

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