Estratégias de Proteção de Dados Governamentais

Governança, Prontidão e Defesa Cibernética

José L. Medeiros

gov DADOS

Membro Fundador

- MBA Gestão de Projetos
- Pós Graduado Direito
- Bacharel em Direito
- Análise Desenv. Sistemas
- Defesa Cibernética
- Banco de Dados

SEC. REPRESENTAÇÃO GOV. RJ EM BRASÍLIA

daryus

QMS CERTIFICATION

BUREAU VERITAS

Índice

01	Introdução: Cenário Geral do Cibercrime
02	Diagnóstico TCU: Fiscalização em 2020
03	Desafios Atuais no Setor Público
04	Cenários Comuns nas Organizações
05	Conclusão: Necessidade da Implementação do SGSI

Cenário do Cibercrime

Edi Rama

Primeiro Ministro da Albânia

"Se o cibercrime fosse um Estado seria a terceira maior economia do mundo, depois dos Estados Unidos e China, com um PIB de U$ 10 Trilhões."

Mundo

360 bi

Tentativas de ataque somente na América Latina e Caribe

86%

Organizações em todo o mundo sofreram algum tipo de ataque no ano 2022

10%

É o crescimento dos ataques mundialmente, entre 2021 e 2022

1ª Posição

Entre os países **mais visados,** para golpes por meio de links no WhatsApp

103 bi

Tentativas de ataques cibernéticos em 2022

16%

O crescimento de ataques do ano 2021 para 2022

5ª Posição

É a colocação do Brasil no **Ranking Global**

Fonte: Fortinet, Roland Berger, Kapersky e Índice Global de Proteção de Dados (GDPI), da Dell Technologies.

Diagnóstico
TCU - 2020

1 Carência de estrutura

2 Deficiência de atos normativos que regulem o tema

3 Falta de investimentos em seg. info e defesa cibernética

Governança

Deficiências identificadas

Falta de políticas, normas e procedimentos de Segurança da Informação

Carência de profissionais capacitados

Políticas e Procedimentos

74,6 %

(306 de 410) Organizações analisadas não possuíam política de backup aprovada formalmente pela alta gestão

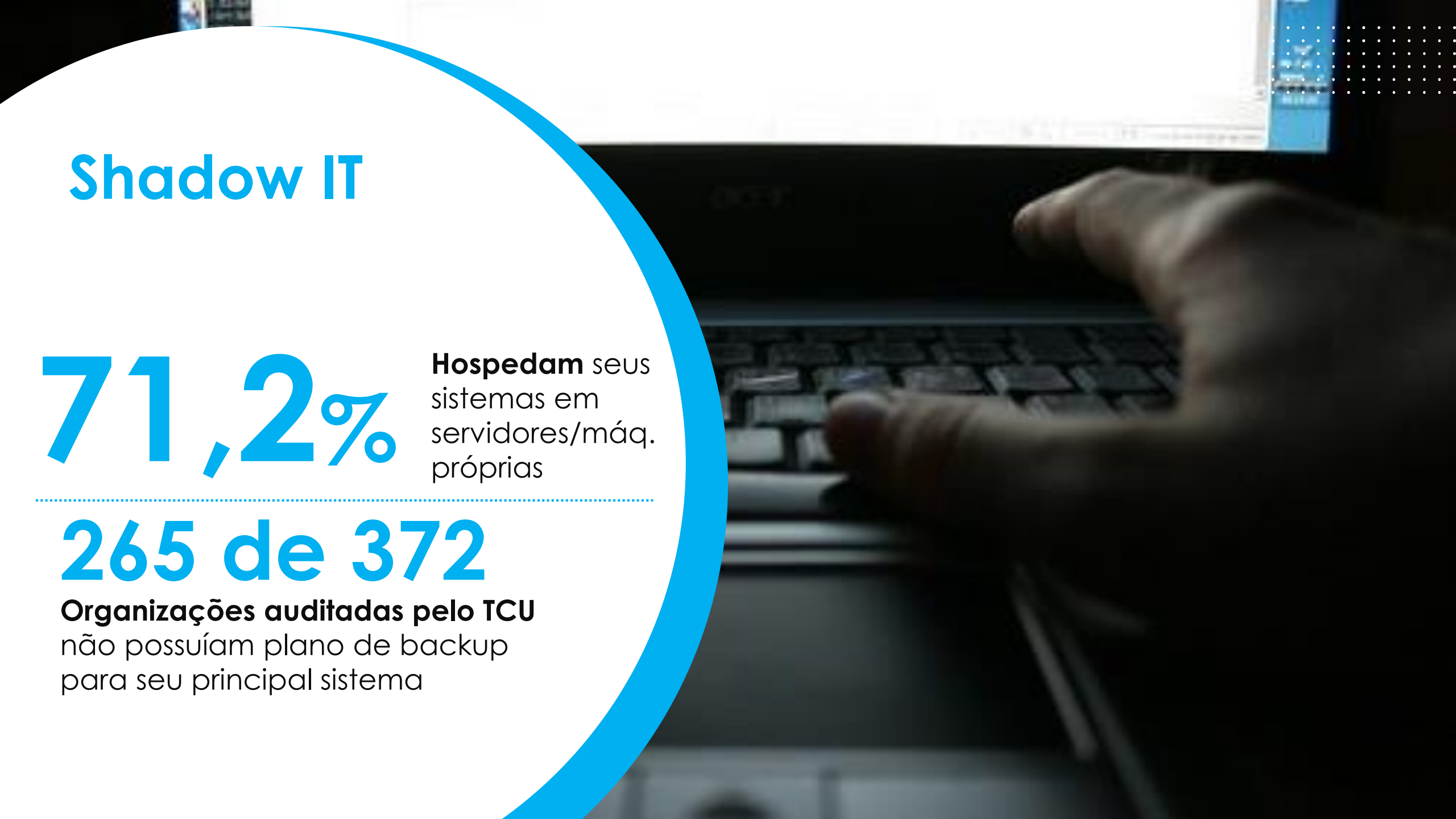
A informalidade ou falta desses documentos aumentam os riscos cibernéticos

Shadow IT

71,2% **Hospedam** seus sistemas em servidores/máq. próprias

265 de 372

Organizações auditadas pelo TCU não possuíam plano de backup para seu principal sistema



Backups

66%

(254 de 385) organizações afirmaram não aplicar controle criptográfico no banco de dados

Disaster Recovery

60,2%

(247 de 310) organizações não mantém ao menos uma das cópias sem acesso remoto

Ataque Cibernético

Maior risco de paralização integral das atividade da organização

Maturidade organizacional

+ 80%

Das organizações estão no estágio inicial de capacidade de gestão de continuidade

Esta realidade foi identificada em 2021 pelo TCU ao avaliar práticas de governança e gestão de TI

Desafios Atuais no Setor Público

É impossível proteger.....

O que não é conhecido.

Cenário Comum nas Organizações

Ausência ou deficiência
Gestão de Riscos de Segurança da Informação

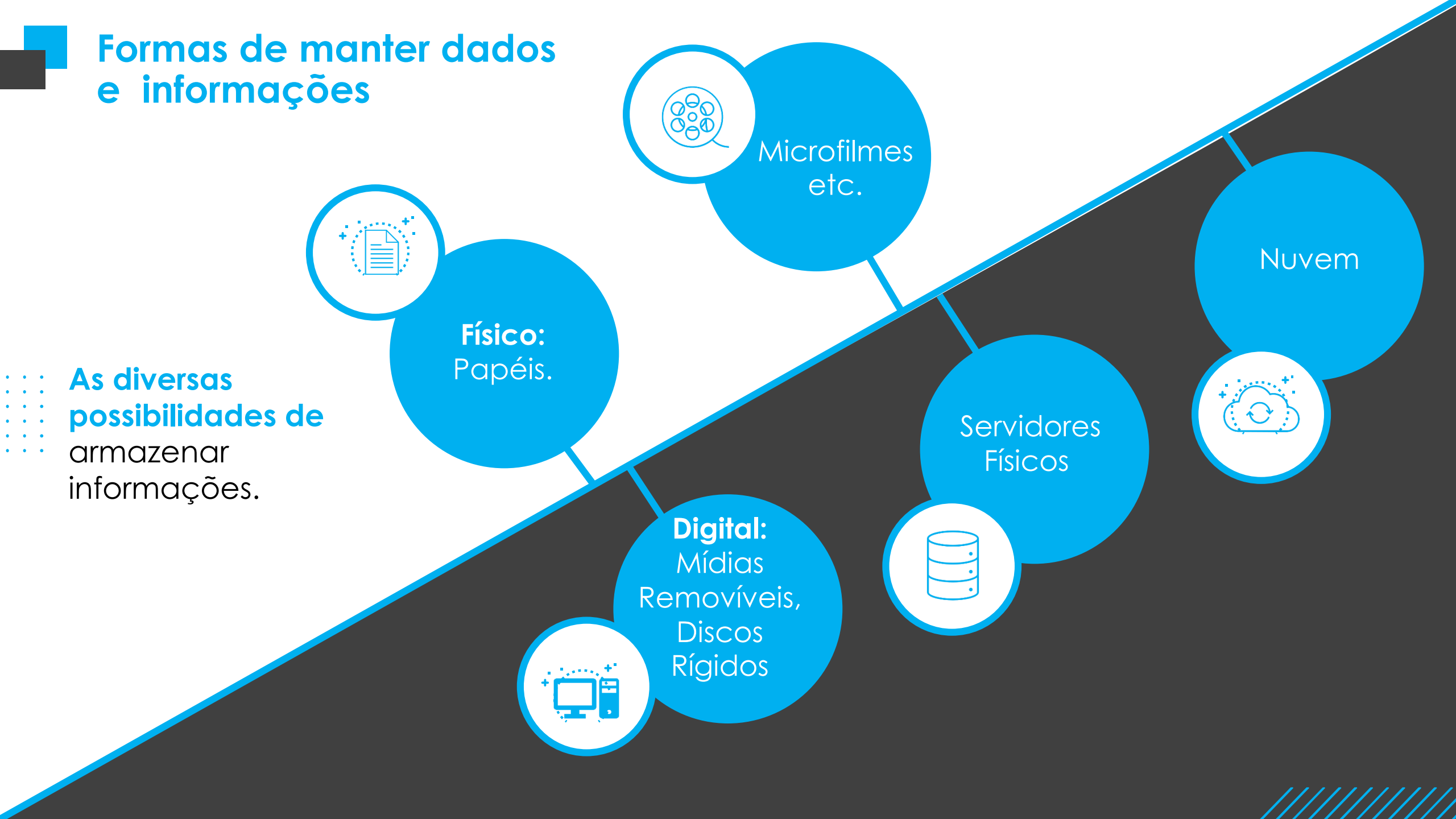
Falsa impressão de segurança
deficiência no processo de Gestão de Incidentes.

Falha nas avaliações periódicas
Deficiência nas fiscalizações, supervisões e auditorias internas

Indefinição de Indicadores
Falta de métricas de melhoria do SGSI

Formas de manter dados e informações

As diversas possibilidades de armazenar informações.



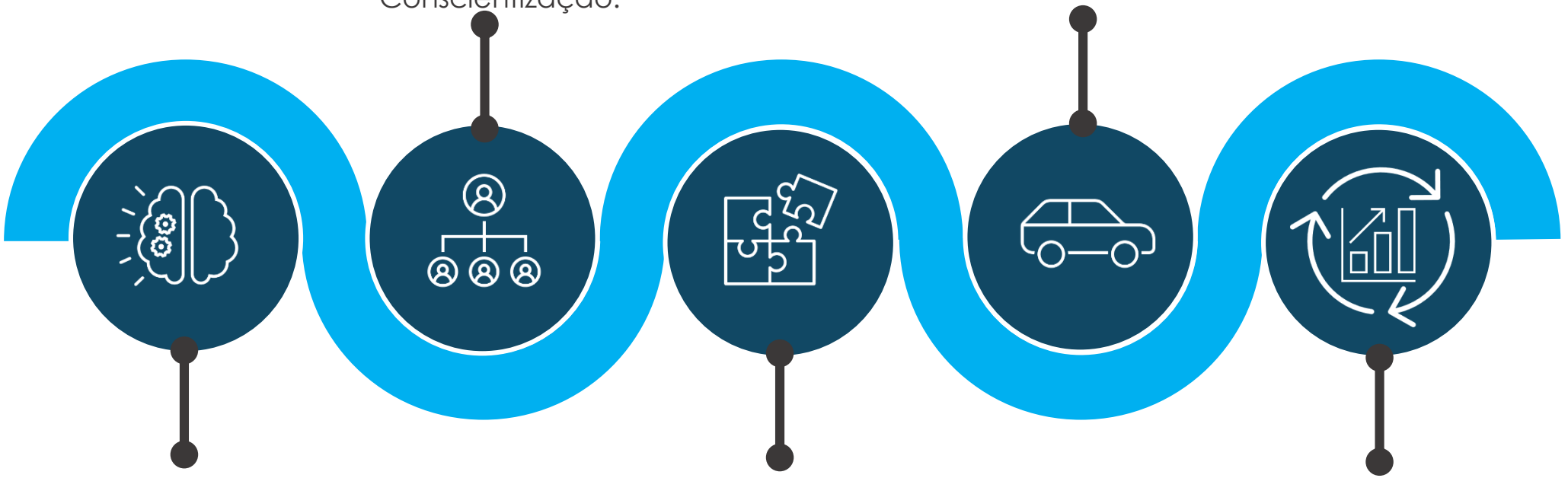
A Necessidade de Implementação do SGSI

Organização

Definições de papéis e responsabilidades do SGSI, Treinamentos, Conscientização.

Governança

Gestão de Ativos, Acessos, Operações, Incidentes, Fornecedores, Riscos etc.



Planejamento

Atividades de Análises (Gap e Riscos)

Implementação

Investimentos, Definição de Diretrizes e Implementação de Políticas e Normas

Avaliação e Melhoria

Análises Críticas, Auditoria, Due Dillligence, Gap Analysis

Contatos

Telefone (61) 99221-9336
E-mail medeiros@brasilia.rj.gov.br

GOVERNO DO ESTADO
RIO DE JANEIRO
Secretaria Extraordinária de Representação do Governo em Brasília

@jose.lmedeiros

José L.
Medeiros

OBRIGADO!