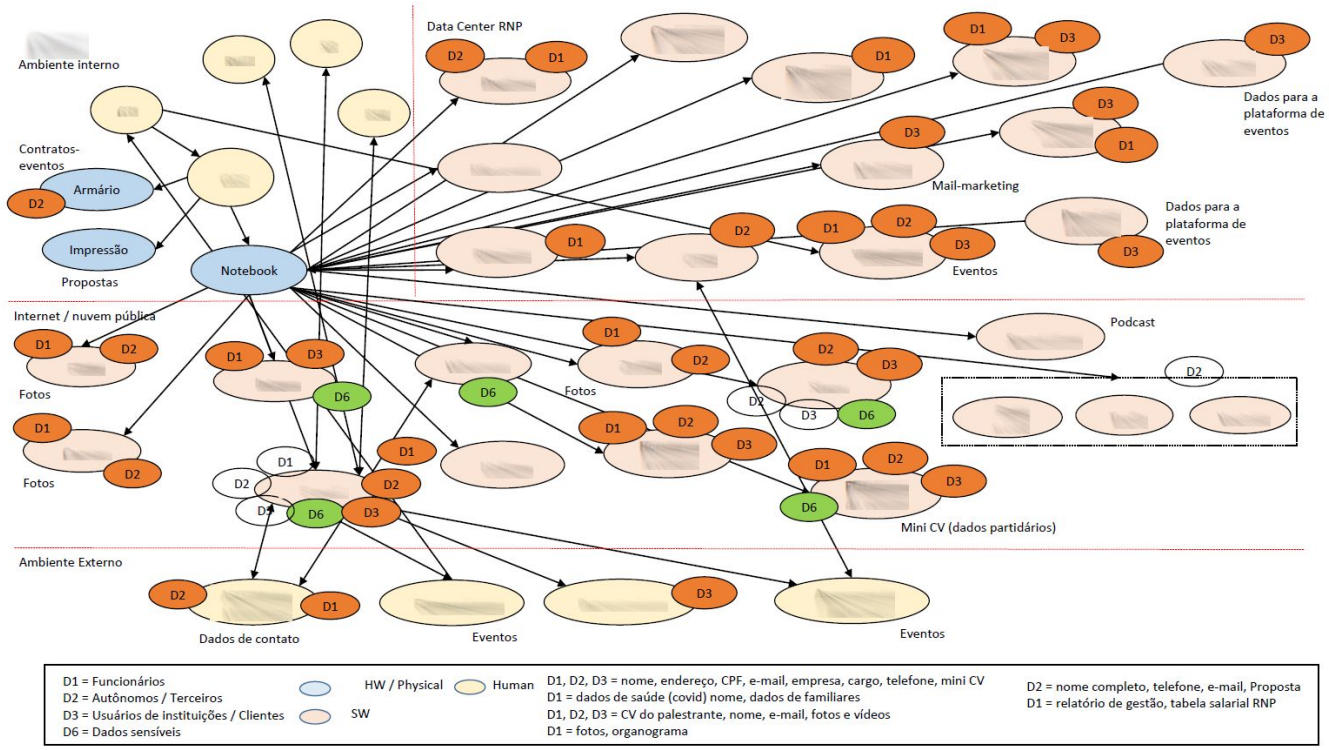
Quais dados pessoais são mais críticos?

(RH x Sistema acadêmico x Mailing)

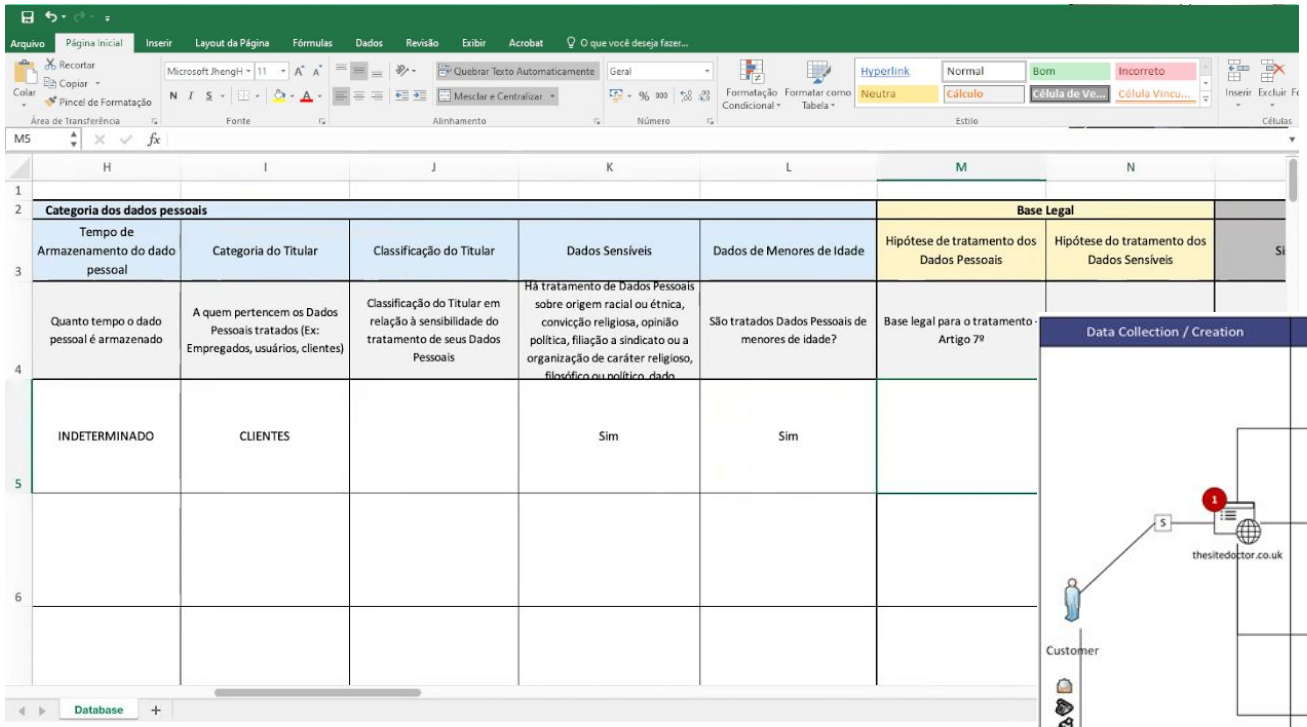
Identificação dos pontos críticos

Onde estão os possíveis pontos de vazamento?

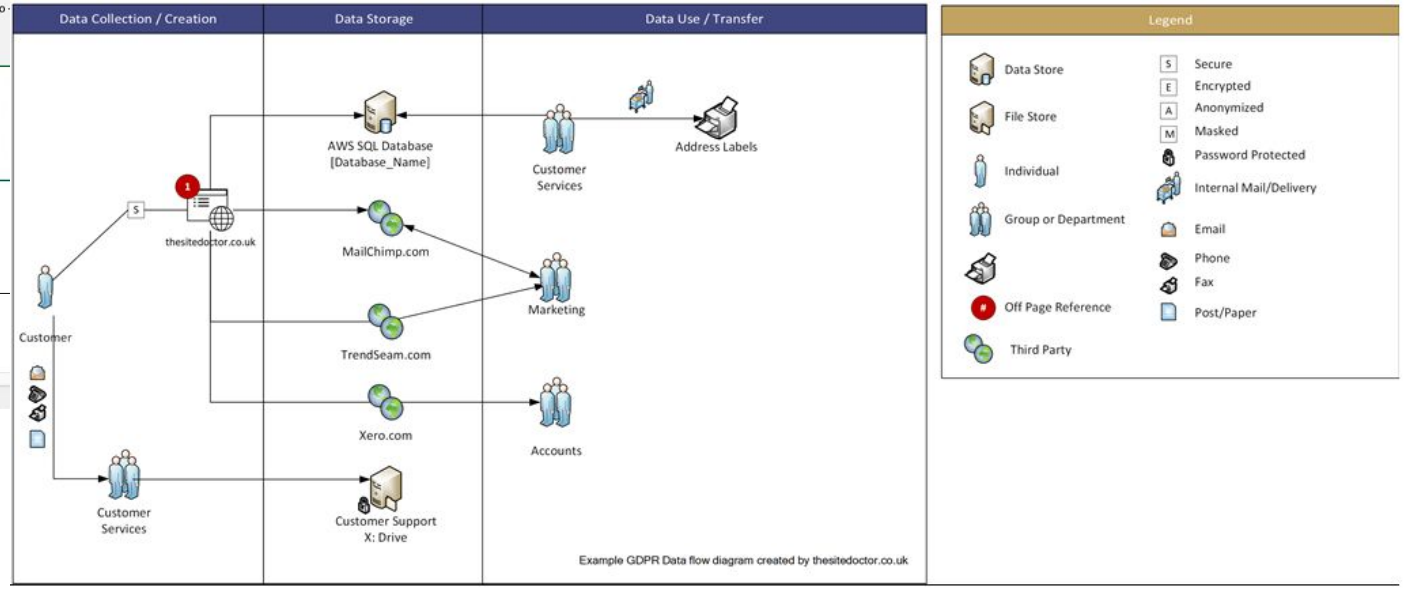
Quais são os pontos de menor controle?



Step 2 – Mapeamento de dados e riscos



Categoria dos dados pessoais					Base Legal	
Tempo de Armazenamento do dado pessoal	Categoria do Titular	Classificação do Titular	Dados Sensíveis	Dados de Menores de Idade	Hipótese de tratamento dos Dados Pessoais	Hipótese do tratamento dos Dados Sensíveis
Quanto tempo o dado pessoal é armazenado	A quem pertencem os Dados Pessoais tratados (Ex: Empregados, usuários, clientes)	Classificação do Titular em relação à sensibilidade do tratamento de seus Dados Pessoais	Há tratamento de Dados Pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado	São tratados Dados Pessoais de menores de idade?	Base legal para o tratamento - Artigo 7º	
INDETERMINADO	CLIENTES		Sim	Sim		



Step 2 – Mapeamento de dados e riscos

Mapeamento de Dados

Quais dados pessoais são tratados?

Qual o fluxo dos dados?

Caracterização dos dados

Quais dados pessoais são mais críticos?

(RH x Sistema acadêmico x Mailing)

Identificação dos pontos críticos

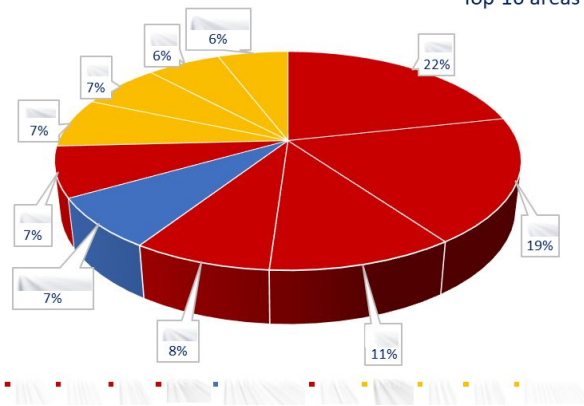
Onde estão os possíveis pontos de vazamento?

Quais são os pontos de menor controle?

	Análise de risco - Dados Pessoais												
Propabilidade	Pontos de Ataques que processam dados pessoais	17	27	24	15	36	38	31	23	18	9	26	20
	Número de sistemas não homologados para armazenar dados	0	4	4	2	1	8	2	0	0	0	1	1
	Pontos de ataques em ambiente externo	3	3	0	1	10	4	2	7	4	0	1	2
	Pontos de ataques fora do processo de gestão de vulnerabilidades	4	3	11	7	9	15	17	10	7	6	17	11
	Percentual de execução do plano de adequação LGPD	0	0	0	0	0%	0	0	0	0	0	0	0
	Quantidade de vazamentos de dados pessoais (últimos 24 meses)	0	0	0	0	0	0	0	0	0	0	0	0
	Total Probabilidade	24	37	39	25	56	65	52	40	29	15	45	34
	(1 a 19 Baixo, 20 a 39 Médio, acima de 40 Alto)	MÉDIO	MÉDIO	MÉDIO	MÉDIO	ALTO	ALTO	ALTO	ALTO	MÉDIO	BAIXO	ALTO	MÉDIO
Impacto	Sensibilidade dos Dados: (Sensíveis 10, não sensíveis 1)	1	1	1	1	10	10	1	1	1	1	1	1
	Quantidade de dados pessoais - Alto 1500 (5), Médio 1000 (3), Baixo 500 (1)	3	3	3	3	3	3	3	3	3	3	3	3
	Número de tipos de dados pessoais	3	3	1	3	3	3	3	3	3	2	4	4
	Total Impacto	7	7	5	7	16	16	7	7	7	6	8	8
	(1 a 5 Baixo, 6 a 8 Médio, acima de 9 Alto)	MÉDIO	MÉDIO	BAIXO	MÉDIO	ALTO	ALTO	MÉDIO	MÉDIO	MÉDIO	MÉDIO	MÉDIO	MÉDIO
Risco	Calculo de Risco (Probabilidade x Impacto)	168	259	195	175	896	1040	364	280	203	90	360	272
	0 a 99 Muito Baixo, 100 a 180 Baixo, 181 a 318 Médio, 319 a 351 Alto, acima de 320 Muito Alto	BAIXO	MEDIO	MEDIO	BAIXO	MUITO ALTO	MUITO ALTO	MUITO ALTO	MEDIO	MEDIO	MUITO BAIXO	MUITO ALTO	MEDIO

Dados por área | Dados por sistema | Calculo | Evidências | Vulnerabilidades por sistema | contr.segurança | Estrate ...

Top 10 áreas



Step 2 – Mapeamento de dados e riscos

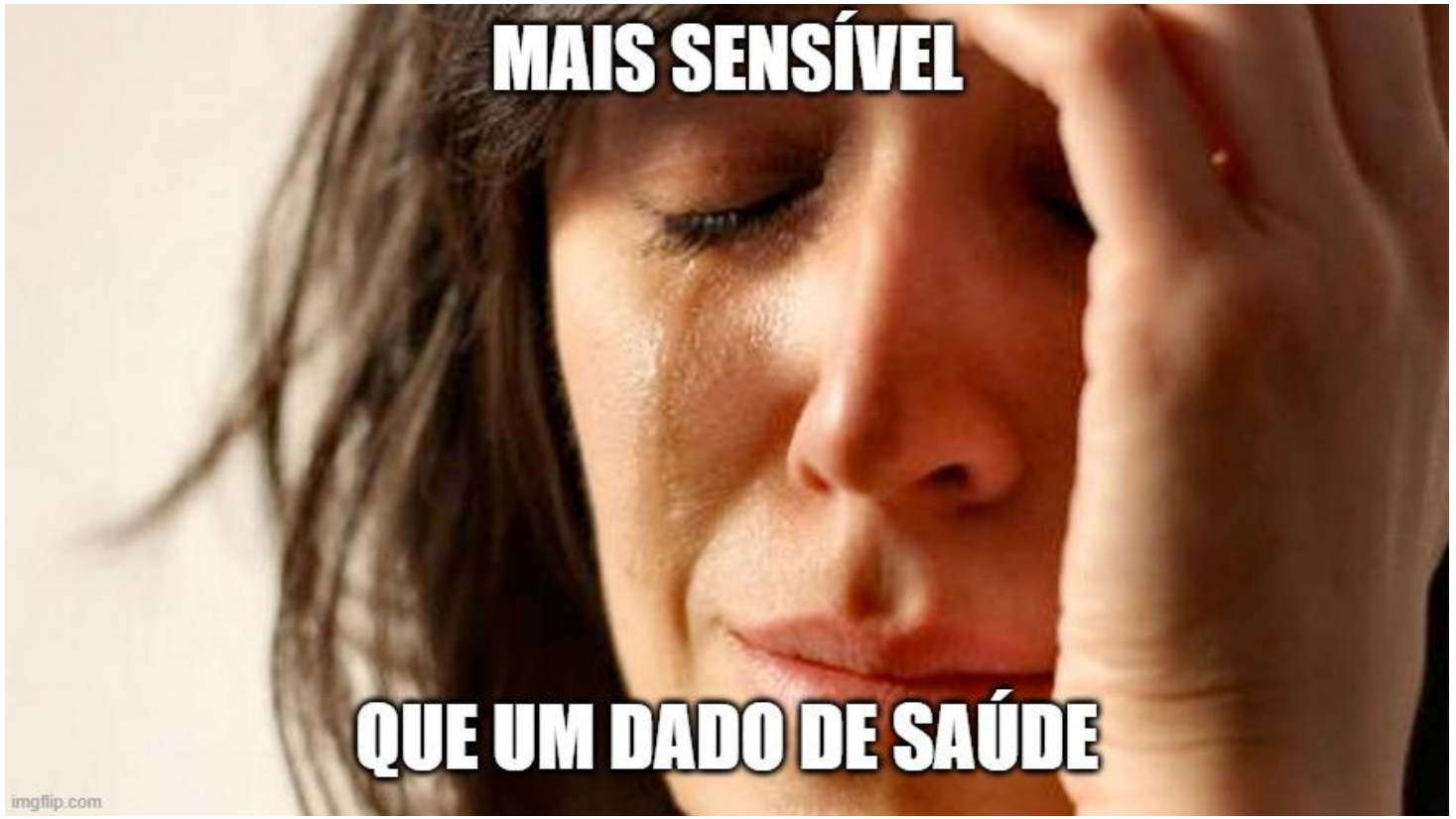
Atenção especial a:

Dados sensíveis

Artigo 11 estabelece condições especiais de tratamento de dados

Dados de menores

Artigo 14 estabelece condições especiais de tratamento de dados



Step 3 – Adequação das atividade de tratamento

Instrumentos normativos

Diretrizes corporativas

Orientações a nível estratégico

Normas (Ex. Tratamento dos dados pessoais)

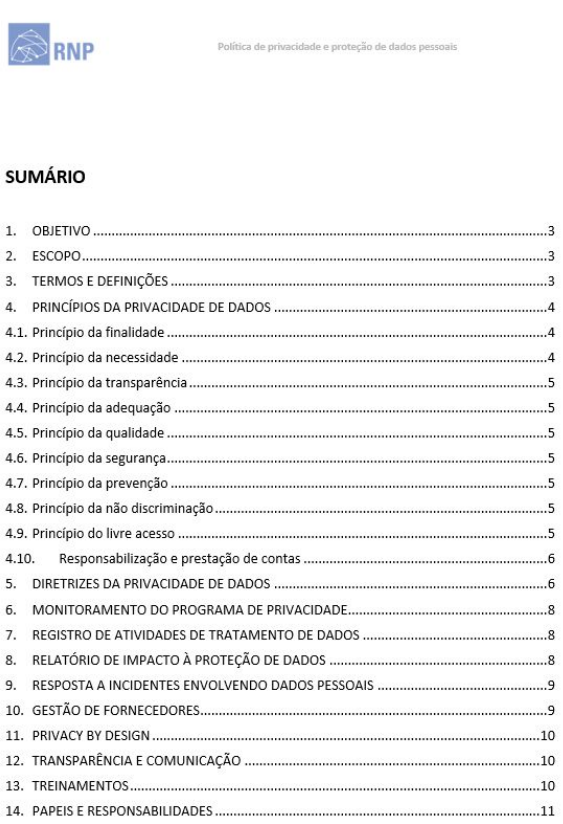
Termos de uso e Termos de privacidade

(para usuários de sistemas)


RNP

Política de Privacidade e Proteção de Dados Pessoais

Privacidade e Segurança dos Dados | *Rede Nacional de Ensino e Pesquisa*

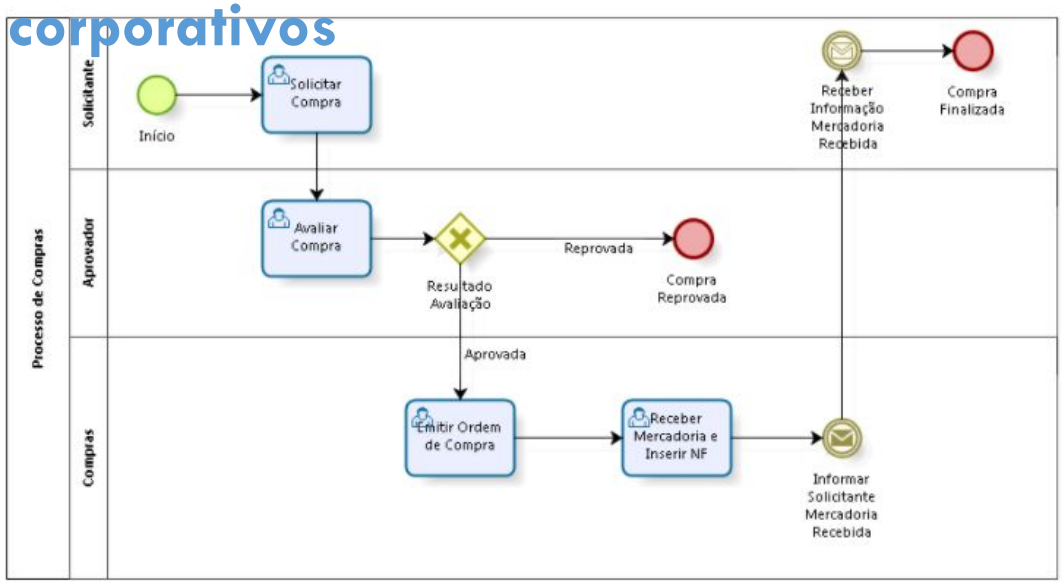

RNP

Política de privacidade e proteção de dados pessoais

SUMÁRIO

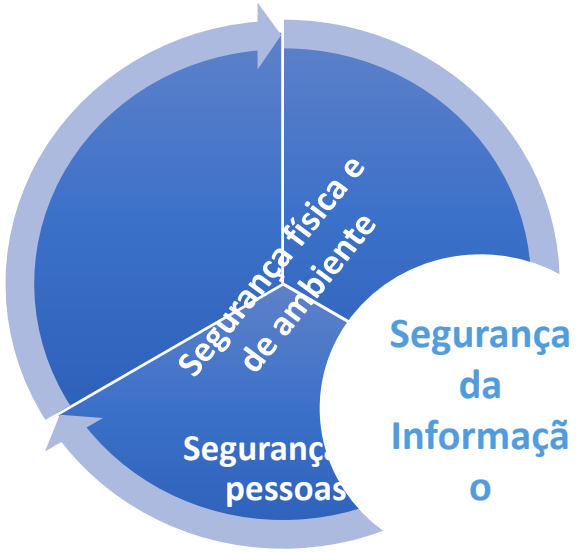
Step 3 – Adequação das atividade de tratamento

Adequação dos processos corporativos



Adequação dos sistemas e produtos

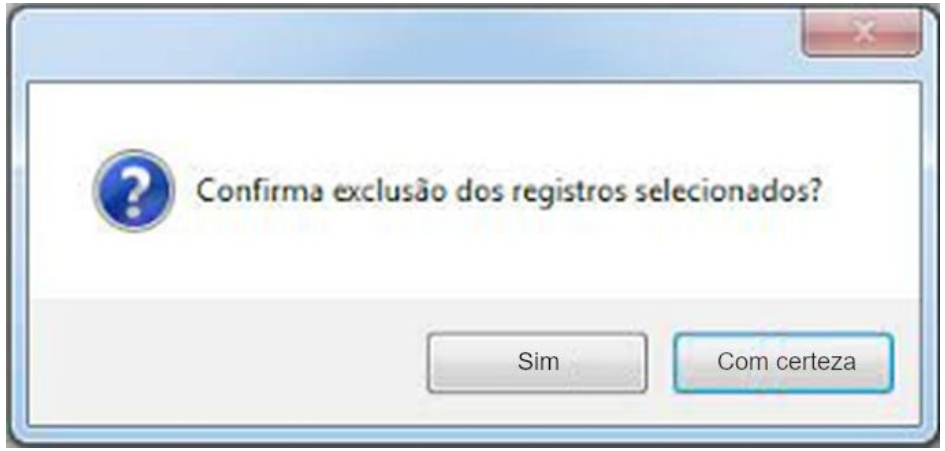
Step 4 – Assegurar a segurança da informação



Resposta a incidentes envolvendo dados pessoais

- A DESCRIÇÃO DA NATUREZA DOS DADOS PESSOAIS AFETADOS
- AS INFORMAÇÕES SOBRE OS TITULARES ENVOLVIDOS
- A INDICAÇÃO DAS MEDIDAS TÉCNICAS E DE SEGURANÇA UTILIZADAS PARA A PROTEÇÃO DOS DADOS
- OS RISCOS RELACIONADOS AO INCIDENTE
- OS MOTIVOS DA DEMORA, NO CASO DE A COMUNICAÇÃO NÃO TER SIDO IMEDIATA
- AS MEDIDAS QUE FORAM OU QUE ESTÃO SENDO TOMADAS PARA REVERTER OU MITIGAR OS EFEITOS DO PREJUÍZO

Step 5 – Eliminar corretamente os dados pessoais



End-of-life dos dados pessoais

Finalidade foi atingida?

O consentimento foi retirado?

O dado pessoal ainda é necessário?

Existe alguma obrigação legal ou regulatória para manter o dado pessoal?

Exclusão dos dados

Dado foi excluído de todas as bases de dados?

Existe registros contidos em backups?

Dados podem ser anonimizados?

Step 6 – Atendimento às solicitações dos titulares

Canais de comunicação para os titulares

Definição dos processos de atendimento
(incluindo identificação positiva do titular)

Step 7 – Educação e treinamento para toda a organização

Estratégias/Planos de comunicação

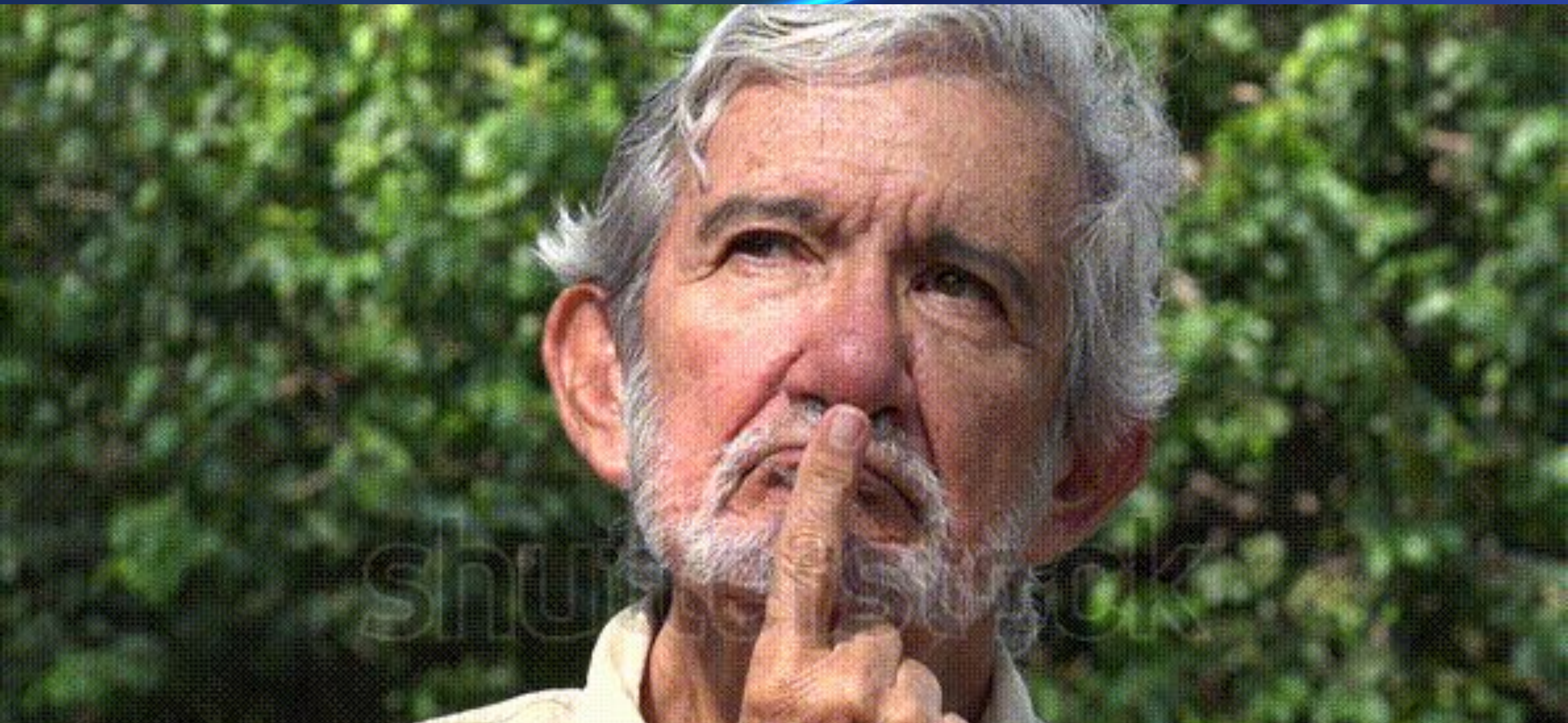
- Pílulas de conhecimento/informação
- Palestras/webinares
- Treinamentos/capacitação corporativa
- Gamification

Step 8 – Monitoramento e conformidade

PDCA e Melhoria contínua

- Indicadores e métricas
- Auditorias internas e externas
- Acompanhamento do cenário normativo
- Levantamento de melhorias
- Revisão do programa de governança

That’s all, folks!



Obrigado

yuri.ferreira@rnp.br

WTR
WORKSHOP
DE TECNOLOGIA DE REDES DO POP-ES
2022

PATROCÍNIO

INTELLI WAY

REALIZAÇÃO

PoP-ES
Ponto de Presença da RNP no Espírito Santo

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

MINISTÉRIO DO TURISMO
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DAS COMUNICAÇÕES
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES