

OWASP LatamTour
CHILE 2016

Ubi sunt: La atribución en el ciberespacio

Sebastián Koch M.
Investigador y analista
CEEAG

 OWASP
The Open Web Application Security Project



 OWASP
The Open Web Application Security Project

- Presentación: producto de un artículo académico. Por publicar.
- Estudios de seguridad.
- Político-estratégico v/s técnico.
- ¿Dónde están?



OWASP
The Open Web Application Security Project

- Atribuir ataque a (x).
- Prevenir.
- Reaccionar (legítima defensa).
- Realidad física: medianamente simple (actores tradicionales).
- ¿En el ciberespacio?

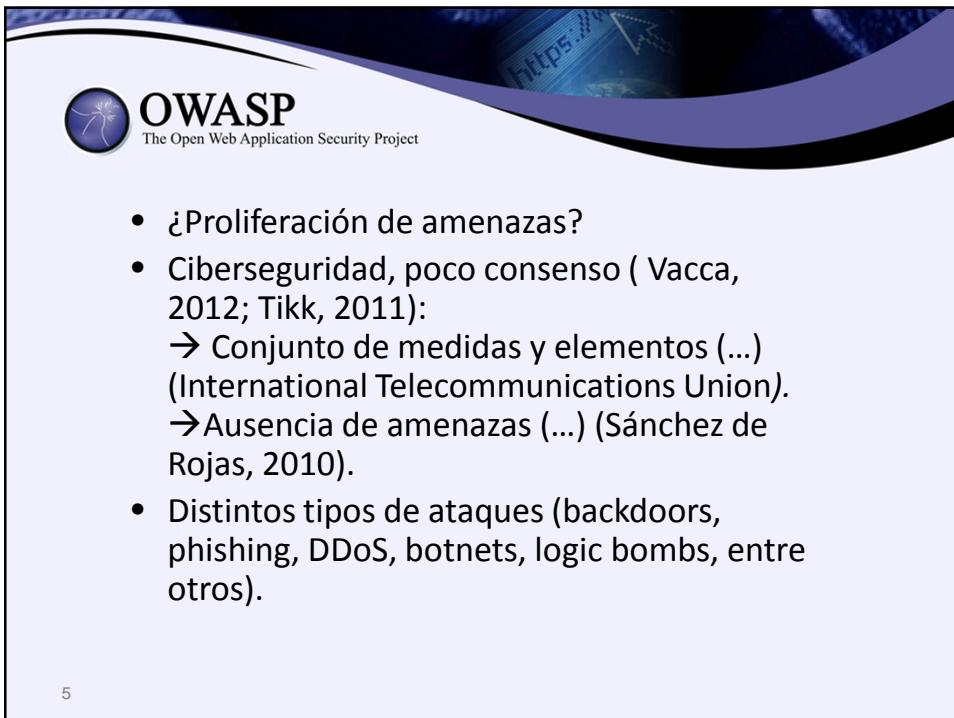


OWASP
The Open Web Application Security Project

- Crecimiento exponencial.
- Interconectividad.
- Multiplicidad de sectores y de labores.
- Nuevas opciones de acción y de participación para todo tipo de actores (Betz y Stevens, 2011).
- “Quinta dimensión de combate”

Tierra	Mar	Aire	Espacio exterior
 Ciberespacio			

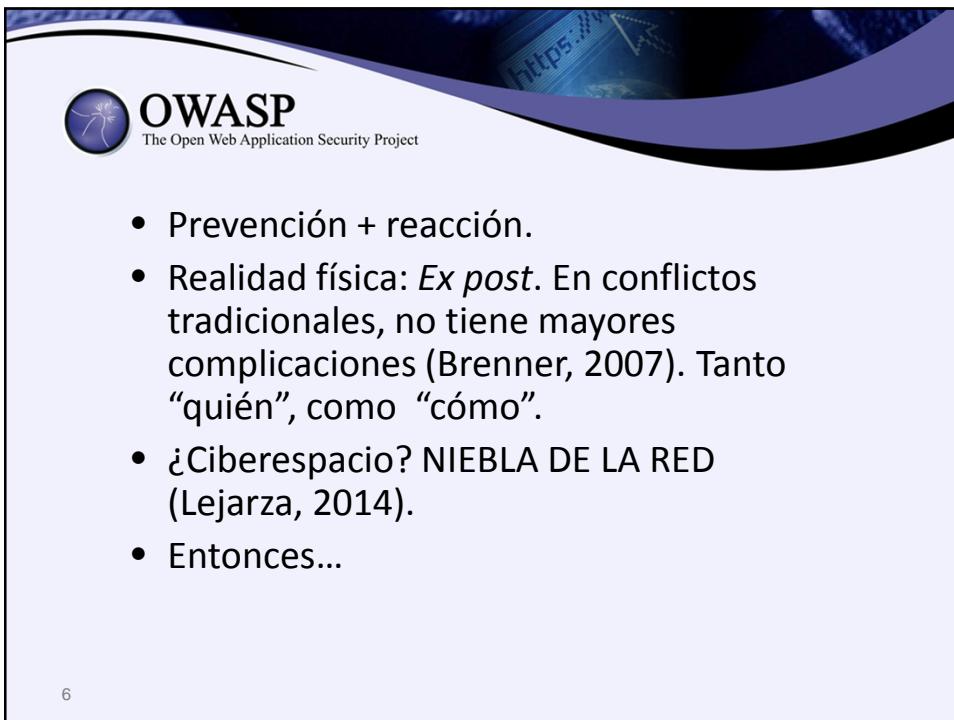
4



The Open Web Application Security Project

- ¿Proliferación de amenazas?
- Ciberseguridad, poco consenso (Vacca, 2012; Tikk, 2011):
 - Conjunto de medidas y elementos (...)
 - (International Telecommunications Union).
 - Ausencia de amenazas (...) (Sánchez de Rojas, 2010).
- Distintos tipos de ataques (backdoors, phishing, DDoS, botnets, logic bombs, entre otros).

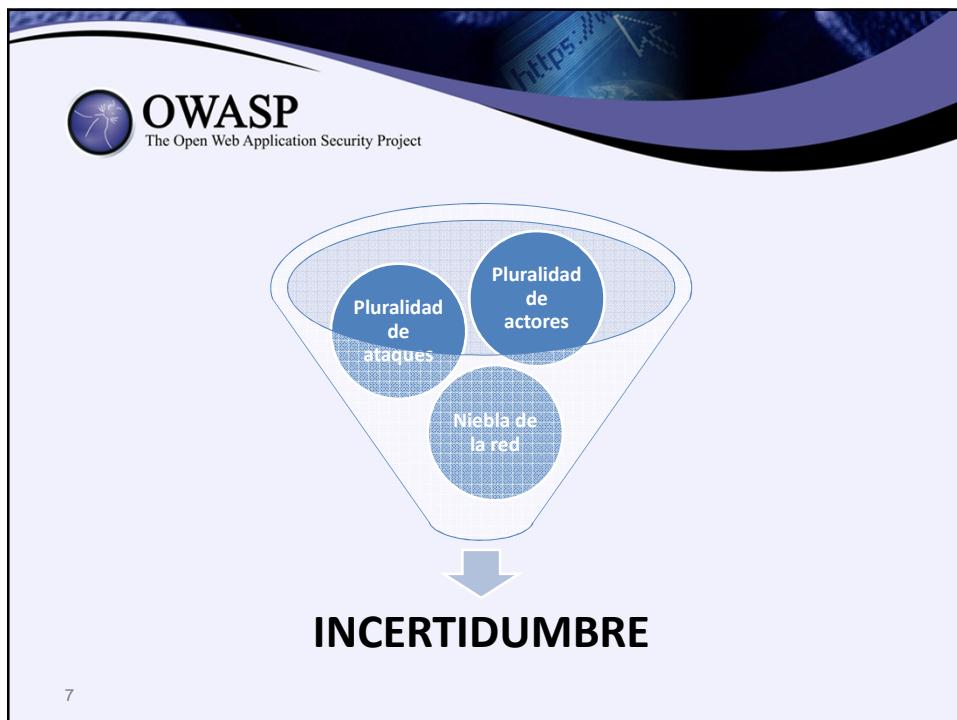
5



The Open Web Application Security Project

- Prevención + reacción.
- Realidad física: *Ex post*. En conflictos tradicionales, no tiene mayores complicaciones (Brenner, 2007). Tanto “quién”, como “cómo”.
- ¿Ciberespacio? NIEBLA DE LA RED (Lejarza, 2014).
- Entonces...

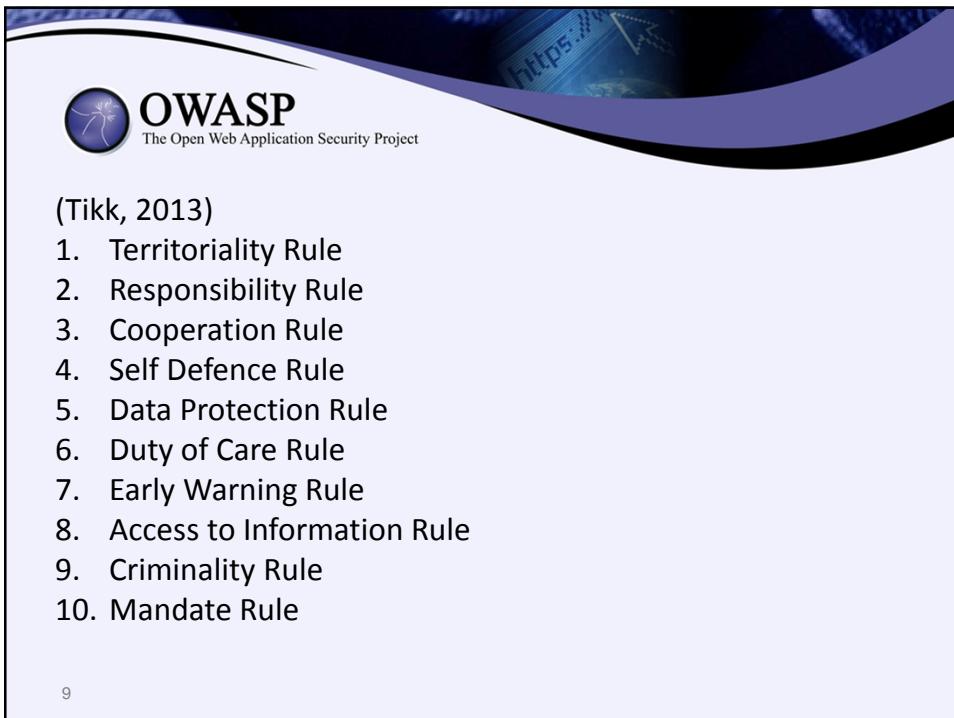
6



7

-
- The diagram features the OWASP logo at the top left. Below it is a funnel-shaped graphic, similar to the one above, but it is mostly empty except for a small portion of the background image visible at the top.
- Attacker-attribution v/s attack-attribution (Brenner, 2007).
 - Dimensión territorial se vuelve irrelevante (Íbid).
 - Intencionalidad se complejiza, al igual que la identificación del atacante (Íbid).

8

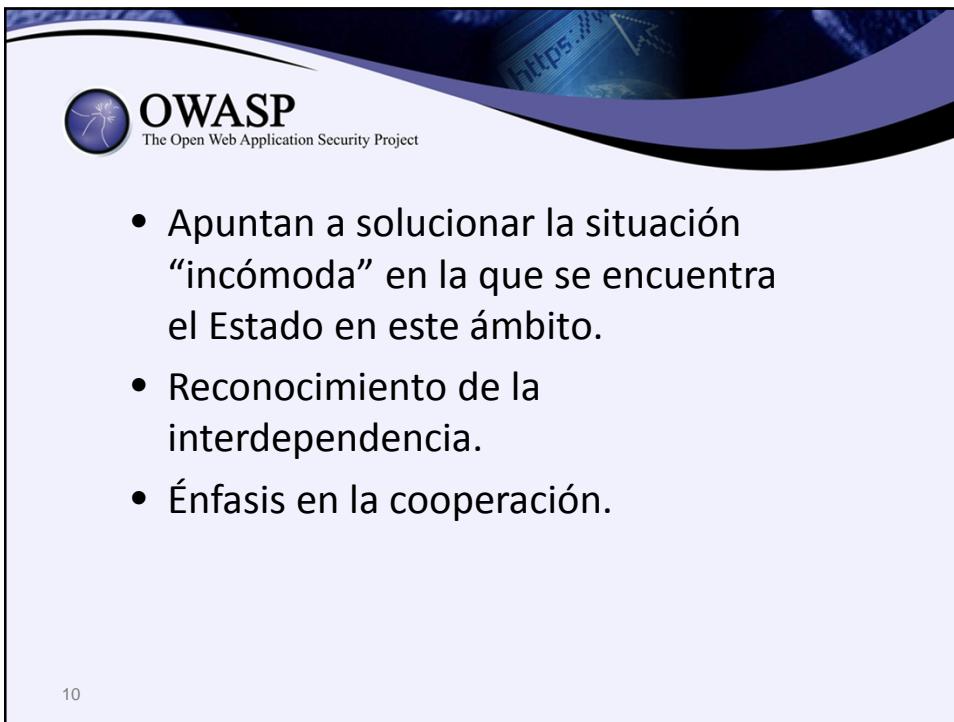


The slide features the OWASP logo at the top left, followed by the text "The Open Web Application Security Project". Below this, a list of ten rules is presented, each preceded by a small blue circular icon. The background of the slide is a dark blue gradient with a wavy pattern.

(Tikk, 2013)

1. Territoriality Rule
2. Responsibility Rule
3. Cooperation Rule
4. Self Defence Rule
5. Data Protection Rule
6. Duty of Care Rule
7. Early Warning Rule
8. Access to Information Rule
9. Criminality Rule
10. Mandate Rule

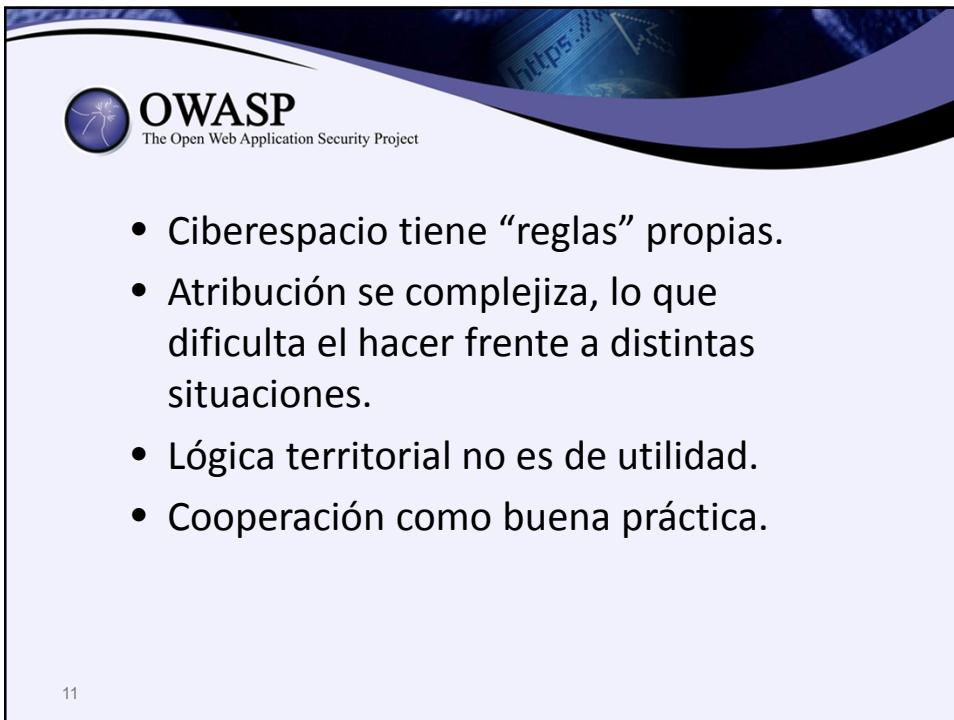
9



The slide features the OWASP logo at the top left, followed by the text "The Open Web Application Security Project". Below this, a bulleted list of three items is presented. The background of the slide is a dark blue gradient with a wavy pattern.

- Apuntan a solucionar la situación “incómoda” en la que se encuentra el Estado en este ámbito.
- Reconocimiento de la interdependencia.
- Énfasis en la cooperación.

10



The slide features the OWASP logo at the top left, followed by the text "The Open Web Application Security Project". Below this is a bulleted list of five items:

- Ciberespacio tiene “reglas” propias.
- Atribución se complejiza, lo que dificulta el hacer frente a distintas situaciones.
- Lógica territorial no es de utilidad.
- Cooperación como buena práctica.

At the bottom left of the slide is the number "11".



The slide features the OWASP logo at the top left, followed by the text "The Open Web Application Security Project". Below this is a large photograph showing a wall of orange reflective spheres, likely Mylar balloons, covering a window or glass partition. Several people are standing in front of the wall, looking through it. The background shows a dark, possibly night-time scene with some lights visible.

At the bottom left of the slide is the number "12".