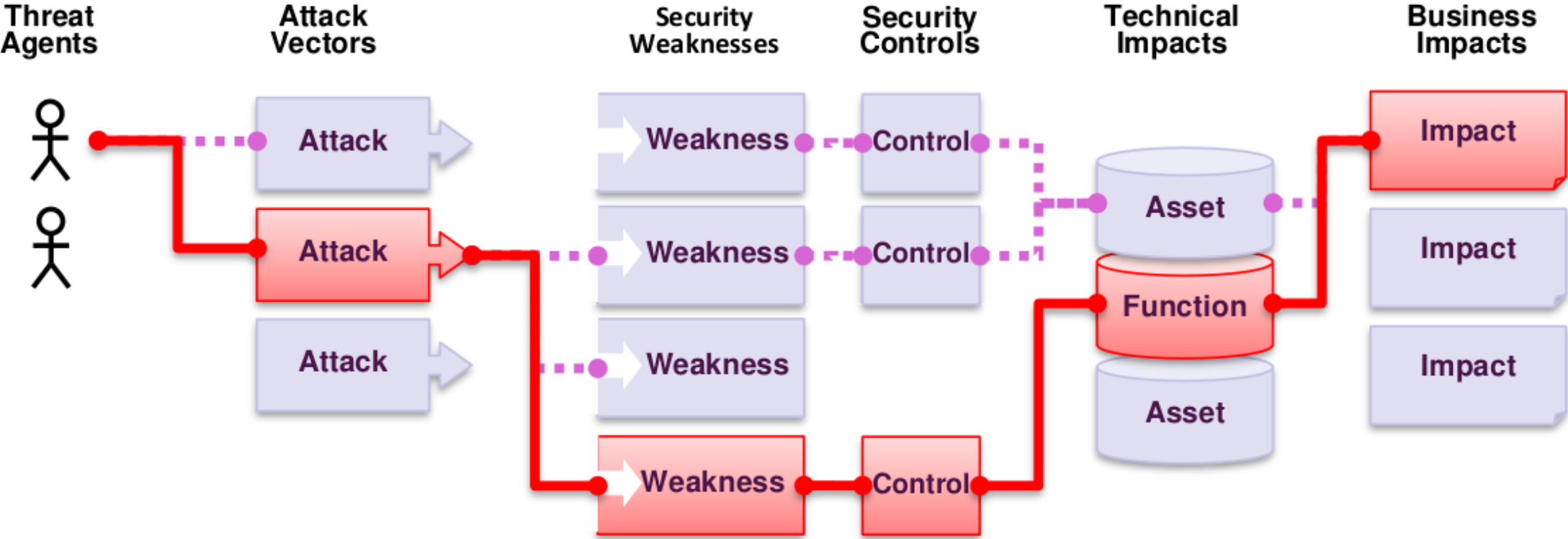


# Riesgo como proceso



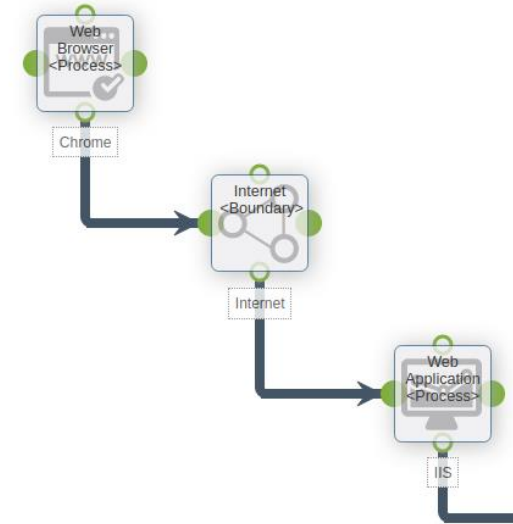
# Thread Modeling

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?

Fuente: Thread Modelling Manifesto  
<https://www.threatmodelingmanifesto.org/>

# Threat Modeling: cómo hacerlo

1. Scope: Diagrama de arquitectura
2. Threats STRIDE
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure
  - Denial-of-service
  - Elevation privilege
3. Contramedidas o gestión del riesgo
4. Evaluar



Herramientas: Microsoft Threat Modeling Tool

<https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>

# Demo de MS Threat Modeling Tool

# Risk Rating

$$\text{Risk} = \text{Likelihood} * \text{Impact}$$

- Steps:
  - 1: Identifying a Risk
  - 2: Factors for Estimating Likelihood
  - 3: Factors for Estimating Impact
  - 4: Determining Severity of the Risk
  - 5: Deciding What to Fix
  - 6: Customizing Your Risk Rating Model
- Sacado del OWASP, así que empecemos a utilizarlo  
[https://owasp.org/www-community/OWASP Risk Rating Methodology](https://owasp.org/www-community/OWASP_Risk_Rating_Methodology)

Fuente: [https://owasp.org/www-community/OWASP Risk Rating Methodology](https://owasp.org/www-community/OWASP_Risk_Rating_Methodology)

Alternativas: NIST-800-30, Magerit

# Calculadora de riesgos OWASP

Threat Agent Factors

Skill Level

5 - Advanced computer user

Motive

4 - Possible reward

Opportunity

9 - No access or resources reqd

Size

9 - Anonymous Internet users

Threat Agent Factor: High (TAF: 6.75)

Vulnerability Factors

Ease of Discovery

7 - Easy

Ease of Exploit

4

Awareness

4 - Hidden

Intrusion Detection

3 - Logged and reviewed

Vulnerability Factor: Medium (VF: 4.5)

Technical Impact Factors

Loss of Confidentiality

0 - N/A

Loss of Integrity

0 - N/A

Loss of Availability

9 - All services completely lost

Loss of Accountability

0 - N/A

Technical Impact Factor: Low (TIF: 2.25)

Business Impact Factors

Financial Damage

9 - Bankruptcy

Reputation Damage

1 - Minimal damage

Non-compliance

0 - N/A

Privacy Violation

0 - N/A

Business Impact Factor: Low (BIF: 2.5)

Likelihood Factor: Medium (LF: 5.625)

Impact Factor: Low (IF: 2.5)

Overall Risk Severity: Low

# Tipos de atacantes

	Corporations	Hacktivists	Cyber criminals	Cyber terrorists	Script kiddies	Online social hackers	Employees	Nations states
Physical attacks	✓	-	✓	✓	-	-	✓	✓
Disasters	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Failures/ Malfunctions	✓	-	-	-	-	-	✓	-
Outages	✓	✓	✓	✓	✓	✓	✓	✓
Unintentional damages	✓	-	-	-	-	-	✓	-
Damage/Loss	✓	✓	✓	✓	✓	✓	✓	✓
Nefarious activity/Abuse	✓	✓	✓	✓	✓	✓	✓	✓
Eavesdropping/ Interception/ Hijacking	✓	✓	✓	✓	✓	✓	✓	✓
Legal	✓	✓	✓	✓	✓	✓	✓	✓