TRIBUNAL DE CONTAS DA UNIÃO

Riscos e Oportunidades nas Configurações de Serviços em URLs do Setor Público

André Torres, Renato Braga, Thiago Menegardo, Valclayton Duarte

12º Fórum de CSIRTs, 30jul24

TLP:CLEAR

Who Am I

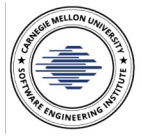
- Marido, Pai, Filho e Avô
- No pets
- *Chef de cuisine* (para minha família)
- Esportes:
  - Corredor de rua (muito amador)
  - Jogava futebol antes de operar o joelho
  - Já quis ser aprendiz de golfe
- Gostos “comuns”
  - Cinema
  - Filmes de ação na TV (tiro, pancadaria e morte)
  - Dorama! (recentemente)

TLP:CLEAR

root@kali: ~

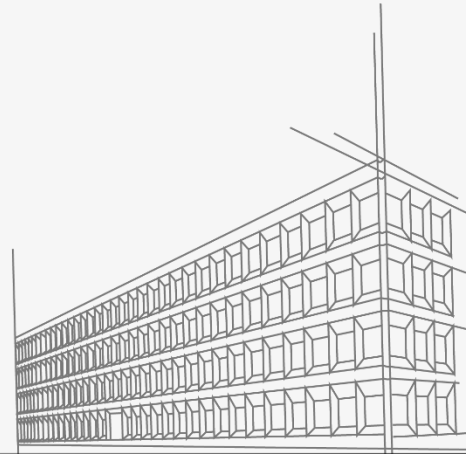
File Edit View Search Terminal Help

```
root@kali:~# whoami
```



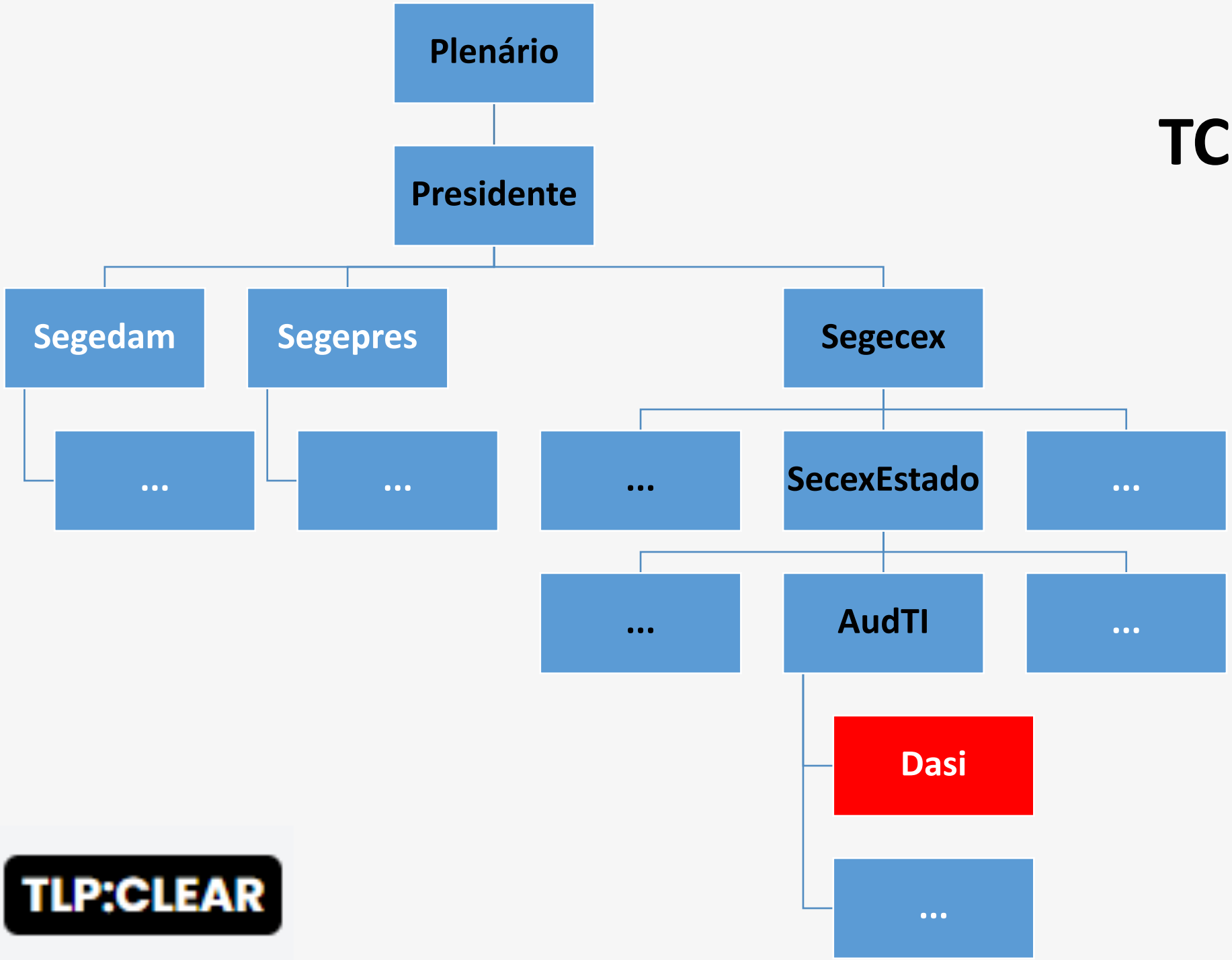
CERT
Incident Response Process Professional
Certificate Holder

TLP:CLEAR

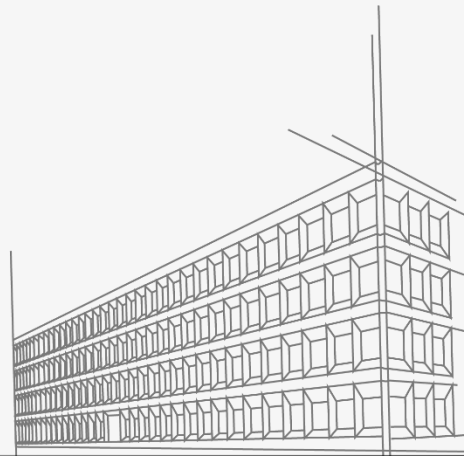



O TCU faz auditorias em SI?
Método e Resultados
Matriz de Riscos e Controles
TLP:CLEA

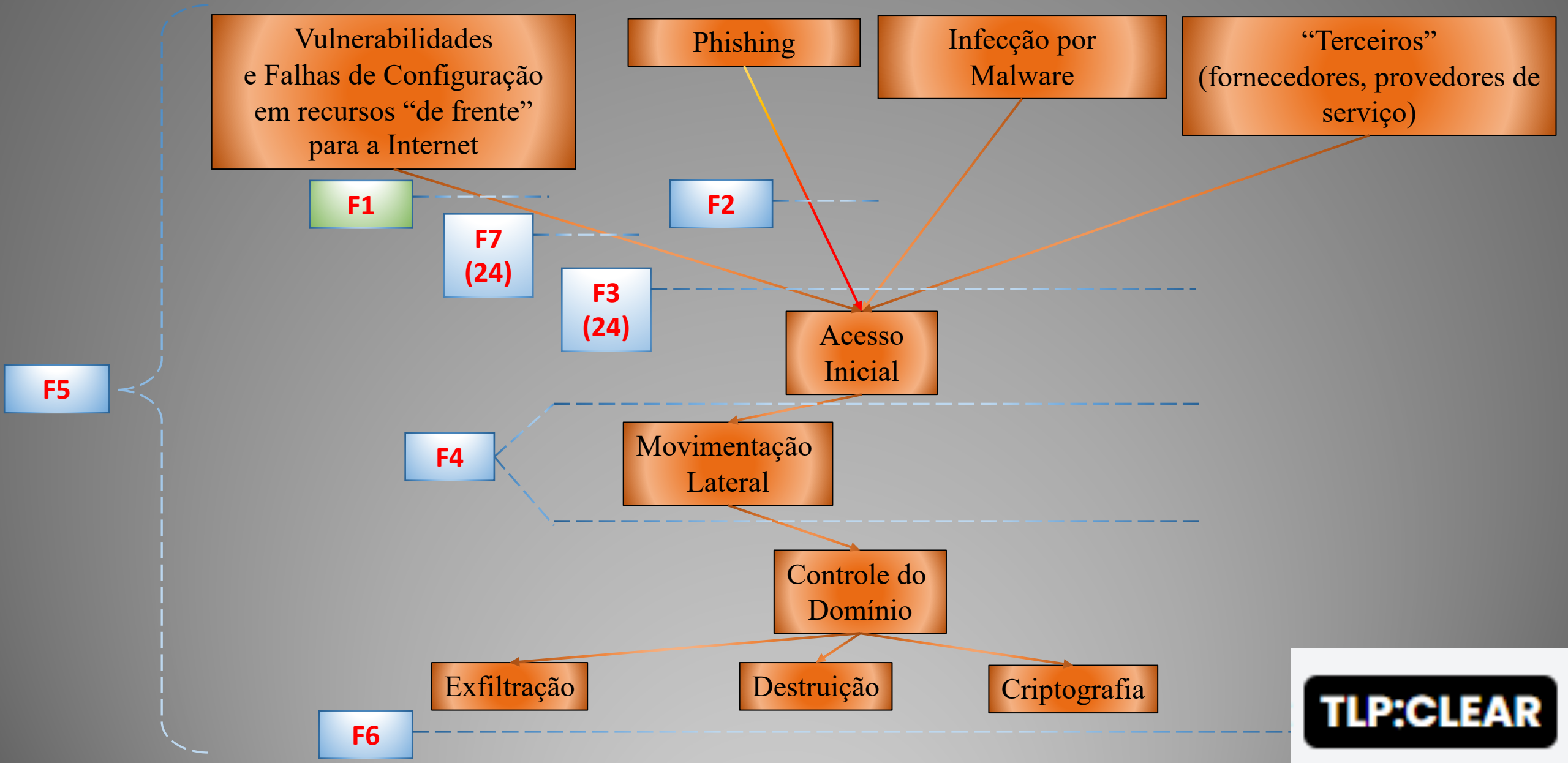
TCU fiscaliza SI?



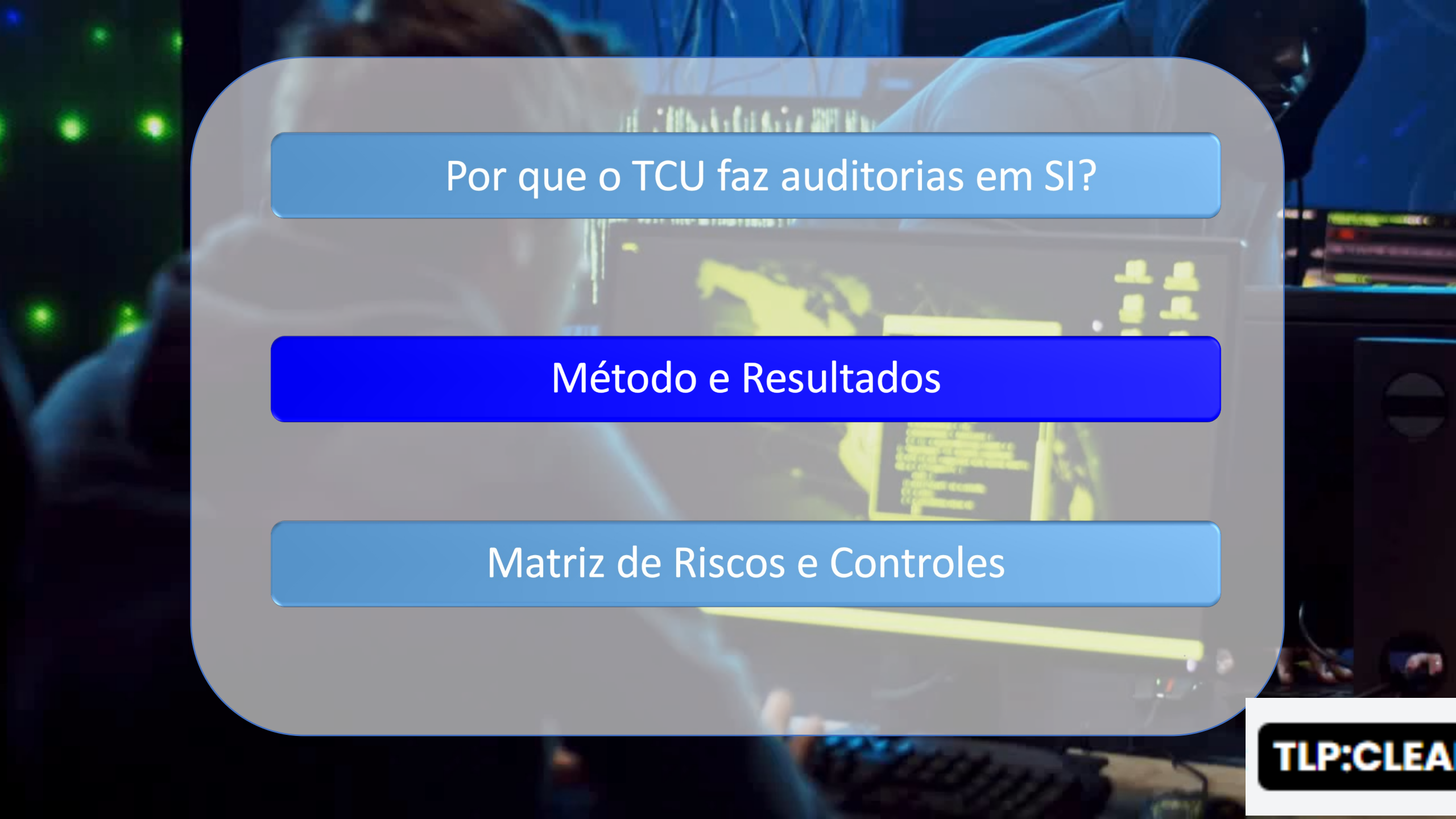
TLP:CLEAR



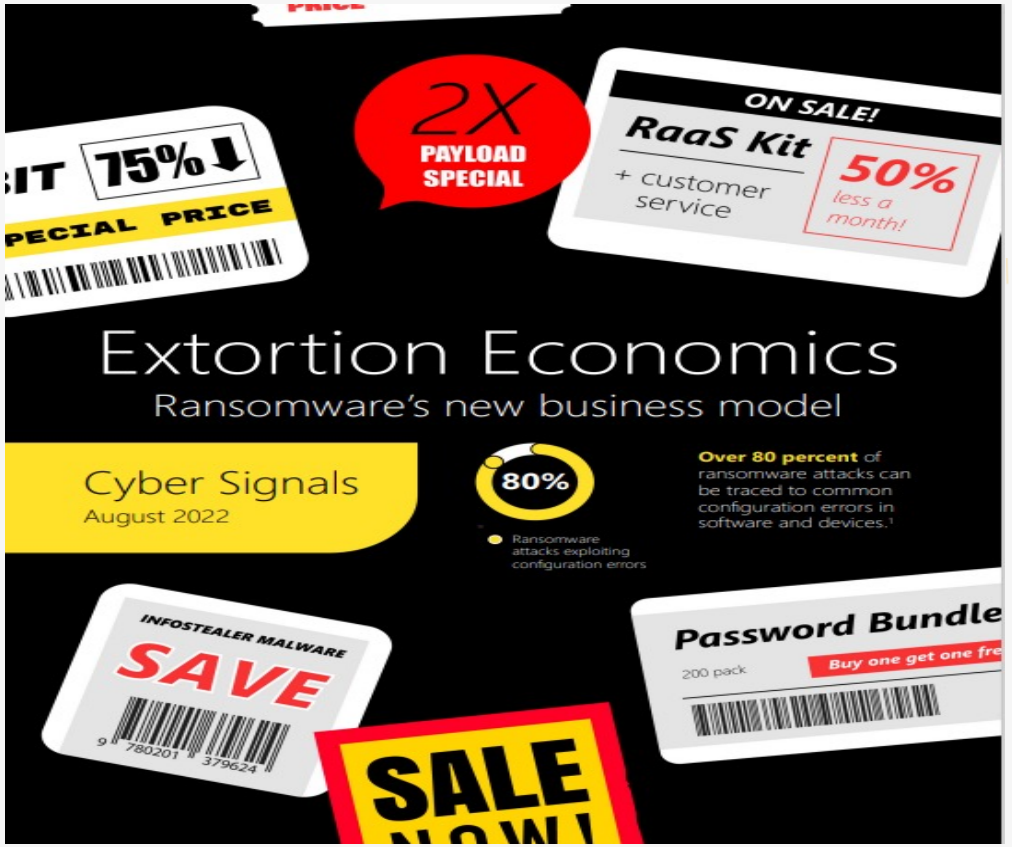
Anatomia de um ataque *ransomware*



TLP:CLEAR


Por que o TCU faz auditorias em SI?
Método e Resultados
Matriz de Riscos e Controles
TLP:CLEA

Mais de 80% dos ataques de ransomware podem ser atribuídos <u>a erros de configuração em software e em dispositivos</u>.



TLP:CLEAR

Microsoft Cyber Signals 2022. Disponível em https://news.microsoft.com/cyber-signals. Acessado em 15/8/2023.

Teste para padrões técnicos mod

top.nic.br

Visitante

nic.br cgi.br

TESTE OS PADRÕES

Quem é TOP Sobre Referências Comunicados

Os padrões técnicos modernos de Internet aumentam a confiabilidade e permitem o crescimento da rede. Você está usando esses padrões?

Teste TOP - *Site*

Endereço IP moderno? Domínio assinado? Conexão segura? Opções de segurança?

Nome de domínio do seu *site*:

www.exemplo.com.br

Iniciar o teste

» Sobre o teste

Teste TOP - *E-mail*

Endereço IP moderno? Domínio assinado? Proteção contra *phishing*? Conexão segura?

Nome de domínio do seu e-mail:

@exemplo.com.br

Iniciar o teste

» Sobre o teste

Teste TOP - IPv6 e DNSSEC da sua rede

Endereços modernos acessíveis? Assinaturas de domínio validadas?

Iniciar o teste

» Sobre o teste

TLP:CLEAR

Cerca de 14K URLs

TODAS as organizações públicas federais, estaduais, distritais e municipais que tiverem serviços web, e-mail e DNS em URL localizadas pela equipe de fiscalização

TLP:CLEAR

Objetivo da fiscalização

- Promover a melhoria na gestão de riscos de segurança da informação no contexto dos serviços de hospedagem *web*, *e-mail* e resolução de nomes em organizações públicas federais, estaduais e municipais

*.gov.br
*.jus.br
*.leg.br
*.mp.br
*.def.br
*.tc.br

TLP:CLEAR

3 Fases

Enumeração dos domínios

Testes, tratamento e armazenamento dos dados

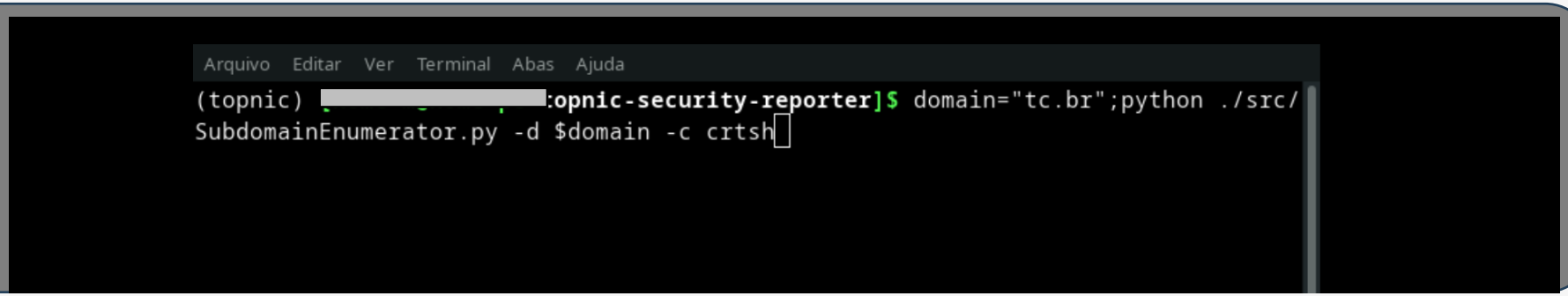
Tabulação dos Dados e Análise dos Resultados

TLP:CLEAR

Fase 1 - Enumeração dos domínios

1. Zone Walk

2. Certificate Transparency Logs



3. Amass

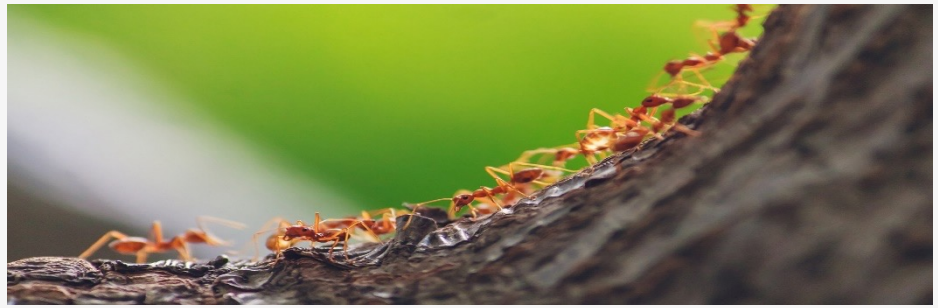
TLP:CLEAR

Fase 1 - Enumeração dos domínios

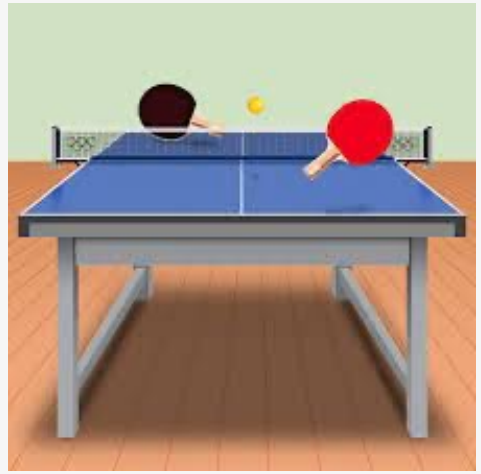
4. Força bruta

IBGE

5. Consolidação



6. Filtragem dos domínios ativos



TLP:CLEAR

14.782 URLs responderam requisições Web
10.168 URLs responderam requisições MX

TLP:CLEAR

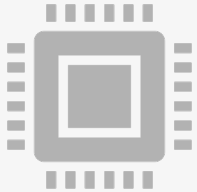
Fase 2 - Testes, tratamento e armazenamento dos dados

Requisição dos testes

à ferramenta TOP (+ ajustes)

Tratamento dos dados

Extração dos dados dos HTML



Armazenamento dos dados

Planilhas Excel

TLP:CLEAR

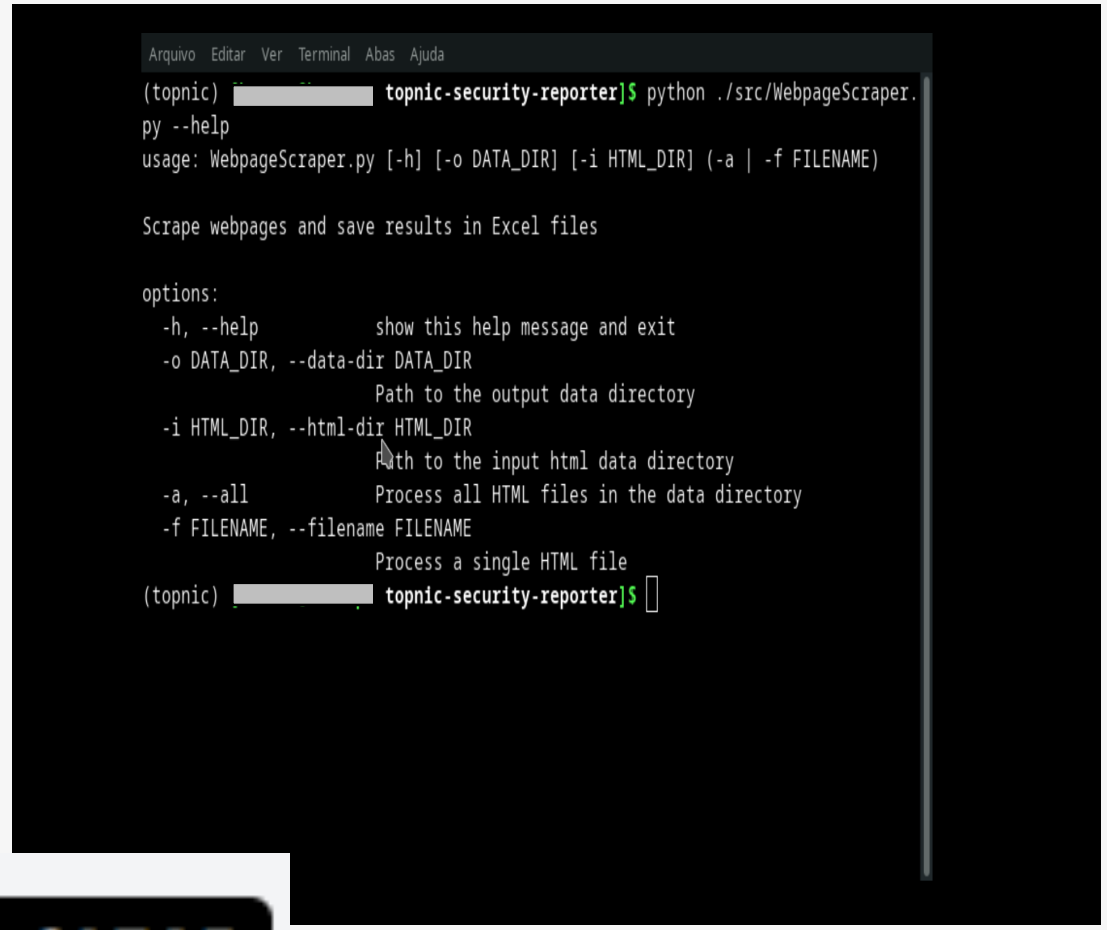
Requisição dos testes

src > WebpageDownloader.py > WebpageDownloader > get_tested_sites

```python
import time
import sys
import argparse
from selenium import webdriver
from selenium.webdriver.chrome.options import Options
from selenium.webdriver.chrome.service import Service
from webdriver_manager.chrome import ChromeDriverManager
from selenium.common.exceptions import NoSuchElementException
from concurrent.futures import ThreadPoolExecutor
from multiprocessing import Value
from log_config import setup_logger

class WebpageDownloader:
    def __init__(self, data_dir="./data/", type="site"):
        self.data_dir = data_dir
        self.type = type
        self.url_base = f"https://top.nic.br/{type}/"
        # webdriver setup
        self.options = Options()
        self.options.add_argument("--headless")
        # self.driver = driver = webdriver.Chrome(service=Service(ChromeDriverManager().install()), options=options)

        self.logger = setup_logger(self.__class__.__name__)

        self.logger.debug(f'WebpageDownloader initialized with: data_dir: {self.data_dir}, type: {self.type}')

    def get_tested_sites(self):
        tested_sites = set()
        try:
            with open(self.data_dir + "links_permanentes.csv", "r") as f:
```

TLP:CLEAR

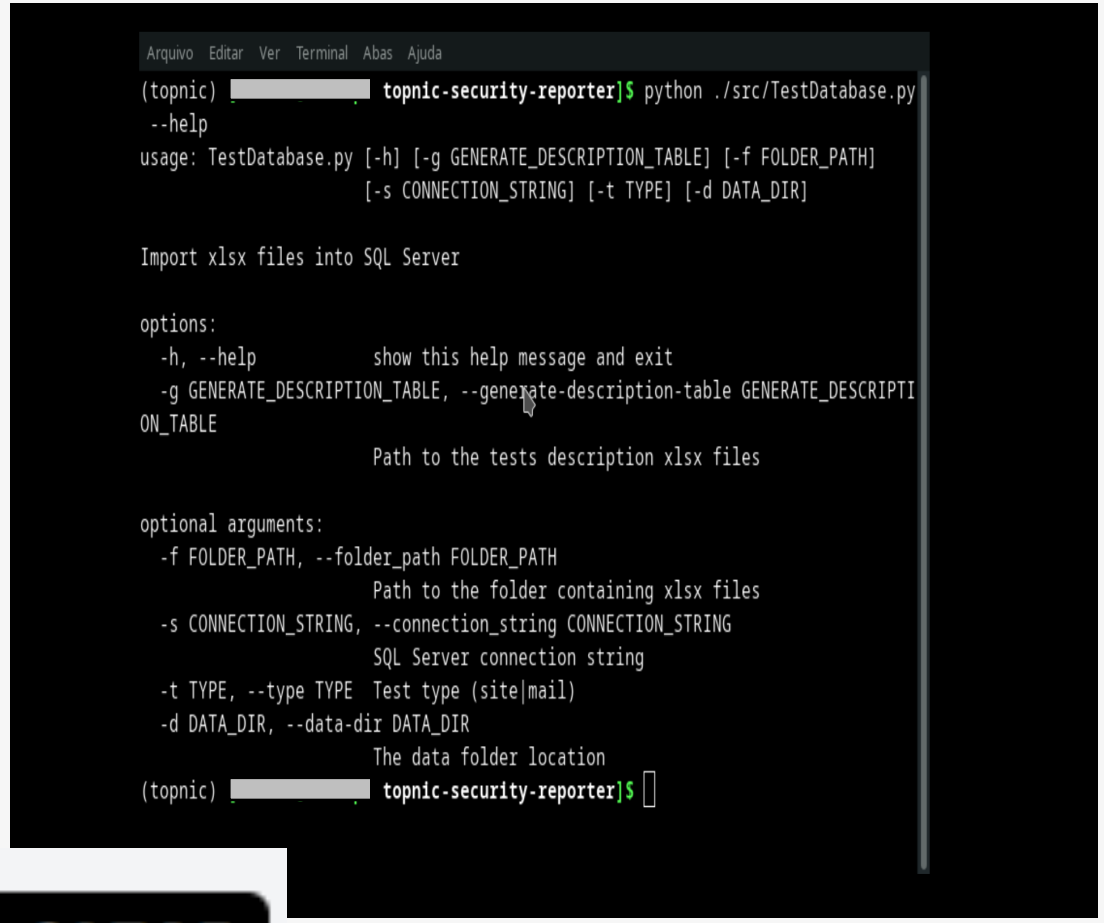
Tratamento dos dados



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	id	main topic	test title	result	t-description										
2	0	Falha:End	Endereços	Nenhum d	Verificamos se seu nome de domínio tem pelo menos dois servidores de nomes com um endereço IPv6. Isto é co										
3	1	Falha:End	Acessibilid	Este subte	Verificamos se todos os servidores de nomes, que têm um registro AAAA com endereço IPv6, são acessíveis via IP										
4	2	Falha:End	Endereços	Nenhum d	Verificamos se há pelo menos um registro AAAA com endereço IPv6 para o seu servidor web.										
5	3	Falha:End	Acessibilid	Este subte	Verificamos se podemos nos conectar ao(s) seu(s) servidor(es) web via IPv6 em qualquer das portas disponíveis										
6	4	Falha:End	Mesmo sit	Este subte	Comparamos o conteúdo web que recebemos do seu servidor web em endereços IPv6 e IPv4 em qualquer das p										
7	5	Falha:Non	Existência	Seu domín	Verificamos se seu domínio, mais especificamente seu registro SOA, possui assinatura DNSSEC.Se um domínio fo										
8	6	Falha:Non	Validade d	Este subte	Verificamos se seu domínio, mais especificamente seu registro SOA, é assinado com uma assinatura válida, torna										
9	7	Falha:Con	HTTPS disp	Seu site of	Verificamos se seu site está acessível por HTTPS. Em caso afirmativo, também verificamos nos subtestes abaixo s										
10	8	Falha:Con	Redirecion	Seu servid	Verificamos se seu servidor web redireciona automaticamente os visitantes de HTTP para HTTPS no mesmo dom										
11	9	Falha:Con	Compress	Seu servid	Verificamos se o seu servidor web oferece suporte à compressão HTTP. A compressão HTTP torna a conexão seg										
12	10	Falha:Con	HSTS	Seu servid	Verificamos se seu servidor web oferece suporte a HSTS. Os navegadores se "lembram" do HSTS por (sub)domín										
13	11	Falha:Con	Versão de	Seu servid	Verificamos se seu servidor web oferece suporte apenas a versões seguras de TLS. Um servidor web pode oferec										
14	12	Falha:Con	Cifras (Sel	Seu servid	Verificamos se seu servidor web oferece suporte somente a cifras seguras, ou seja, cifras Boas e/ou Suficientes. (										
15	13	Falha:Con	Ordem da	Seu servid	Verificamos se seu servidor web impõe sua própria preferência de cifras (I) e oferece cifras de acordo com a ord										
16	14	Falha:Con	Parâmetro	Seu servid	Verificamos se os parâmetros públicos usados na troca de chaves Diffie-Hellman por seu servidor web são segur										
17	15	Falha:Con	Função ha	Seu servid	Verificamos se seu servidor web oferece suporte a funções de hash seguras para criar a assinatura digital durant										
18	16	Falha:Con	Compress	Seu servid	Verificamos se seu servidor web oferece suporte à compressão TLS. O uso de compressão pode dar ao atacante										
19	17	Falha:Con	Renegocia	Seu servid	Verificamos se seu servidor web oferece suporte a uma renegociação segura. As versões mais antigas de TLS, ant										
20	18	Falha:Con	Renegocia	Seu servid	Verificamos se um cliente, normalmente um navegador web, pode iniciar uma renegociação com o seu servidor v										
21	19	Falha:Con	0-RTT	Este subte	Verificamos se o seu servidor web oferece suporte a Zero Round Trip Time Resumption (0-RTT).0-RTT é uma opç										
22	20	Falha:Con	OCSP stap	Seu servid	Verificamos se seu servidor web oferece suporte à RFC 6961: The Transport Layer Security (TLS) Multiple Certifica										
23	21	Falha:Con	Cadeia de	A cadeia d	Verificamos se somos capazes de construir uma cadeia de confiança válida para o certificado do seu site. Para te										
24	22	Falha:Con	Chave púb	A assinatu	Verificamos se a assinatura digital (ECDSA ou RSA) do certificado do seu site utiliza parâmetros seguros. A verifica										
25	23	Falha:Con	Assinatura	O certifica	Verificamos se a assinatura do certificado do site foi criada com um algoritmo de hash seguro.Ver IT Security Gui										

TLP:CLEAR

Armazenamento dos dados



	id	main_topic	test_title	test_description	test_type	test_number
0	1	Falha:Endereço IP moderno (IPv6)	Endereços IPv6 para servidores de nomes	Verificamos se seu nome de domínio tem pelo me...	mail	0
1	2	Falha:Endereço IP moderno (IPv6)	Acessibilidade IPv6 dos servidores de nomes	Verificamos se todos os servidores de nomes, q...	mail	1
2	3	Falha:Endereço IP moderno (IPv6)	Endereços IPv6 para servidor(es) de e-mail	Verificamos se há pelo menos um registro AAAA ...	mail	2
3	4	Falha:Endereço IP moderno (IPv6)	Acessibilidade IPv6 do(s) servidor(es) de e-mail	Verificamos se podemos nos conectar com seus s...	mail	3
4	5	Falha:Nomes de domínio assinados (DNSSEC)	Existência de DNSSEC	Verificamos se o seu domínio, mais especificam...	mail	4
...	...	...	...	...	...	...
57	58	Recomendação:Opções de segurança	X-Frame-Options	Verificamos se seu servidor web fornece um cab...	site	27
58	59	Recomendação:Opções de segurança	X-Content-Type-Options	Verificamos se seu servidor web fornece um cab...	site	28
59	60	Recomendação:Opções de segurança	Content-Security-Policy (CSP)	Verificamos se o seu servidor web fornece um c...	site	29
60	61	Recomendação:Opções de segurança	Existência de Referrer-Policy	Verificamos se seu servidor web fornece um cab...	site	30
61	62	Recomendação:Opções de segurança	Existência de Referrer-Policy	Verificamos se seu servidor web fornece um cab...	mail	30

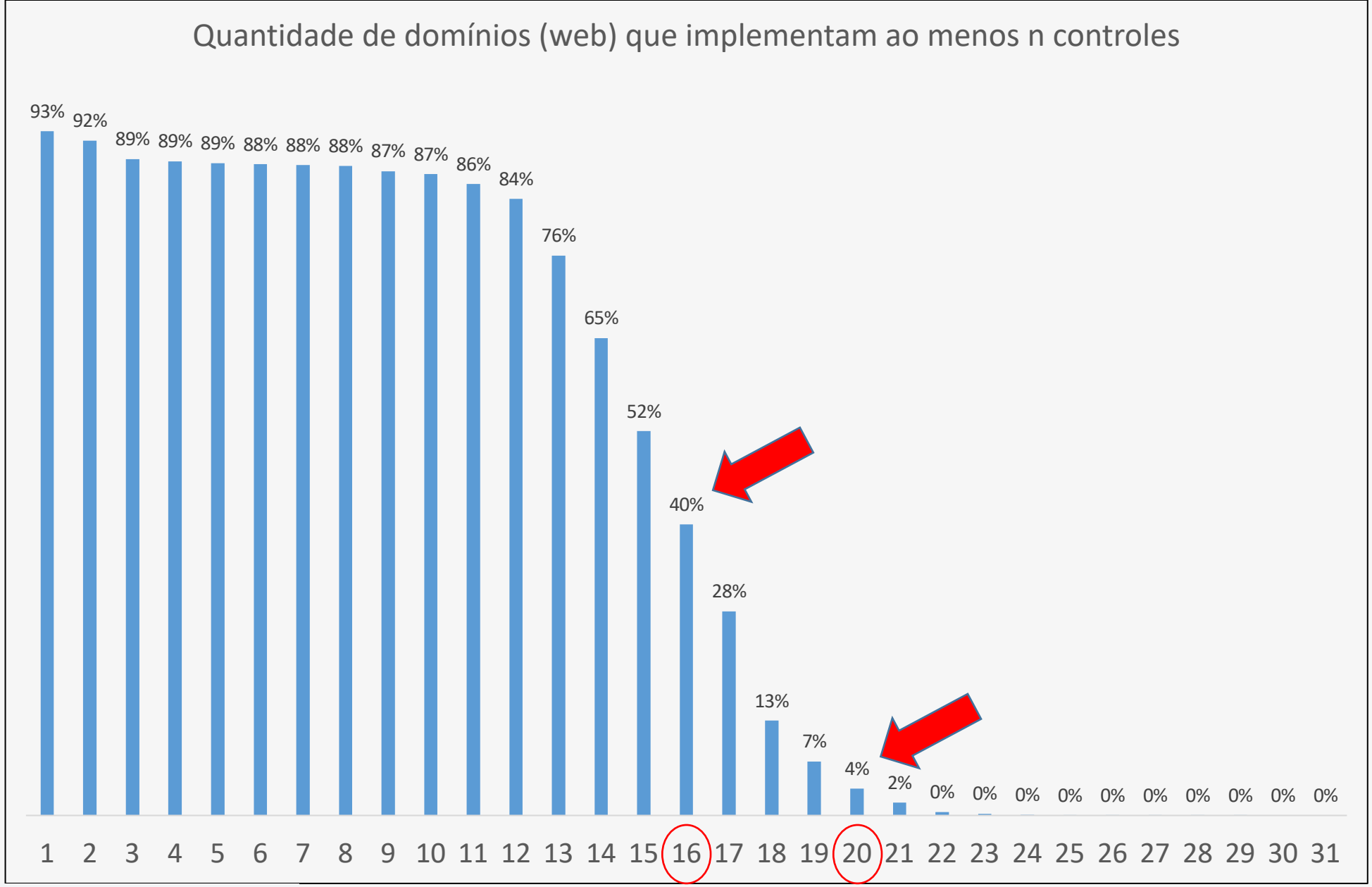
62 rows × 6 columns

TLP:CLEAR

TRIBUNAL DE CONTAS DA UNIÃO

Fase 3 - Tabulação dos Dados e Análise dos Resultados

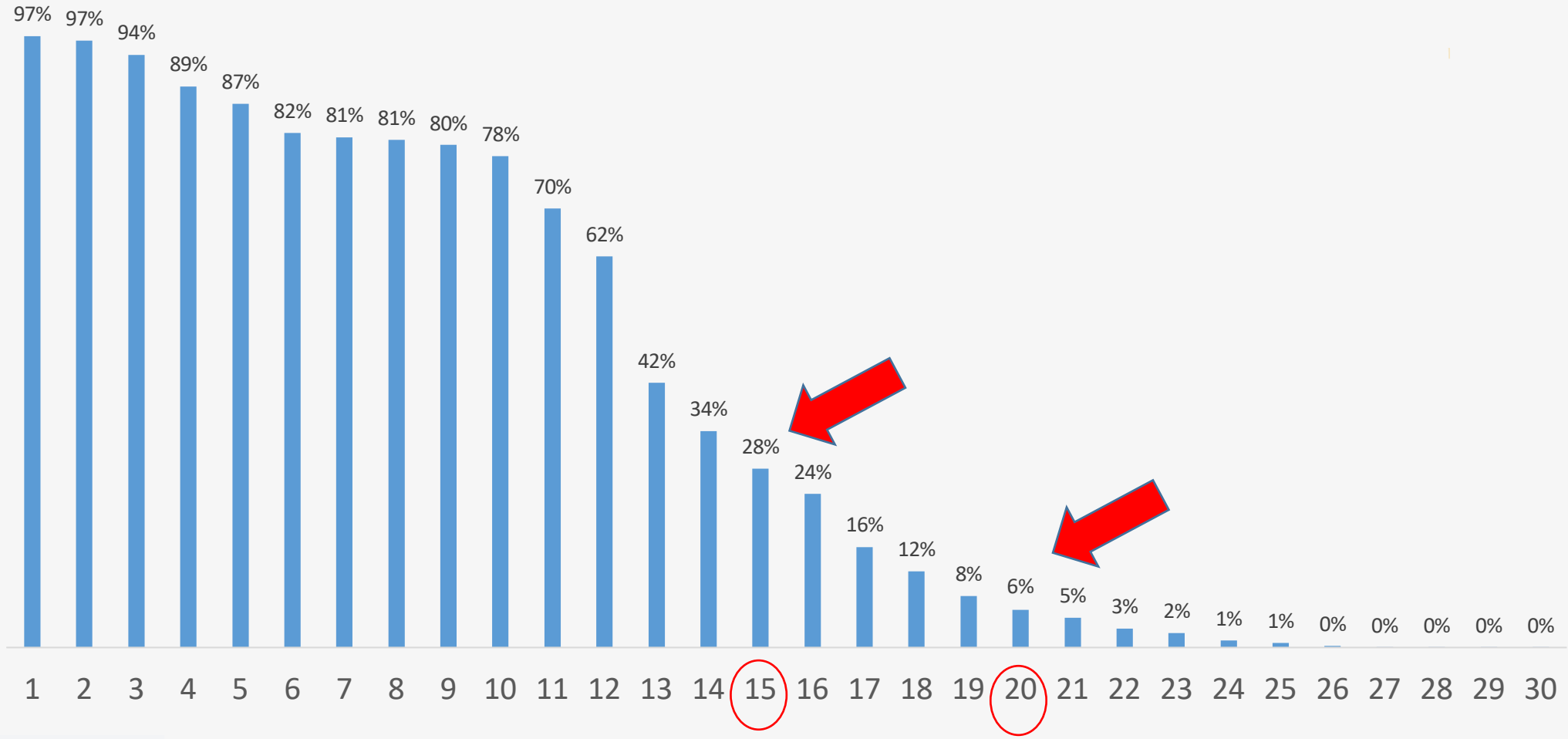
TLP:CLEAR



Controles	Quantidade	%
31	0	0%
30	0	0%
29	1	0%
28	1	0%
27	2	0%
26	2	0%
25	3	0%
24	17	0%
23	35	0%
22	64	0%
21	255	2%
20	537	4%
19	1084	7%
18	1905	13%
17	4096	28%
16	5841	40%
15	7710	52%
14	9579	65%
13	11235	76%
12	12371	84%
11	12668	86%
10	12867	87%
9	12928	87%
8	13034	88%
7	13048	88%
6	13068	88%
5	13085	89%
4	13129	89%
3	13171	89%
2	13545	92%
1	13731	93%
0	0	0%

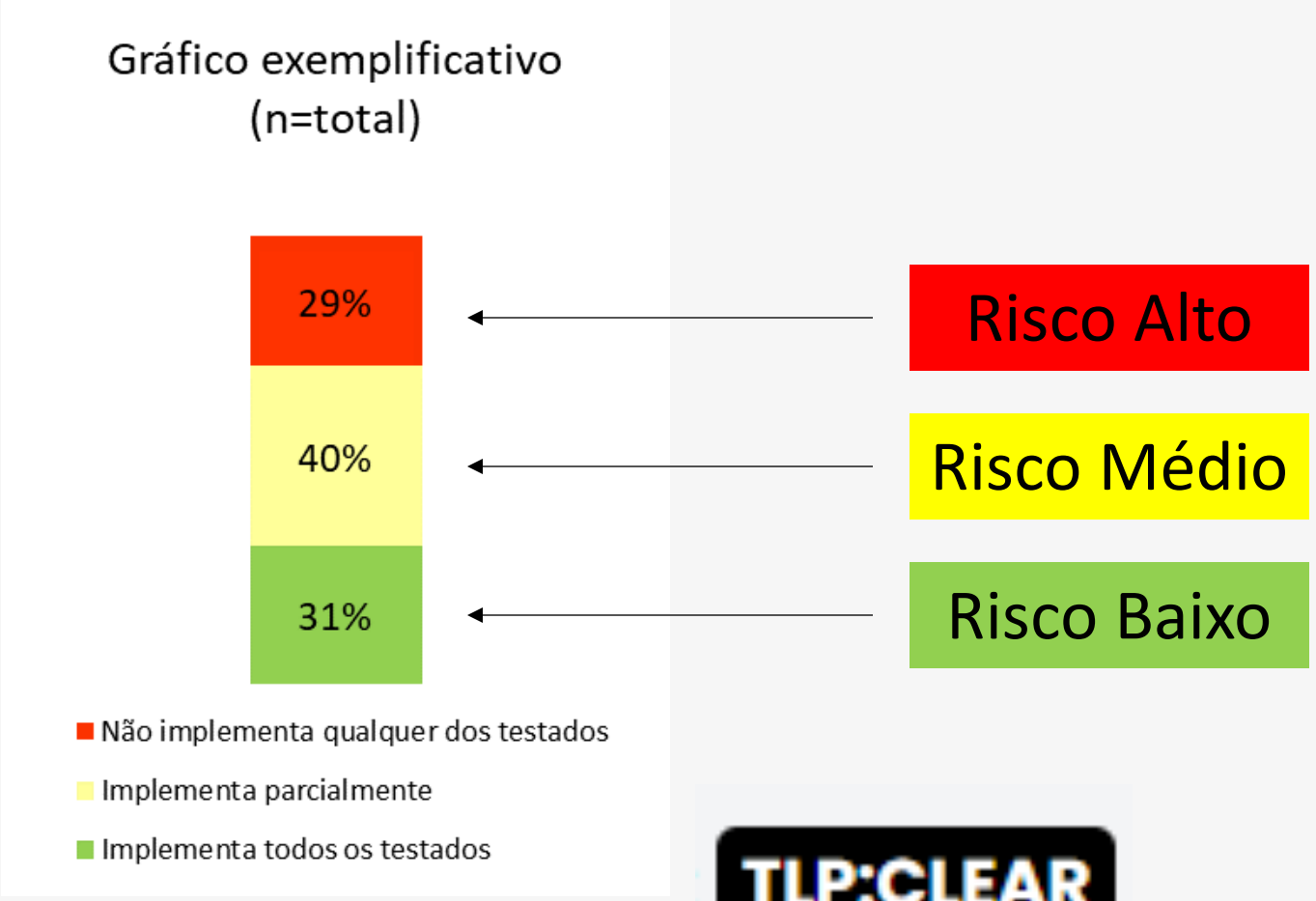
TLP:CLEAR

Quantidade de domínios (email) que implementam ao menos n controles



TLP:CLEAR

Avaliação Qualitativa



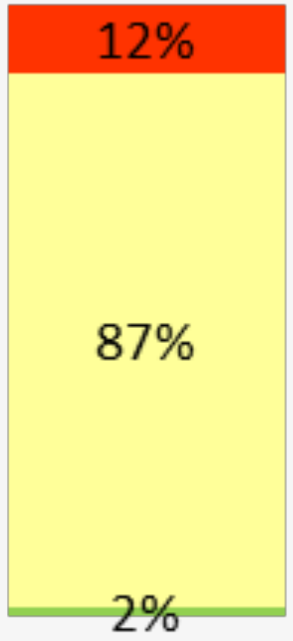
TLP:CLEAR

TRIBUNAL DE CONTAS DA UNIÃO

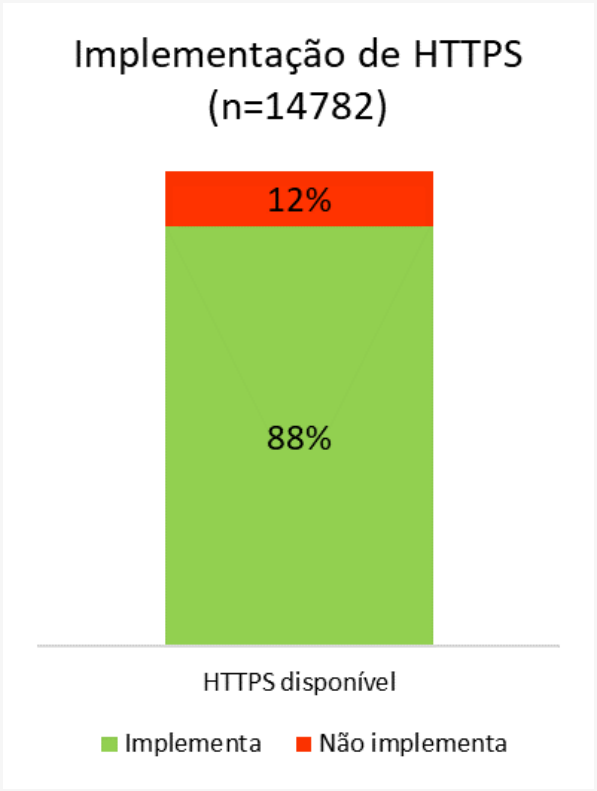
Conexão Web Segura (HTTPS)

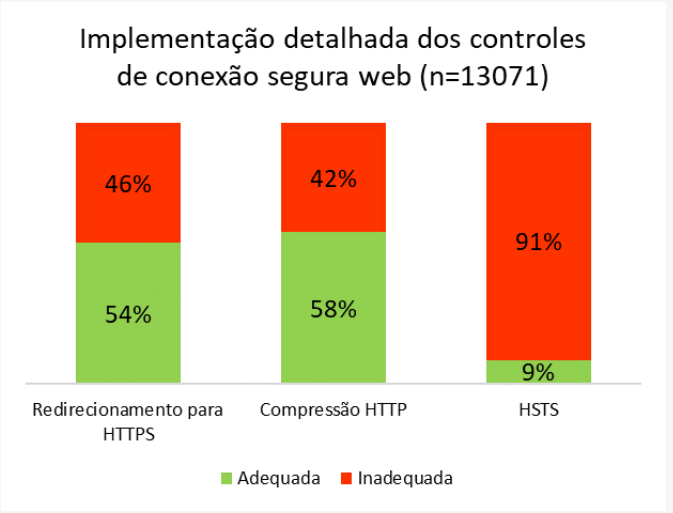
TLP:CLEAR

Implementação dos controles de conexão segura web (n=14782)

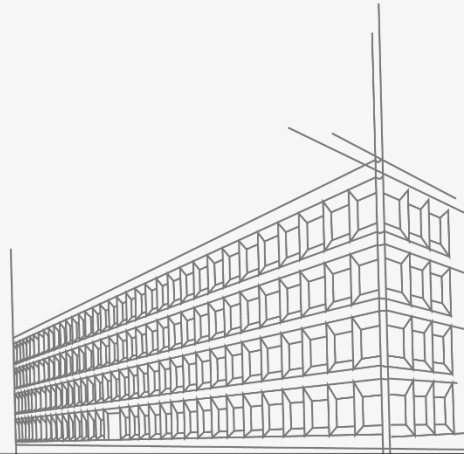


- Não implementa qualquer dos testados
- Implementa parcialmente
- Implementa todos os testados





TLP:CLEAR

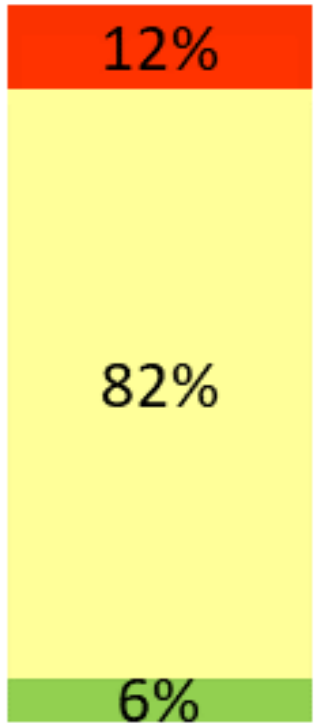


TRIBUNAL DE CONTAS DA UNIÃO

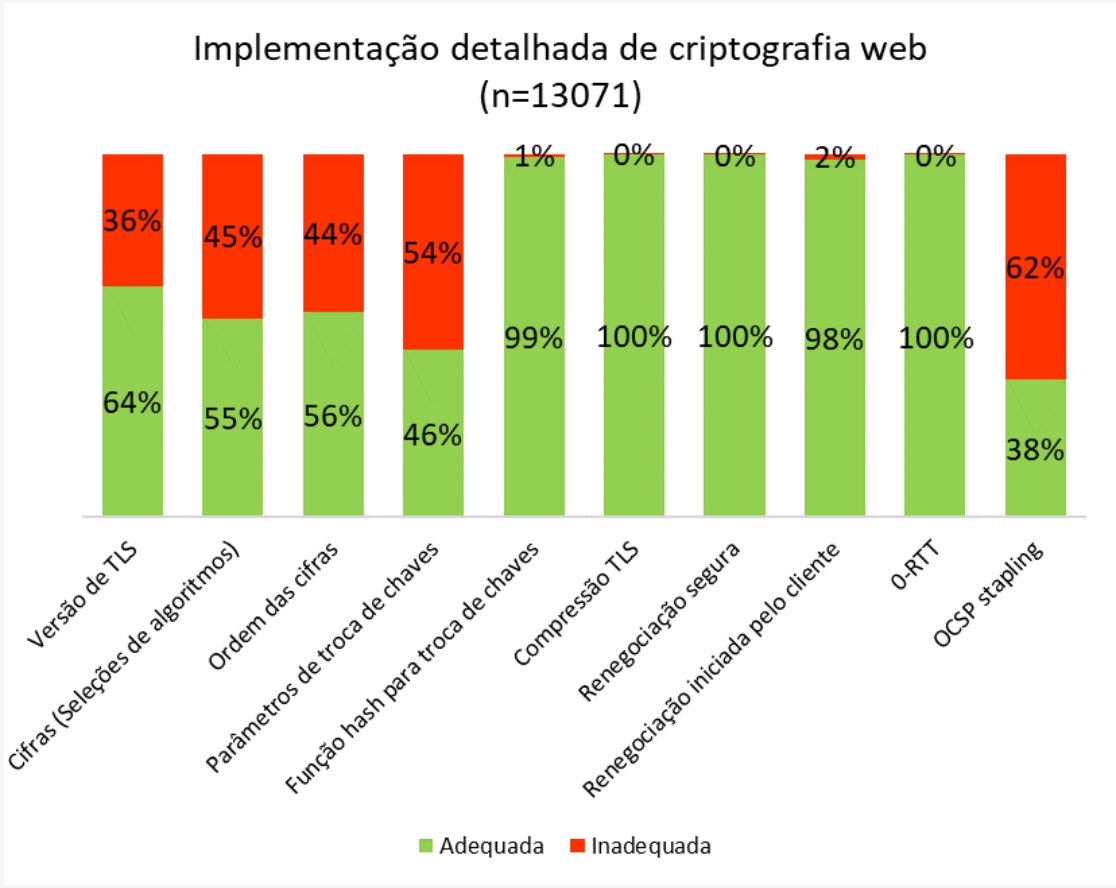
Criptografia na Comunicação (e-mail e Web)

TLP:CLEAR

Implementação de criptografia web (n=14782)

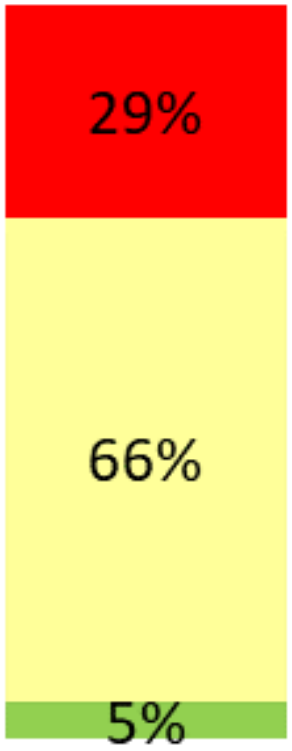


- Não implementa qualquer dos testados
- Implementa parcialmente
- Implementa todos os testados

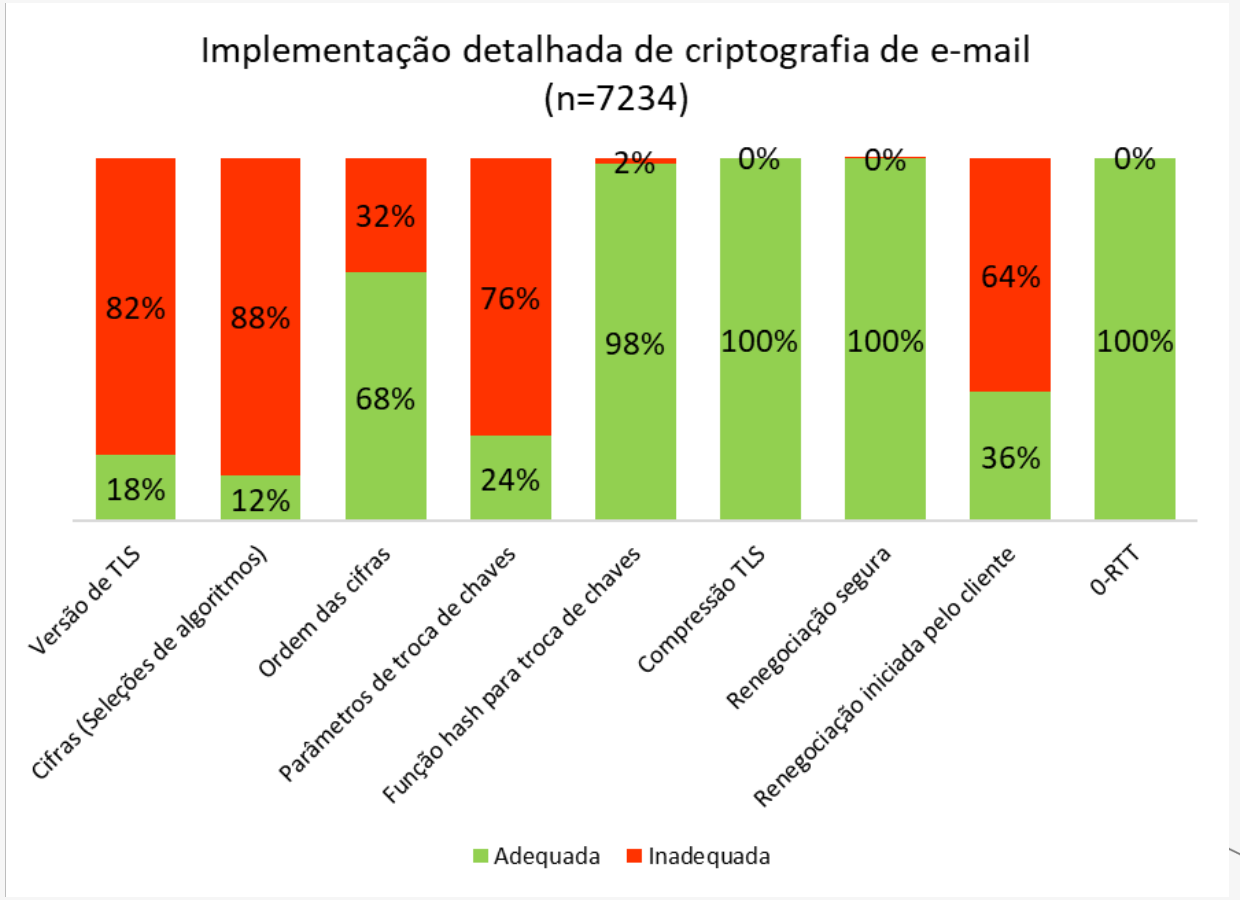


TLP:CLEAR

Implementação de criptografia de e-mail (n=10162)



- Não implementa qualquer dos testados
- Implementa parcialmente
- Implementa todos os testados



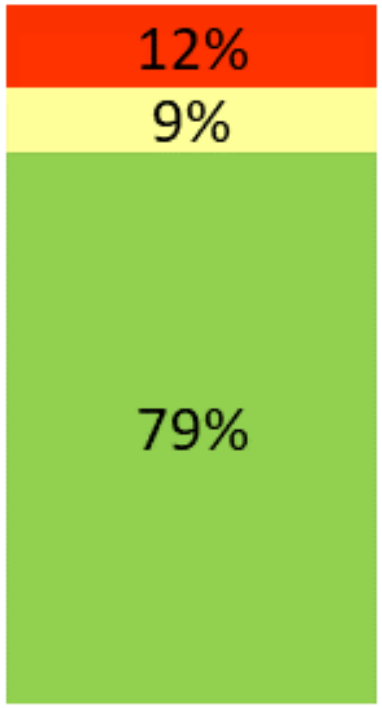
TLP:CLEAR

TRIBUNAL DE CONTAS DA UNIÃO

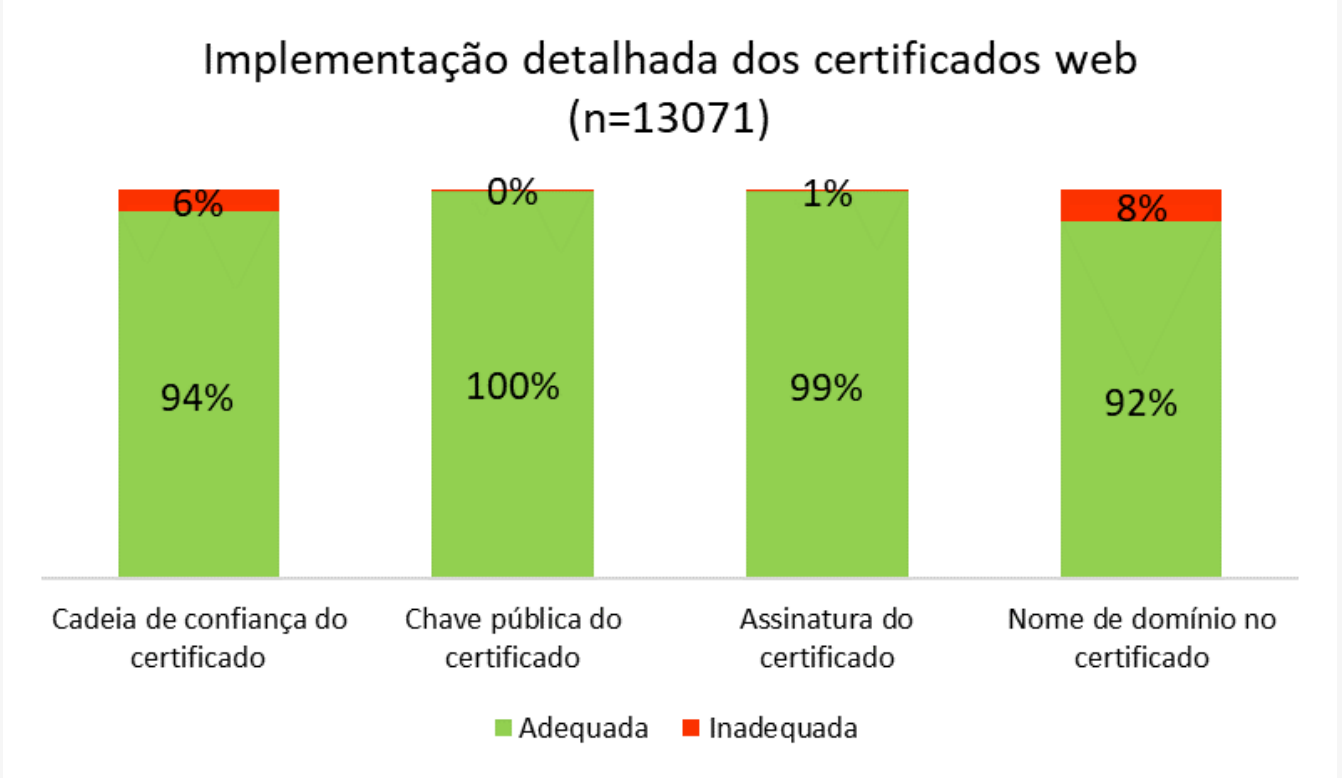
Certificados de Assinatura Digital (Web e e-mail)

TLP:CLEAR

Implementação dos certificados web (n=14782)

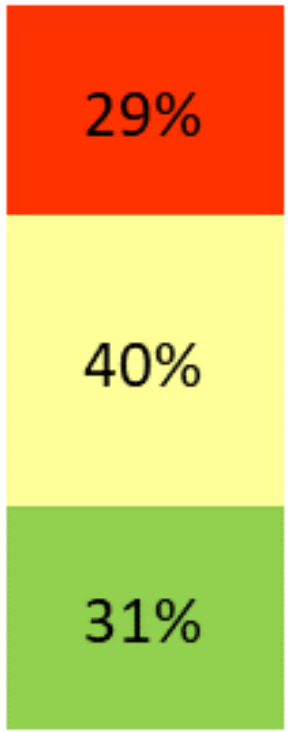


- Não implementa qualquer dos testados
- Implementa parcialmente
- Implementa todos os testados

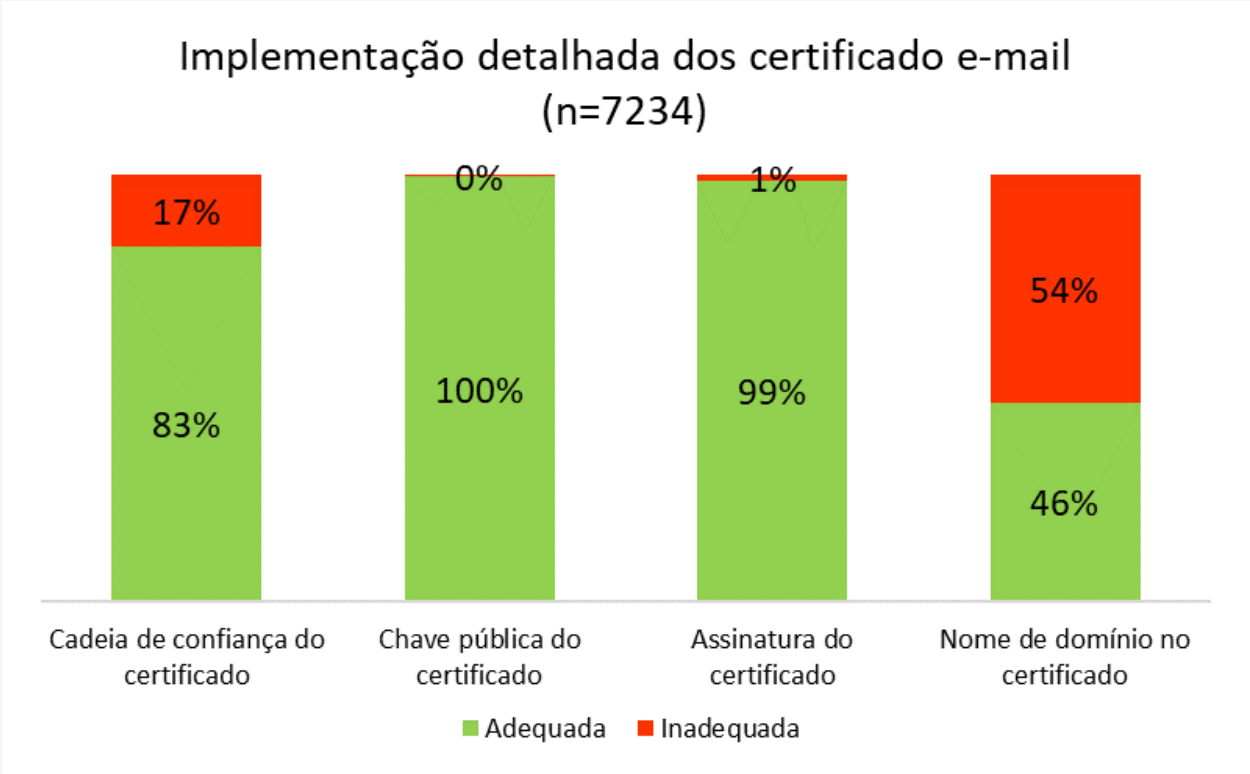


TLP:CLEAR

Implementação de certificado e-mail (n=10162)



- Não implementa qualquer dos testados
- Implementa parcialmente
- Implementa todos os testados



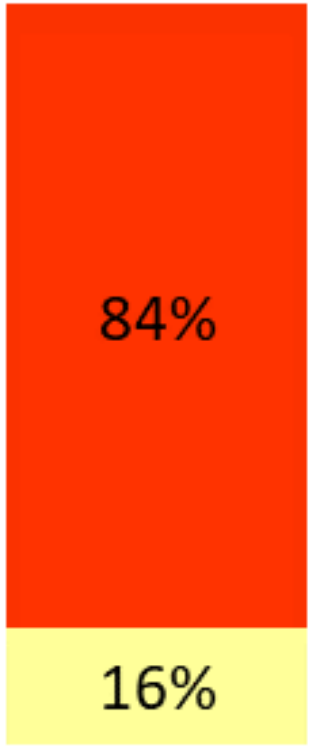
TLP:CLEAR

TRIBUNAL DE CONTAS DA UNIÃO

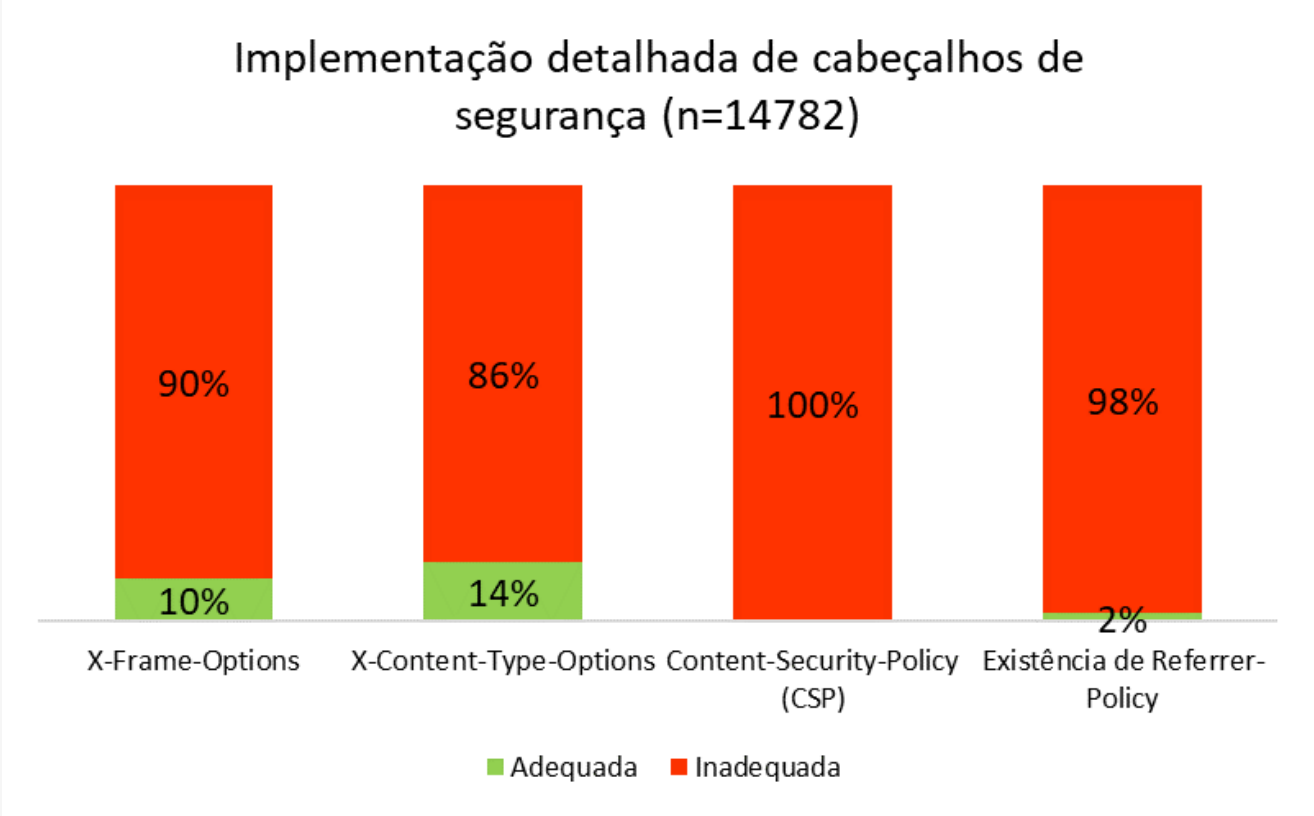
Cabeçalhos de Segurança Web

TLP:CLEAR

Implementação de cabeçalhos de segurança (n=14782)



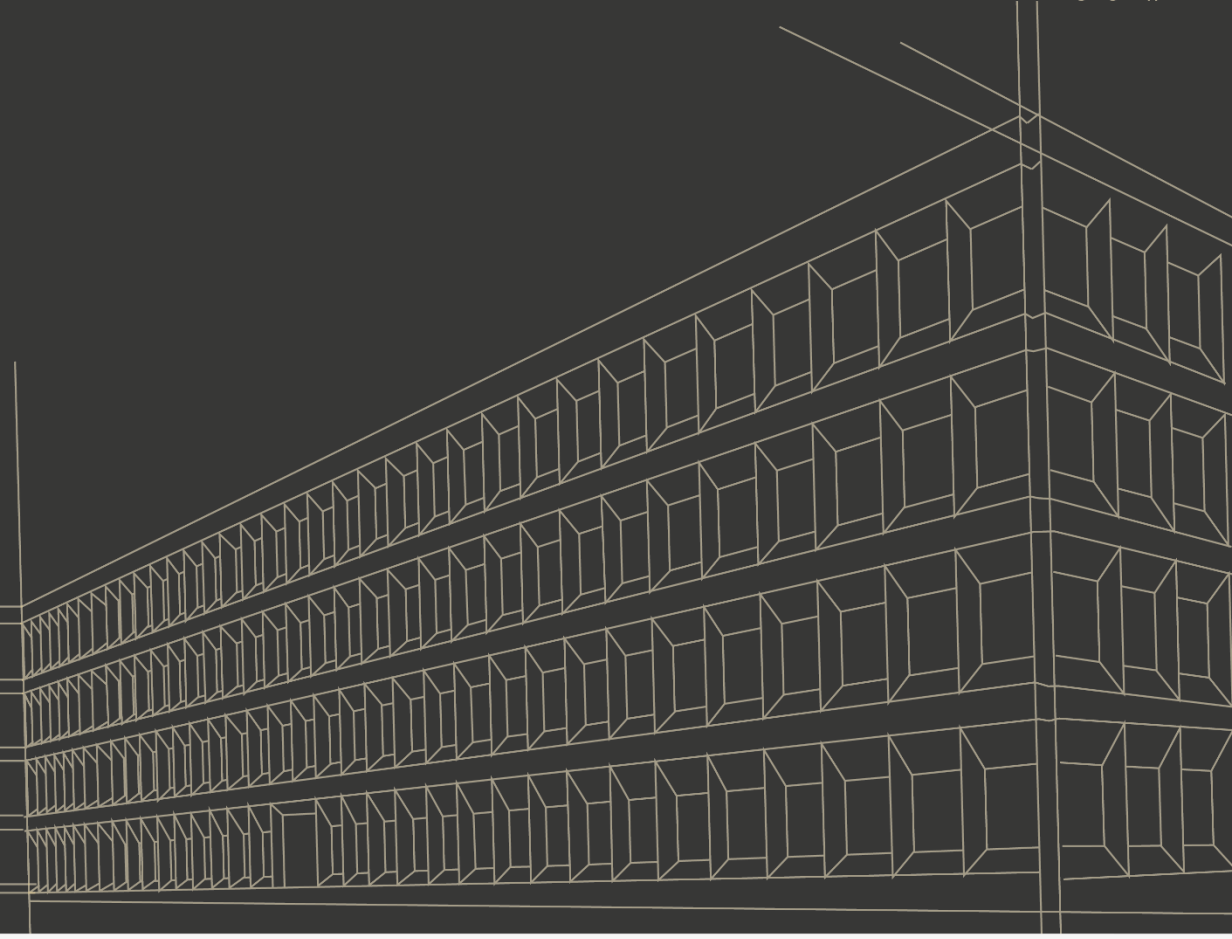
- Não implementa qualquer dos testados
- Implementa parcialmente
- Implementa todos os testados



TLP:CLEAR

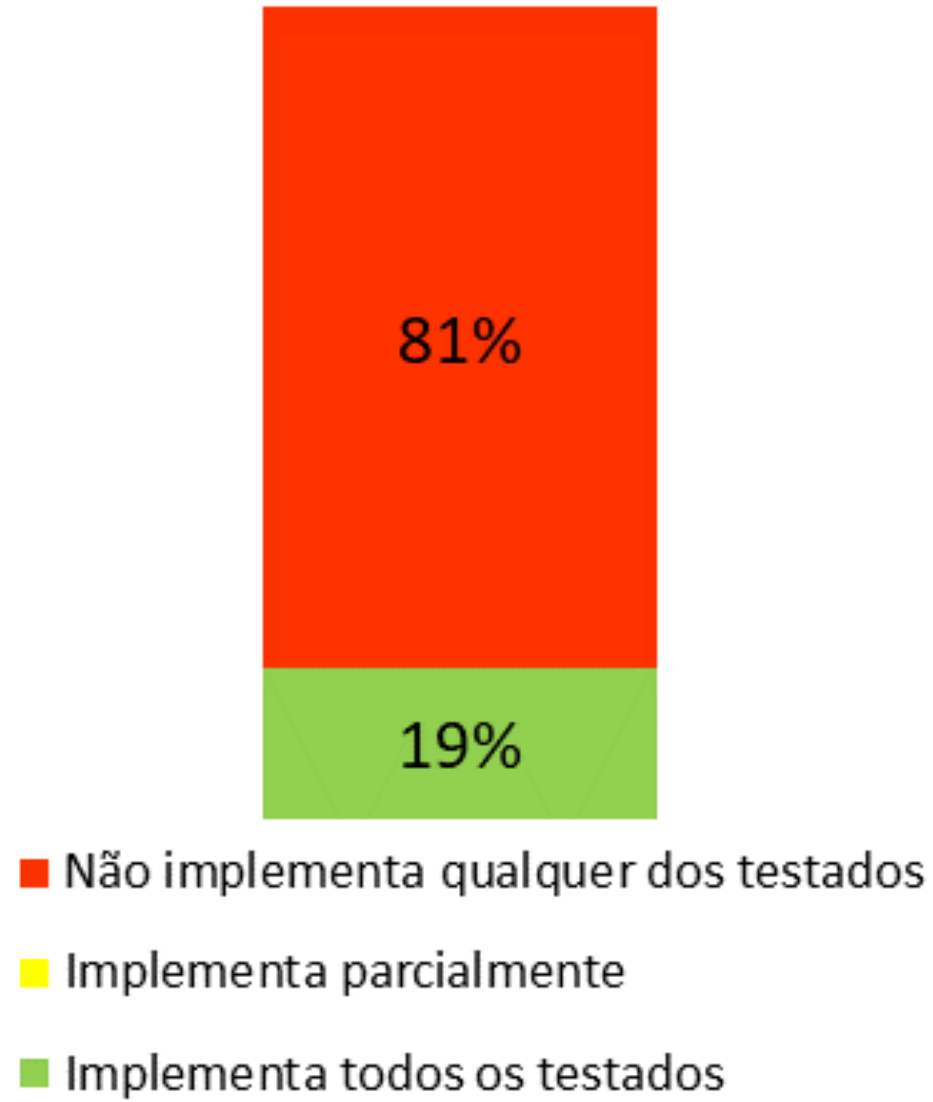
TRIBUNAL DE CONTAS DA UNIÃO

DNSSEC (Web e e-mail)



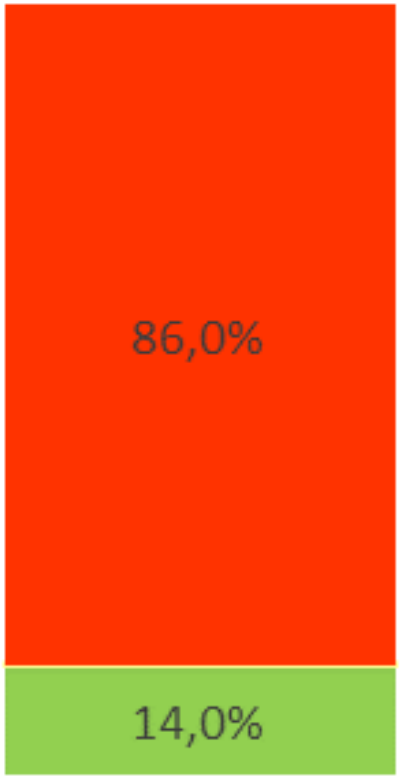
TLP:CLEAR

Implementação de DNSSEC web (n=14782)



TLP:CLEAR

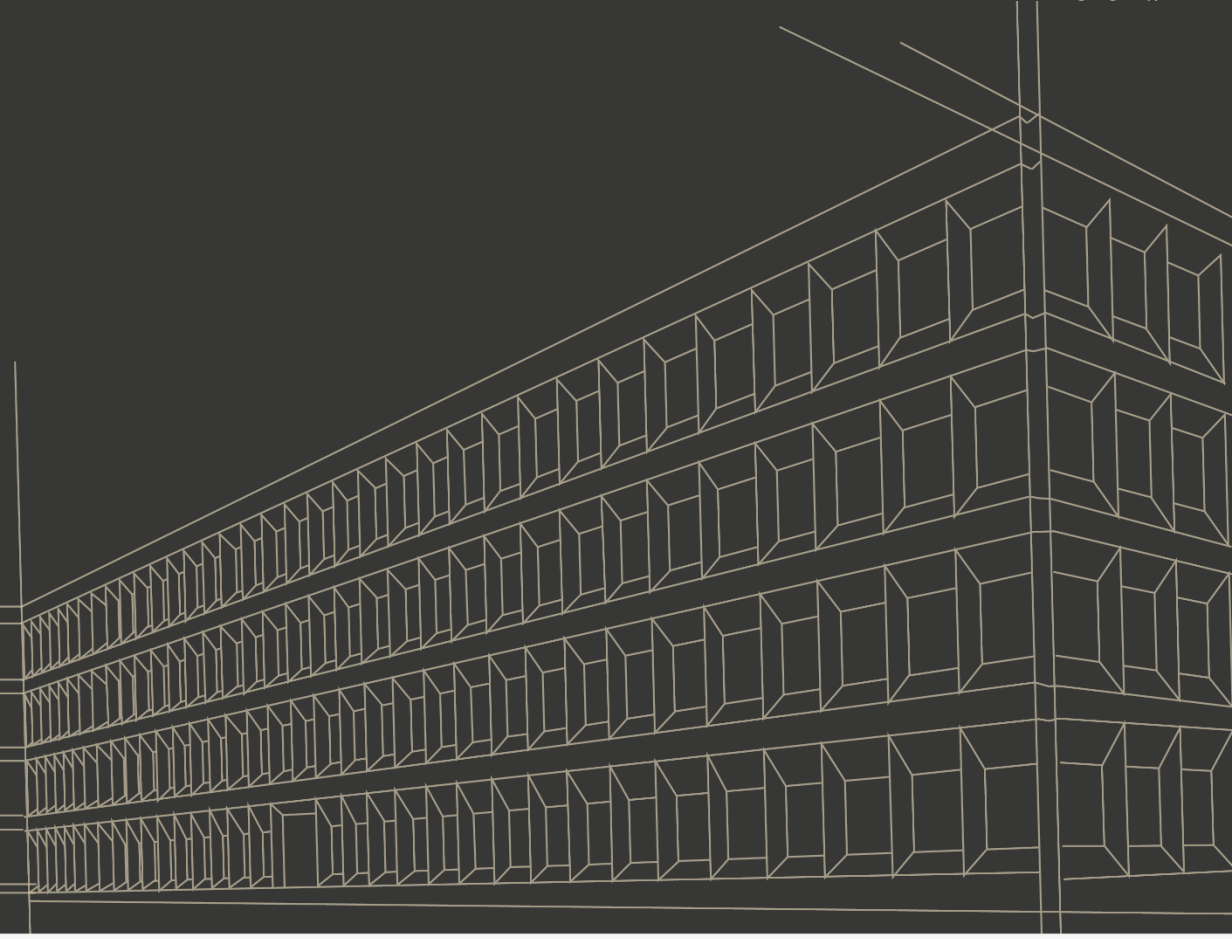
Implementação de DNSSEC e-mail (n=10162)



- Não implementado
- Parcialmente implementado
- Implementado

TLP:CLEAR

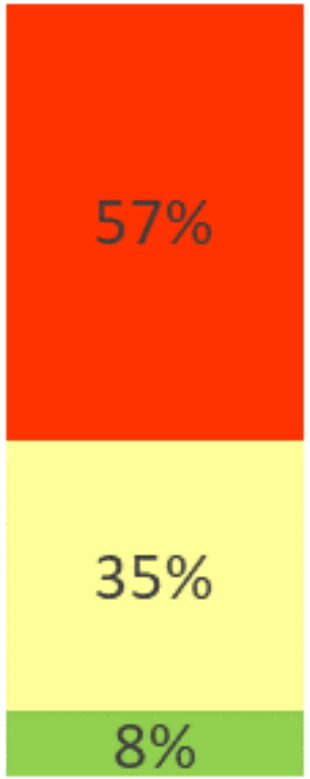
TRIBUNAL DE CONTAS DA UNIÃO



IPv6
(Web e e-mail)

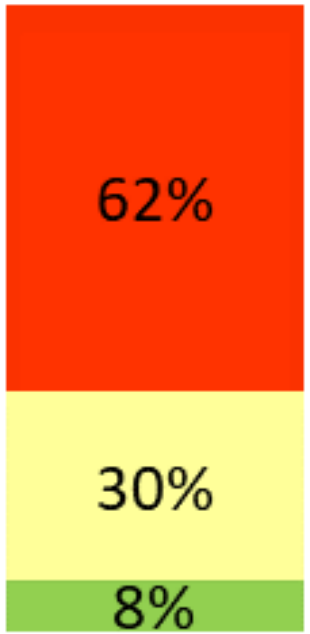
TLP:CLEAR

Implementação de IPv6 web (n=14782)



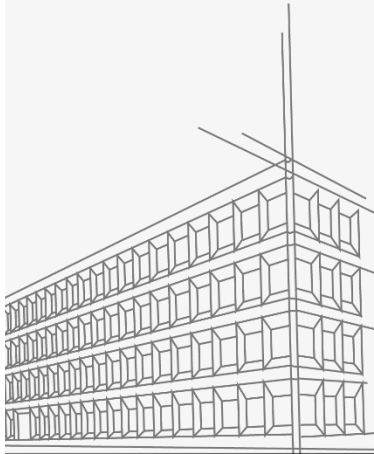
- Não Implementa qualquer dos testados
- Implementa parcialmente
- Implementa todos os testados

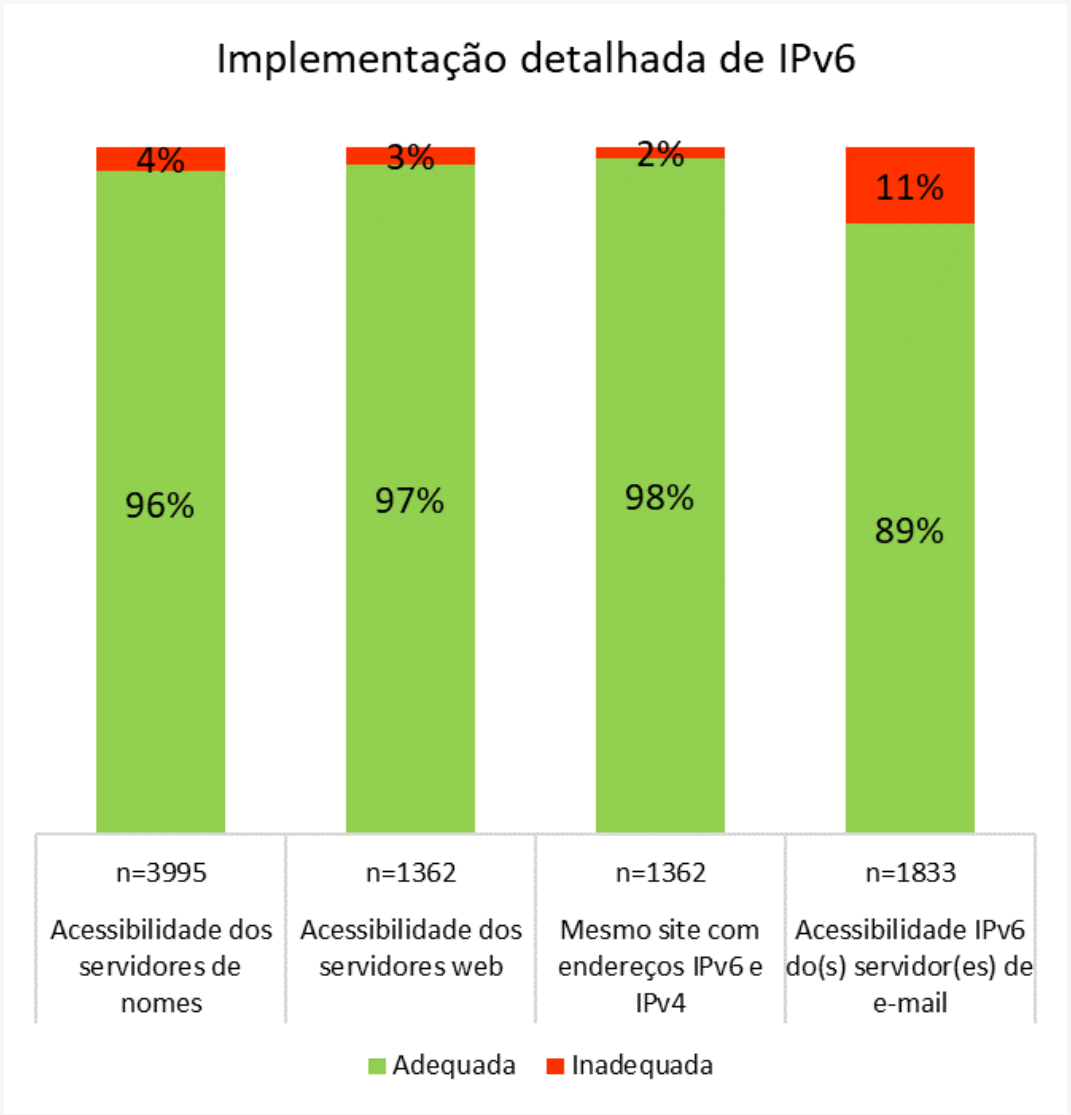
Implementação de IPV6 e-mail (n=10162)

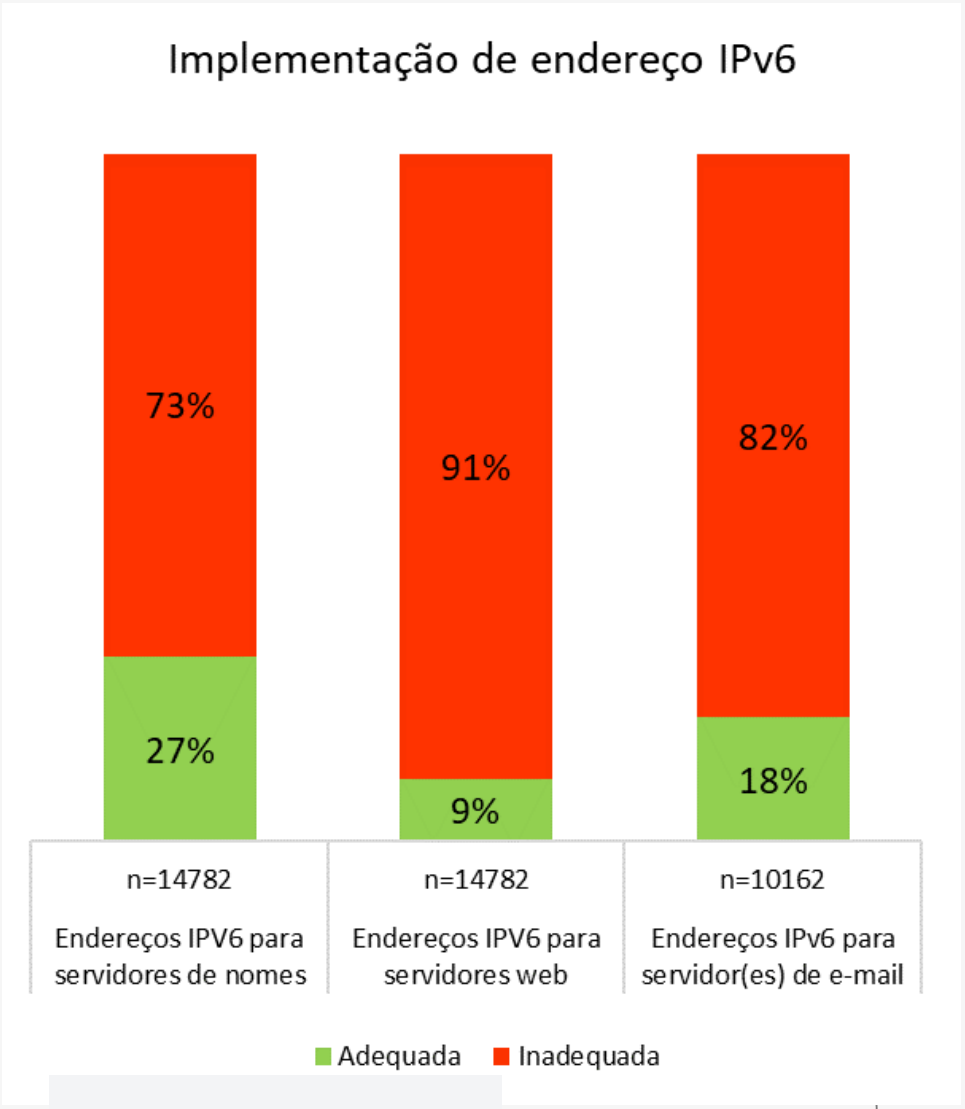


- Não Implementa qualquer dos testados
- Implementa parcialmente
- Implementa todos os testados

TLP:CLEAR




Implementação detalhada de IPv6
4%
3%
2%
11%
96%
97%
98%
89%
n=3995
Acessibilidade dos servidores de nomes
n=1362
Acessibilidade dos servidores web
n=1362
Mesmo site com endereços IPv6 e IPv4
n=1833
Acessibilidade IPv6 do(s) servidor(es) de e-mail
Adequada
Inadequada


Implementação de endereço IPv6
73%
91%
82%
27%
9%
18%
n=14782
Endereços IPV6 para servidores de nomes
n=14782
Endereços IPV6 para servidores web
n=10162
Endereços IPv6 para servidor(es) de e-mail
Adequada
Inadequada

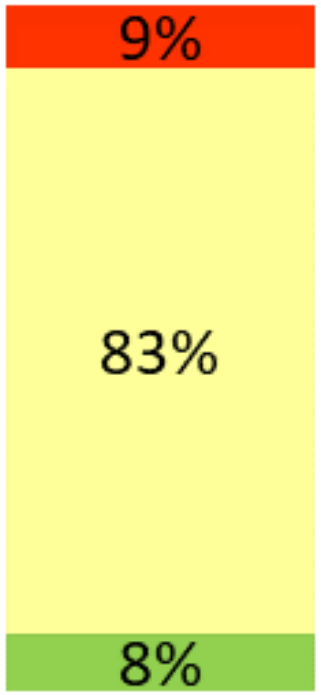
TLP:CLEAR

TRIBUNAL DE CONTAS DA UNIÃO

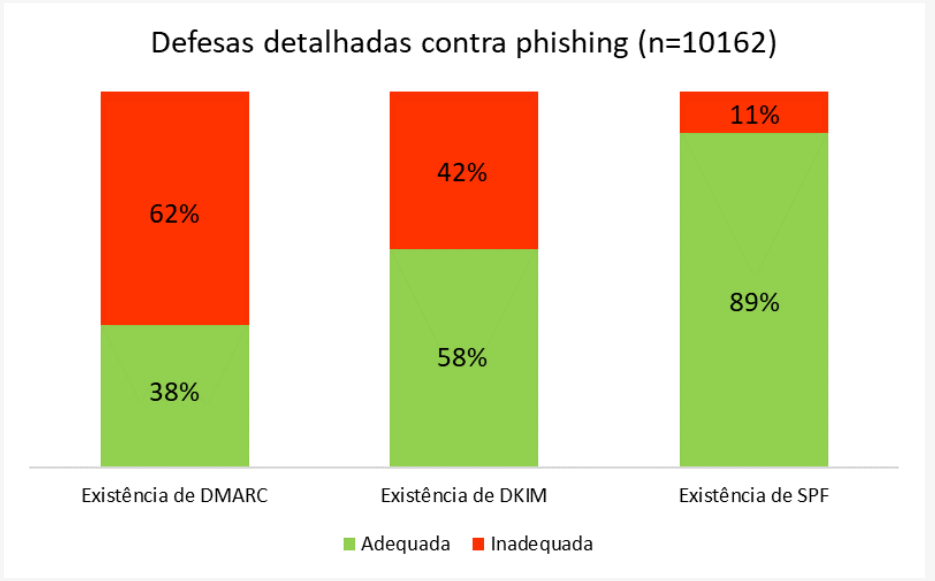
Proteções contra Phishing

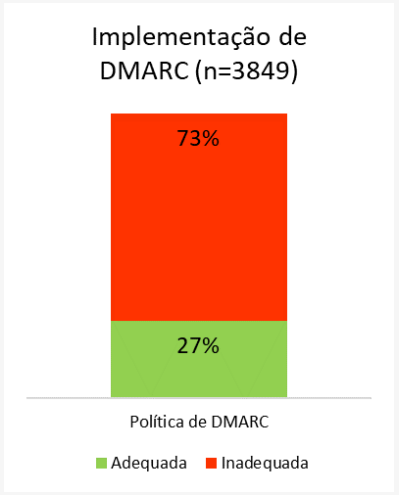
TLP:CLEAR

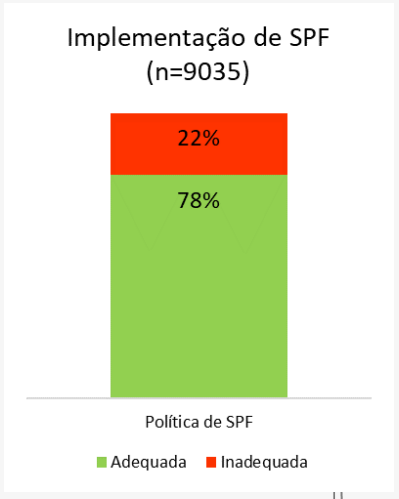
Defesas contra phishing (n=10162)



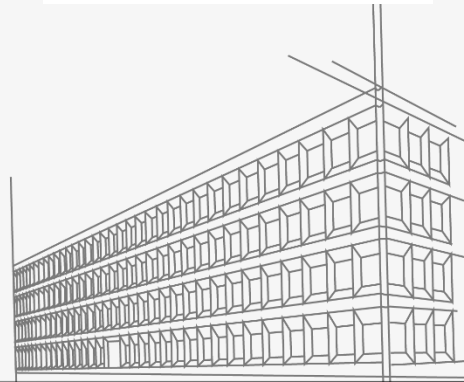
- Não implementa qualquer dos testados
- Implementa parcialmente
- Implementa todos os testados

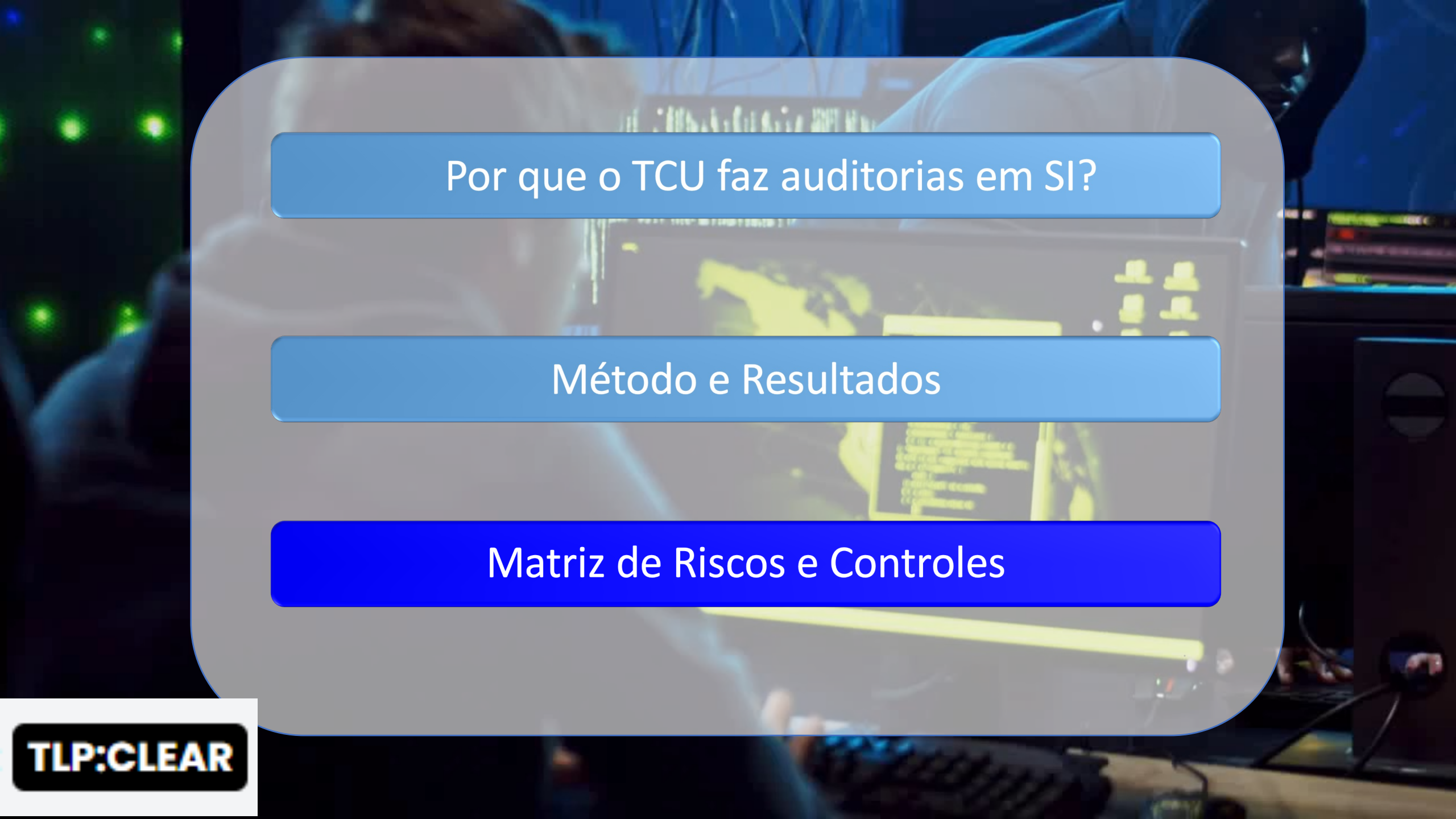






TLP:CLEAR

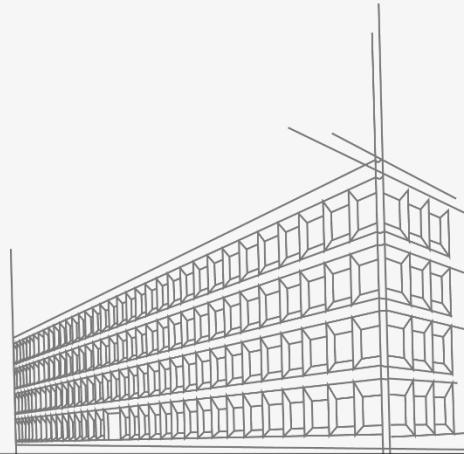



Por que o TCU faz auditorias em SI?
Método e Resultados
Matriz de Riscos e Controles
TLP:CLEAR

Entendendo riscos para estimar custos e benefícios esperados com os controles

1. **Descrição Sucinta do Controle**
2. **Descrição do teste**
3. **Exemplos de riscos (não implementação do controle)**
4. **Critérios**
5. **Exemplos de Referências para Implementação**
6. **Custo estimado**
7. **Benefício estimado**

TLP:CLEAR



Acórdão 523/2024-TCU-Plenário
(Relator: Min. Aroldo Cedraz)

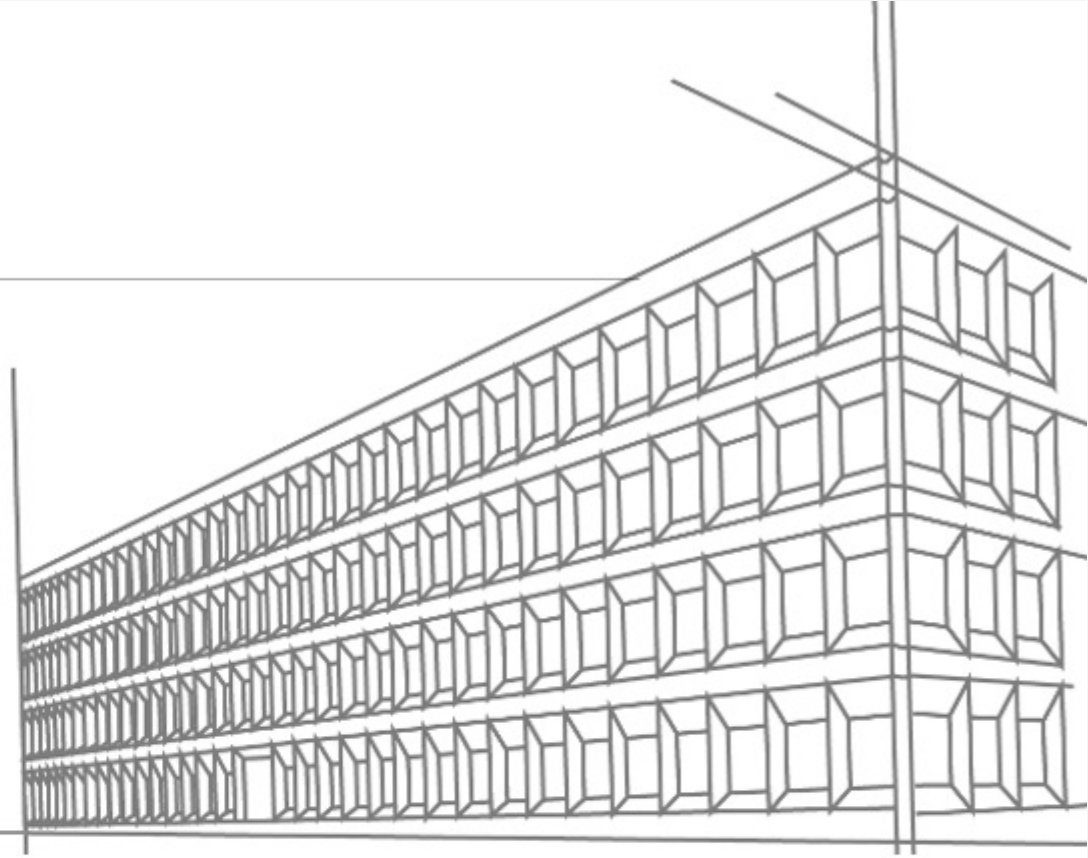
9.1. encaminhar cópia [...] às seguintes [OITO] organizações para que avaliem, se entenderem conveniente e oportuno, a adoção de medidas e a elaboração de estratégias para orientar organizações que se encontram na sua área de atuação sobre a gestão dos riscos decorrentes da não implantação dos controles ora analisados: [...]

9.2. autorizar a AudTI a divulgar as informações [...];

9.3. classificar [...] as peças 8, 9, 10 e 22 deste processo como sigilosas, em grau reservado, {...]

9.4. levantar o sigilo dos autos, exceto pelas peças mencionadas no subitem [illegible] uivar o presente processo.

TLP:CLEAR



Obrigado!

dasi@tcu.gov.br

TLP:CLEAR