

1ª REUNIÃO DA CSI

16/11/2023

Tópicos

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

Legislação Aplicada

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

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

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)

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	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)	Sobreposição de funções do Gestor de Segurança da Informação com várias outras atribuições no Tribunal	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	Designação de Gestor de Segurança da Informação Dedicado junto à Presidência ou DG. 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

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

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)

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	Submissão, para aprovação, de normas táticas nos temas previstos na PSI.	Elaboração de fluxos operacionais para cada norma tática
TREs de Médio Porte (RN, AM, PA, PE, BA, CE, SC, GO, PB, PI, MA)	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
TREs de Grande Porte (SP, RS, MG, PR, RJ)		Submissão, para aprovação, de normas táticas nos temas previstos na PSI.	Divulgação e implantação de procedimentos e fluxos aprovados
		Submissão, para aprovação, de procedimentos e fluxos operacionais para cada norma tática.	Revisão das normas táticas e procedimentos operacionais

Norma Prevista	Situação
1. Gestão de Ativos	Port. PR. n° 241 /2023
2. Controle de Acesso Físico e Lógico	Port. PR. n° 27/2022 - Atualizar
3. Gestão de Riscos de SI	Pendente - Jun/2024
4. Uso Aceitável de Recursos de TI	Port. PR. n° 27/2022 - Atualizar
5. Geração e Restauração de Cópias de SI	Port. PR. n° 69/2021
6. Plano de Continuidade de Serviços Essenciais TI	0003655-96 - Atualizar Out/2024
7. Gestão de Incidentes de SI	Port. PR. N° 122/2021
8. Gestão de Vulnerabilidades e Padrões de Configuração	Pendente - Out/2024
9. Gestão e Monitoramento de Registros de Atividades (logs)	Port. PR. n° 27/2022 - Atualizar
10. Desenvolvimento Seguro de Sistemas	Pendente - Fev/2025
11. Uso de Recursos Criptográficos	Pendente - Jun/2025

Política de Segurança da Informação da J.E.

Normas Táticas Complementares de cada Tribunal

Procedimentos Operacionais de cada norma

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

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

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, configuradas 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 .
		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)	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 3 ³ .	Controles de cibersegurança implementados, automatizados e reportados à direção.
TREs de Grande Porte (SP, RS, MG, PR, RJ)		Aquisição, configuração e implantação de ferramentas de prioridade 2 ³ .		

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, McAfee, 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

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 Patches 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

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)

	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 TRÉs	<p>No TSE, há contratações em curso para Inteligência Cibernética, Apoio Técnico em Segurança e Apoio à Elaboração de Normas.</p> <p>No caso da maioria dos TRÉs, não há contratação de serviços especializados.</p>	<p>Conclusão da contratação de serviços especializados.</p> <p>Levantamento da maturidades do entes da J.E. (item 1 da tabela anterior)</p>	<p>Implantação e entrada em operação de SOC (item 2).</p> <p>Realização de capacitações para as equipes operacionais, para gestores táticos e para a alta gestão (item 3).</p> <p>Realização de simulações de ataque (item 5)</p>	<p>Realização de trilhas de treinamentos para unidades de Segurança de TI e ETIRs (item 4)</p> <p>Reavaliação de possíveis novos escopos de contratação de serviços especializados.</p>

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

Ações Realizadas em 2022/2023

EI - 5: Sensibilização e Consciência

	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

EI - 5: Sensibilização e Consciência



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_capitacao
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

EI - 5: Sensibilização e Consciência



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

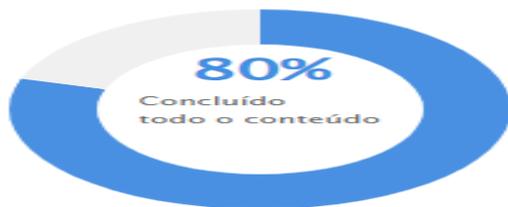
EI - 5: Sensibilização e Consciência

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**

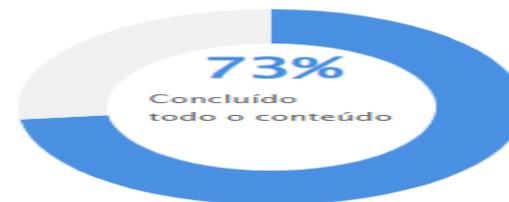
Inscrição automática **Sim**

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

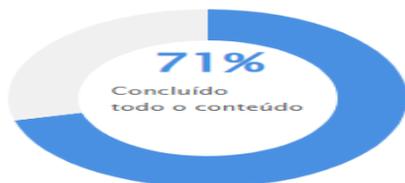
EI - 5: Sensibilização e Consciência

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**

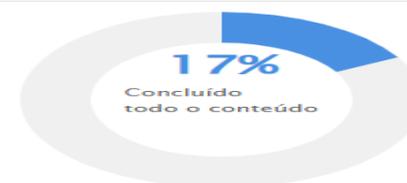
Inscrição automática **Sim**

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

Solução de Web Application Firewall - WAF



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

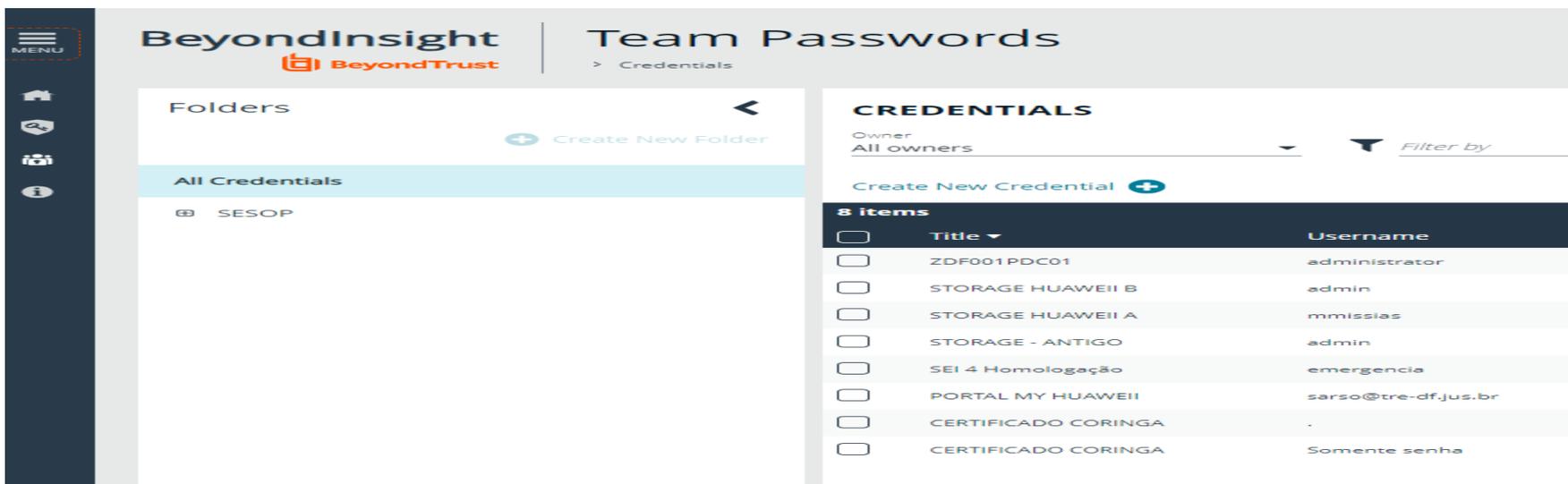
The screenshot shows the SonicWall Administration console interface. The main content area displays the 'Virtual Servers : Virtual Server List' page. A search bar is at the top of the table. The table has columns for Status, Name, Description, Application, Destination, Service Port, Type, Resources, and Partition / Path. Red arrows point to the following entries:

Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
ONLINE	acervodigital_tre-df_jus_br_https			10.20.100.26	443 (HTTPS)	Standard	Edit...	Common
ONLINE	vs_app3_tre-df_gov_br			10.20.100.23	8180	Standard	Edit...	Common
ONLINE	vs_app3_tre-df_jus_br_4200			10.20.100.22	4200	Standard	Edit...	Common
ONLINE	vs_app3_tre-df_jus_br_80			10.20.100.22	80 (HTTP)	Standard	Edit...	Common
ONLINE	vs_app3_tre-df_jus_br_8080			10.20.100.22	8080	Standard	Edit...	Common
ONLINE	vs_app3_tre-df_jus_br_8081			10.20.100.22	8081	Standard	Edit...	Common
ONLINE	vs_app3_tre-df_jus_br_8089			10.20.100.22	8089	Standard	Edit...	Common
ONLINE	vs_app3_tre-df_jus_br_8180			10.20.100.22	8180	Standard	Edit...	Common
ONLINE	vs_app3_tre-df_jus_br_8181			10.20.100.22	8181	Standard	Edit...	Common
ONLINE	vs_app3_tre-df_jus_br_8182			10.20.100.22	8182	Standard	Edit...	Common
ONLINE	vs_app3_tre-df_jus_br_https			10.20.100.22	443 (HTTPS)	Standard	Edit...	Common
ONLINE	vs_apps_tre-df_jus_br_443			10.20.100.21	443 (HTTPS)	Standard	Edit...	Common
ONLINE	vs_archivematica_tre-df_jus_br_http			10.20.100.28	80 (HTTP)	Standard	Edit...	Common
ONLINE	vs_archivematica_tre-df_jus_br_https			10.20.100.28	443 (HTTPS)	Standard	Edit...	Common
ONLINE	vs_atom_tre-df_jus_br_http			10.20.100.27	80 (HTTP)	Standard	Edit...	Common
ONLINE	vs_atom_tre-df_jus_br_https			10.20.100.27	443 (HTTPS)	Standard	Edit...	Common
ONLINE	vs_sei_tre-df_jus_br_https			10.20.100.25	443 (HTTPS)	Standard	Edit...	Common
ONLINE	vs_sge_tre-df_jus_br_8080			10.20.100.24	8080	Standard	Edit...	Common
ONLINE	vs_sge_tre-df_jus_br_https			10.20.100.24	443 (HTTPS)	Standard	Edit...	Common
ONLINE	vs_teste_https			10.20.100.29	443 (HTTPS)	Standard	Edit...	Common
ONLINE	vs_testes_8081			10.20.100.29	8081	Standard	Edit...	Common

Atividades Rotineiras

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

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



The screenshot displays the BeyondTrust Team Passwords interface. On the left, there is a navigation menu with icons for home, search, and information. The main content area is divided into two sections: 'Folders' and 'CREDENTIALS'. The 'Folders' section shows a single folder named 'SESOP'. The 'CREDENTIALS' section displays a list of 8 items with columns for 'Title' and 'Username'.

	Title	Username
<input type="checkbox"/>	ZDF001PDC01	administrator
<input type="checkbox"/>	STORAGE HUAWEII B	admin
<input type="checkbox"/>	STORAGE HUAWEII A	mmissias
<input type="checkbox"/>	STORAGE - ANTIGO	admin
<input type="checkbox"/>	SEI 4 Homologação	emergencia
<input type="checkbox"/>	PORTAL MY HUAWEII	sarso@tre-df.jus.br
<input type="checkbox"/>	CERTIFICADO CORINGA	.
<input type="checkbox"/>	CERTIFICADO CORINGA	Somente senha

Atividades Rotineiras

Solução de Gestão de Vulnerabilidade – TENABLE.SC

tenable Security Center Plus | Dashboards

Vulnerabilities Search By CVE Refresh All Switch Dashboard Options

Vulnerability Overview

Severity Trending

Last Updated: 21 hours ago

Vulnerability Trending

Last Updated: 21 hours ago

Vulnerabilidades Mitigadas

Last Updated: 19 hours ago

Top 10 Vulnerabilities

10 Item(s) 1 to 10 of 10 Page 1 of 1

Plugin ID	Total	Severity	Name	Family
51192	672	MEDIUM	SSL Certificate Cannot Be Trusted	General
57582	412	MEDIUM	SSL Self-Signed Certificate	General
157288	170	MEDIUM	TLS Version 1.1 Protocol Deprecated	Service detection
104743	133	MEDIUM	TLS Version 1.0 Protocol Detection	Service detection
42873	92	HIGH	SSL Medium Strength Cipher Suites Supported (SWEET32)	General
45411	86	MEDIUM	SSL Certificate with Wrong Hostname	General
153953	83	LOW	SSH Weak Key Exchange Algorithms Enabled	Misc.
70858	57	LOW	SSH Server CBC Mode Ciphers Enabled	Misc.
42057	53	LOW	Web Server Allows Password Auto-Completion	Web Servers
85582	49	MEDIUM	Web Application Potentially Vulnerable to Clickjacking	Web Servers

Last Updated: 21 hours ago View Data

Top 10 IP Summary

10 Item(s) 1 to 10 of 10 Page 1 of 1

IP Address	Score	Repository	Total	Vulnerabilities
10.20.1.213	5.224	Repositório	1.286	89 148 59 983
10.20.1.27	3.809	Repositório	407	77 68 245
10.20.1.238	2.181	Repositório	459	338
10.20.1.195	1.642	Repositório	278	167
10.20.1.195	1.551	Repositório	254	153
10.20.1.93	876	Repositório	88	66
10.20.1.237	899	Repositório	380	303
10.20.10.2	610	Repositório	218	168
10.20.2.40	579	Repositório	577	525
10.20.1.43	574	Repositório	285	225

Last Updated: 21 hours ago View Data

Atividades Rotineiras

Solução de Gestão de Vulnerabilidade – TENABLE.AD

tenable.ad | Active Directory

Indicators of Exposure

Search for an indicator

Critical

- Unsecured Configuration of Netlogon Protocol**
CVE-2020-1472 ("ZeroLogon") affects Netlogon protocol and allows elevation of privilege
TRE-DF Complexity
- Domain Controllers Managed by Illegitimate Users**
Some domain controllers can be managed by non-administrative users due to dangerous access rights.
TRE-DF Complexity
- ADCS Dangerous Misconfigurations**
List dangerous permissions and misconfigured parameters related to the Windows Public Key Infrastructure (PKI)
TRE-DF Complexity
- Application of Weak Password Policies on Users**
Some password policies applied on specific user accounts are not strong enough and can lead to credentials theft.
TRE-DF Complexity
- Root Objects Permissions Allowing DCSync-Like Attacks**
The permissions set on root objects could allow illegitimate users to steal authentication secrets
TRE-DF Complexity
- Dangerous Kerberos Delegation**
Check that no dangerous Kerberos delegation (unconstrained, protocol transition, etc.) is authorized, and that privileged users are protected against such delegation
TRE-DF Complexity
- Native Administrative Group Members**
Abnormal accounts in the native administrative groups of Active Directory
TRE-DF Complexity

High

- Potential Clear-Text Password**
Some clear-text passwords seem to be readable by every domain's users
TRE-DF Complexity
- Protected Users Group not Used**
Some privileged users are not members of the Protected Users group.
TRE-DF Complexity
- Logon Restrictions for Privileged Users**
Privileged users can connect to less privileged machines thus risking credential theft
TRE-DF Complexity
- Computers Running an Obsolete OS**
Obsolete systems are not supported by the vendor anymore and greatly increase the infrastructure vulnerability
TRE-DF Complexity

Medium

- Sleeping Accounts**
Unused sleeping accounts are still activated
TRE-DF Complexity
- Insufficient Hardening Against Ransomware**
Ensure hardening measures against ransomware have been deployed on the domain
TRE-DF Complexity
- User Account Using Old Password**
User account passwords must be changed regularly
TRE-DF Complexity
- Domains Have an Outdated Functional Level**
A low functional level prevents the use of advanced functionalities or improvements
TRE-DF Complexity
- Local Administrative Account Management**
Ensure local administrative accounts are managed centrally and securely using LAPS
TRE-DF Complexity

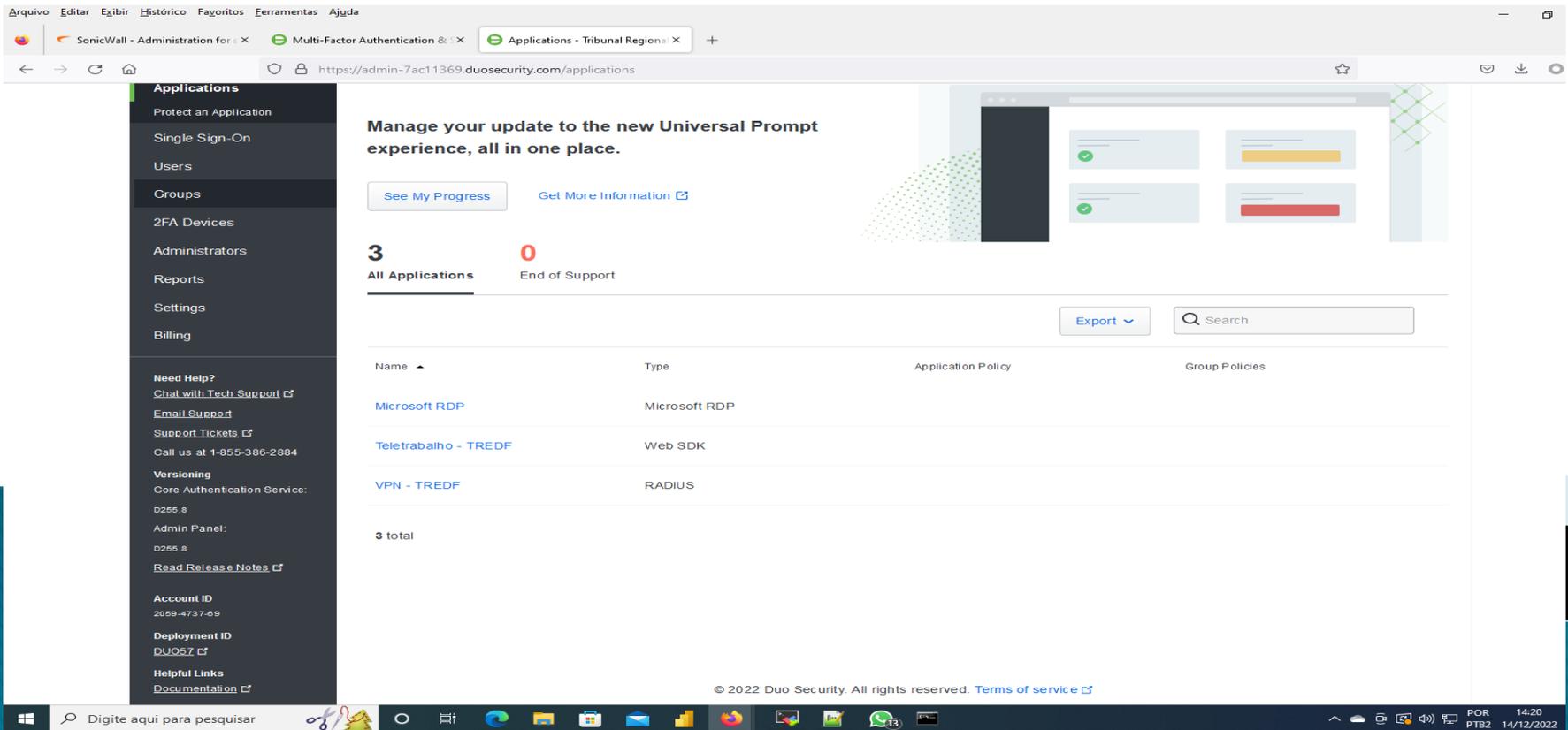
Low

- Unlinked, Disabled or Orphan GPO**
Having unlinked, disabled or orphan GPOs can lead to administrative errors
TRE-DF Complexity

Ações realizadas por Projeto

Solução MFA –  

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



The screenshot displays the Duo Security Administration console. The left sidebar contains navigation options: Applications, Protect an Application, Single Sign-On, Users, Groups, 2FA Devices, Administrators, Reports, Settings, Billing, Need Help?, Chat with Tech Support, Email Support, Support Tickets, Call us at 1-855-386-2884, Versioning, Core Authentication Service, Admin Panel, Read Release Notes, Account ID, Deployment ID, and Helpful Links. The main content area features a header with a message about the new Universal Prompt experience, a progress indicator showing 3 All Applications and 0 End of Support, and a table of applications. The table has columns for Name, Type, Application Policy, and Group Policies. The applications listed are Microsoft RDP, Teletrabalho - TREDF, and VPN - TREDF. The footer of the console shows the copyright notice: © 2022 Duo Security. All rights reserved. Terms of service.

Name	Type	Application Policy	Group Policies
Microsoft RDP	Microsoft RDP		
Teletrabalho - TREDF	Web SDK		
VPN - TREDF	RADIUS		

Ações realizadas por Projeto

Solução de Inventário e aplicação de Patches – **ivanti**

Solução instalada (Atende 800 desktops e 150 servidores)

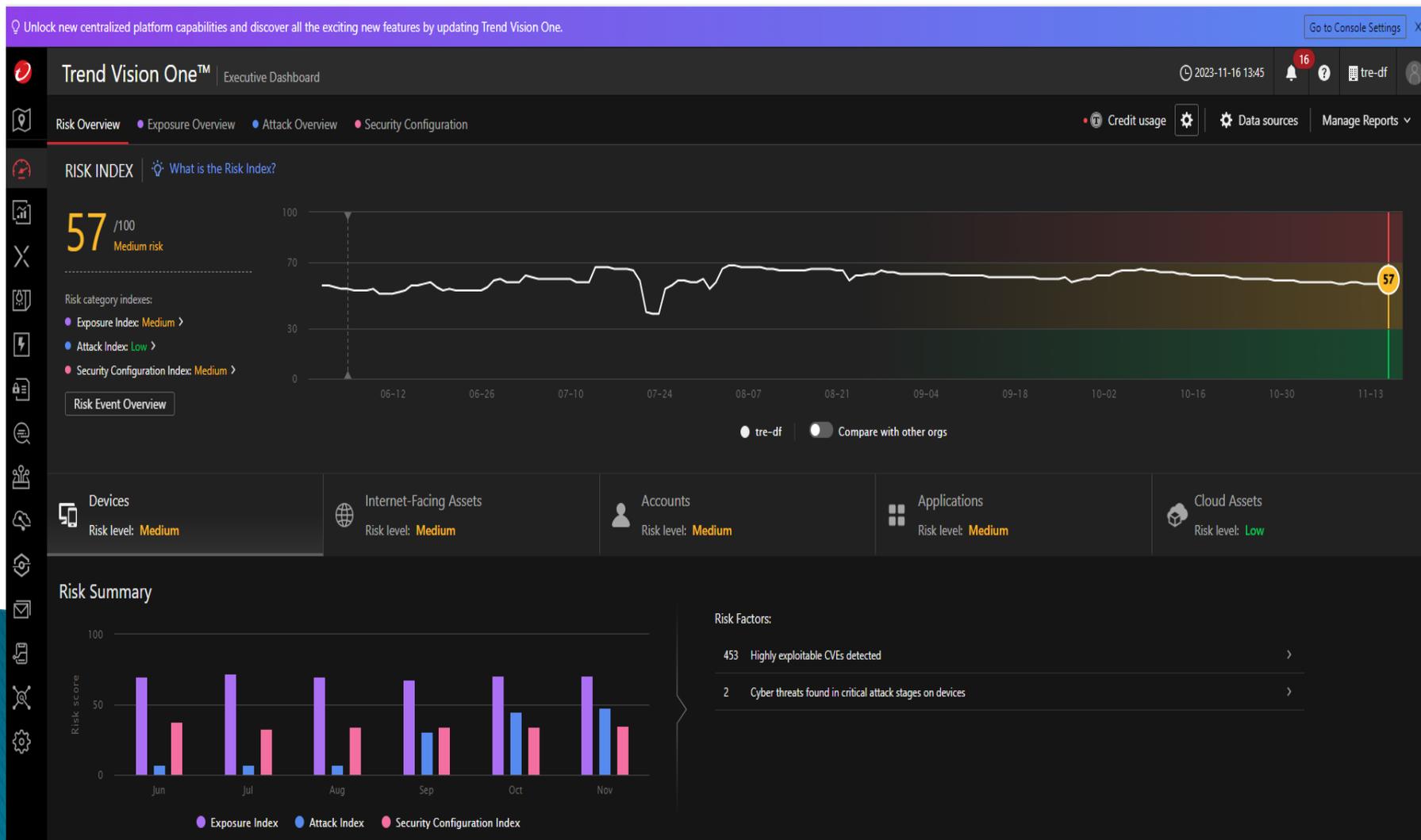
The screenshot displays the Ivanti Management Console interface. The top navigation bar includes 'Dashboard', 'Welcome', and several open tabs: 'IVANT-EPM(2.164)', 'IVANT-ALL(2.165)', and 'DFSISO1(240)'. The main interface is divided into several sections:

- Left Sidebar:** Contains navigation options such as 'Agent settings', 'Cloud storage', 'Content replication / Preferred servers', 'Distribution packages', 'Manage scripts', 'Rollout projects', 'Scheduled tasks', 'Favorites', 'Tutorials', 'Administration', 'Configuration', 'Data Analytics', 'Distribution', 'Modern Device Management', 'Power management', 'Provisioning', 'Reporting / Monitoring', and 'Security and Compliance'.
- Network View:** A table showing a list of devices. The table has columns for 'Device Name', 'IP address', 'Owner', 'Last scanned', 'OS Name', and 'Agent Version'. One device is listed: 'IVANT-ALL' with IP address '010.020.002.165', owned by 'CN=adm Diego Lima,OU=...', last scanned on '12/14/2022 11:04 AM', OS Name 'Microsoft Windows Server ...', and Agent Version 'Unknown'.
- Agent Configuration:** A table showing configuration details for 'Agente_ivanti'. The table has columns for 'Name', 'Operating system', 'Owner', 'Last saved by', 'Last saved date', 'Source core', 'Tenant', 'Revi...', and 'Auto sync'. The configuration is for 'Agente_ivanti' on 'Windows', owned by 'TRE-DF\adm.diegolima', last saved by 'TRE-DF\adm.diegolima' on '12/14/2022 11:15:26 AM', with source core 'IVANT-ALL.tre-df.jus.br', tenant 'TRE-DF', revision '0', and auto sync 'No'.

The bottom of the screenshot shows the Windows taskbar with the search bar, taskbar icons, and system tray showing the time as 3:16 PM on 12/14/2022.

Atividades Rotineiras

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



Ações Futuras

El- 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

El- 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

El- 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. Contratação de solução de SSE

El- 4: Serviços Especializados

1. Consumir a ARP nº 2/2023 do TSE

El- 5: Sensibilização e Conscientização

1. Aplicar novas capacitações em cibersegurança para todos os usuários

Obrigado