Guardia Civil

Mando de Apoyo

Jefatura de Servicios Técnicos

Seguridad en las Tecnologías de la Información y la comunicación

Seminario de Amenazas y Vulnerabilidades

Cap. Jesús
Cano Carrillo

ACADEMIA DE INGENIEROS

Estado de alarma, 3 junio de 2020

Entrar

En una pagina pirata y sentirte un hacker

Introducción

- AMENAZA = Elemento capaz de atacar un sistema de información, aprovechando una vulnerabilidad.

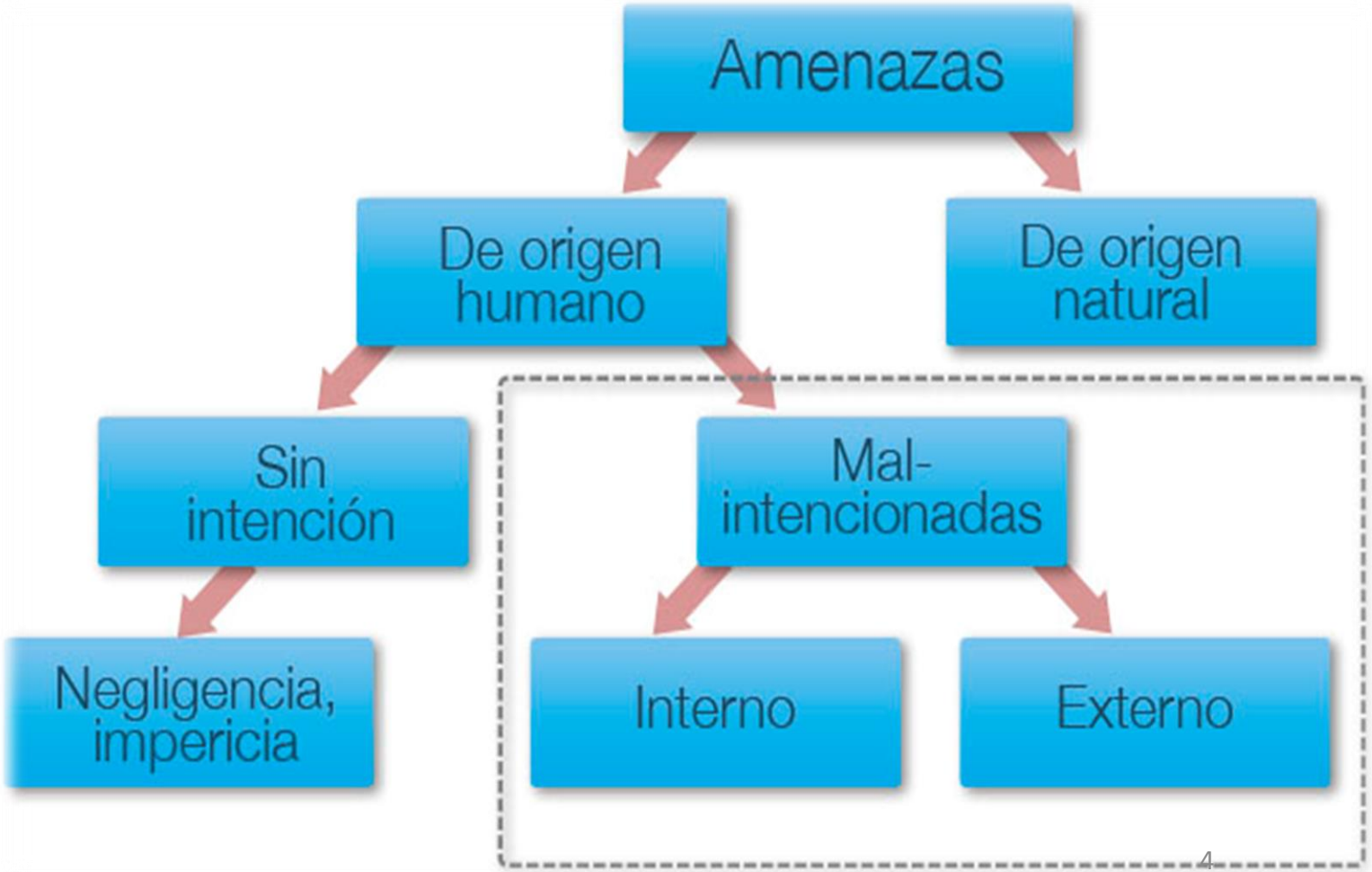
- Advertencia de un posible daño a algún activo de la información

Cualquier elemento del ciberentorno puede considerarse un riesgo de seguridad, que en general se trata de una evaluación ponderada de las amenazas. El análisis de amenazas incluye la descripción del tipo de posibles ataques, los agresores potenciales y sus métodos y las consecuencias del éxito

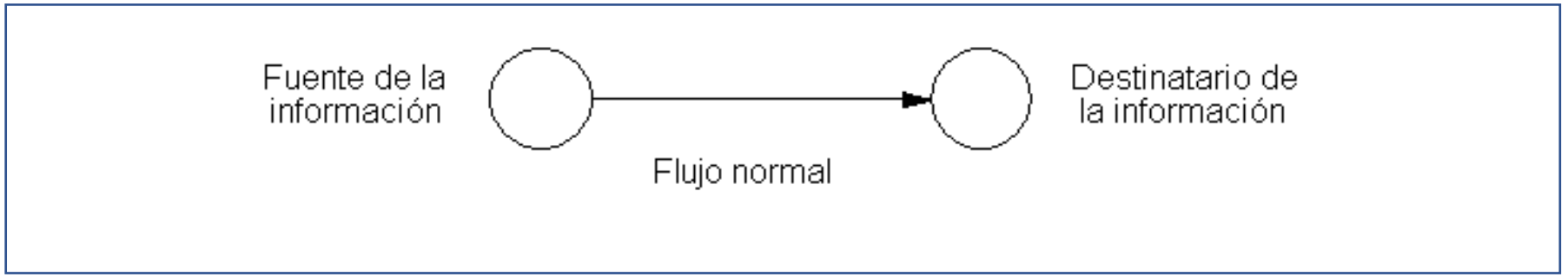
X.1205

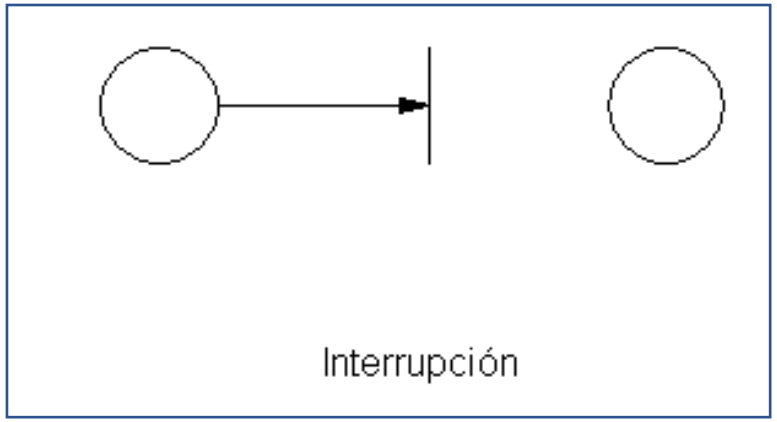
Clasificación general de las amenazas

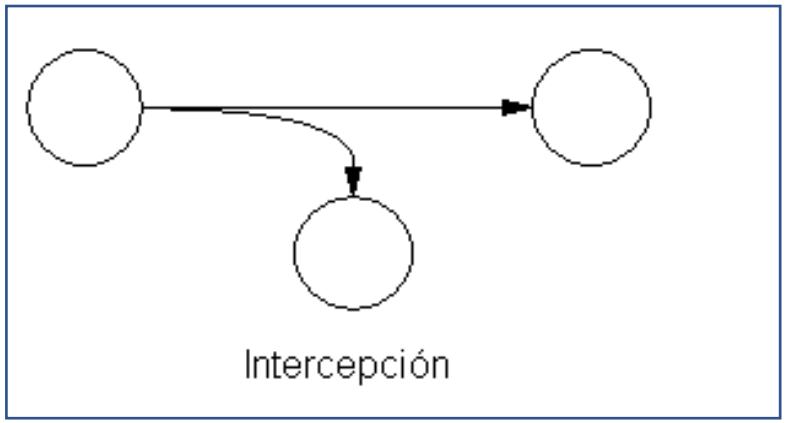
- Humanas / Naturales
- Accidentales: existen sin que sean premeditadas (Ej. bugs, amenazas naturales..)
- Intencionales – Mal intencionadas
- Pasivas: no causarían ninguna modificación de la información, estado o funcionamiento. (Ej. escuchas)
- Activa: alteran la información, estado o funcionamiento. (Ej. Envenenamiento de enrutado)

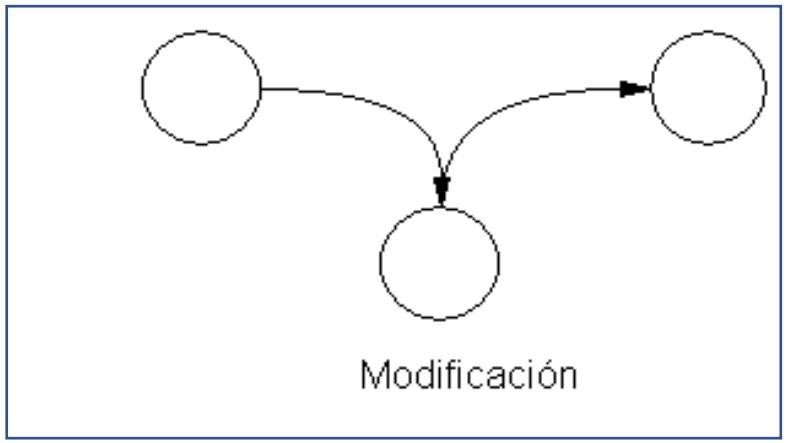


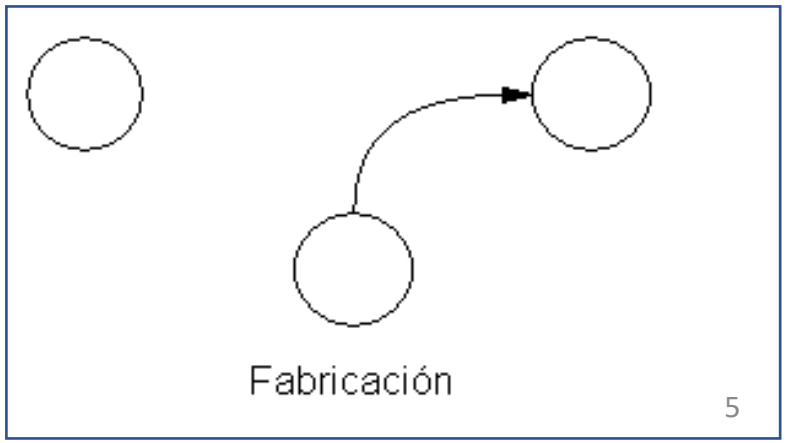
Modelo de amenaza a la información



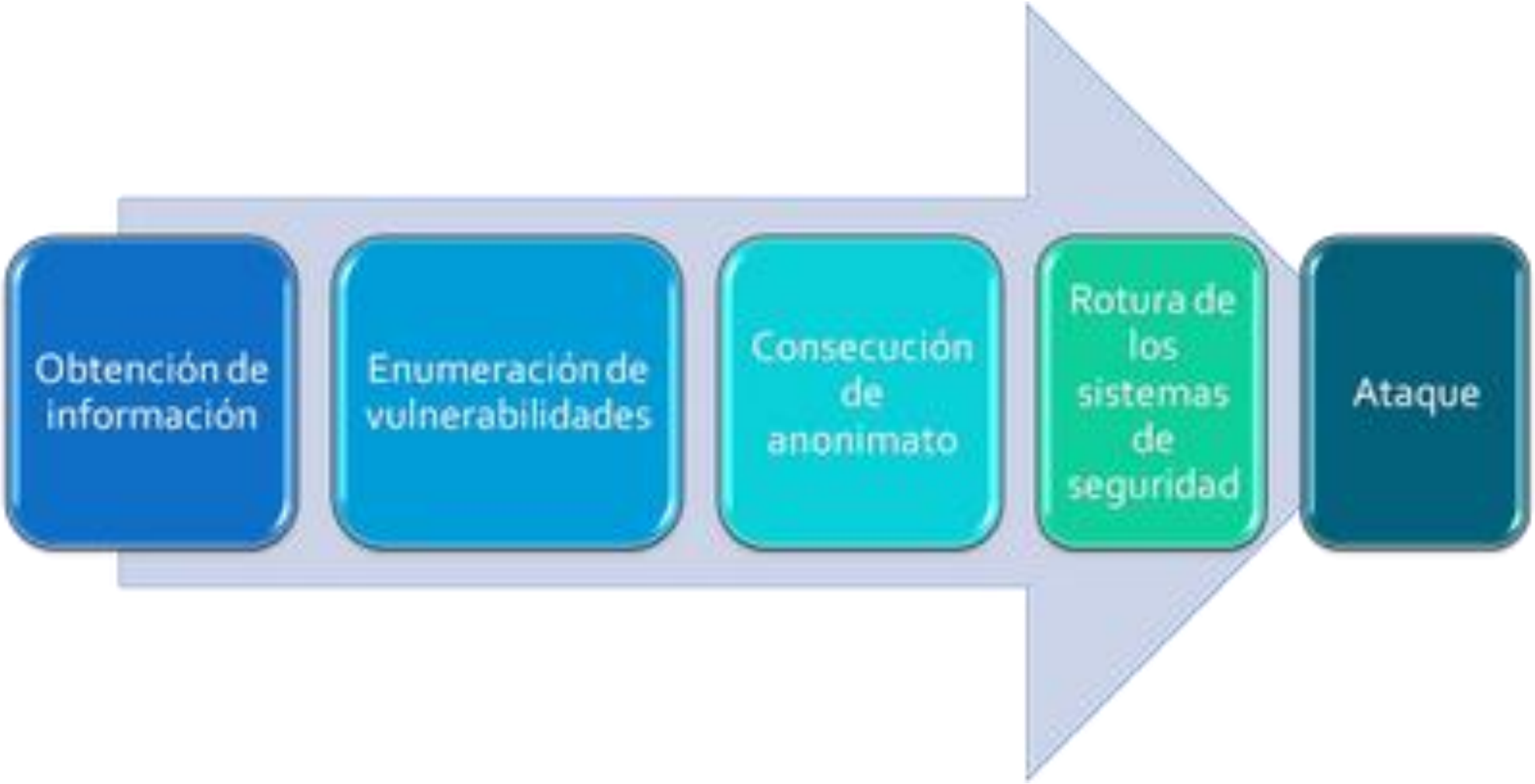








Fases de un ataque informático



Vectores de ataques

These are the attack vectors used by attackers to trigger or reach a vulnerability in a program

Fuente: secunia.com

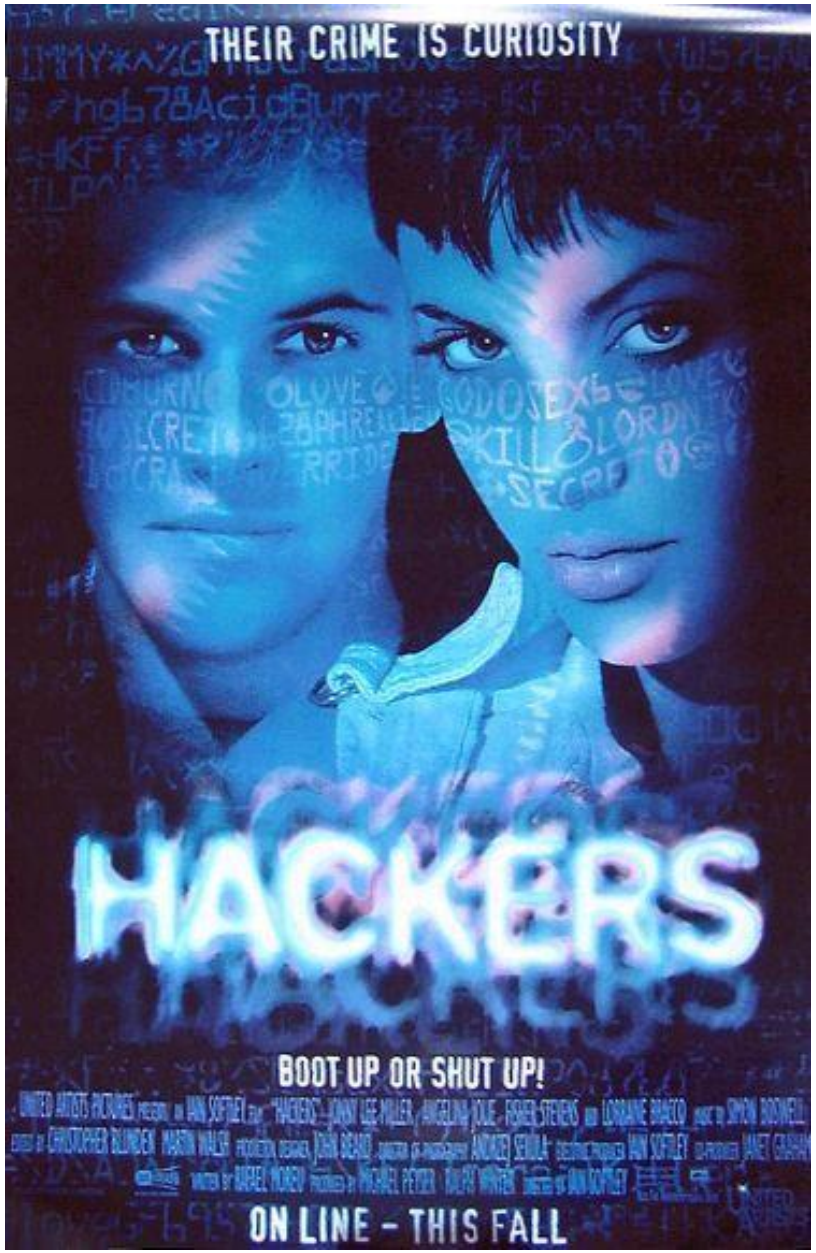
Otras formas

¿Creatividad?

Card skimming. FUENTE: Europol

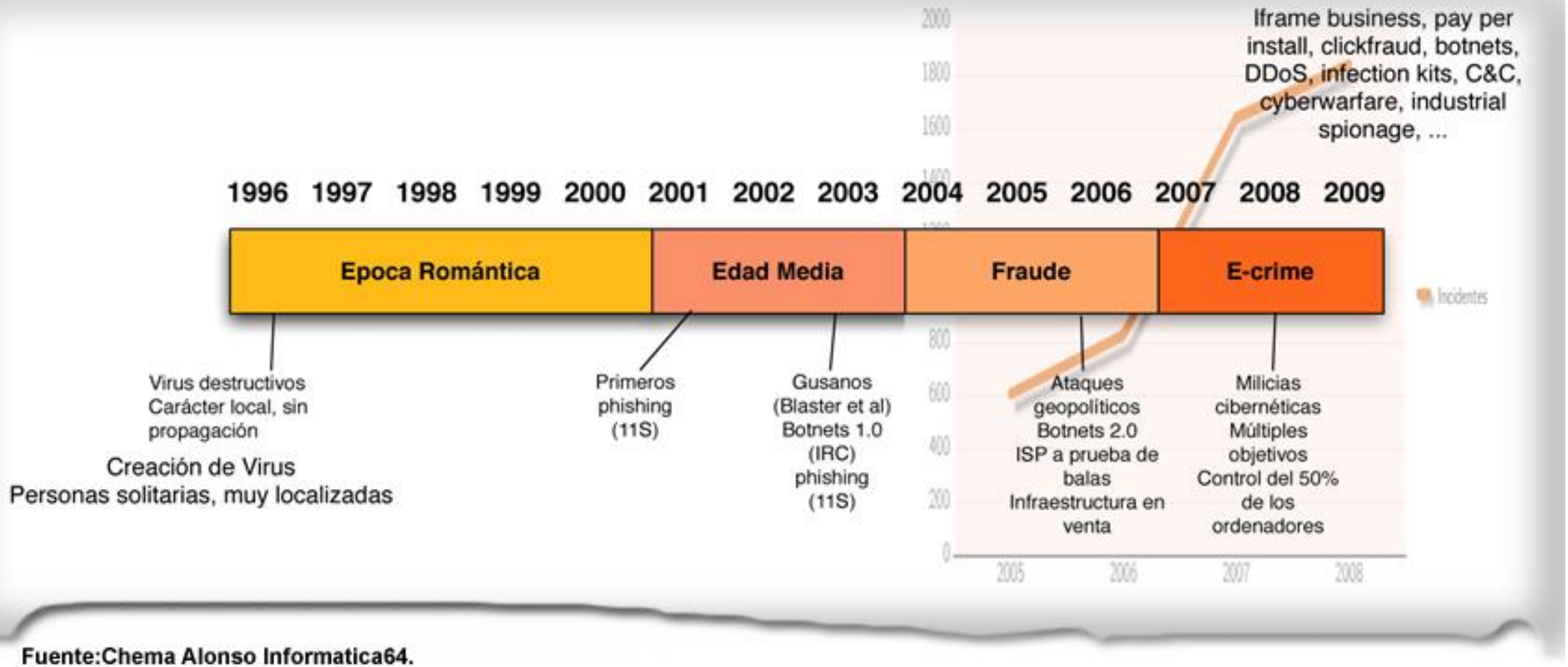
Clases de atacantes

- Hackers
- Crackers (blackhats)
- Sniffers
- Lammers
- Script Kiddies
- Newbies (noob, newb)
- Spammers



Urban Dictionary: lammer
www.urbandictionary.com/define.php?term=**lammer**
lammer. A Person who knows very little about computers/computing. It also refers to a person who pretends to be a hacker but is not. He/She is a **lammer** ...

Las eras de las amenazas



Fuente:Chema Alonso Informatica64.

Conceptualización de la vulnerabilidad

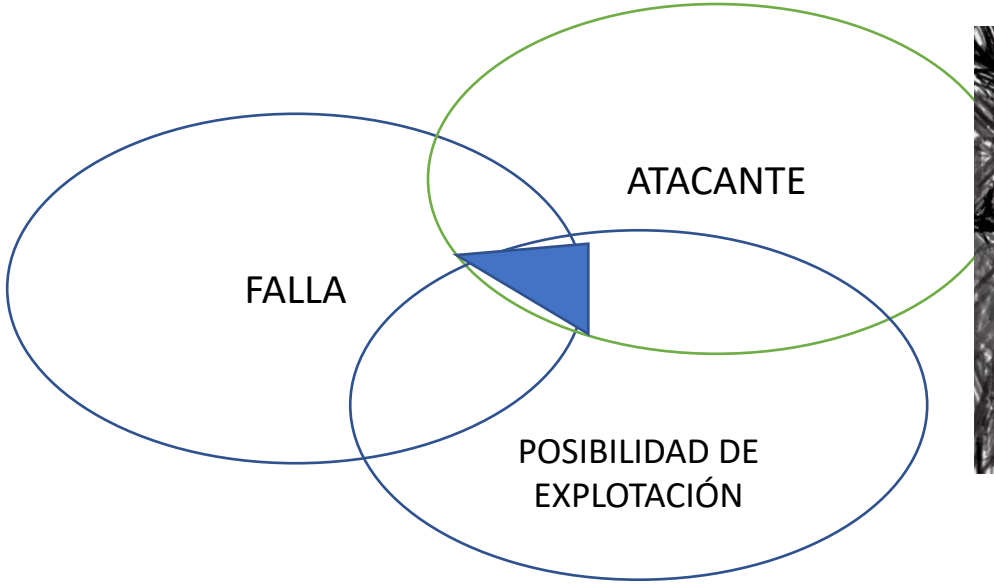
- VULNERABILIDAD = Punto débil de un sistema de información.
- Permite a un atacante comprometer la confidencialidad, integridad o la disponibilidad de la información o del sistema de información.

Def. según UIT-T X.1205

de un ataque. Por otra parte, en esta Recomendación, vulnerabilidad hace referencia a un punto débil que puede ser explotado por un agresor. La evaluación de riesgos sumada al análisis de amenazas permite a la organización evaluar los posibles riesgos a que se enfrenta su red.

Explotar una vulnerabilidad

- “Un sistema tiene muchas vulnerabilidades, pero sólo algunas de ellas son explotables, porque el agresor carece de oportunidades o porque el resultado no justifica los esfuerzos necesarios ni el riesgo de ser detectado”.

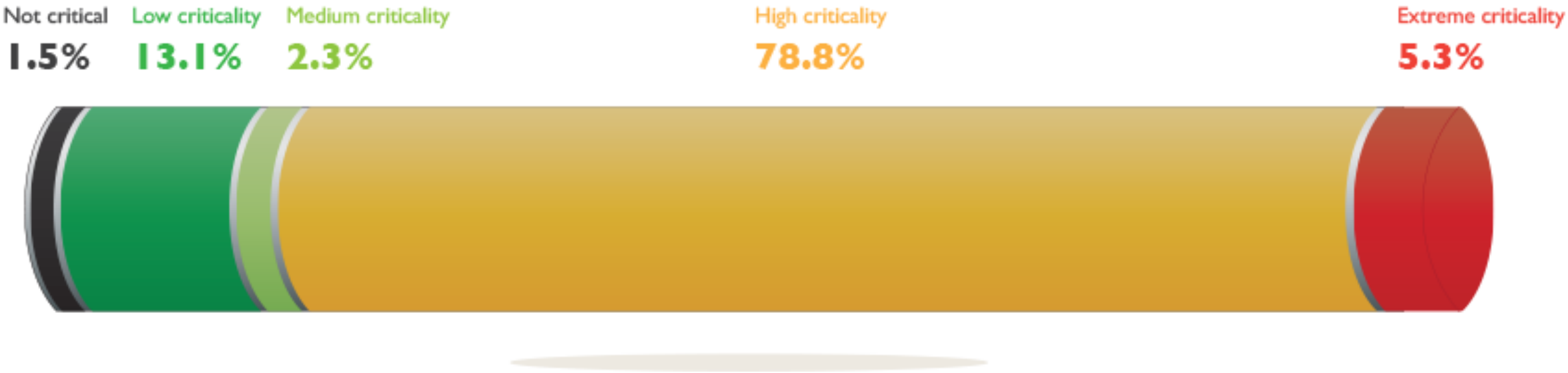


Ciclo de vida de una vulnerabilidad

Investigación y ventana de vulnerabilidad

Fuente: http://twitter.com/godofdez

Peligrosidad estadística



La investigación de vulnerabilidades

- CVE = Diccionario de vulnerabilidades conocidas (cve.mitre.org/)

Vulnerabilidades en aplicaciones web

- **OWASP: Open Web Application Security Project**
- **WASC: Web Application Security Consortium**
- Comunidades formada por empresas, universidades y expertos en seguridad…
- Buenas prácticas, herramientas, documentos, código y recomendaciones …

A vueltas con el control de seguridad

ISO/IEC 27002 lo define en el punto

13. Gestión de Incidentes de Seguridad de la Información

13.1. Comunicación de eventos y debilidades en la SI

13.1.1 Comunicación de eventos en seguridad

13.1.2. Comunicación de **debilidades** en seguridad

Vulnerabilidad más difícil de parchear

“Los cambios no autorizados en la configuración y en la instalación de nuevo software explotan la "vulnerabilidad humana", que es una vulnerabilidad que no puede ser parcheada”.

Bibliografía

Microsoft Security Intelligence Report http://www.microsoft.com/security/sir/default.aspx		web
Liang, H., and Xue Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," MIS Quarterly (33:1), pp. 71-90. Maddux, J. E., Norton, L. W., and Stoltenberg, C. D. 1986. "Self-Efficacy Expectancy, Outcome Expectancy, and Outcome Value: Relative Effects on Behavioral Intentions," Journal of Personality and Social Psychology (51:4), pp. 783-789. Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," MIS Quarterly (34:3), pp. 613-643. La Rose, R., Rifon, N. J., and Enbody, R. 2008. "Promoting Personal Responsibility for Internet Safety," Communications of the ACM (51:3), pp. 71-76.		

ACADEMIA DE INGENIEROS

Seminario de ciberseguridad sobre amenazas y vulnerabilidades