Tribunal Regional Eleitoral-DF

1ª REUNIÃO DA CSI
16/11/2023

Tribunal Regional Eleitoral-DF

Tópicos

- Legislação aplicada
- Ações realizadas 2022/2023
- Atividades Rotineiras
- Ações Futuras

Legislação Aplicada

Tribunal Regional Eleitoral-DF

Resolução CNJ nº 396/2021 – ENSEC-PJ

Portaria CNJ nº 162/2021 – Protocolos e Manuais previstos na ENSEC-PJ

Resolução TSE nº 23664/2021 – PSI da JE

Estratégia Nacional de Cibersegurança da JE – 2021/2024

Legislação Aplicada

Tribunal Regional Eleitoral-DF

Estratégia Nacional de Cibersegurança da JE – 2021/2024

Eixos Estruturantes

1. Pessoas e Unidades Organizacionais

2. Políticas e Normatização

3. Ferramentas Automatizadas

4. Serviços Especializados

5. Sensibilização e Conscientização

Ações Realizadas em 2022/2023

Tribunal Regional Eleitoral-DF

EI - 1: Pessoas e Unidades Organizacionais

	Cenário Atual	Metas de Curto Prazo (até o fim de 2021)	Metas de Médio Prazo (até o fim de 2022)	Metas de Médio-Longo Prazo (até o fim de 2023)
TREs de Pequeno Porte (SE, AL, MS, ES, DF, TO, RR, AC, RO, AP, MT)	ETIRs não operacionalizadas Ninguém dedicado à cibersegurança na maioria dos TREs Sobreposição de funções do Gestor de Segurança da Informação com várias outras atribuições no Tribunal	Montagem de equipe de segurança com, pelo menos, 1 pessoa dedicada ao assunto	Capacitação e operacionalização da ETIR	Implementação da estrutura técnica mínima prevista pelo GT-SI e designação de gestor para acumular as funções da gestão de negócio da Segurança da Informação[1].
TREs de Médio Porte (RN, AM, PA, PE, BA, CE, SC, GO, PB, PI, MA)		Montagem de equipe de segurança com, pelo menos, 1 pessoa dedicada ao assunto	Capacitação e operacionalização da ETIR	Implementação da estrutura técnica mínima prevista pelo GT-SI e designação de gestor para acumular as funções da gestão de negócio da Segurança da Informação[1].
TREs de Grande Porte (SP, RS, MG, PR, RJ)		Capacitação e operacionalização da ETIR Montagem de equipe de segurança com, pelo menos, 1 pessoa dedicada ao assunto	Implementação da estrutura técnica mínima prevista pelo GT-SI e designação de gestor para acumular as funções da gestão de negócio da Segurança da Informação[1]	Designação de Gestor de Segurança da Informação Dedicado junto à Presidência ou DG.

1. Indicação do Gestor de SI – Portaria DG nº 83/2022

2. Criação da ETIR e Gestão de Incidentes – Portaria PR nº 122/2021

3. Iniciada capacitação - 2023

- Curso de Ethical Hacker – TRE-SP
- MBA em Cyber Security - 2024

Ações Realizadas em 2022/2023

Tribunal Regional Eleitoral-DF

EI - 2: Políticas e Normatização

	Cenário Atual	Metas de Curto Prazo (até o fim de 2021)	Metas de Médio Prazo (até o fim de 2022)	Metas de Longo Prazo (até o fim de 2024)
TREs de Pequeno Porte (SE, AL, MS, ES, DF, TO, RR, AC, RO, AP, MT)	PSI aprovada Normas táticas e procedimentos operacionais inexistentes na maior parte dos TREs	Submissão, para aprovação, de normas táticas nos temas previstos na PSI.	Elaboração de fluxos operacionais para cada norma tática	Divulgação e implantação de procedimentos e fluxos aprovados Revisão das normas táticas e procedimentos operacionais
TREs de Médio Porte (RN, AM, PA, PE, BA, CE, SC, GO, PB, PI, MA)		Submissão, para aprovação, de normas táticas nos temas previstos na PSI.	Elaboração de fluxos operacionais para cada norma tática	Divulgação e implantação de procedimentos e fluxos aprovados Revisão das normas táticas e procedimentos operacionais
TREs de Grande Porte (SP, RS, MG, PR, RJ)		Submissão, para aprovação, de normas táticas nos temas previstos na PSI. Submissão, para aprovação, de procedimentos e fluxos operacionais para cada norma tática.	Divulgação e implantação de procedimentos e fluxos aprovados	Designação de Gestor de Segurança da Informação Dedicado junto à Presidência ou DG. Revisão das normas táticas e procedimentos operacionais

Norma Prevista	Situação
1. Gestão de Ativos	Port. PR. nº 241/2023
2. Controle de Acesso Físico e Lógico	Port. PR. nº 27/2022 - Atualizar
3. Gestão de Riscos de SI	Pendente - Jun/2024
4. Uso Aceitável de Recursos de TI	Port. PR. nº 27/2022 - Atualizar
5. Geração e Restauração de Cópias de SI	Port. PR. nº 69/2021
6. Plano de Continuidade de Serviços Essenciais TI	0003655-96 - Atualizar Out/2024
7. Gestão de Incidentes de SI	Port. PR. Nº 122/2021
8. Gestão de Vulnerabilidades e Padrões de Configuração	Pendente - Out/2024
9. Gestão e Monitoramento de Registros de Atividades (logs)	Port. PR. nº 27/2022 - Atualizar
10. Desenvolvimento Seguro de Sistemas	Pendente - Fev/2025
11. Uso de Recursos Criptográficos	Pendente - Jun/2025

Entrega dos protocolos de Cibersegurança

- PPINC – Prevenção de Incidentes Cibernéticos – 38%
- PGCRC – Gerenciamento de Crises Cibernéticas – 32%
- PIILC – Investicação de Ilícitos Cibernéticos – 20%

Ações Realizadas em 2022/2023

Tribunal Regional Eleitoral-DF

EI - 2: Políticas e Normatização

5. Proposta para atualização da PARTIC – Portaria PR nº 27/2022

0000284-51.2023.6.07.8100 - Despacho SGP 1435926 - Gestão de usuários e credenciais

0004647-18.2022.6.07.8100 - Relatório de Auditoria - Processo Gestão de Segurança da Informação (1193668) - Atendimento aos achados 2, 3, 4 e 5

0000319-11.2023.6.07.8100 - Relatório de Auditoria Integrado do TSE
No processo de Gestão de Segurança da informação (1325238) - Atendimento ao achado 2

6. Proposta para revogar Portaria PR nº 189/2010 – Dispõe sobre o acesso aos sistemas de informação do TRE-DF, após a publicação da nova versão da PARTIC

https://apps.tre-df.jus.br/Normativo/20100050189_1278020795000.doc

7. Necessária atualização da Portaria DG nº 83/2022, p/ indicação do Substituto do Gestor de Segurança da Informação

8. Indicar novo representante da DG na CSI

Ações Realizadas em 2022/2023

Tribunal Regional Eleitoral-DF

EI - 3: Ferramentas Automatizadas

	Cenário Atual	Metas de Curto Prazo (até o fim de 2021)	Metas de Médio Prazo (até o fim de 2022)	Metas de Longo Prazo (até o fim de 2024)
TREs de Pequeno Porte (SE, AL, MS, ES, DF, TO, RR, AC, RO, AP, MT)	Heterogeneidade de ferramentas adquiridas, cofiguradas e implantadas.	Aquisição, configuração e implantação de ferramentas de prioridade 1[3].	Aquisição, configuração e implantação de ferramentas de prioridade 2[3].	Aquisição, configuração e implantação de ferramentas de prioridade 3[3].
TREs de Médio Porte (RN, AM, PA, PE, BA, CE, SC, GO, PB, PI, MA)		Aquisição, configuração e implantação de ferramentas de prioridade 1[3].	Aquisição, configuração e implantação de ferramentas de prioridade 2[3].	Aquisição, configuração e implantação de ferramentas de prioridade 3[3].
TREs de Grande Porte (SP, RS, MG, PR, RJ)	Muitos TREs com carências graves de ferramentas.	Aquisição, configuração e implantação de ferramentas de prioridade 1[3]. Aquisição, configuração e implantação de ferramentas de prioridade 2[3].	Aquisição, configuração e implantação de ferramentas de prioridade 3[3].	Controles de cibersegurança implementados, automatizados e reportados à direção.

Ferramentas de Segurança de Borda

- 1: Firewall de Borda (por exemplo, Sonic Wall, Checkpoint)
- 1: Anti-Spam (por exemplo, Spam Assassin, Symantec)
- 2: WAF (por exemplo, F5, Mod_Security)
- 3: Visibilidade do tráfego de rede (por exemplo, Corelight, Zeek)
- 3: Gerenciador de APIs (por exemplo, 3Scale)
- 3: Proteção contra Intrusão (por exemplo, Sonic Wall, Checkpoint)
- 3: Anti-DDOS (por exemplo, Netscout Arbor, Radware)
- 3: Balanceador de Links (por exemplo, F5 Link Controller, A10 Networks)

Ferramentas de Segurança Interna

- 1: Anti-virus (por exemplo, Trend, McAffee, Symantec)
- 2: Firewall TSE-TREs (por exemplo, Sonic Wall, Checkpoint)
- 2: Proxy de Navegação/FiltroWeb/Inspeção SSL (por exemplo, SonicWall CFS, Symantec WebFilter)
- 2: Monitoração e auditoria de E-mail, arquivos e AD (por exemplo, Varonis)
- 2: Concentrador de logs (por exemplo, Graylog, ElasticSearch)
- 3: Análise estática de Código-fonte (por exemplo, Microfocus Fortify, Veracode)
- 0: Infraestrutura Hiper-convergente (somente no TSE, onde já se encontra disponível)

Ferramentas de Autenticação

- 2: Duplo Fator de Autenticação (por exemplo, Duo Security, RSA SecurID)
- 3: Autenticação Single Sign-on (por exemplo, RHSSO)

Governança e Continuidade

- 1: Inventário integrado de HW e SW (por exemplo, Altiris, SpiceWorks/ELK)
- 1: Solução de Backup (por exemplo, Veritas Netbackup, CommVault)
- 1: Gestão de Vulnerabilidades (por exemplo, Tenable, Qualys, OpenVAS)
- 3: Gestão de Acesso Privilegiado (Cofre de Senhas) (por exemplo, Microsoft LAPS, HashiCorp)

Soluções Previstas: 20
Soluções Investidas: 16
% de aderência: 80%

Ações Realizadas em 2022/2023

Tribunal Regional Eleitoral-DF

EI - 3: Ferramentas Automatizadas

Aquisições 2022

1. Solução WAF(F5) - SEI (0007621-28) – R$ 1.391.886,69
2. Solução de Cofre de Senhas(BeyondTrust) - SEI (0003710-08) – R$ 559.000,00
3. Solução de capacitação(Knowbe4) – SEI (0004336-27) – R$ 20.996,50
4. Solução de Gestão Vulnerabilidade (Tenable-AD) – SEI (0004823-94) – R$ 506.456,00
5. Solução de 2FA(Cisco DUO) - SEI (0005187-66) – R$ 317.700,00
6. Solução de Patchs e Inventário(Ivanti) - SEI (0005994-86) – R$ 198.490,00
7. Licenças de Segurança para Oracle - SEI (0005190-21) – R$ 594.800,00

Aquisições 2023

1. Solução de cibersegurança avançada – SEI (0005153-57) - R$ 4.197.771,70
2. Solução de auditoria de dados não estruturados – SEI (0000418-78) - R$ 3.268.720,54
3. Modernização da solução de backup – SEI (0009132-27) - R$ 1.720.920,88

Investimento Total R$ 3.589.329,19

Investimento Total Estimado R$ 9.187.413,12

Ações Realizadas em 2022/2023

Tribunal Regional Eleitoral-DF

EI - 4: Serviços Especializados

	Cenário Atual	Metas de Curto Prazo (até o fim de 2021)	Metas de Médio Prazo (até o fim de 2022)	Metas de Longo Prazo (até o fim de 2024)
TSE e TREs	No TSE, há contratações em curso para Inteligência Cibernética, Apoio Técnico em Segurança e Apoio à Elaboração de Normas. No caso da maioria dos TREs, não há contratação de serviços especializados.	Conclusão da contratação de serviços especializados. Levantamento da maturidades do entes da J.E. (item 1 da tabela anterior)	Implantação e entrada em operação de SOC (item 2). Realização de capacitações para as equipes operacionais, para gestores táticos e para a alta gestão (item 3). Realização de simulações de ataque (item 5)	Realização de trilhas de treinamentos para unidades de Segurança de TI e ETIRs (item 4) Reavaliação de possíveis novos escopos de contratação de serviços especializados.

1) Realização de Diagnóstico/Análise de maturidade em Cibersegurança – **ARP TSE nº 01e 02/2023**

2) Provimento de serviço de Security Operations Center (SOC) para toda JE – **Somente TSE**

3) Realização de capacitações para equipes operacionais, gestores táticos e para alta gestão – **Trilha de Capacitação em cibersegurança em andamento – Knowbe4**

4) Realização de trilhas de treinamentos de formação de profissionais de SI para TI e ETIR – **Já iniciada capacitação Ethical Hacker / MBA em Cyber Security – IBMEC – 2024**

5) Realização de simulações de ataques, Red Teams e Blue Teams da JE – **ARP TSE nº 01e 02/2023**

Ações Realizadas em 2022/2023

Tribunal Regional Eleitoral-DF

EI - 5: Sensibilização e Consciêntização

	Cenário Atual	Metas de Curto Prazo (até o fim de 2021)	Metas de Médio Prazo (até o fim de 2022)	Metas de Longo Prazo (até o fim de 2024)
TSE	Alta Gestão sensibilizada e patrocinadora de mudanças em cibersegurança	Disponibilização, em consonância com priorização pela CDTI, de Portal de Segurança da Informação, que deverá ser usado por toda a J.E. ***Mentoring*** a STIs dos TREs para que conduzam reuniões de sensibilização com suas gestões. Condução de eventos de sensibilização e conscientização com a comunidade de TI do TSE.	Condução de eventos de sensibilização e conscientização com a comunidade institucional. Criação de vídeos curtos, em parceria com a SECOM/TSE, para postagem nas redes sociais e canais da Justiça Eleitoral.	Condução de eventos específicos para partidos, órgãos de Imprensa, pesquisadores e candidatos, com o objetivo de sensibilizar sobre cibersegurança.
TREs de Pequeno Porte (SE, AL, MS, ES, DF, TO, RR, AC, RO, AP, MT)		Reuniões com altas gestões para sensibilização e conscientização, com o objetivo de obter apoio para recursos previstos nesta Estratégia.	Condução de eventos de sensibilização e conscientização com a comunidade institucional e com a comunidade de TI do Tribunal. Levantamento de peças midiáticas, informações e instruções a serem inseridas no Portal de Segurança da Informação.	Condução de eventos específicos para partidos, órgãos de Imprensa, pesquisadores e candidatos, com o objetivo de sensibilizar sobre cibersegurança.

Uso da solução Knowbe4
03 Trilhas de capacitações realizadas
Média de 78% de participação nos treinamentos

Ações Realizadas em 2022/2023

Tribunal Regional Eleitoral-DF

EI - 5: Sensibilização e Consciêntização

KnowBe4
Human error. Conquered.

Teste Controlado de Phishing

Teste de phishing iniciado em: 01/12/2022, 17:37

Campanha: avaliacao_inicial
Uma vez da categoria: Baseline

Este teste de phishing	
Status	Encerrada
% de propensão ao phishing	25,19%
Destinatários	266
Falhas	67
Término da campanha	04/12/2022, 17:37

Teste de phishing iniciado em: 09/10/2023, 09:21

Campanha: Teste_apos_1ª_trilha_capacitacao
Uma vez das categorias: Government, Holiday, Scam of the Week (Not PST), Current Event of the Week

Este teste de phishing	
Status	Encerrada
% de propensão ao phishing	7,83%
Destinatários	317
Falhas	17
Término da campanha	30/10/2023, 09:21

Ações Realizadas em 2022/2023

Tribunal Regional Eleitoral-DF

EI - 5: Sensibilização e Consciêntização

KnowBe4 Human error. Conquered.

Teste Controlado de Phishing

Teste de phishing iniciado em: 01/12/2022, 17:37

← Voltar às Campanhas

Campanha: avaliacao_inicial
Uma vez da categoria: Baseline

Visão geral | Usuários

266 Destinatários	100% 266 Entregue	56,8% 151 Aberto	24,8% 66 Clicado	0% 0 Código QR escaneado	0,4% 1 Respondido	0% 0 Anexo aberto	0% 0 Macro habilitada	0% 0 Dados inseridos	0,8% 2 Reportado	0% 0 Devolvido

Teste de phishing iniciado em: 09/10/2023, 09:21

← Voltar às Campanhas

Campanha: Teste_apos_1ª_trilha_capacitacao
Uma vez das categorias: Government, Holiday, Scam of the Week (Not PST), Current Event of the Week

Visão geral | Usuários

317 Destinatários	68,5% 217 Entregue	68,2% 148 Aberto	7,8% 17 Clicado	0% 0 Código QR escaneado	0% 0 Respondido	0% 0 Anexo aberto	0% 0 Macro habilitada	0% 0 Dados inseridos	5,5% 12 Reportado	31,5% 100 Devolvido

Ações Realizadas em 2022/2023

Tribunal Regional Eleitoral-DF

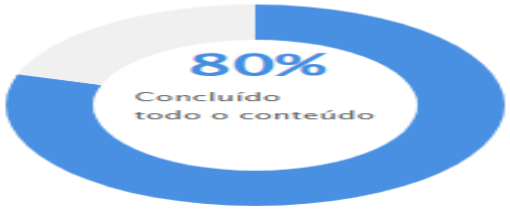
EI - 5: Sensibilização e Consciêntização

1ª Trilha de Capacitação em Cibersegurança - 2022

Avaliação do conhecimento antes dos treinamentos

Grupos: Todos os usuários

Resumo da campanha



Status	Em andamento
Data de início	01/12/2022, 12:00
Duração relativa	5 meses
Usuários	321
Inscrição automática	Sim

80,4%
258
Concluído

1ª Trilha de capacitação em Cibersegurança_Dez_2022

Grupos: Todos os usuários

Resumo da campanha

Status	Em andamento
Data de início	05/12/2022, 09:00
Duração relativa	5 meses
Usuários	321
Inscrição automática	Sim

73,5%
236
Concluído

Ações Realizadas em 2022/2023

Tribunal Regional Eleitoral-DF

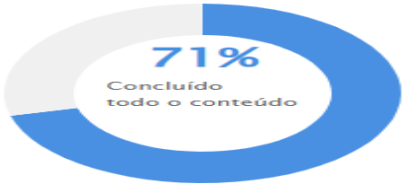
EI - 5: Sensibilização e Consciêntização

2ª Trilha de Capacitação em Cibersegurança - 2023

LGPD

Grupos: Todos os usuários

Resumo da campanha



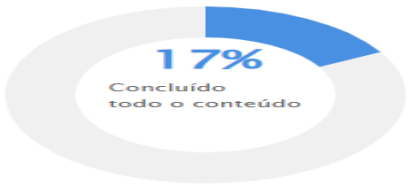
Status	Em andamento
Data de início	31/01/2023, 09:00
Duração relativa	5 meses
Usuários	321
Inscrição automática	Sim

71,3%
229
Concluído

2ª_Trilha_Capacitacao_Cibersegurança

Grupos: Todos os usuários

Resumo da campanha



Status	Em andamento
Data de início	04/09/2023, 09:00
Duração relativa	3 meses
Usuários	321
Inscrição automática	Sim

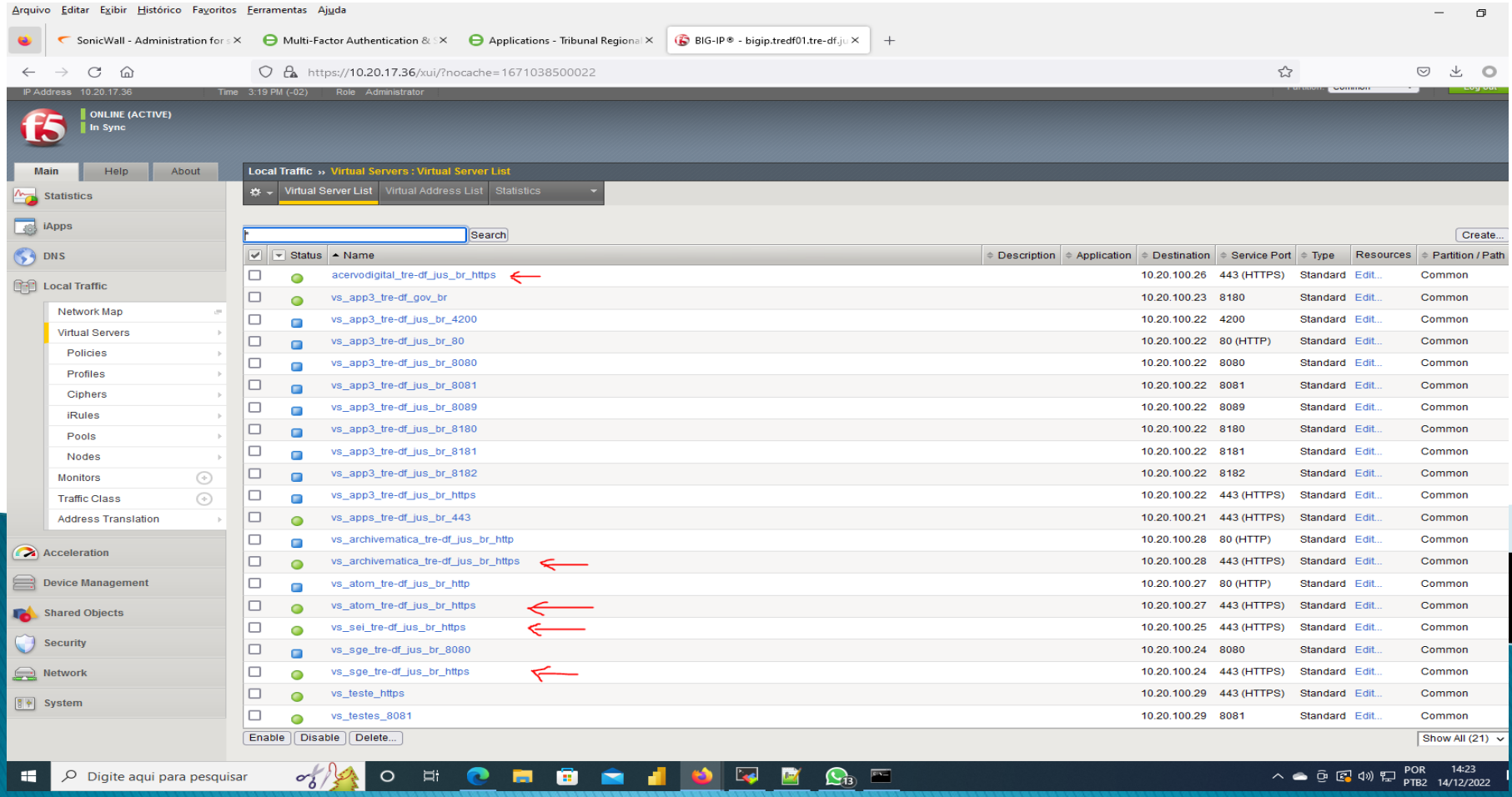
17,4%
56
Concluído

Atividades Rotineiras

Tribunal Regional Eleitoral-DF

Solução de Web Application Firewall - WAF

Aplicações monitoradas (bloking) : SEI, ATOM, ARQVEMÁTICA, Acervo Digital – Demais críticas em aprendizado

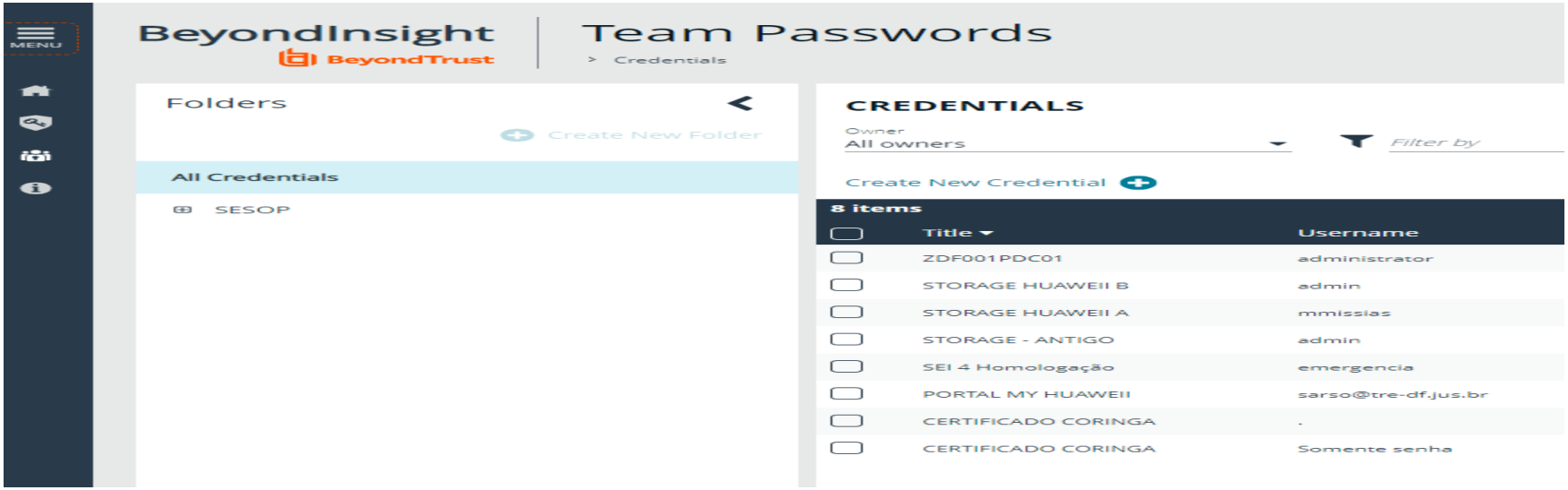


Atividades Rotineiras

Tribunal Regional Eleitoral-DF

Solução de Privileged Access Manager – BeyondTrust - (Cofre de senhas - TSE)

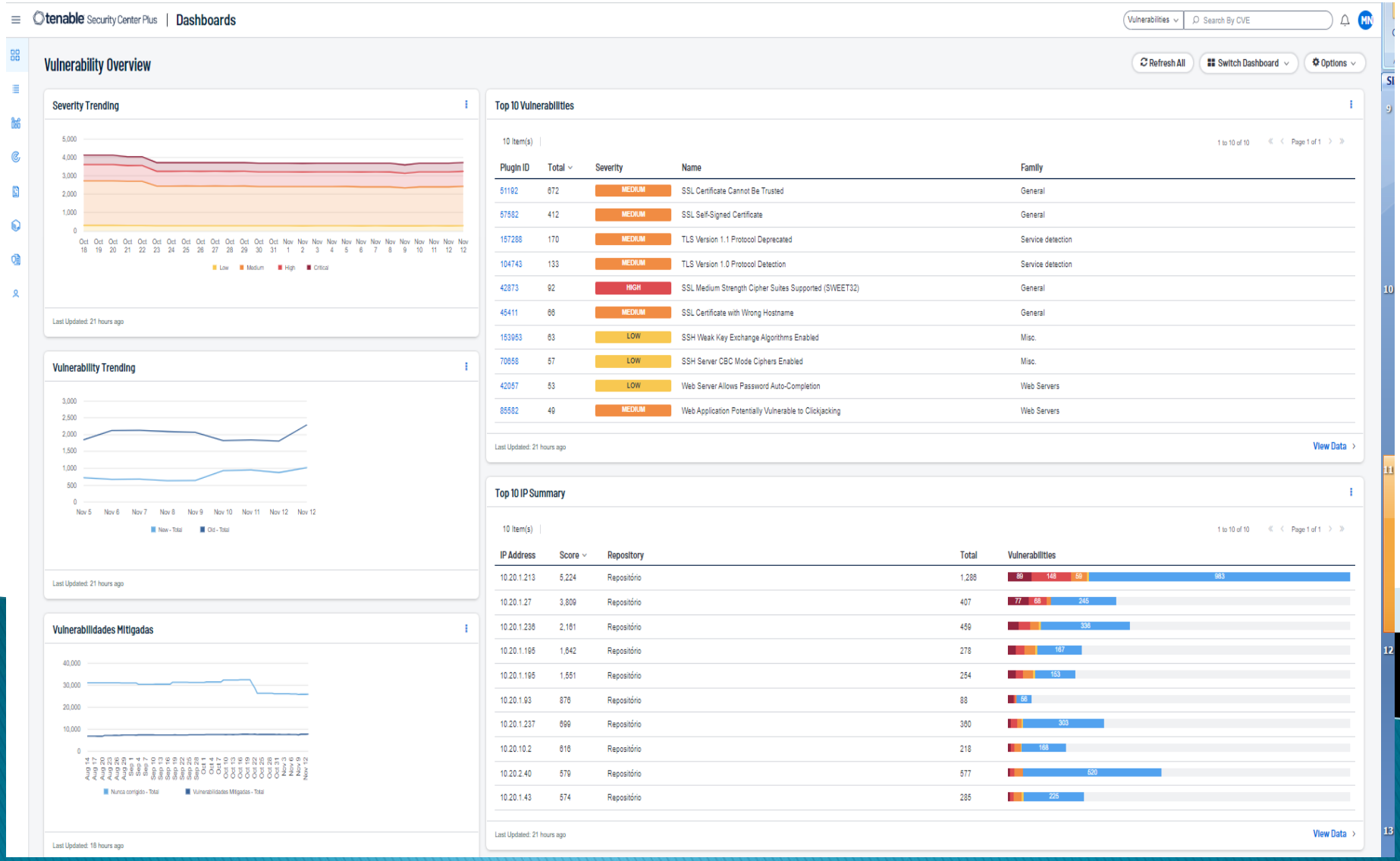
Credenciais em uso pelo cofre: Adm. do AD (Contas Oracle, de serviço e da SETEL em implementação)



Atividades Rotineiras

Tribunal Regional Eleitoral-DF

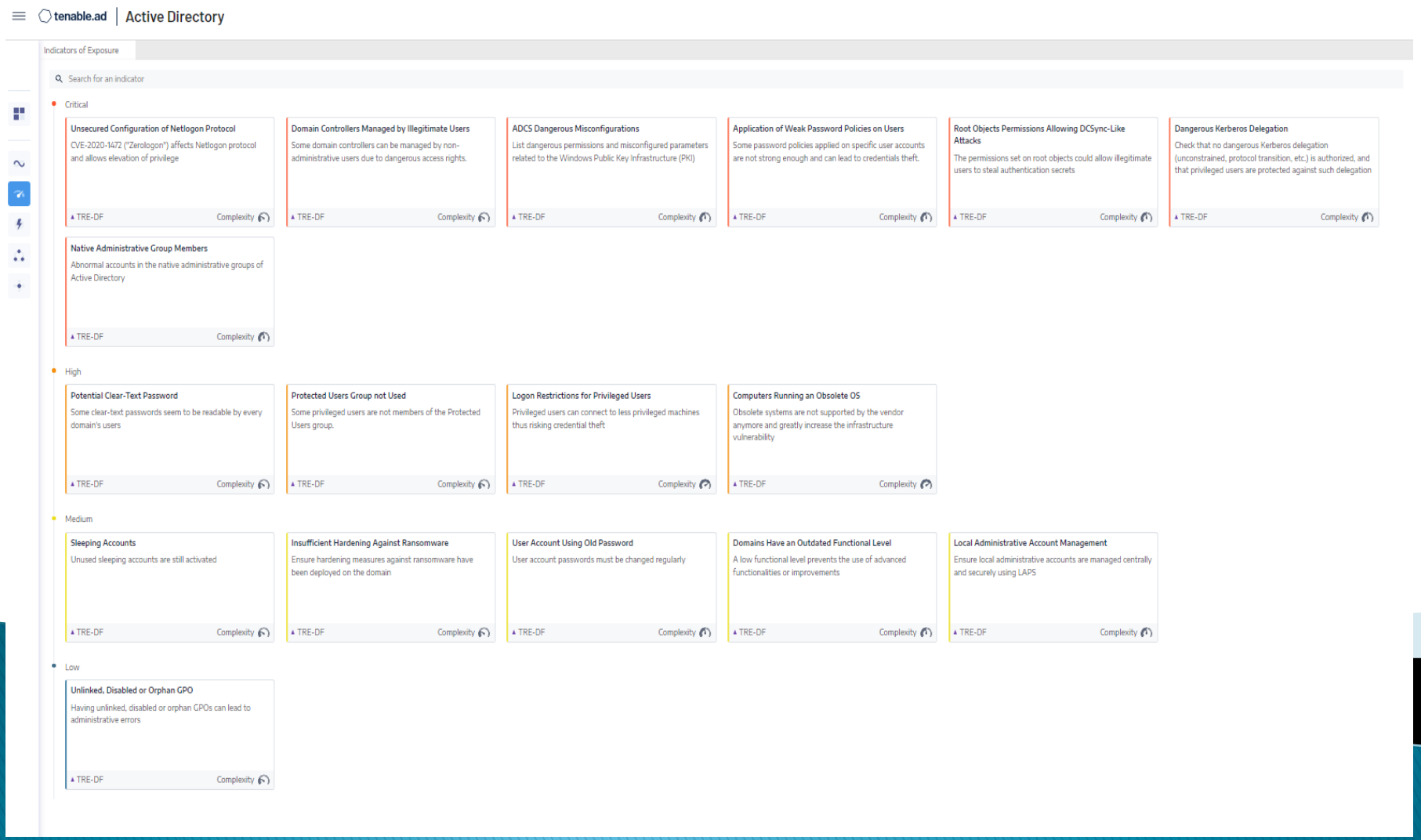
Solução de Gestão de Vulnerabilidade – TENABLE.SC



Atividades Rotineiras

Tribunal Regional Eleitoral-DF

Solução de Gestão de Vulnerabilidade – TENABLE.AD

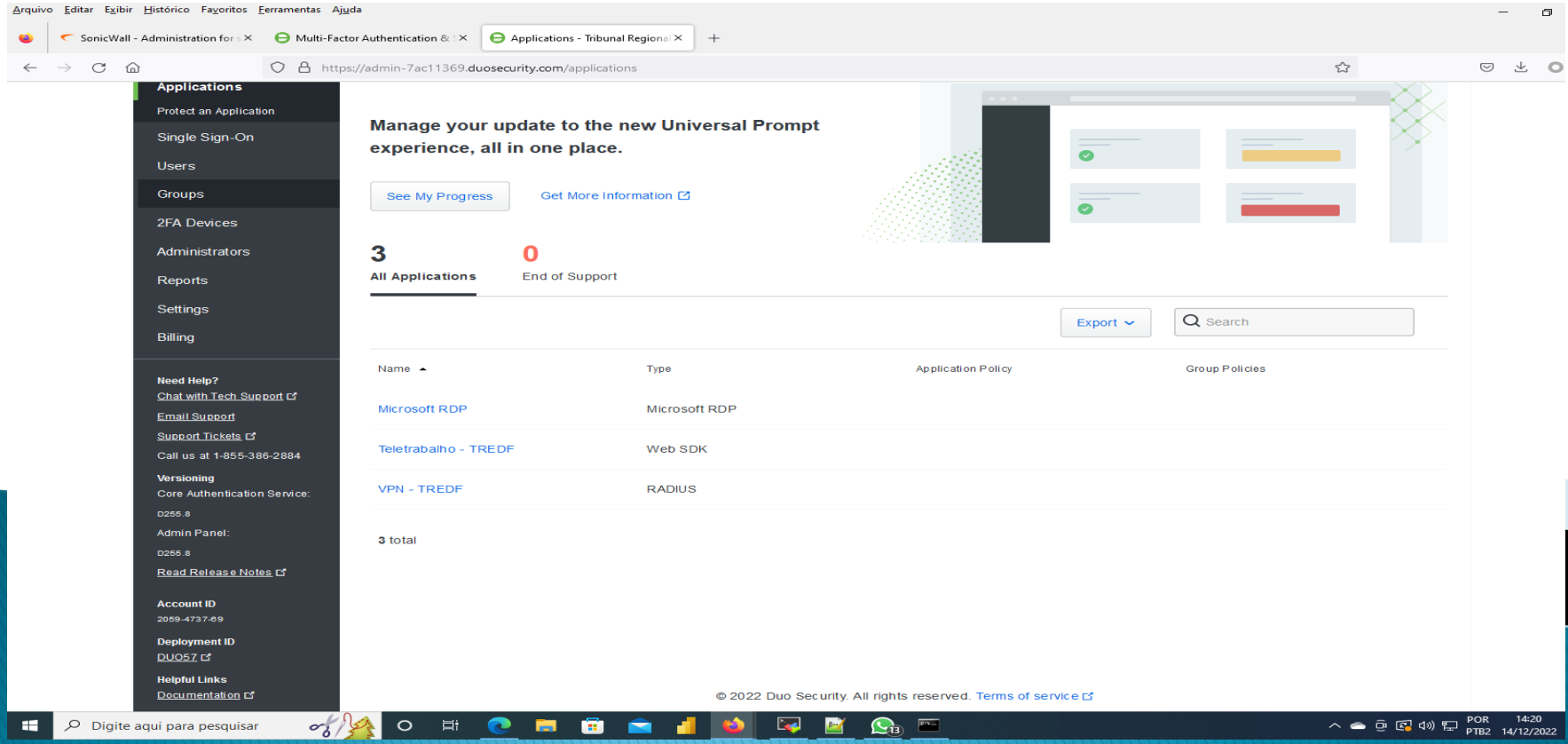


Ações realizadas por Projeto

Tribunal Regional Eleitoral-DF

Solução MFA – DUO | cisco

Aplicações onde será implantado: Acesso RDP, VPN SonicWall e Guacamole, Portal de Acesso remoto do F5, SEI e SGRH

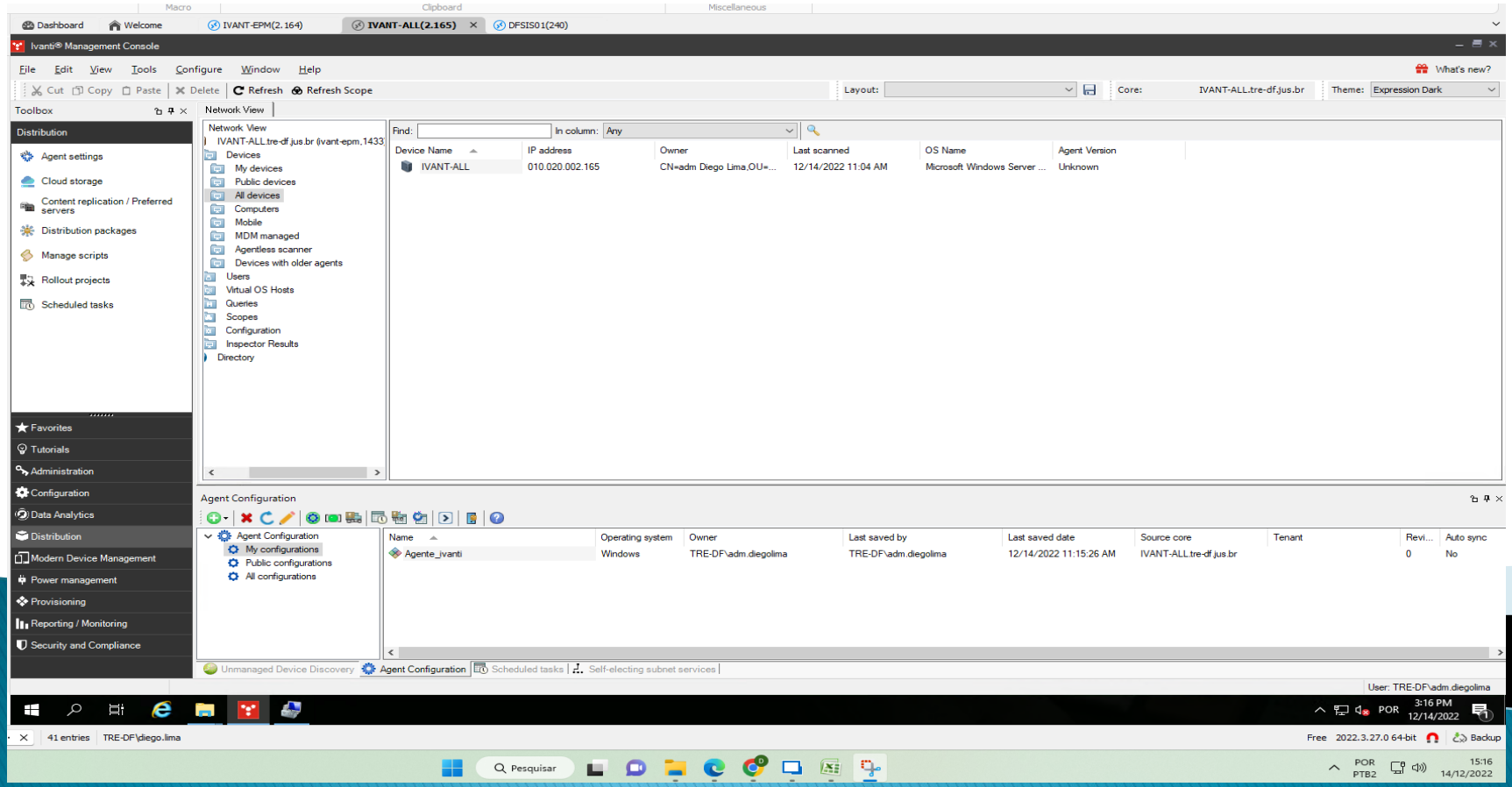


Ações realizadas por Projeto

Tribunal Regional Eleitoral-DF

Solução de Inventário e aplicação de Patchs – ivanti

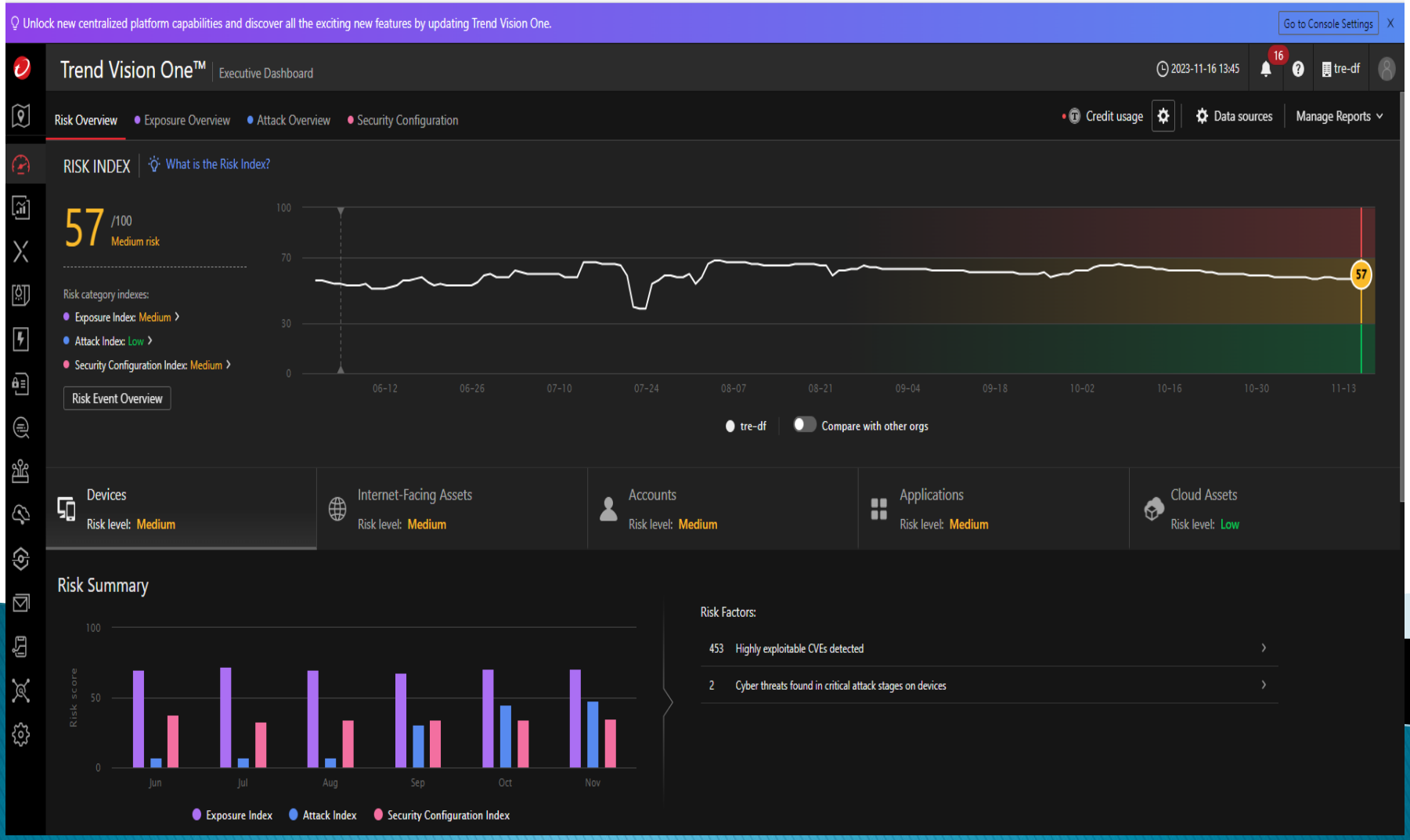
Solução instalada (Atende 800 desktops e 150 servidores)



Atividades Rotineiras

Tribunal Regional Eleitoral-DF

Solução de Gestão de Dispositivos – TRENDMICRO (Apex / Visio One)



Ações Futuras

Tribunal Regional Eleitoral-DF

EI- 1: Pessoas e Unidades Administrativas

1. Implementar a estrutura técnica mínima da equipe de ETIR (03 servidores)
    1.1 Terceirização de equipe – Nova contratação Service Desk - 2024
    1.2 Criar vagas para SI após estudo do TSE

EI- 2: Políticas e Normatização

1. Gestão de Riscos de SI – Jun/2024
2. Gestão de Vulnerabilidades e Padrões de Configuração – Set/2024
3. Plano de Continuidade de Serviços Essenciais TI – Out/2024
4. PPINC – 59% - Jun/2024
5. PGCRC – 55% - Ago/2024
6. PIILC – 47% - Set/2024
7. Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital – Port. CNJ nº 162/2021 – Nov/2024
8. Manual de Gestão de Identidade e Controle de Acesso – Port. CNJ nº 162/2021 – Dez/2024

Propostas

Tribunal Regional Eleitoral-DF

EI- 3: Ferramentas Automatizadas

1. Consumir a ARP da solução de análise avançada de Cibersegurança
2. Consumir a ARP da solução de auditoria de dados não estruturados – TRE-PA
3. Contratação de solução de modernização de backup – 2024
4. Contratação de solução de GRC + SIEM
5. Contrataçao de solução de SSE

EI- 4: Serviços Especializados

1. Consumir a ARP nº 2/2023 do TSE

EI- 5: Sensibilização e Conscientização

1. Aplicar novas capacitações em cibersegurança para todos os usuários

Tribunal Regional Eleitoral-DF

Obrigado