

# **REUNIÃO EXTRAORDINÁRIA DA CSI 05/2025**

# Tópicos

**Reporte incidentes recentes**

**Ações futuras e Melhorias**

# Reporte Incidentes Recentes

1. Usuário remoto com equipamento contaminado
2. Infecção por uso de mídia externa
3. Estagiários presos por aplicar golpes

# Reporte Incidentes Recentes

## 1. Usuário remoto com equipamento contaminado

**Data do incidente:** 13/02/2025

**Resumo do incidente:** XDR – TrendMicro, identificou SEPAG-001, alerta alto de vírus, aplicativo WinVNC comprometido

**Causa do incidente:** Uso de pendrive contaminado, que infectou versão antiga do WinVNC com malware.

### Ações realizadas:

- 1) Identificada usuário e IP da máquina;
- 2) Identificada fonte da contaminação (D:/);
- 3) Identificado arquivo contaminado (ferramenta de backdoor – hacktool.winvnc);
- 4) Laptop institucional recolhido para análise profunda;
- 5) Laptop formatado pela equipe da SEAPU;
- 6) Orientações quanto ao procedimento para uso de mídias.

# Reporte Incidentes Recentes

## 2. Infecção por uso de mídia externa

**Data do incidente:** 12/03/2025

**Resumo do incidente:** XDR – TrendMicro, identificou ZDF001WKS36, alerta alto, 253 vírus.

**Causa do incidente:** Necessidade de cópia de mídias de processo para disponibilização para consulta pelas partes envolvidas

### **Ações realizadas:**

- 1) Identificada usuária e IP da máquina;
- 2) Identificada fonte da contaminação (F:);
- 3) Identificados arquivos contaminados (ferramentas de hacking, backdoor, exploit);
- 4) Desktop isolado da rede;
- 5) Identificamos contaminação lateral nas máquinas ZDF001WKS26 e ZDF001WKS24;
- 6) Senhas de todos os usuários das máquinas infectadas foram resetadas;
- 7) Todas as máquinas recolhidas e formatadas pela equipe da SEAPU;
- 8) Orientações quanto ao procedimento de cópia de mídias.
- 9) Instalação de equipamento específico para realização das cópias de mídias fora da rede;
- 10) Abertura de processo SEI relatando a ocorrência (0002195-30.2025.6.07.8100).

# Reporte Incidentes Recentes

## 3. Estagiários presos por aplicar golpes

Data do incidente: 31/03/2025

Resumo do incidente: Estagiários do TRE-DF presos por aplicar golpes com documentos falsificados

### Ações realizadas:

- 1) Contas no AD e no Google Workspace desativadas;
- 2) Verificados e-mails, google drive e demais serviços do Google Workspace;
- 3) Verificado logs dos acessos á rede e domínio do TRE-DF;

# Ações Futuras e Melhorias

- 1. Ativação de bloqueio de dispositivo de armazenamento externo**
- 2. Automação de isolamento de desktop da rede interna**
- 3. Substituição do ILovePDF pelo STIRLING**
- 4. Remoção dos links disponibilizado no Google Drive**
- 5. Divulgação e publicidade para todos usuários antes das ativações**

# Ações Futuras e Melhorias

## 1. Ativação de bloqueio de dispositivo de armazenamento externo

Trend Vision One™ Standard Endpoint Protection

2025-04-30 15:17

Dashboard Directories Policies Suspicious Object Sync Investigation Logs & Reports Administration

Policy Management

- Policy Management
- Policy Resources >

Product: Apex One Security A...

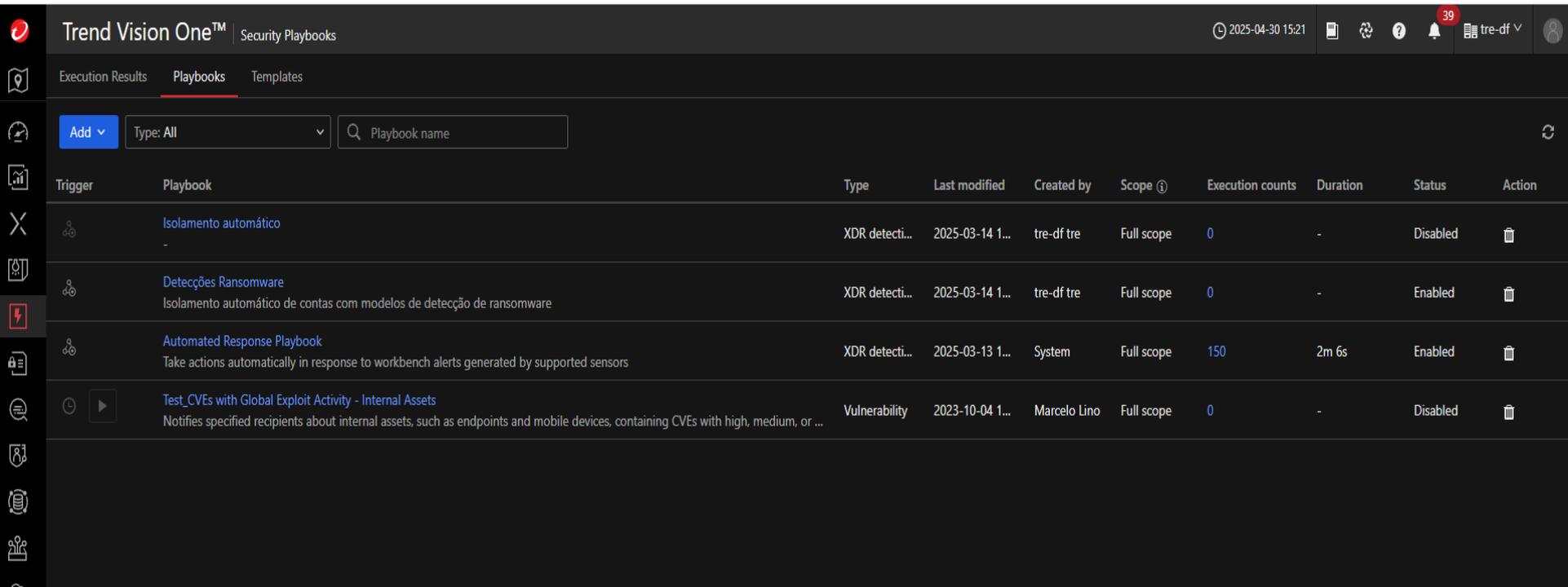
+ Create Copy Settings Inherit Settings Import Settings Export Settings Delete Reorder Change Owner Refresh

<input type="checkbox"/>	Priority	Policy	Policy Version	Parent Policy	Deviations	Owner	Last Editor	Last Edited	Targets ↑	Deployed
<input type="checkbox"/>	Locked	Bloqueio_USB_Armazename nto	1745860666	N/A	N/A	carlos.ferreira@tre-df.jus.br	carlos.ferreira@tre-df.jus.br	04/28/2025 14:17:46	✦ Specified	11
<input type="checkbox"/>	Locked	SISPOL	1742924856	N/A	N/A	carlos.ferreira@tre-df.jus.br	carlos.ferreira@tre-df.jus.br	03/25/2025 14:47:36	✦ Specified	4
<input type="checkbox"/>	Locked	SEDE	1730147460	N/A	N/A	pcarvalho@tre-df.jus.br	pcarvalho@tre-df.jus.br	10/28/2024 17:31:00	✦ Specified	0
<input type="checkbox"/>	1	Desktops	1744655579	N/A	N/A	carlos.ferreira@tre-df.jus.br	carlos.ferreira@tre-df.jus.br	04/14/2025 15:32:59	🏷 Labels	725
<input type="checkbox"/>	2	Servidores	1743008588	N/A	N/A	carlos.ferreira@tre-df.jus.br	carlos.ferreira@tre-df.jus.br	03/26/2025 14:03:08	🏷 Labels	60
									Total:	800

Endpoints/Products without policies: 0

# Ações Futuras e Melhorias

## 2. Automação de isolamento de desktop da rede interna



The screenshot displays the Trend Vision One Security Playbooks interface. The top navigation bar includes the product name, a date and time indicator (2025-04-30 15:21), and user information (tre-df). Below the navigation bar, there are tabs for Execution Results, Playbooks (selected), and Templates. A search bar and a filter dropdown (Type: All) are present. The main content area is a table listing various playbooks.

Trigger	Playbook	Type	Last modified	Created by	Scope	Execution counts	Duration	Status	Action
	Isolamento automático	XDR detecti...	2025-03-14 1...	tre-df tre	Full scope	0	-	Disabled	
	Detecções Ransomware Isolamento automático de contas com modelos de detecção de ransomware	XDR detecti...	2025-03-14 1...	tre-df tre	Full scope	0	-	Enabled	
	Automated Response Playbook Take actions automatically in response to workbench alerts generated by supported sensors	XDR detecti...	2025-03-13 1...	System	Full scope	150	2m 6s	Enabled	
	Test_CVEs with Global Exploit Activity - Internal Assets Notifies specified recipients about internal assets, such as endpoints and mobile devices, containing CVEs with high, medium, or ...	Vulnerability	2023-10-04 1...	Marcelo Lino	Full scope	0	-	Disabled	

# Ações Futuras e Melhorias

## 3. Substituição do ILovePDF pelo STIRLING

### 3. [http://web-stirling-pdf.apps.ocp-hml.tre-df.jus.br/?lang=pt\\_BR](http://web-stirling-pdf.apps.ocp-hml.tre-df.jus.br/?lang=pt_BR)

Seu tudo-em-um hospedado localmente para tudo relacionado a PDFs

Novos e Recentemente Atualizados



Ocultação de Texto Manual



Multiferramentas de PDF



Verificar Assinatura com Certificado

🔍 Pesquisar funcionalidades...

Ordenar por: Alfabética



#### Organizar

- Ajustar Dimensões da Página
- Dividir
- Extrair Página(s)
- Girar
- Layout de Múltiplas Páginas
- Mesclar
- Multiferramentas de PDF
- Organizar Páginas
- PDF para Página Única

#### Converter para PDF

- Converter Arquivo para PDF
- Converter URL/Site para PDF
- HTML para PDF
- Imagem para PDF
- Markdown para PDF

#### Converter de PDF

- PDF para Apresentação
- PDF para CSV
- PDF para HTML
- PDF para Imagem
- PDF para Markdown
- PDF para PDF/A
- PDF para TXT/RTF
- PDF para Word
- PDF para XML

#### Assinatura & Segurança

- Adicionar Carimbo ao PDF
- Adicionar Marca d'água
- Alterar Permissões
- Assinar
- Assinar com Certificado
- Desproteger PDF
- Higienizar
- Ocultação de Texto Automática
- Ocultação de Texto Manual

#### Visualizar & Editar

- Achatar
- Adicionar Imagem
- Adicionar Números de Página
- Alterar Metadados
- Comparar
- Extrair Imagens
- Obter Informações de um PDF
- Processamento de OCR
- Remover Anotações

#### Avançado

- Ajuste Visual do PDF
- Comprimir
- Detectar/Dividir Fotos Digitalizadas
- Divide PDF por Capítulos
- Dividir PDF por Seções
- Divisão Automática de Páginas
- Divisão Manual do PDF
- Mostrar Javascript
- Pipeline

# Ações Futuras e Melhorias

## 4. Remoção dos links disponibilizado no Google Drive

VARONIS

Investigation × Resources × +

### Resources

Match: All filters Deleted: False Tags: (Match any) shared externally + Add Filter Clear Filter

Showing 11,680 results [Select Columns](#) [Export](#)

<input type="checkbox"/>	Name	Type	Service	Last Viewed	Last Modified	Category	Tags
<input type="checkbox"/>	 Relação de Funcionár... File	File	 tre-df.jus.br	--	Apr 29, 2025 11:12 AM (GMT-3:00)		<span>no expiration</span> <span>shared externally</span>
<input type="checkbox"/>	 RE TRE.pdf File	File	 tre-df.jus.br	Apr 29, 2025 10:52 PM (GMT-3:00)	Apr 23, 2025 01:48 PM (GMT-3:00)		<span>no expiration</span> <span>shared externally</span>
<input type="checkbox"/>	 Detalhamento GFD R... File	File	 tre-df.jus.br	Apr 29, 2025 10:53 PM (GMT-3:00)	Apr 10, 2025 03:21 PM (GMT-3:00)		<span>no expiration</span> <span>shared externally</span>
<input type="checkbox"/>	 TRCT - TATIANA DO N... File	File	 tre-df.jus.br	Apr 29, 2025 10:53 PM (GMT-3:00)	Apr 10, 2025 03:21 PM (GMT-3:00)		<span>no expiration</span> <span>shared externally</span>
<input type="checkbox"/>	 Comprovante GRF re... File	File	 tre-df.jus.br	Apr 29, 2025 10:53 PM (GMT-3:00)	Apr 10, 2025 03:21 PM (GMT-3:00)		<span>no expiration</span> <span>shared externally</span>
<input type="checkbox"/>	 Comprovante GRRF O... File	File	 tre-df.jus.br	Apr 29, 2025 10:53 PM (GMT-3:00)	Apr 10, 2025 03:21 PM (GMT-3:00)		<span>no expiration</span> <span>shared externally</span>
<input type="checkbox"/>	 RET TRE.pdf File	File	 tre-df.jus.br	Apr 29, 2025 10:52 PM (GMT-3:00)	Apr 23, 2025 01:48 PM (GMT-3:00)		<span>no expiration</span> <span>shared externally</span>

# Obrigado