

**Instituto Politécnico Nacional
Centro de Investigación en Computación
Laboratorio de Ciberseguridad**

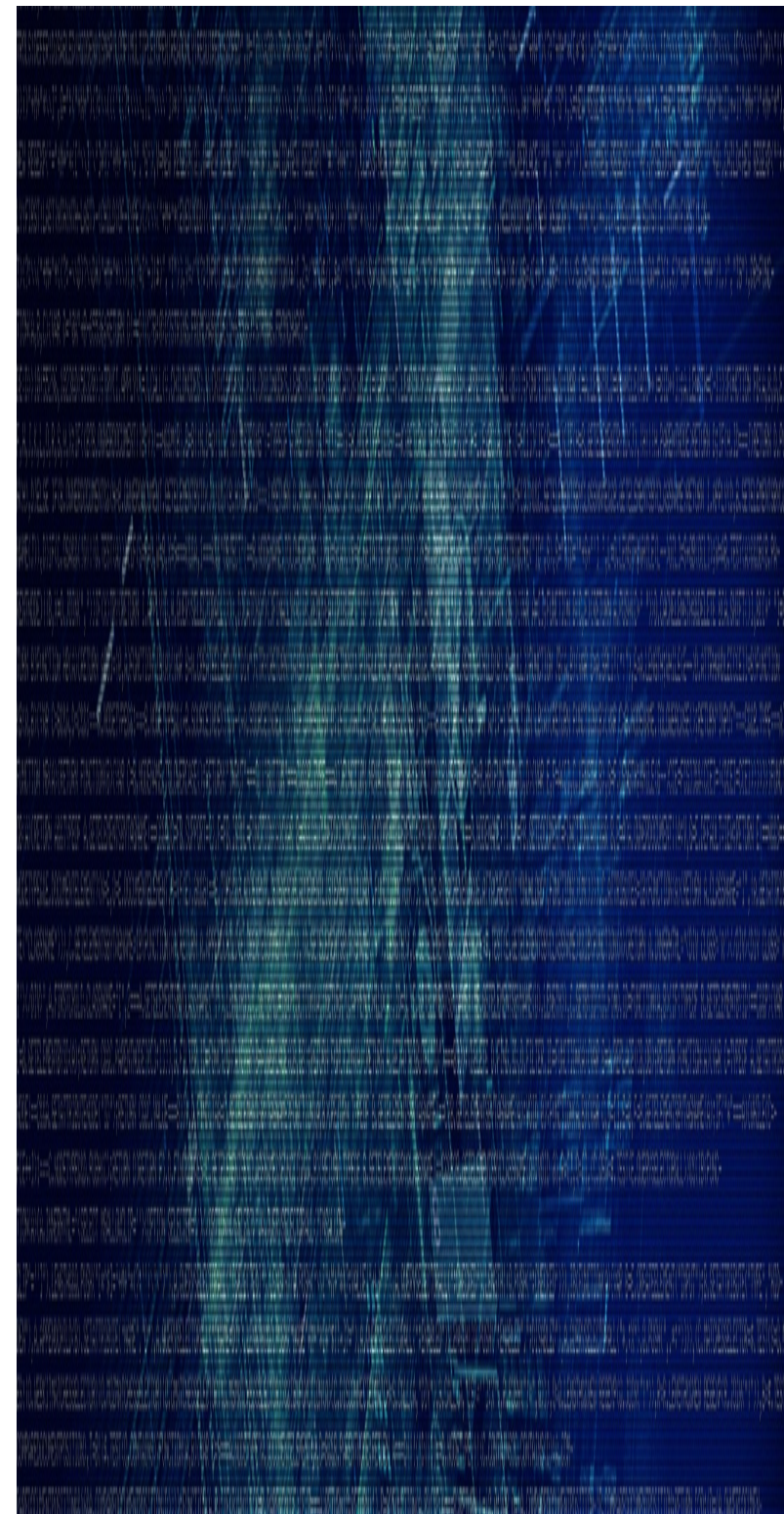
Temas de Tesis

Raúl Acosta Bermejo
2022-B

14 de octubre del 2022



INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Temas de Tesis 1

Descripción

❖ Attack tree

- They are conceptual diagrams showing how an asset, or target, might be attacked..
- Cual es el costo, tiempo y probabilidad de un ataque?

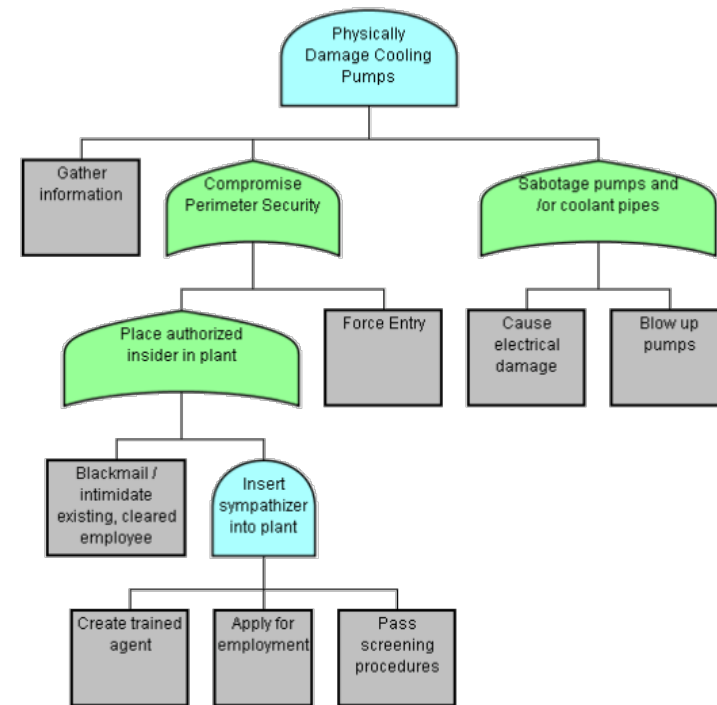
❖ Defense Tree

- Mitigation tree.
- Attack-defense tree

❖ Others

- Fail tree.

Threat Analysis and
Risk Assessment
Modeling threats



INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Temas de Tesis 1

Aplicaciones reales

❖ Software comercial

- Isograph
- SecurlTree/Amenaza.

Costo de \$3,750 a \$84,000 USD (\$1.68 millones).

- Cual es el costo, tiempo y probabilidad de un ataque?

❖ Herramientas similares

- CAIRIS
 - Comercial, Demo
 - Open Source: <https://github.com/cairis-platform/cairis>



Temas de Tesis 1

SCOPUS

Attack tree: 12,2k
Computer Science: 5.6k
Biological Sciences: 4k
Engineering: 3k

Conference: 3k, Articles: 2k
2023 (13), 2022 (637), 2021 (906), 2020 (656)

Threat Modeling:
A Summary of Available Methods
SEI: August 2018, White Paper

12 metodos incluidos los árboles

Foundations of Attack–Defense Trees
Barbara Kordy, Sjouke Mauw, Saša Radomirović, Patrick Schweitzer
Conference paper, LNSC, volume 6561.

Ejemplos de artículos muy citados

- **Scalable**, graph-based network vulnerability analysis.
- Model inversion attacks that exploit confidence information and basic countermeasures.
- Dynamic security risk management using **Bayesian** attack graphs.
- Naive **Bayes** vs decision trees in intrusion detection systems.
- Cybersecurity for critical infrastructures: Attack and defense modeling.

Exploiting attack–defense trees to find an **optimal** set of countermeasures, IEEE.
A **Minimum** Defense Cost Calculation Method for Attack Defense Trees, Hindawi.

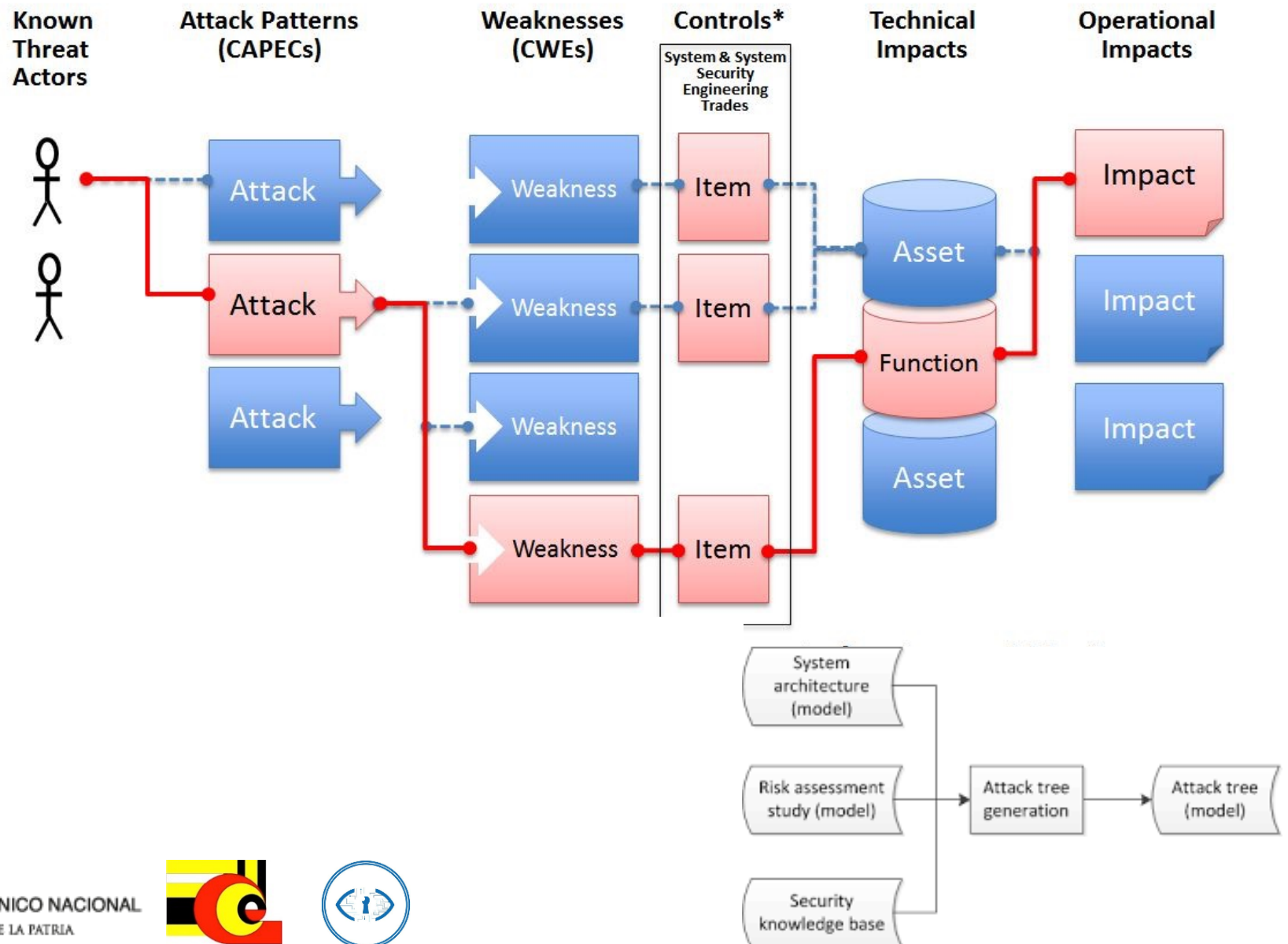


INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Temas de Tesis 1

Engineering for Attacks



TICs graph

Attack tree

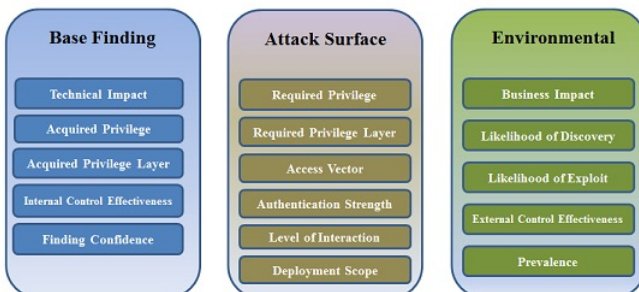
MITRE ATT&CK

Defense tree

CIS Controls (Critical Security Controls)

	CIS Controls Version 8
01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

Common
Weakness
Enumeration

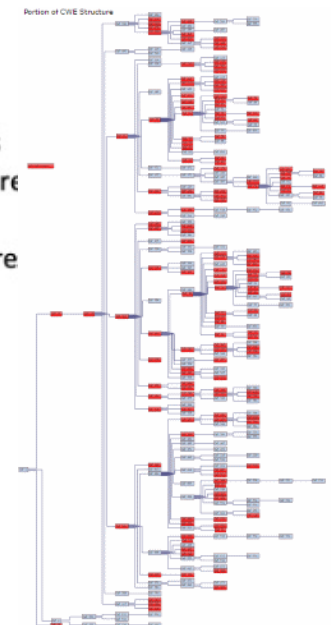


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 Items	31 Items	56 Items	28 Items	59 Items	20 Items	19 Items	17 Items	13 Items	9 Items	21 Items
Drive-by Compromise	AppleScript	Batch_profile and Scripts	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Binary Padding	Binary Padding	Binary Padding	Automated Collection	Data Compressed Through Removable Media	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shim	Appinit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shim	CMSTP	Credentials in Registry	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Browser Extensions	DLL Search Order Hijacking	Component Object Model Hijacking	Forced Authentication	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Change Default File Association	Dylib Hijacking	Control Panel Items	Hooking	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Domain Fronting	Fallback Channels
Trusted Relationship	InstallUtil	Component Firmware	Exploitation for Privilege Escalation	DCShadow	Input Prompt	Permission Groups Discovery	Remote File Copy	Exfiltration Over Physical Medium	Multi-hop Proxy	Multi-Stage Channels
Valid Accounts	Launchctl	Component Object Model Hijacking	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Kerberoasting	Process Discovery	Replication Through Removable Media	Man in the Browser	Scheduled Transfer	Multilayer Encryption
	Local Job Scheduling	Create Account	File System Permissions Weakness	Disabling Security Tools	Kinship	Query Registry	Shared Webroot	Screen Capture	Port Knocking	Multitask Communication
	Mshta	Dylib Hijacking	DLL Search Order Hijacking	DLL Side-Loading	Network Sniffing	Security Software Discovery	Taint Shared Content	Third-party Software	Remote Access Tools	Remote File Copy
	Powershell	External Remote Services	Image File Execution Options Injection	Extra Window Memory Injection	Private Keys	System Information Discovery	Windows Admin Shares	Standard Application Layer Protocol	Standard Cryptographic Protocol	Standard Non-Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Launch Daemon	File Deletion	Security Memory	System Network Configuration Discovery	Windows Remote Management	Uncommonly Used Port	Web Service	
	Rundll32	Hidden Files and Directories	Path Interception	File System Logical Offsets	Two-Factor Authentication Interception	System Time Discovery				
	Scheduled Task	Hooking	Port Monitors	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Hypervisor	Process Injection	Hidden Files and Directories						
	Signed Script Proxy Execution	Image File Execution Options Injection	Scheduled Task	Hidden Users						
	Source	Kernel Modules and Extensions	Service Registry Weakness	Hidden Window						
	Space after Filename	Launch Agent	Setuid and Setgid	Image File Execution Options Injection						
	Third-party Software	Launch Daemon		Indicator Blocking						
	Trap	Launchctl								
	Trusted Developer									

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failure
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failure
- A10:2021-Server-Side Request Forgery (SSRF)*



NVD / NIST
National Vulnerability Database

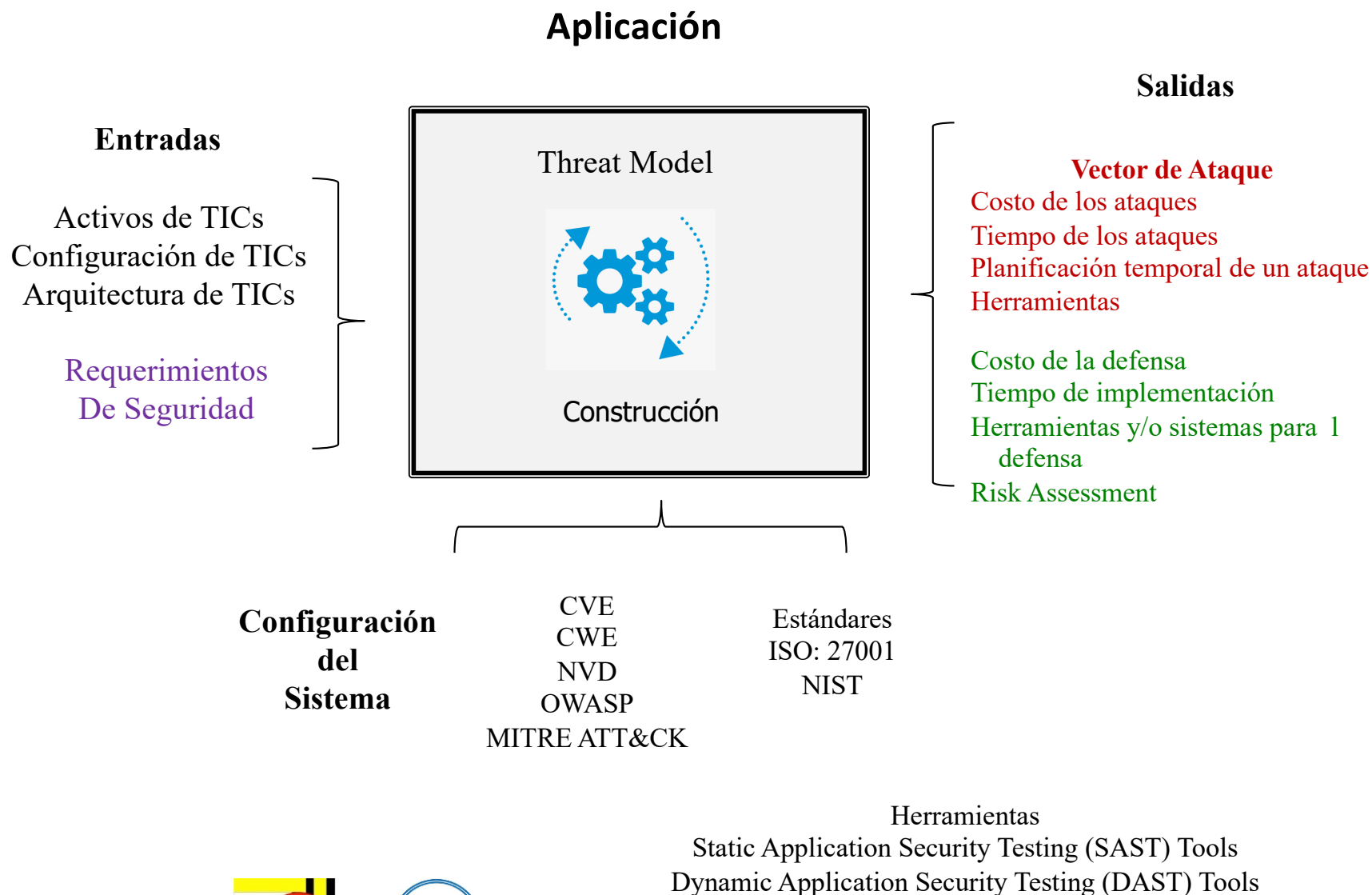


Objetivos

- Prototipo, PoC (Proof of Concept)
- Centrado en el modelo (gráfico) y no en la GUI.
- Elegir un Caso(s) de Prueba
App en la Nube? Security by Design?

Problemas

- Como abordar la complejidad de los sistemas?
Modelo a capas, encapsulación, etc.
- Usar funciones multi-objetivo sencillas.



INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA



Gracias

Preguntas o comentarios



Sitio web [personal](https://www.cic.ipn.mx/~racostab)

<https://www.cic.ipn.mx/~racostab>

Email

racostab@ipn.mx

racostab@cic.ipn.mx

Tel.

55-57-59-60-00

Ext.56652



INSTITUTO POLITÉCNICO NACIONAL
LA TÉCNICA AL SERVICIO DE LA PATRIA

