



mindthesec[™]

2025

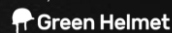


O MAIOR E MAIS QUALIFICADO EVENTO DE CYBER SECURITY DA AMÉRICA LATINA

MAIS UM EVENTO



REALIZAÇÃO



Aviso legal / Disclaimer / Descargo de responsabilidad

As apresentações destinam-se apenas a fins educacionais e não substituem o julgamento profissional independente. As declarações de fato e opiniões aqui expressas são de total responsabilidade dos participantes e não representam a opinião ou posição do Mind The Sec ou de quaisquer outros co-patrocinadores. O Mind The Sec não endossa, aprova ou assume responsabilidade pelo conteúdo, precisão ou integridade das informações aqui apresentadas. Os participantes devem observar que as sessões podem ser gravadas em áudio ou vídeo e podem ser publicadas em diversos meios, incluindo formatos impressos, de áudio e vídeo, sem aviso prévio adicional. O modelo de apresentação e qualquer captura de mídia estão sujeitos à proteção por direitos autorais.

The presentations are intended for educational purposes only and are not a substitute for independent professional judgment. The statements of fact and opinions expressed herein are solely the responsibility of the participants and do not represent the opinion or position of Mind The Sec or any other co-sponsors. Mind The Sec does not endorse, approve or assume responsibility for the content, accuracy or integrity of the information presented here. Participants should note that sessions may be audio or video recorded and may be published in a variety of media, including print, audio and video formats, without further notice. The presentation template and any media capture are subject to copyright protection.

Las presentaciones están destinadas únicamente a fines educativos y no sustituyen el juicio profesional independiente. Las declaraciones de hecho y las opiniones aquí expresadas son las de los participantes y no representan la opinión o posición de Mind The Sec ni de ningún otro copatrocinador. Mind The Sec no respalda, aprueba ni asume responsabilidad por el contenido, exactitud o integridad de la información aquí presentada. Los participantes deben tener en cuenta que las sesiones pueden grabarse en audio o vídeo y publicarse en diversos medios, incluidos los formatos impreso, de audio y de vídeo, sin previo aviso. La plantilla de presentación y cualquier captura multimedia están sujetas a la protección de los derechos de autor.

Fortalecendo a Segurança Institucional: Implantação dos Controles CIS e a Proteção Avançada



quem sou eu



Édipo Avelino dos Santos Palha é um experiente profissional de TI com mais de 16 anos de atuação no setor, especializado em segurança da informação.

Graduado em Sistemas de Informação, especializou-se em Computação Forense e Perícia Digital pelo Instituto de Pós-graduação (IPOG) de Osasco-SP e em Rede e Computação Distribuída pelo Instituto Federal de Mato Grosso (IFMT).

Atualmente, é Chief Information Officer (CIO) do Ministério Público do Estado de Mato Grosso (MPMT) e Coordenador do Comitê de Governança da ANETI (Associação Nacional dos Especialistas em TI).

Algumas Certificações: EC-Council CEH, EC-Council EHE, EC-Council CSCI, EXIN ISFS ISO27001, Comptia Security+, ITIL4.

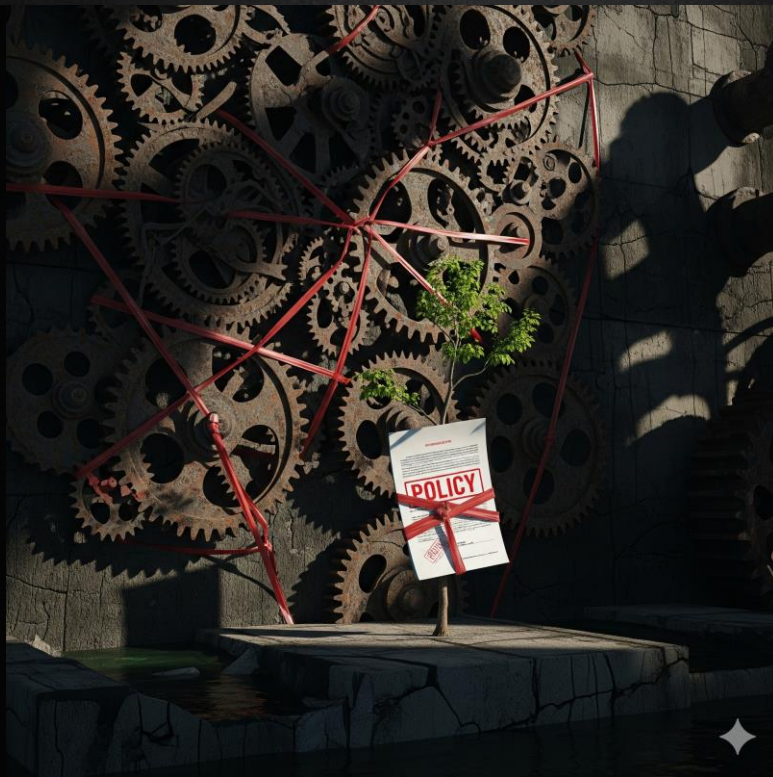


Édipo Avelino

CIO do Ministério Público do
Estado de Mato Grosso

Desafios

- 1 – A necessidade de uma estrutura de segurança cibernética robusta.
- 2 - Continuidade do projeto com a inevitável e contínua troca de gestão.
- 3 – Como traduzir a estratégia em ação prática.



Necessidade de uma estrutura de segurança robusta

- Implementar um framework de segurança da informação (Estabelecer a direção).
- O Conselho Nacional dos Ministérios Públicos (CNMP) recomendou a implementação dos **Controles CIS** nos Ministérios Públicos.
- O TCU publicou um documento que recomenda a implementação dos **Controles CIS**.

10100
010011-
10100

Cinco controles de segurança cibernética para ontem

10100
010011
10100



Continuidade do projeto com a inevitável e contínua troca de gestão

- Institucionalizar o projeto.
- Incluímos como um **Projeto Estratégico** do Planejamento Estratégico Institucional (PEI).



Traduzir a estratégia em ação

- O **NIST CSF** oferece um plano estratégico amplo.
- Os **Controles CIS** oferecem um “mapa rodoviário” prático e detalhado.





Host Info

- Name
- IP/MAC address
- Active Users
- OS/use of Active Directory

Process details

- File process path
- Process commands
- PID
- Parent process path
- User
- Logon session ID
- Session type (interactive, remote, etc.)
- Process integrity level
- User membership in privileged groups

Verdict

- Detect type (i.e. on execute)
- Response status (Quarantined/Disinfected)
- Detection technology

File/suspicious process description

- File Type
- File path
- Hash (Md5/Sha256)
- Size
- Creation /Change date
- Owner
- Attributes
- ADS value
- Signature, etc.

File appearance history

- First identified execution
- Number of executions
- Process path that changed the file, etc.

Network connections

- URL
- Referrer
- User Agent
- Request type GET/POST

Autorun detects

- Detected object type (service image path, reg key, WMI, Ink, etc.)
- Registry key edits
- Service installation date, etc.

Estabelecer um conjunto organizado e priorizado de práticas recomendadas em segurança cibernética e medidas defensivas no ambiente tecnológico, que auxiliem na prevenção de ataques cibernéticos.

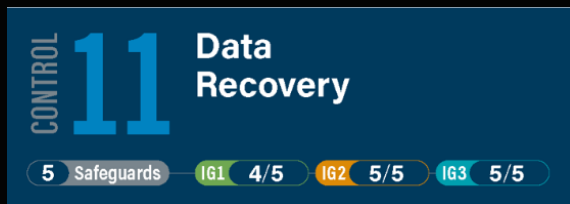


Fonte: <https://www.cisecurity.org/controls/implementation-groups>

CONTROL 01 Inventory and Control of Enterprise Assets 5 Safeguards 161 2/5 162 4/5 163 5/5	CONTROL 02 Inventory and Control of Software Assets 7 Safeguards 161 3/7 162 6/7 163 7/7	CONTROL 03 Data Protection 14 Safeguards 161 6/14 162 12/14 163 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software 12 Safeguards 161 7/12 162 11/12 163 12/12	CONTROL 05 Account Management 6 Safeguards 161 4/6 162 6/6 163 6/6	CONTROL 06 Access Control Management 8 Safeguards 161 5/8 162 7/8 163 8/8
CONTROL 07 Continuous Vulnerability Management 7 Safeguards 161 4/7 162 7/7 163 7/7	CONTROL 08 Audit Log Management 12 Safeguards 161 3/12 162 11/12 163 12/12	CONTROL 09 Email and Web Browser Protections 7 Safeguards 161 2/7 162 6/7 163 7/7
CONTROL 10 Malware Defenses 7 Safeguards 161 3/7 162 7/7 163 7/7	CONTROL 11 Data Recovery 5 Safeguards 161 4/5 162 5/5 163 5/5	CONTROL 12 Network Infrastructure Management 8 Safeguards 161 1/8 162 7/8 163 8/8
CONTROL 13 Network Monitoring and Defense 11 Safeguards 161 0/11 162 6/11 163 11/11	CONTROL 14 Security Awareness and Skills Training 9 Safeguards 161 8/9 162 9/9 163 9/9	CONTROL 15 Service Provider Management 7 Safeguards 161 1/7 162 4/7 163 7/7
CONTROL 16 Applications Software Security 14 Safeguards 161 0/14 162 11/14 163 14/14	CONTROL 17 Incident Response Management 9 Safeguards 161 3/9 162 8/9 163 9/9	CONTROL 18 Penetration Testing 5 Safeguards 161 0/5 162 3/5 163 5/5

Controles CIS – SAFEGUARDS

Os **Safeguards** constituem um subconjunto dos 18 controles da CIS e são definidos como um conjunto de práticas e medidas específicas destinadas a proteger sistemas e redes contra ameaças cibernéticas.



Fonte: <https://www.cisecurity.org/controls/v8-1>

Safeguard 11.1: Establish and Maintain a Data Recovery Process

Asset Type: **Documentation** Security Function: **Govern** **IG1** **IG2** **IG3**

Establish and maintain a documented data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 11.2: Perform Automated Backups

Asset Type: **Data** Security Function: **Recover** **IG1** **IG2** **IG3**

Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.

Safeguard 11.3: Protect Recovery Data

Asset Type: **Data** Security Function: **Protect** **IG1** **IG2** **IG3**

Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

Safeguard 11.4: Establish and Maintain an Isolated Instance of Recovery Data

Asset Type: **Data** Security Function: **Recover** **IG1** **IG2** **IG3**

Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.

Safeguard 11.5: Test Data Recovery

Asset Type: **Data** Security Function: **Recover** **IG2** **IG3**

Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.



153
TOTAL
SAFEGUARDS

IG3

IG3 assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23 SAFEGUARDS

IG2

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74
SAFEGUARDS

IG1

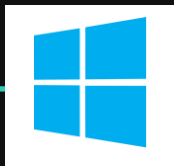
IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56 SAFEGUARDS

Controls?_gl=1*ir73xv*_gcl_au*MTI1MzM3Mzg1Ni4xNzUxOTMzNzMyLjg0NzAyNDEzOS4xNzU2NzcyNDMwLjE3NTY3NzI0NTY.*_ga*MTU1NzM4ODcxOS4xNzQyNjM1OTQ1*_ga_N70Z2MKMD7*czE3NTY3ODAzNzIkbzEwJGcxJHoxNzU2NzgxNigwJGozNSRsMCRoMA.*_ga_3FW1B1JC98*czE3NTY3ODAzNzIkbzEwJGcxJHoxNzU2NzgxNigwJGozNSRsMCRoMA..



Solução completa de gerenciamento, detecção e reposta de incidentes de endpoint



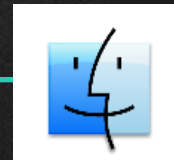
Windows OS

Proteger os desktops,
servidores e máquinas
virtuais no Windows com
recursos de EDR



Linux OS

Proteger as máquinas
baseadas em Linux com
recursos EDR



Mac OS

Proteger as máquinas
no Mac OS com
recursos de EDR

Detecção e resposta automáticas a ameaças avançadas em qualquer dispositivo

Como medir o progresso?

- Avaliação de 0 a 5.
- A nota é determinada com base nas respostas às perguntas a seguir para cada Safeguard:
 - 1- A política está aprovada?
 - 2- O controle foi implementado?
 - 3- O controle é automatizado?
 - 4- O controle é reportado?



Ferramentas dos Controles CIS



CIS BENCHMARKS



CIS CSAT



CONTROLES CIS

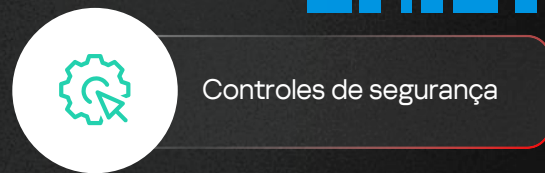


Fonte: <https://www.cisecurity.org/controls/implementation-groups>

Principais capacidades da solução

Controles de segurança e fortalecimento do sistema

- Controle de Aplicativos
- Controle de Dispositivos
- Controle da Web
- Verificação de vulnerabilidades
- Inventário de hardware e software
- Gerenciamento de criptografia



Fortalecimento do sistema

Verificação de vulnerabilidades

Visão geral compreensiva dos aplicativos instalados nos dispositivos corporativos, junto com uma lista de correções disponíveis, assegurando que todo software esteja atualizado e seguro

Detecção e Respostas automatizadas

Ferramenta para gerenciar e tomar ações proativas, assegurando que o ambiente esteja em conformidade com as políticas de segurança corporativas

Inventário de hardware e software

Visão geral dos ativos, marcando software desatualizado

Gerenciamento de criptografia

Gerenciamento de todos os endpoints através de um console para controlar criptografia de arquivos e discos

1 - Levantar os safeguards que já estão em implantados.

3 - Entre os safeguards não implantados, identificar aqueles que podem ser aplicados com as ferramentas e a infraestrutura disponíveis.

4 - Para os safeguards restantes, verificar quais podem ser implementados por meio de **software open-source**.

5 - Para os safeguards que ainda faltam, identificar as soluções que precisam ser adquiridas.



Projeto em execução - Desafios

- Equilíbrio entre as tarefas diárias e as atividades do projeto.
- A metodologia SCRUM ajudou a manter esse equilíbrio.



Resultados Alcançados

01

IDENTIFICAÇÃO DE
VULNERABILIDADES
DESCONHECIDAS PELA
INSTITUIÇÃO

02

ATENDIMENTO ÀS
RECOMENDAÇÕES DOS
ÓRGÃOS DE CONTROLE

03

AUMENTO DA MATURIDADE
DE SEGURANÇA
CIBERNÉTICA

04

OTIMIZAÇÃO DO USO DE
FERRAMENTAS EXISTENTES

05

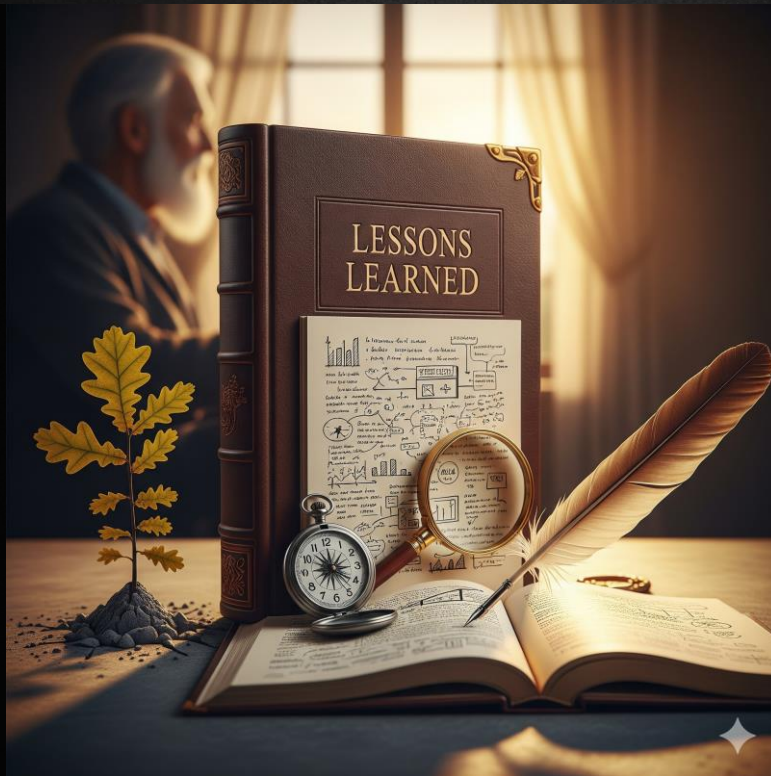
MELHORA NA VISIBILIDADE
DO AMBIENTE

06

A TI TEM RESPALDO

Lições Aprendidas

- **Comece pequeno, mas comece agora:** A agilidade do Scrum foi fundamental.
- **O open-source é seu aliado:** A comunidade pode ser uma extensão da sua equipe.
- **Métricas são suas melhores amigas:** O que não se mede, não se melhora.
- **A segurança é um esporte de equipe:** Envolver todas as áreas da TI desde o início.



"Há um ditado popular que diz que um computador seguro é aquele que está desligado. Isso é inteligente, mas é falso: O hacker convencerá alguém a entrar no escritório e ligar aquele computador. Tudo é uma questão de tempo, paciência, personalidade e persistência." Kevin Mitnick

entre em contato
Édipo Avelino

[in/edipo-avelino](#) | edipo.palha@mpmt.mp.br | +55 65 99976-4645

mindthese[®]
2025

**Obrigado pela
sua atenção**

mindtheseccom.br | [@mindthesecc](https://twitter.com/mindthesecc)