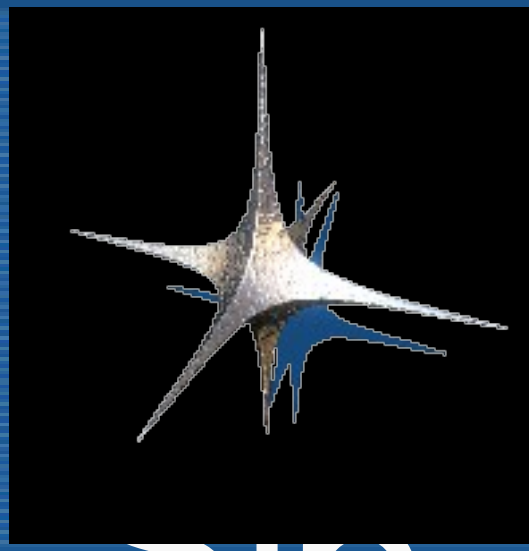
Instituto de Investigaciones Científicas y Técnicas para la Defensa

Ciberdefensa: Relación entre el MinDef y Organismos de I+D



SIO

Dpto. Seguridad Informática
Gcia. de Informática

Agenda

- **Introducción**
- **CITEFA**
- **Proyectos de I+D**
- **Vinculaciones**
- **Modelo**

Introducción

- Necesidad de I+D
  - Falta de conocimientos formales en el area.
- RRHH Limitados
  - Poca gente con conocimientos y experiencia en I+D en seguridad informatica.
- Recursos escasos para I+D
  - Competencia por recursos con otras areas de I+D tradicionales

CITEFA

50+ Años en I+D

Creación del Si6 (2004)

CITEDEF (2009)

Proyectos de I+D Si6

Paranoid (perfiles de intrusos)

iProfiler (perfiles de intrusos)

Protección Aplicaciones Web

Centro de Operaciones de CiberSeguridad

Proyectos Si6 (Líneas de Investigación I)

- Honeypots
  - Ocultamiento de módulos de captura de datos para Honeypots
  - Desarrollo e Instalación de Honeypots virtualizados
  - Análisis de intrusiones sobre Honeypots

- Análisis de utilización de comandos (*Command Behavior*)
  - Clasificación por Complejidad de Kolmogorov
    - Aproximación por algoritmos de compresión
  - Clasificación por SVM (*Support Vector Machines*)
  - Clasificación por redes neuronales tipo SOM (*Self Organizing Maps*)
    - SOM
    - SOM Supervisada
    - LVQ (*Learning Vector Quantization*)
  - Reducción de dimensionalidad
    - PCA (*Principal Component Analysis*), FA (*Factor Analysis*)
    - Extracción de comandos

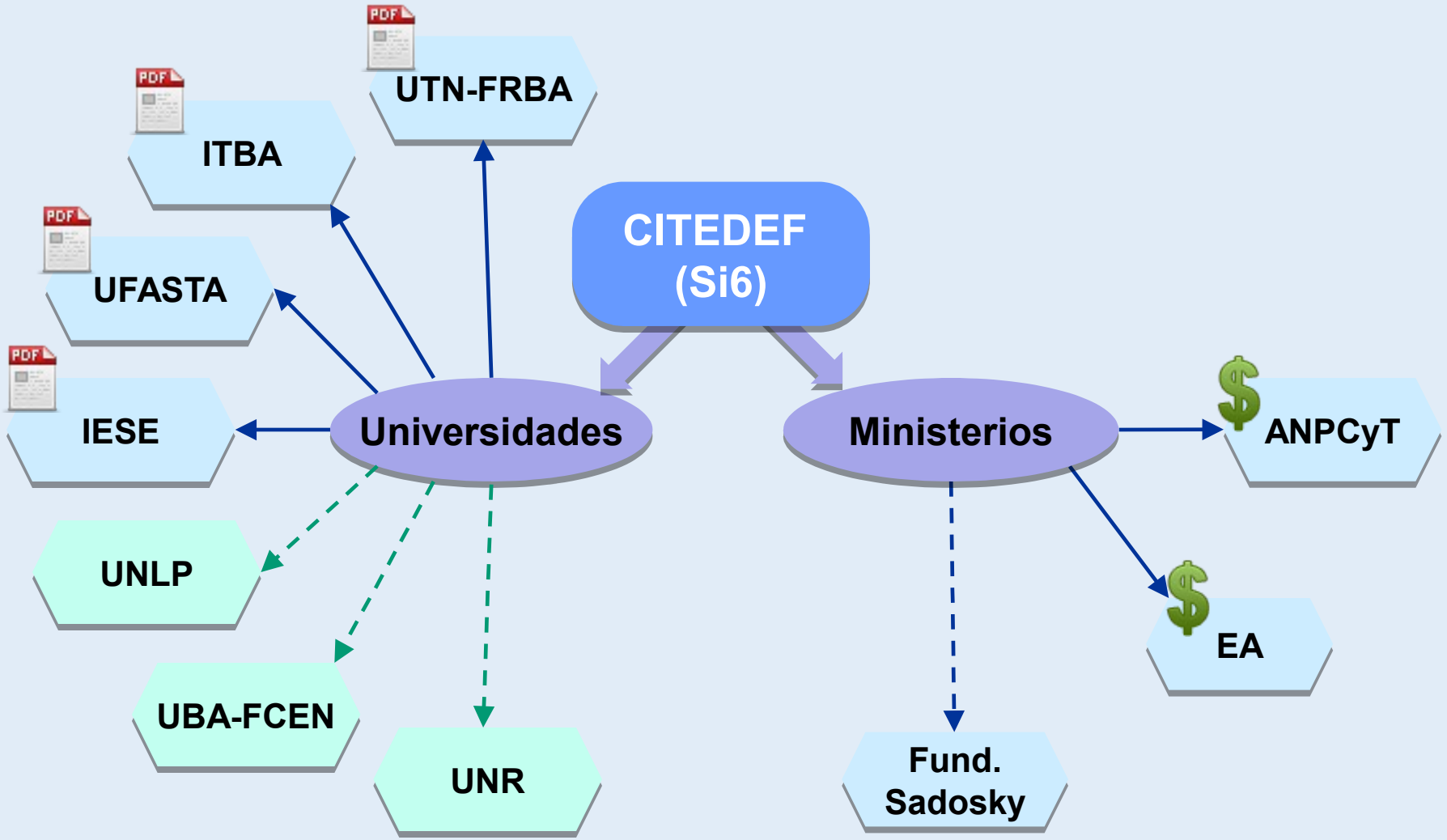
Proyectos Si6 (Líneas de Investigación II)

- Análisis de patrones de tipeo (*Keystroke Dynamics*)
  - Autenticación por patrones de tipeo a través de Internet
  - Sistema k-Profiler

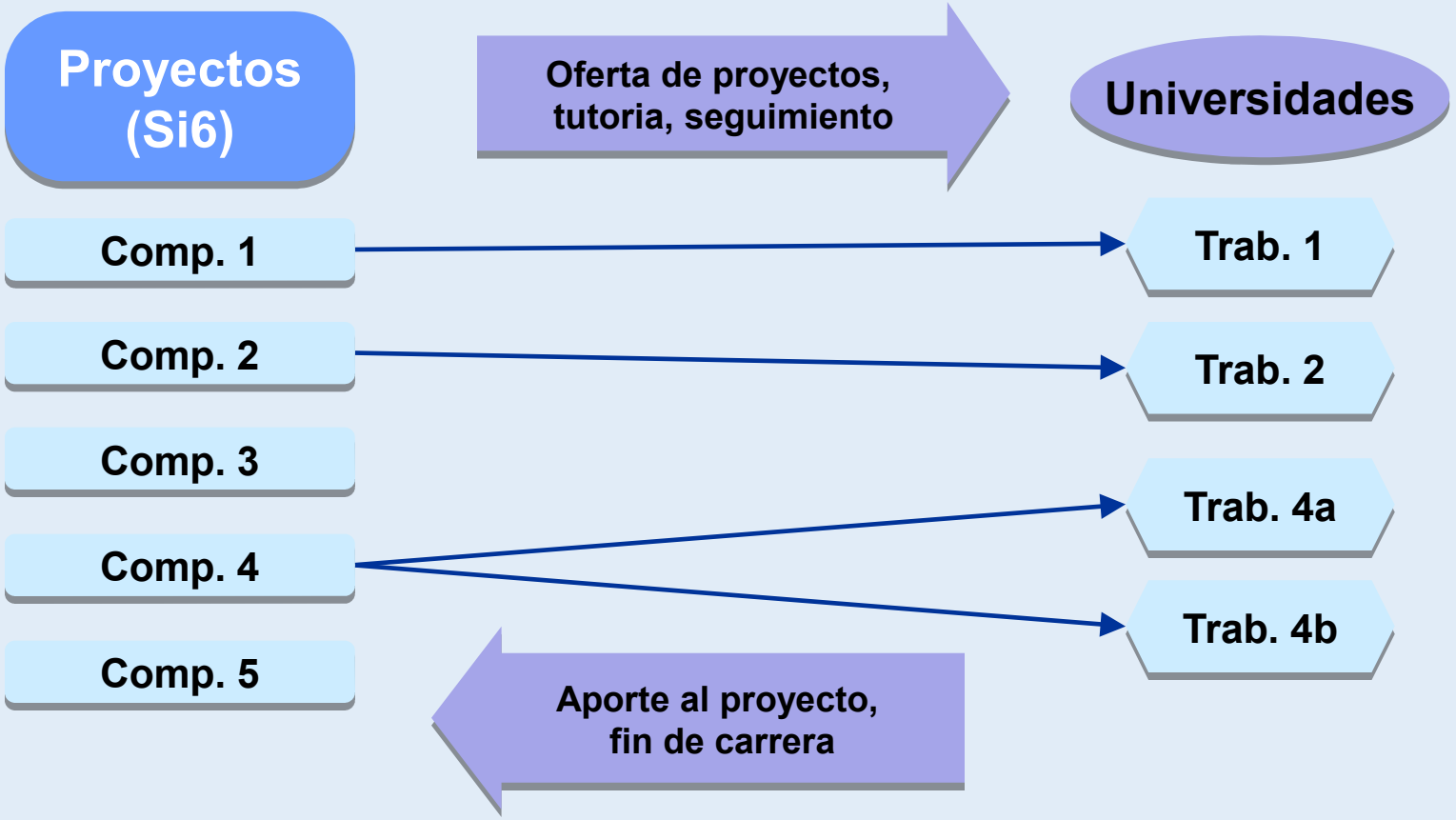
- Análisis de anomalías en aplicaciones web
  - Extracción de características
    - Redes neuronales
    - SVM (*Support Vector Machines*)
    - Perceptron multicapa
    - Regresión logística
    - K-means

- Implementacion de Centro de Operaciones de Ciberseguridad

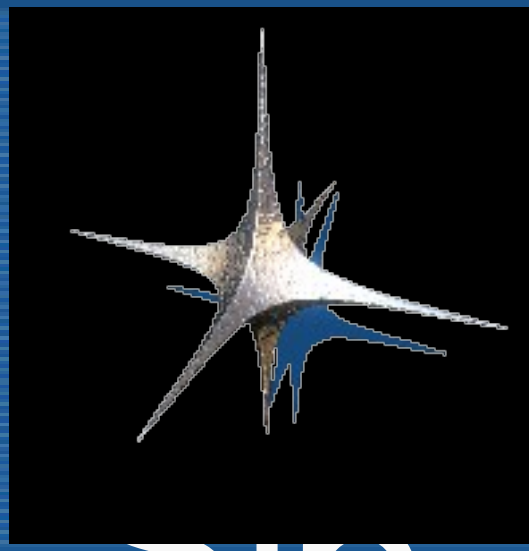
Vinculaciones



Modelo


Proyectos (Si6)
Oferta de proyectos, tutoria, seguimiento
Universidades
Comp. 1
Comp. 2
Comp. 3
Comp. 4
Comp. 5
Trab. 1
Trab. 2
Trab. 4a
Trab. 4b
Aporte al proyecto, fin de carrera

Instituto de Investigaciones Científicas y Técnicas para la Defensa



Hugo Ballesteros
hballesteros<at>citedef.gob.ar
Carlos Benitez
cbenitez<at>citedef.gob.ar
http://www.citedef.gob.ar/

muchas gracias

Dpto. Seguridad Informática
Gcia. Informática