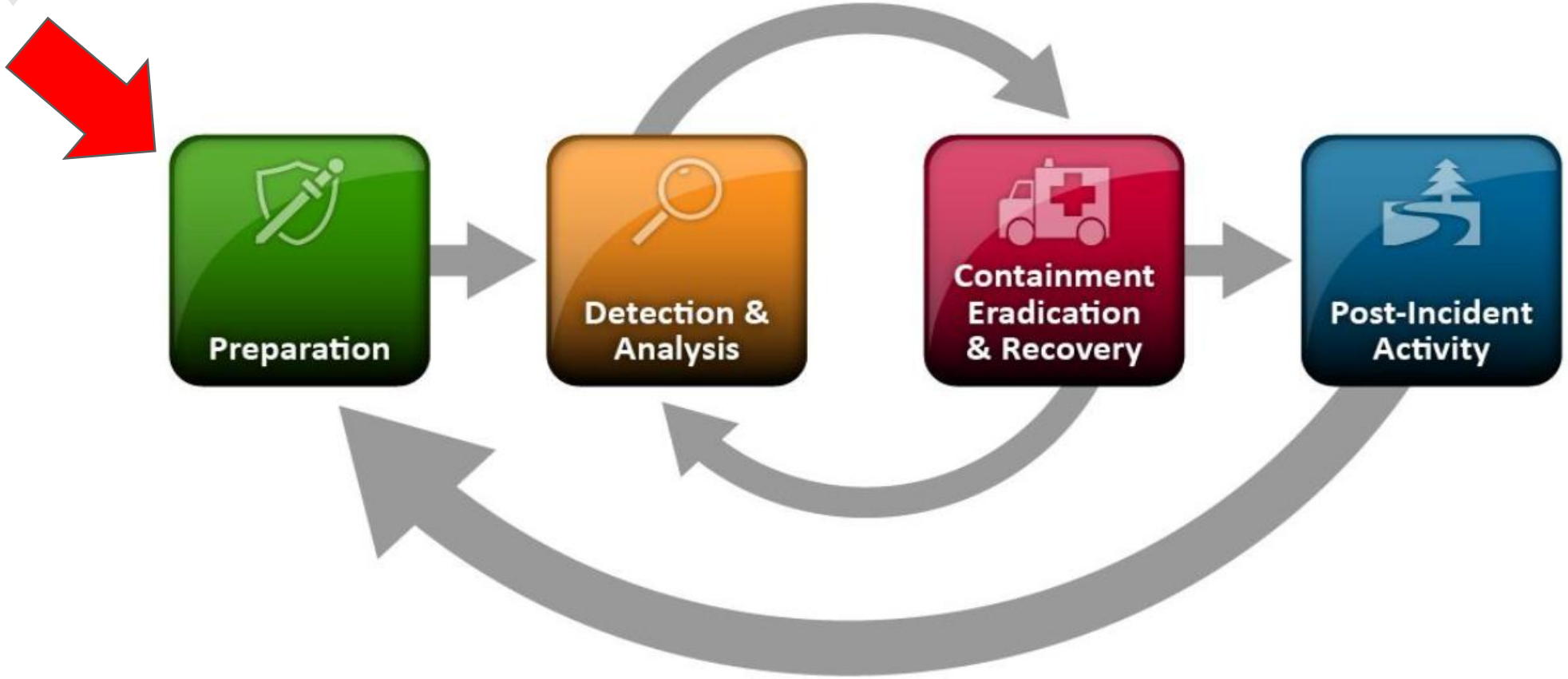
TLP:CLEAR

Ransoware: Preparação com Control Self-Assessment

Renato Braga (TCU)

Live IntraRede (06/ago/25)

NIST 800-61 rev. 2



A preparação inclui ações de prevenção a incidentes

A vida como ela é ...

Etapa 1: Campanha de *phishing*

Usuário da TI, que **executa atividades com contas privilegiadas na sua máquina de uso diário**, abre um e-mail de *phishing* e acessa um *link* malicioso

Correios <nao-responda@clienteexterno.com>
Para: Raony Luna Ribeiro Ferreira Lima
Ter, 22/08/2023 16:21

Alerta: pendência em encomenda

Caro(a) cliente [redacted]

Sua encomenda (código **AA1234687NZBR**) chegou ao centro de distribuição logistico de sua cidade. O sistema indica que o atual status é:

Encomenda extraviada

Para maiores informações e solicitações de reembolso, acessar a página abaixo:

https://www.correios.com.br/atendimento/statusEncomenda

Central de Atendimento * 3003 0100 - Destinado a capitais e regiões metropolitanas. ** 0800 725 7282 - Demais localidades.

AVISO LEGAL

"Esta mensagem é destinada exclusivamente para a(s) pessoa(s) a quem é dirigida, podendo conter informação confidencial e/ou legalmente privilegiada. Se você não for destinatário desta mensagem, desde já fica notificado de abster-se a divulgar, copiar, distribuir, examinar ou, de qualquer forma, utilizar a informação contida nesta mensagem, por ser ilegal. Caso você tenha recebido esta mensagem por engano, peço que me retorne este e-mail, promovendo, desde logo, a eliminação do seu conteúdo em sua base de dados, registros ou sistema de controle. Fica desprovida de eficácia e validade a mensagem que contiver opiniões particulares e vínculos obrigacionais, expedida por quem não detenha poderes de representação por parte da ECT."

"This message is intended only for the person to whom it is addressed and may contain confidential and/or legally privileged. If you are not a recipient of this message, it is now notified of refraining to disclose; copy; distribute; examine; or in any way use the information contained in this message because it is illegal. If you have received this message in error, please I ask to return this email, promoting as soon as possible the elimination of its content in database, records or system control. It is devoid of effective and valid message that contains the private opinions and dividend bonds, issued by those not holding powers of attorney by the ECT."

© Copyright 2023 Correios

Etapa 2: Acesso inicial

O *link* explora uma vulnerabilidade *0-day* e dá acesso à máquina do usuário, que era adm

CIS Center for Internet Security

ISSUED ON 02.07.2025

2025-061: A Vulnerability in Google Chrome Could Allow for Arbitrary Code Execution

A Vulnerability has been discovered in Google Chrome which could allow for arbitrary code execution. Successful exploitation of the the vulnerabi...

CIS Center for Internet Security

ISSUED ON 10.06.2025

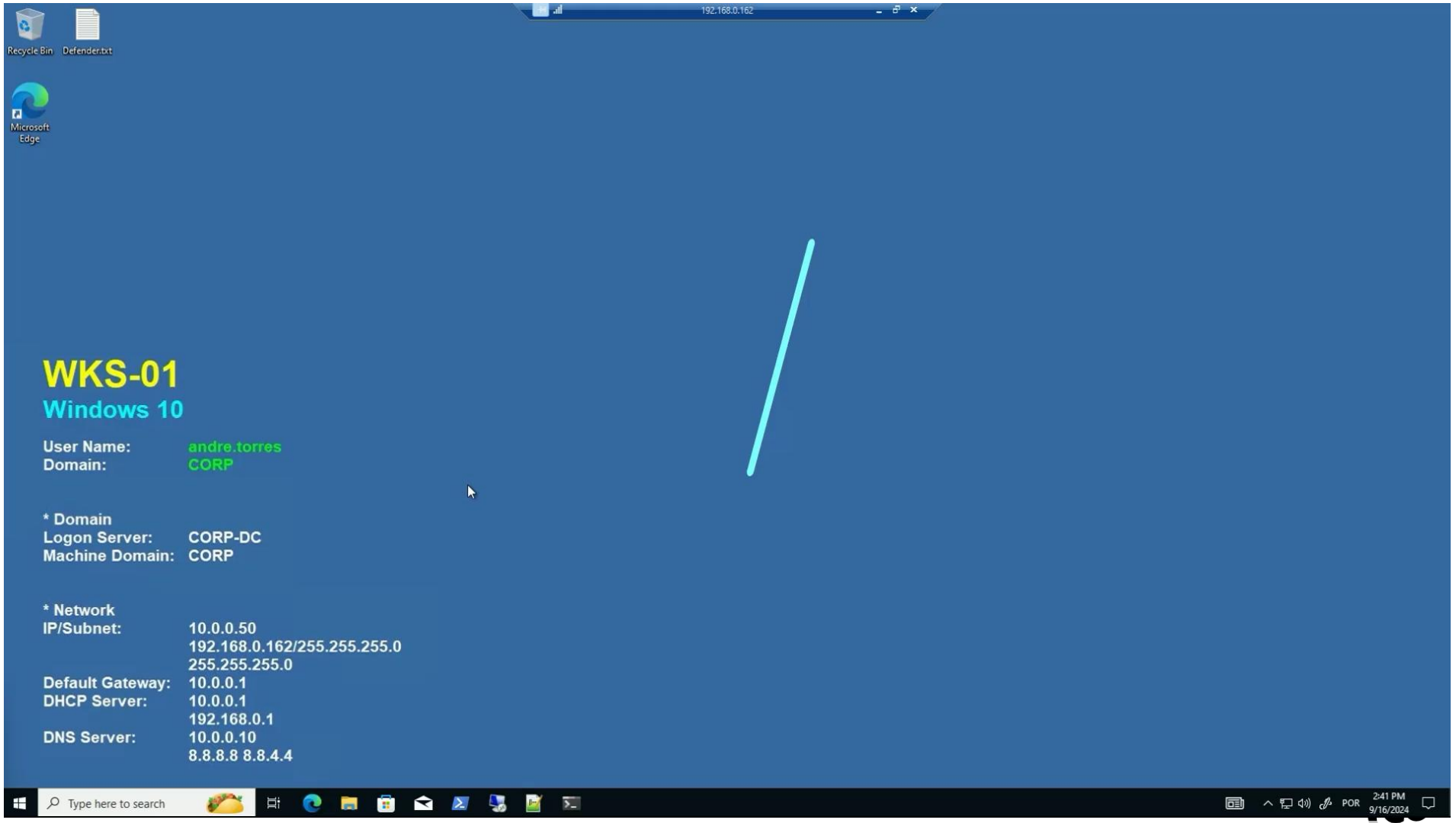
2025-057: Multiple Vulnerabilities in Adobe Products Could Allow for Arbitrary Code Execution

Multiple vulnerabilities have been discovered in Adobe products, the most severe of which could allow for arbitrary code execution. Adobe I...

O agente de ameaça (“hacker”) agora tem acesso remoto à máquina daquele usuário que clicou no e-mail (e.g., shell reverso)

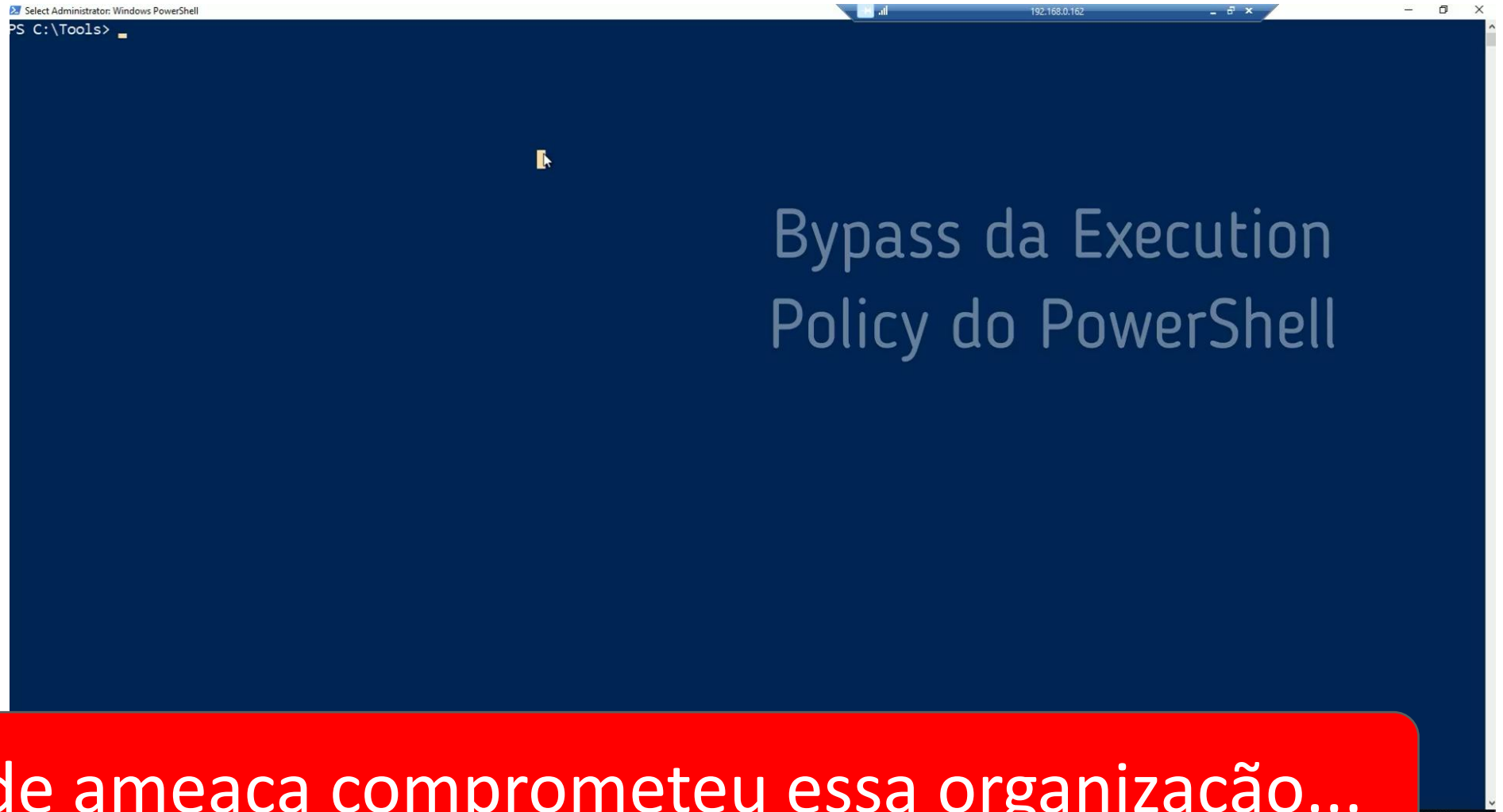
Etapa 2: Acesso inicial

Esse usuário, admin local, realiza tarefas administrativas no domínio



Etapa 3: Movimentação lateral
(c/ escalação de privilégio para DA)

Atacante extrai credenciais da máquina e compromete a organização



O agente de ameaça comprometeu essa organização...

Agora sim, pode pegar seu celular...

menti.com 3779 2184

menti.com 3779 2184

Imagem: https://pixabay.com/en/fortune-telling-future-magic-1989579/

Who Am I: Renato Braga

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# whoami
```

CISA · CIA Certified Internal Auditor · CGAP Certified Government Auditing Professional · CCSA Certification in Control Self Assessment · CRMA Certification in Risk Management Assurance · Association of Certified Fraud Examiners CFE

CompTIA Security+ CERTIFIED·CE · CompTIA CySA+ CERTIFIED·CE · CompTIA PenTest+ CERTIFIED·CE · Certified AppSec Practitioner The SecOps Group · ICCA INE

TCM Security PMPA Certified Practical Mobile Pentest Associate · TCM Security PWPA Certified Practical Web Pentest Associate · OffSec OSWA

eJPTv2 Dynamic Exam · Offensive Security OSWP · Certified Red Team Professional · Certified Enterprise Security Professional (CESP - ADCS)

Certified Azure Web Application Security Professional (CAWASP)

EXIN Information Security Management ISO/IEC 27001 Foundation · EXIN Privacy & Data Protection Foundation · EXIN Privacy & Data Protection Professional · EXIN Data Protection Officer

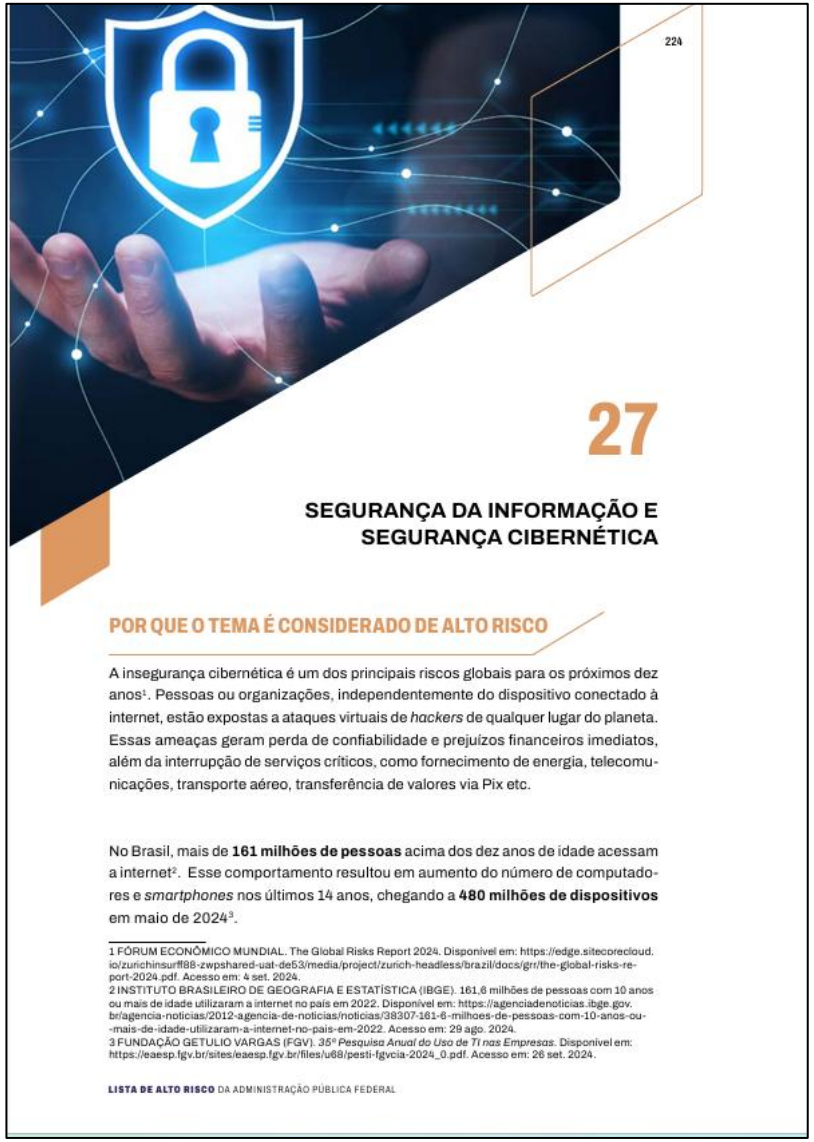
Desde 1988

Desde 2003

Carnegie Mellon University Software Engineering Institute

CERT
Incident Response Process Professional
Certificate Holder

Afeta mais de um milhão de pessoas ou envolve valores superiores a R$ 1 bilhão



224

27

SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

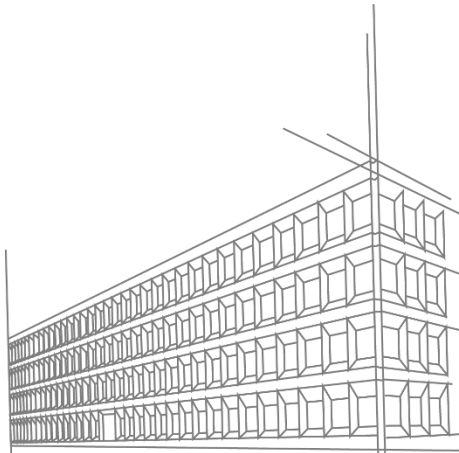
POR QUE O TEMA É CONSIDERADO DE ALTO RISCO

A insegurança cibernética é um dos principais riscos globais para os próximos dez anos[1]. Pessoas ou organizações, independentemente do dispositivo conectado à internet, estão expostas a ataques virtuais de *hackers* de qualquer lugar do planeta. Essas ameaças geram perda de confiabilidade e prejuízos financeiros imediatos, além da interrupção de serviços críticos, como fornecimento de energia, telecomunicações, transporte aéreo, transferência de valores via Pix etc.

No Brasil, mais de **161 milhões de pessoas** acima dos dez anos de idade acessam a internet[2]. Esse comportamento resultou em aumento do número de computadores e *smartphones* nos últimos 14 anos, chegando a **480 milhões de dispositivos** em maio de 2024[3].

1 FÓRUM ECONÔMICO MUNDIAL. The Global Risks Report 2024. Disponível em: https://edge.sitecorecloud.io/zurichinsurff88-zwpshared-uat-de53/media/project/zurich-headless/brazil/docs/grr/the-global-risks-report-2024.pdf. Acesso em: 4 set. 2024.
2 INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). 161,6 milhões de pessoas com 10 anos ou mais de idade utilizaram a internet no país em 2022. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38307-161-6-milhoes-de-pessoas-com-10-anos-ou-mais-de-idade-utilizaram-a-internet-no-pais-em-2022. Acesso em: 29 ago. 2024.
3 FUNDAÇÃO GETULIO VARGAS (FGV). *35ª Pesquisa Anual do Uso de TI nas Empresas*. Disponível em: https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/pesti-fgvcia-2024_0.pdf. Acesso em: 26 set. 2024.

Clique para acessar



O formato de um QACI e como usá-lo

Item	Critérios	Avaliação	Evidências	Situação encontrada
6. Os grupos Operators (Account, Server, Backup, Print) são compostos apenas por usuários estritamente necessários?	- Indicadores de segurança do Purple Knight[x]	0	Lista de usuários membros dos grupos privilegiados, obtidos a partir da execução do script #1 disponível no **PT07 – Roteiro para execução de scripts**.	Existem 23 usuários membros de grupos Operators. Obs: esse número pode estar incompleto devido ao fato da execução do script ter omitido os membros do grupo Account Operators.

attack.mitre.org

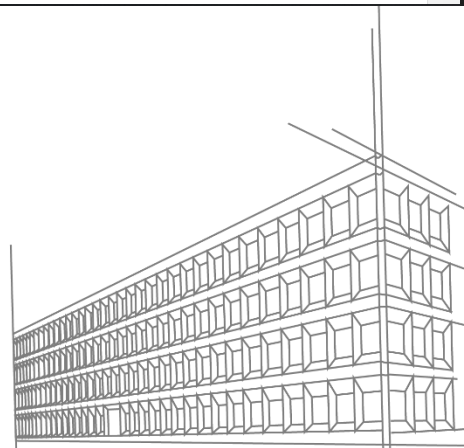
MITRE | ATT&CK

Matrices Tactics Techniques Defenses CTI Resources Benefactors Blog Search

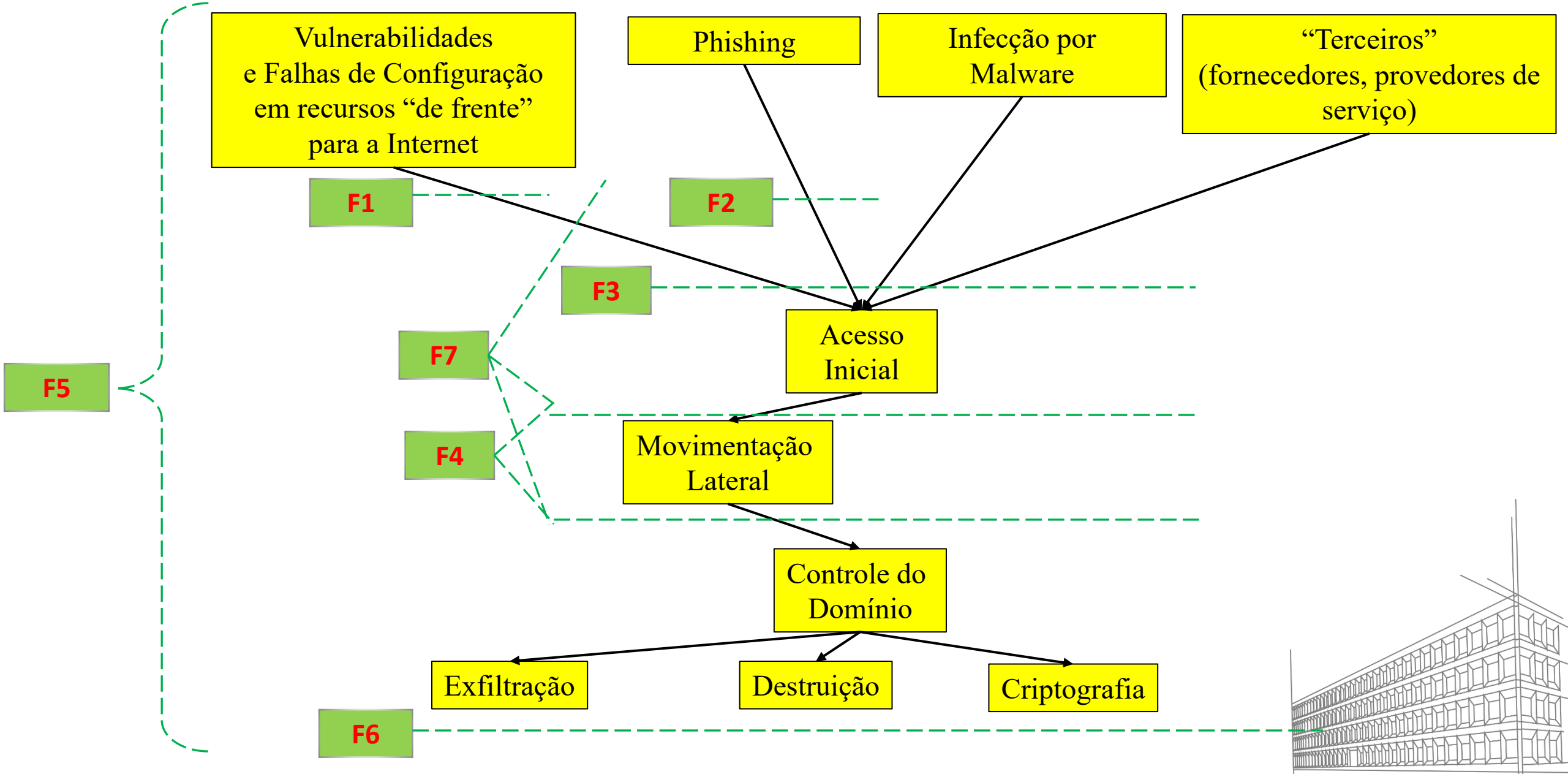
ATT&CK Matrix for Enterprise

layout: side | show sub-techniques | hide sub-techniques

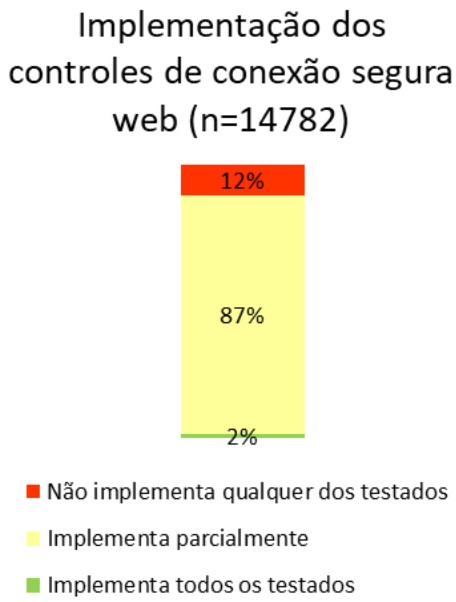
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service (2)
			System Services (2)	Implant Internal Image	Process Injection (12)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking
			User Execution (3)	Modify Authentication Process (9)	Scheduled Task/Job (5)	Hide Artifacts (12)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Hijack Execution Flow (13)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Protocol Tunneling		System Shutdown/Reboot
				Power Settings		Impair Defenses (11)	Steal or Forge Kerberos Tickets (4)	Network Service Discovery		Input Capture (4)	Proxy (4)		
				Pre-OS Boot (5)		Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Remote Access Software		
				Scheduled Task/Job (5)		Indicator Removal (9)		Network Sniffing		Video Capture	Traffic Signaling (2)		
				Server Software Component (5)		Indirect Command Execution		Password Policy Discovery			Web Service (3)		
						Masquerading (9)		Peripheral Device Discovery					
						Modify Authentication Process (9)		Permission Groups Discovery (3)					
						Modify Cloud Compute		Process Discovery					
								Query Registry					
								Remote System Discovery					

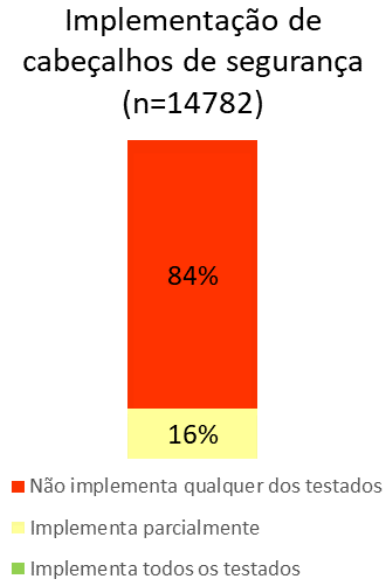


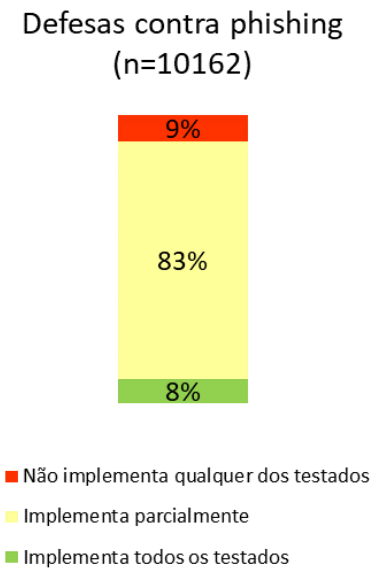
Anatomia de um ataque *ransomware*



F1: Configurações em serviços Web, DNS e email







Apresentado no forum de CSIRTs, em 2024
Também no PTO-01 (site da Dasi)

F1: Configurações em serviços Web, DNS e email

https://top.nic.br

tcu.gov.br/dasi

Entendendo riscos para estimar custos e benefícios esperados com os controles

F2: *Phishing* (defesa em profundidade)

1º eixo (administrativo)

- Normas internas (AUP) e processos relacionados
- Uso do e-mail corporativo pelos usuários

2º eixo (técnico)

- Controles do servidor de e-mail (SPF, DKIM, DMARC)
- Soluções de apoio

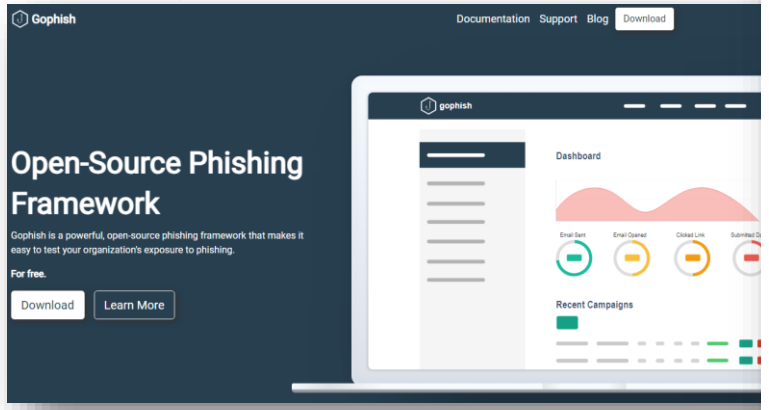
3º eixo (conscientização)

- Programa de conscientização do usuário
- Simulação de *phishing*

F2: *Phishing*

Item de verificação	Referências (Critério)	Resultado da Avaliação (feita	
		Avaliação	Evidência
1.1. Os colaboradores da organização recebem treinamento sobre reconhecer e notificar ataques de *phishing* logo após sua contratação ou antes de receberem as credenciais da conta corporativa de e-mail?	CIS Controls v.8 Safeguard 14.2, 14.5 e 14.6		
1.2. A organização realizou ação de conscientização sobre ataques de phishing para os usuários no último ano?	CIS Controls v.8 Safeguard 14.2, 14.5 e 14.6		
1.3. A ação acima teve como público-alvo todos os usuários da organização, incluindo a alta administração?	CIS Controls v.8 Safeguard 14.2, 14.5 e 14.6		
1.4. A organização realizou teste de simulação de phishing para os usuários nos últimos dois anos?	CIS Controls v.8 Safeguard 14.2		
1.5. A ação acima teve como público-alvo todos os usuários da organização, incluindo a alta administração?	CIS Controls v.8 Safeguard 14.2		

F2: *Phishing*



QE Quarentena de e-mail [redacted]
Para: [redacted]

Mensagem em quarentena

O Filtro de E-mail do Outlook recebeu uma solicitação para colocar em quarentena um e-mail que foi enviado anteriormente. Este e-mail deve ser excluído com segurança usando as opções abaixo.

Por favor, aceite ou negue a exclusão de e-mail:

REMETENTE: sorteio@notafiscal.gov.br - ASSUNTO: 'Vencedores de Julho'

EXCLUIR E-MAIL / RETIRAR E-MAIL DA QUARENTENA

IMPORTANTE:

- Esta é uma mensagem automática e **NÃO DEVE SER RESPONDIDA**.
- Os e-mails excluídos após decorrido o período de quarentena **NÃO PODERÃO SER RECUPERADOS.**

Para maiores informações sobre spam e seus riscos associados, acesse aqui

Atenciosamente,

Equipe Microsoft Outlook

Templates de Phishing

- 2 templates mensurando se o usuário **clicou** em um link malicioso
- 2 templates mensurando se o usuário **acessou** uma página maliciosa e **inseriu** informações pessoais
- 2 templates com **arquivos anexos**, mensurando se o usuário abriu arquivo MS Office e habilitou macros

F3: Gestão de Identidades e Autenticação

2.3 Autenticação multifator

Item	Critérios	Avaliação[5] [6]	Evidências	Observações
8. A organização implementa autenticação multifator para **acesso remoto** a módulos de sistemas *on premises* ou expostos à internet?	CIS *Controls* v8.1 – *Safeguard* 6.4: *Require MFA for Remote Network Access* CIS *Controls* v8.1 – *Safeguard* 6.3: *Require MFA for Externally-Exposed Applications* NIST SP 800-63B: *Digital Identity Guidelines – Authentication and Lifecycle Management*: 4. *Authenticator Assurance Levels*		▪ *Print* da tela exigindo o multi fator ▪ *Print* da configuração que exige o multi fator	
9. A organização implementa autenticação multifator para contas de **acesso privilegiado** ou **administrativo**?	CIS *Controls* v8.1 – *Safeguard* 6.5: *Require MFA for Administrative Access* NIST SP 800-63B: *Digital*		▪ *Print* da tela exigindo o multi fator ▪ *Print* da configuração que exige o multi fator	Como é gerido o acesso de contas privilegiadas?

F4: *Active Directory*

Pessoas, processos e papéis

Configuração do Active Directory

Monitoramento do Active Directory (foco em alertas de segurança)

Backup & recuperação do Active Directory

F4: *Active Directory*

Item	Critérios	Avaliação[i] [ii]	Evidências	Observações
			PT07 – Roteiro para execução de scripts. - Comparativo entre as duas listas acima	contas. - Comparar os usuários que a organização considera como Tier 0 com os usuários dos grupos privilegiados, obtidos no script.
6. Os servidores típicos de categoria Tier 0 estão classificados nessa Tier? Ex: DCs, Exchange, AD-Connect, SCCM.	- Documentação Microsoft sobre modelo de acesso privilegiado[iii] - Documentação SpecterOps sobre tiering[iv] - Documentação Quest sobre tiering[v]		- Tela(s) que liste os servidores classificados em cada Tier.	- Verificar se existem servidores nessa categoria que não estão classificados como servidores Tier 0: DCs, Exchange, AD-Connect, SCCM, entre outros.
7. Caso exista integração do AD on-premises com a nuvem Azure por meio do serviço Entra Connect (antigo Azure AD Connect), apenas usuários Tier 0 possuem acesso administrativo a esse servidor?			- Lista de usuários que a organização considera como Tier 0 (fornecida pela organização) - Resultado do script #2 (comandos 1 e 2) disponível no **PT07 – Roteiro para execução de scripts.**	- Esse servidor é responsável por um serviço cujo usuário (MSOL_*) possui permissões de replicação no domínio, sendo que o seu comprometimento implica no comprometimento do domínio/floresta. <u>Procedimentos</u> - Verificar se o servidor do Entra Connect está devidamente classificado como Tier 0. - Verificar quais são os usuários e grupos que possuem acesso administrativo a esse servidor, através da execução do script. - Comparar os usuários que a organização considera como Tier 0 com os usuários os administrativos desse servidor, obtidos no script.

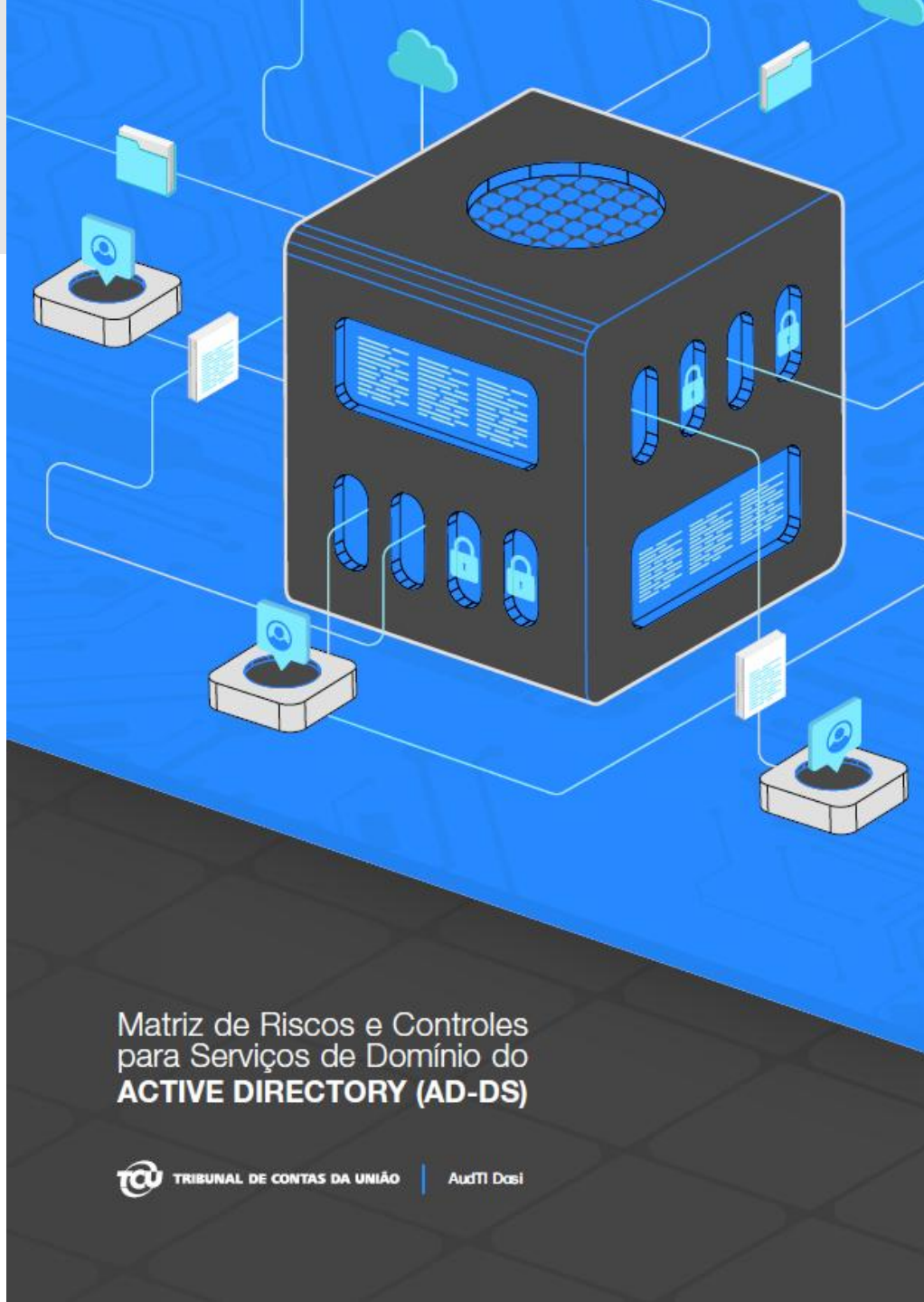
menti.com 3779 2184

Imagem: https://pixabay.com/en/fortune-telling-future-magic-1989579/

F4: *Active Directory*

Será publicado neste ano (2025)

Entendendo riscos para estimar custos e benefícios esperados com os controles



Todos disponíveis em tcu.gov.br/dasi

Material de apoio para gestores

Defesas contra *phishing*

QACI 01 - Controles do programa de conscientização do usuário

QACI 02 - Ações de conscientização do usuário em phishing

QACI 03 - Controles do eixo administrativo

QACI 04 - Controles do eixo técnico

Gestão de identidades

QACI 01 - Governança em IdM

QACI 02 - Gestão de Identidade

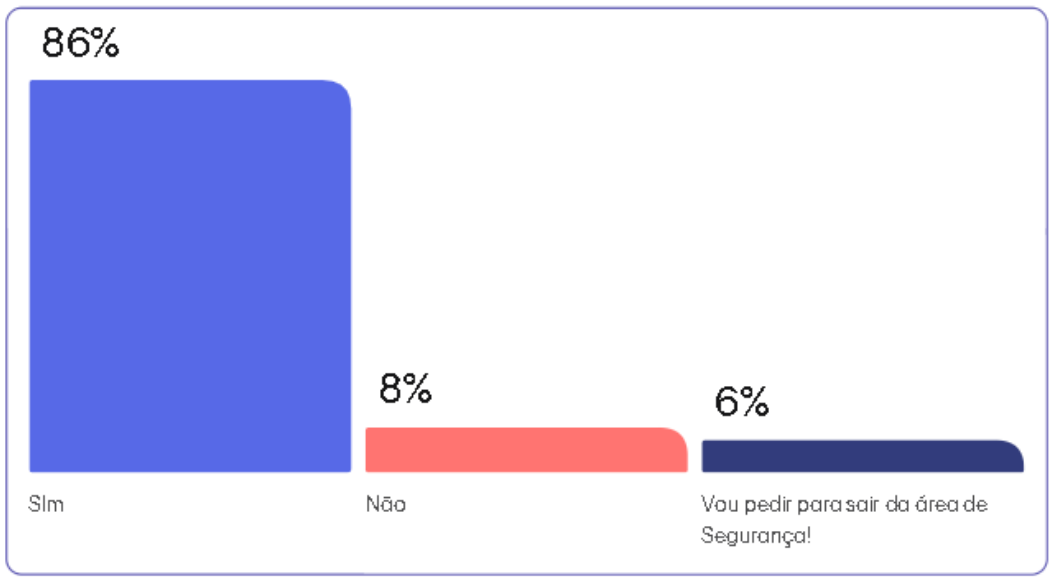
QACI 03 - Autenticação

QACI 04 - Monitoramento

Join at menti.com | use code 3779 2184

Mentimeter

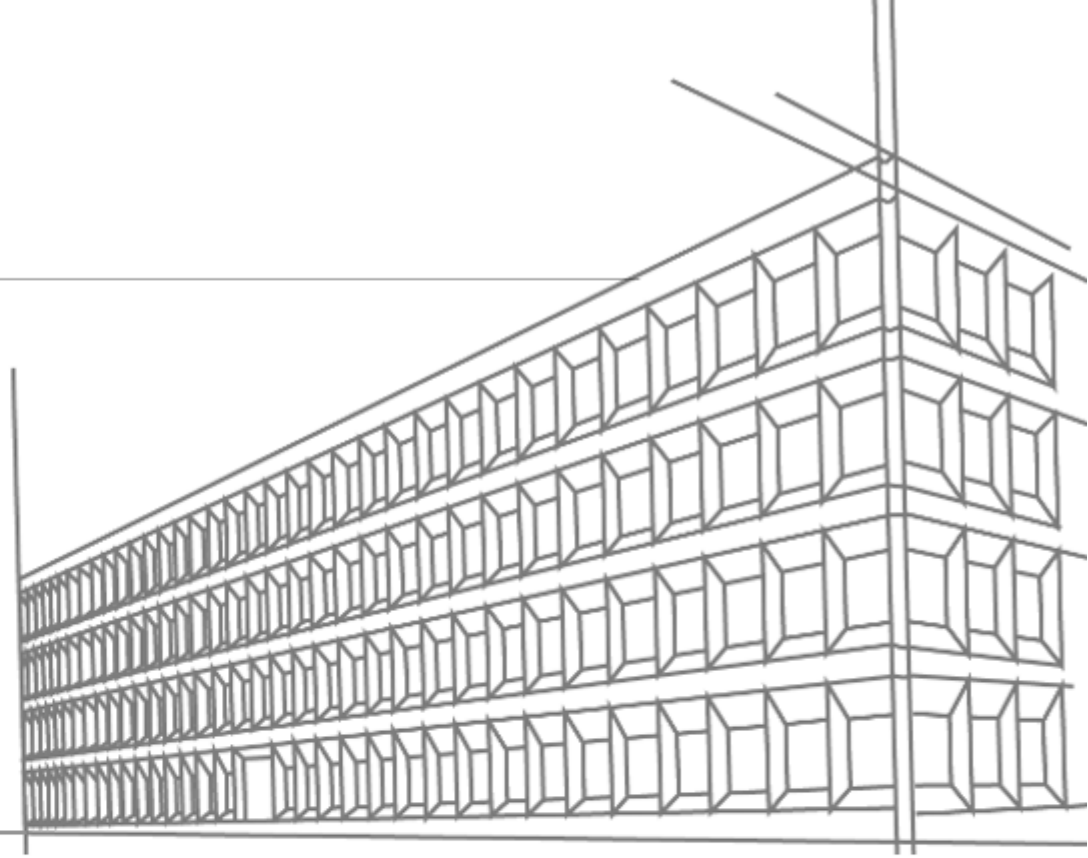
O que você viu e ouviu nessa nossa conversa, ajuda você a melhorar a gestão de riscos de SegCiber na sua organização?



menti.com 3779 2184

Imagem: https://pixabay.com/en/fortune-telling-future-magic-1989579/

TRIBUNAL DE CONTAS DA UNIÃO



Obrigado!

Renato Braga
SI Audit Manager @ Federal Court of Accounts - Brazil (TCU)

dasi at tcu dot gov dot br

Tornar seguro o ambiente digital sob a governabilidade do Brasil