



Tech Talk

CERT-MZ

UEM, 3 de Maio 2018

# Ciber Segurança: Os 10 Mandamentos

André Tenreiro

[andre@cert.mz](mailto:andre@cert.mz)



## Mandamento 1: User Accounts & Privileges

- Implementação de políticas de gestão de contas e identidades
- Implementação de mecanismos de revisão de utilizadores (*User Access Review*)
- Seguir o princípio do “*Least Privileges*”





## Mandamento 2: Patch Management

### Patching de..

- Sistemas operativos
- Equipamentos de rede
- Aplicações (browser, Java, Adobe, etc.)





## Mandamento 3: Cópias de Segurança

### Cópias de segurança de...

- Configurações
- Dados

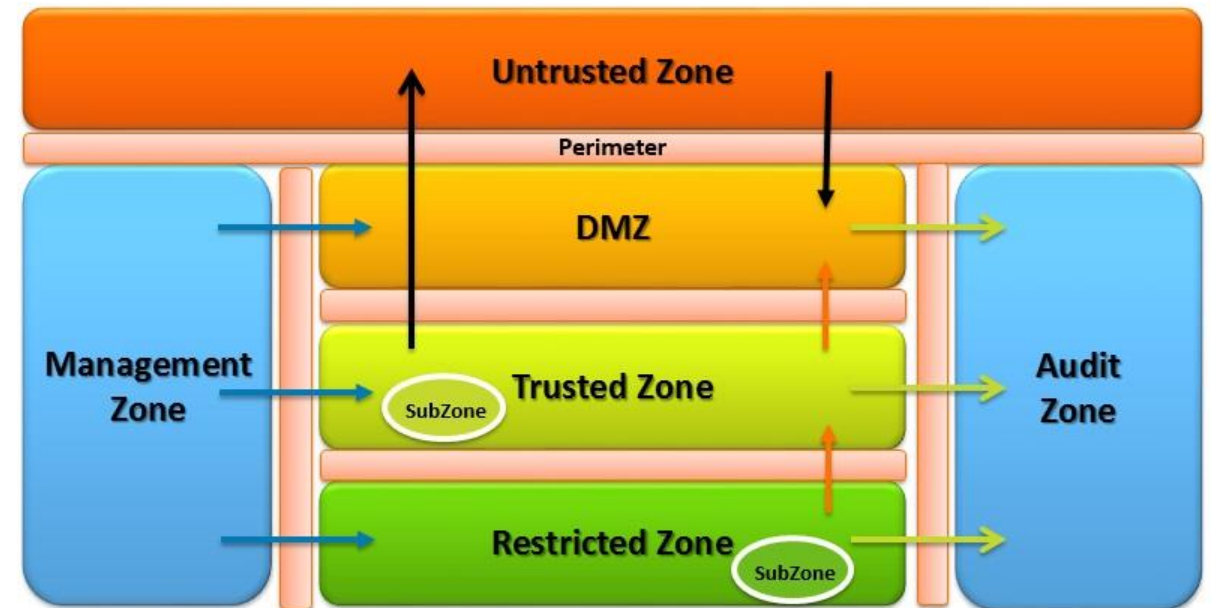
Em caso de catástrofe, conseguir recuperar a informação num estado saudável.





## Mandamento 4: Firewalling e Zoning

- Segregação lógica das diversas redes internas
- Revisão de regras de firewall





# Mandamento 5: Logging & Monitoramento

## Monitorização centralizado de:

- Sistemas operativos
- Base de dados
- Firewalls
- Switches/Routers
- Etc..





## Mandamento 6: Anti-Malware

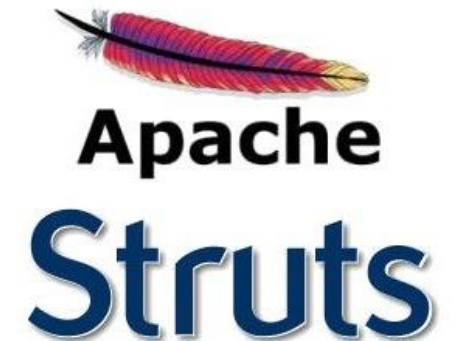
**Antivírus em todos os computadores e servidores! Principalmente Windows**





## Mandamento 7: Gestão de Vulnerabilidades

Conhecer de as vulnerabilidades da nossa rede e priorizar remediações







## Mandamento 8: Protocolos Seguros

Preferir sempre protocolos seguros!

- HTTPS
- SFTP
- LDAPS
- VPN
- SMTPS/IMAPS
- Wi-Fi WPA2

Usar cifras TLS seguras também!





## Mandamento 9: Asset Management

- Rastreio dos equipamentos e software
- Contratos
- Marcas/modelos
- Localização
- Criticidade
- Controlo do Ciclo de vida





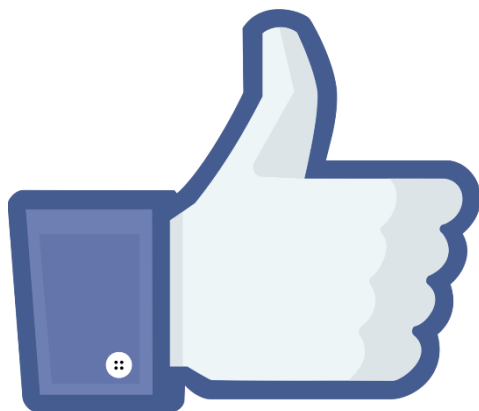
## Mandamento 10: Campanhas de Conscientização

**Informar as pessoas da organização sobre os cuidados a ter!**





# Questões ?



**Segue-nos!**

[www.cert.mz](http://www.cert.mz)

[www.facebook.com/CERTMZ](https://www.facebook.com/CERTMZ)

[www.linkedin.com/company/certmz](https://www.linkedin.com/company/certmz)