Ciencia de Datos
e
Inteligencia Artificial
para
la Ciberseguridad

David Ríos

Real Academia de Ciencias

Y

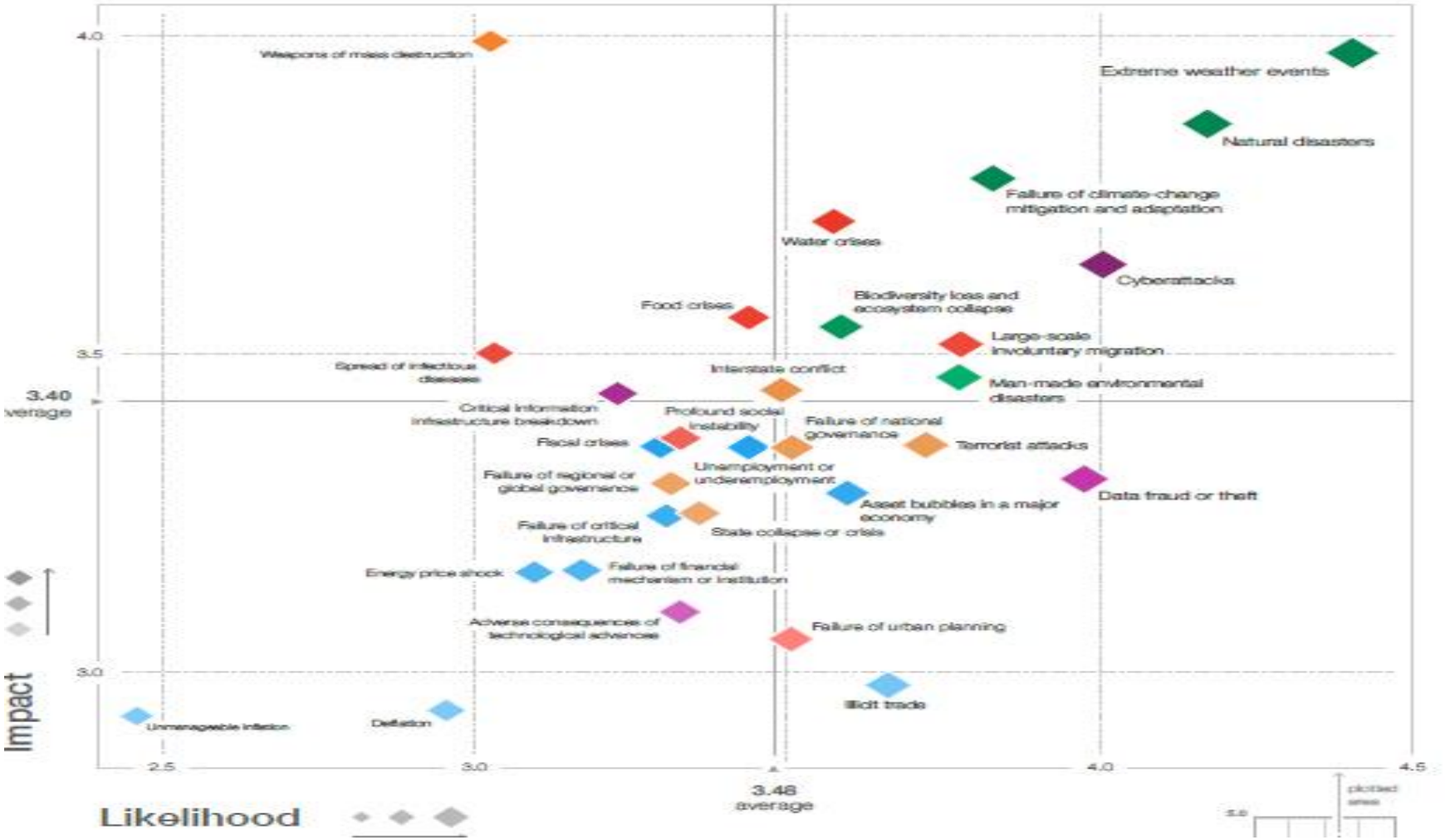
AXA-ICMAT Chair in Adversarial Risk Analysis, DataLab ICMAT, CSIC

Bilbao , Febrero 2018

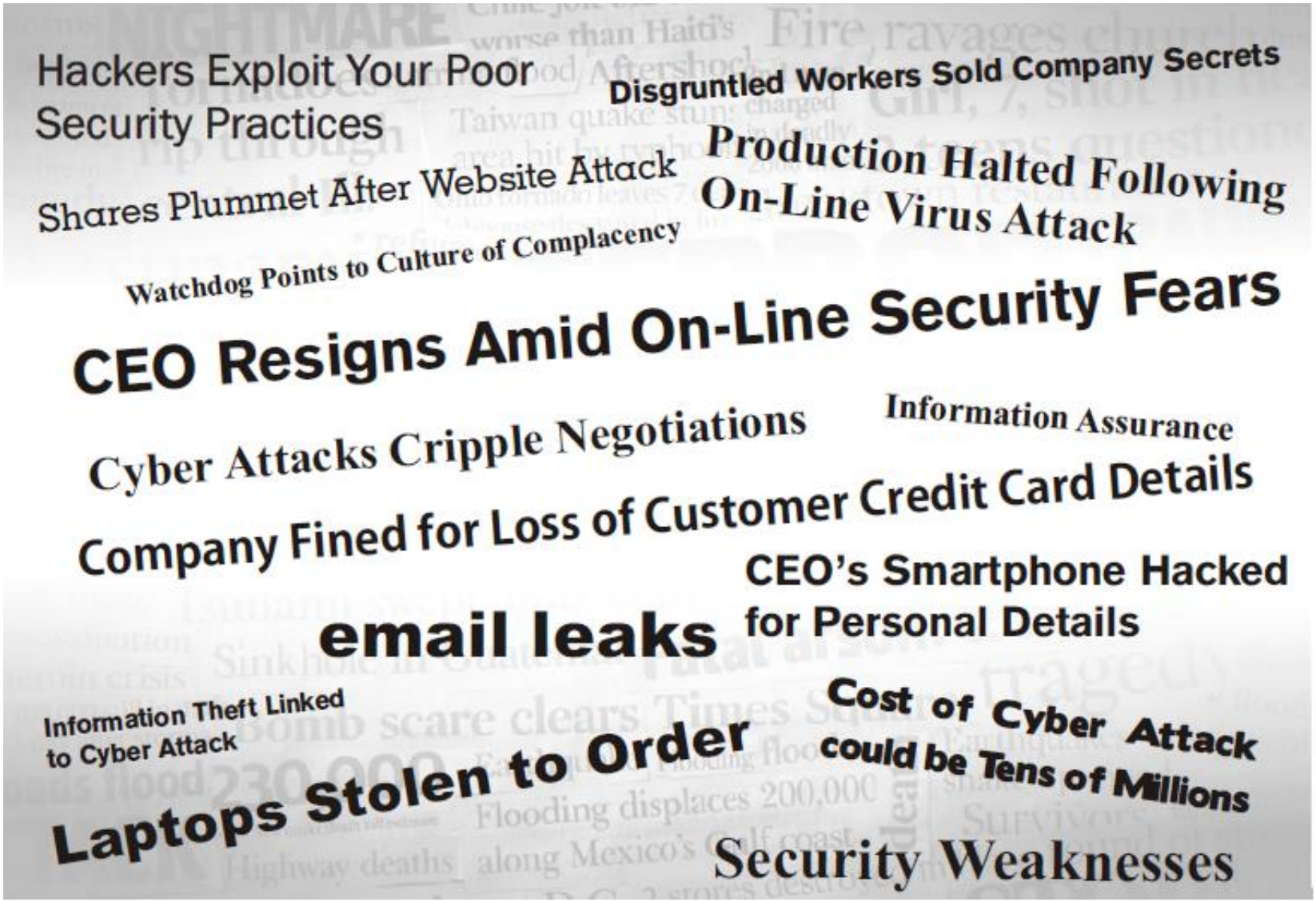
Agenda

- **Ciberseguridad**
- Estándares de ciberseguridad
- Ciencia de Datos e IA para ciberseguridad
- Discusión

World Economic Forum. Global Risks Map 2018



Ciberseguridad en la prensa

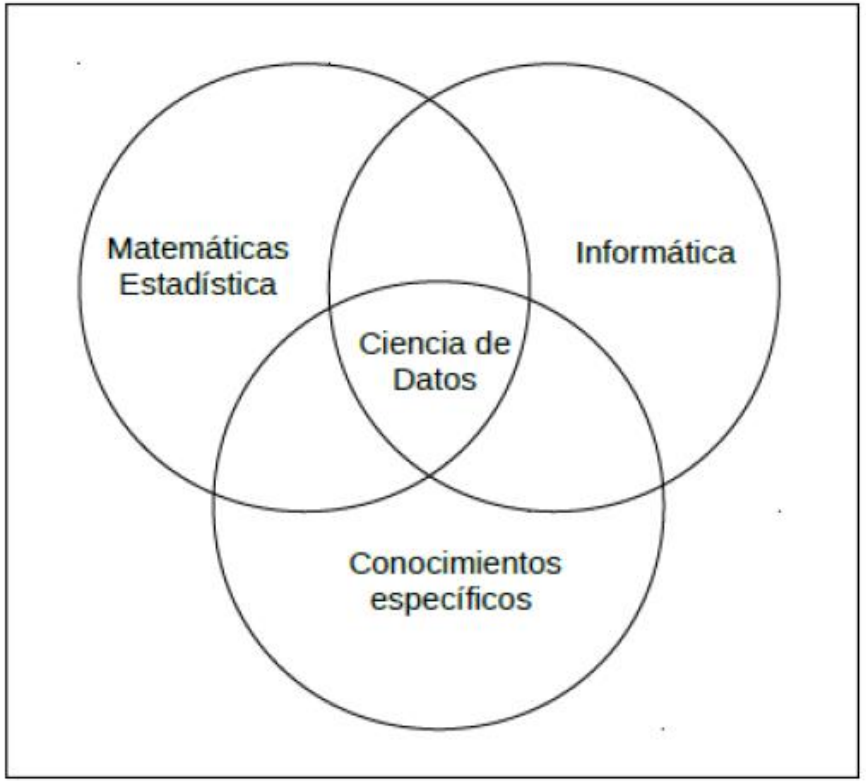


Ciberseguridad. Perspectivas

- Tecnológica
- Económica
- Psicológica
- Sociológica
- Legal
- Política
- Matemática

Ciberseguridad. Perspectivas

- Tecnológica
- Económica
- Psicológica
- Sociológica
- Legal
- Política
- Matemática. Ciencia de Datos



Ciber riesgos

- Virus, Gusanos, Troyanos, Spyware, Ransomware, APTs,…
- Número creciente de ciberamenazas, crecientemente sofisticadas
  - MacAfee cataloga alrededor de 70 nuevas amenazas por minuto
- Tiempo de respuesta es excesivo
- Inmensos daños económicos (ambientales, de salud,….), inteligencia competitiva, seguridad nacional,…
- Coches, aviones, sistemas médicos, de inversión, de votación, infraestructuras críticas, robots,… cada vez más dependientes en TIC
- IoT. Cada vez más sistemas interconectados: 10000 M dispositivos conectados a Inet
- Países, ciberdelincuentes, ciberterroristas, actores internos,…..

Ciber riesgos

- Stuxnet, Flame, Duqu,… **dirigidos contra** programa nuclear iraní
- Shamoon ataque **dirigido contra** ARAMCO
- Ataque **dirigido contra** Estonia

- Wannacry. **No dirigido**. Paró servicio salud GB,….

Ciber riesgos

- 450b$ impacto sobre la economía global 2014.
- 0.8% del PIB global (0.9% del tráfico de drogas, 1.2% de la delincuencia internacional)

- Mercado negro
- Quinto espacio de operaciones

- Ciberriesgos en la cadena de suministro. Sistemas interconectados
  - Ataque a Target a través de su proveedor de aire acondicionado. 40 M tarjetas robadas

Agenda

- Ciberseguridad
- **Estándares de ciberseguridad**
- Modelos para la ciberseguridad
- Discusión

Aproximaciones

- Marcos para el análisis de riesgos: CRAMM, EBIOS, ISAMM, Magerit, ISO 27005, MEHARI, NIST 800-30, ISO 31000,...
- Marcos para la evaluación del control y el cumplimiento: ISO27001, ISO 27002, SANS Critical Security Controls, Common Criteria, Leyes de Protección de Datos, ISO 27031, Cloud Security Alliance Cloud Controls Matrix,…
- Catálogos excelentes de activos, amenazas, contramedidas,….
- Pero los métodos de gestión de riesgos…

Aproximaciones

Matrices de riesgos

VH	100	Very frequent	Daily
H	10	Frequent	Monthly
M	1	Normal	Yearly
L	1/10	Infrequent	Every few years
VL	1/100	Very infrequent	Every century

Impact		Degradation		
		1%	10%	100%
Value	VH	M	H	VH
	H	L	M	H
	M	VL	L	M
	L	VL	VL	L
	VL	VL	VL	VL

Risk		Probability				
		VL	L	M	H	VH
Impact	VH	H	VH	VH	VH	VH
	H	M	H	H	VH	VH
	M	L	M	M	H	H
	L	VL	L	L	M	M
	VL	VL	VL	VL	L	L

Aproximaciones

Defectos bien conocidos!!!!!

- Asignaciones ambiguas
- Evaluaciones erróneas y poco coherentes
- Asignación de recursos subóptima

Intencionalidad?? HMG IS1…..

Pocos datos compartidos…..

Marco ciberseguridad NIST

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

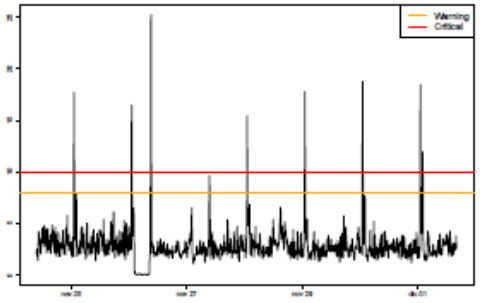
Agenda

- Ciberseguridad
- Estándares de ciberseguridad
- **Modelos para la ciberseguridad**
- Discusión

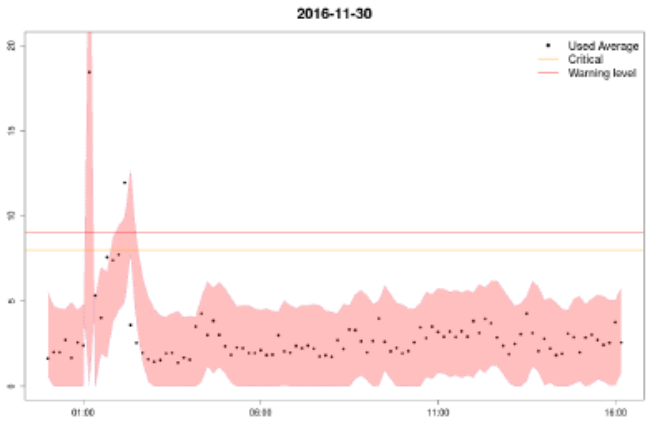
Monitorización de la red para seguridad (safety and security)

- Detect (Anomalies and Events)
- Sistema que recoge medidas +300K de dispositivos conectados a Internet!!!!
- Por cada dispositivo varias medidas
- Cada muy poco tiempo (1 min, 5 min, 10 min)
- Big Data!!!
- Sistema de monitorización descriptivo: si se alcanzan valores críticos, alarma
- Capacidad predictiva???

Monitorización de la red para seguridad



- Tres requisitos
  - Automático
  - Flexible y Versátil
  - Escalable (en tiempo y memoria). Tiempo real
- Diseñar una clase genérica de modelos de predicción Tendencia+estacional(s)+estallidos
- Procedimiento automatizado de identificación
- Alarmas (corto y largo plazo) si
  - Predicen niveles críticos
  - Cambios repentinos detectados



Clasificación adversaria

- Detect (Detection Process)
- Problema de clasificación. Llega un objeto. Debemos decidir a qué clase pertenece:

  spam/no spam; malware/ no malware; severidad 1-2-3-4-5; fake news/no fn
- Modelos estadísticos, IA y ML: Naive Bayes, Support Vector Machines, Deep Neural Nets,…

- Olvidan que hay malos dispuestos a atacar nuestro sistema

Clasificación adversaria

- Aprendizaje máquina adversaria
- Teoría de Juegos

  C calcula su clasificador óptimo

  A lo sabe, calcula su ataque óptimo

  C lo sabe y calcula su defensa óptimo

  ….

  Bajo condiciones de conocimiento común!!!
- Muy poco realista

Clasificación adversaria

- Análisis de riesgos adversarios
- Problema de decisión de C. Incertidumbre: Qué ataque ha utilizado A??
- Problema de A. Incertidumbres sobre sus elementos. Usamos la información disponible. Simulamos para predecir ataque. Incorporamos a problema de C.
- Obtenemos mejoras espectaculares sobre el estándar actual Naive Bayes (sensible a utilidades)
- Todavía muy lento para algunas aplicaciones en tiempo real….

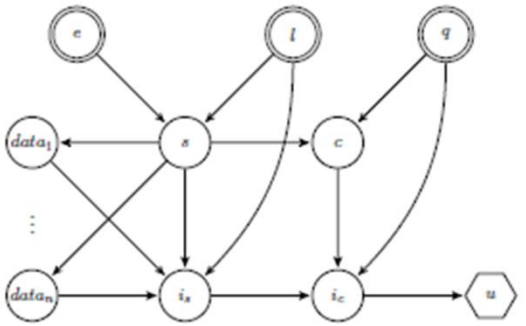
Gestión de ciber riesgos en la cadena de suministro

- Ident. (Risk Assessment), Detect (Cont.Sec.Mon.)
- Sistema inteligencia amenazas. Captura en red:
  - Incidentes (IPs dispositivos contaminados, Malware capaz de afectar la infraestructura,…)
  - Entorno de seguridad (Noticias en blogs hacktivistas,…)
  - Postura de seguridad (Cadencia de parcheo,…)

  sobre una compañía y sus proveedores
- Sistema descriptivo de monitorización
- Evaluación de riesgo?? Predictivo??

Gestión de ciber riesgos en la cadena de suministro

- Big Data/Small Data
- Modelos Ciencia de Datos:
  - Si un proveedor será atacado (dada la información,…)
  - Impacto sobre proveedor (disponibilidad)
  - Si tal ataque se propagará al cliente
  - Si el cliente será atacado directamente
  - Impacto sobre cliente (disponibilidad, reputación)
- Agregación de impactos
- Actitud frente al riesgo



Gestión de ciber riesgos en la cadena de suministro

- Probabilidades de ataque
- Riesgo sobre cliente
- Riesgo sobre cliente debido al proveedor
- Riesgo total

- Predicción sobre esas medidas de riesgo!!!

- Alarmas
- Clasificar proveedores
- Dar recomendaciones a proveedores
- Negociar SLAs
- Seguros

Gestión de ciber riesgos (CYBECO)

- Identify (Risk Management Strategy)
- Cuál es la mejor inversión en medidas de seguridad (incluyendo **ciberseguro**) frente a ciber riesgos?

Cuál es el mejor mantenimiento HW/SW para nuestro ERP?

Modelizar sistema HW/SW (bloques HW y SW que interactúan)

Predecir fiabilidad de bloques

Predecir fiabilidad sistema

Diseñar políticas de mantenimiento

Predecir impacto sobre fiabilidad (y costes)

Política óptima mantenimiento

Cuál es el mejor mantenimiento HW/SW para nuestro ERP?

Modelizar sistema HW/SW (bloques HW y SW que interactúan)

Predecir fiabilidad de bloques

Predecir fiabilidad sistema

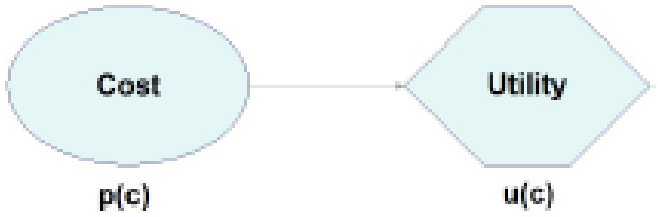
Diseñar políticas de mantenimiento

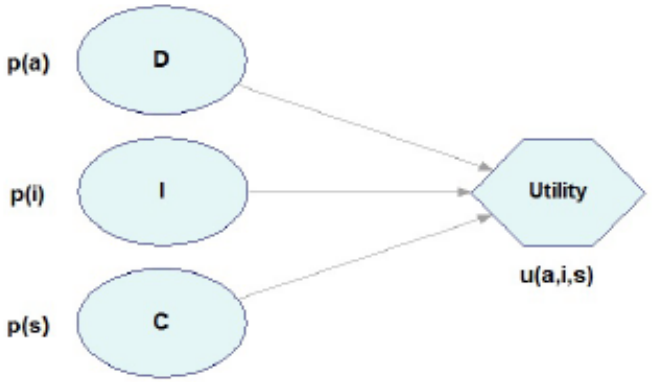
Predecir impacto sobre fiabilidad (y costes)

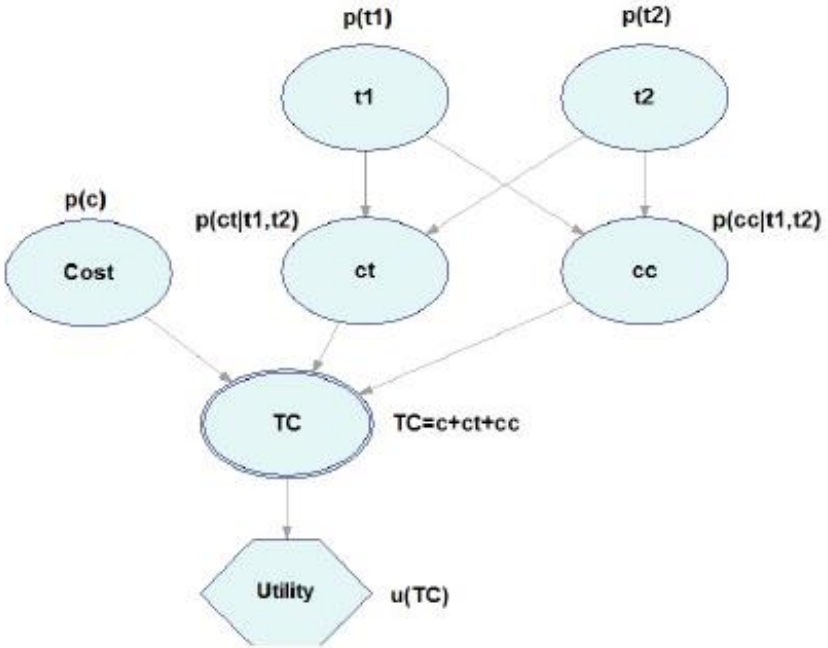
Política óptima mantenimiento

NB: Qué ocurre con los malos que atacan nuestro sistema?

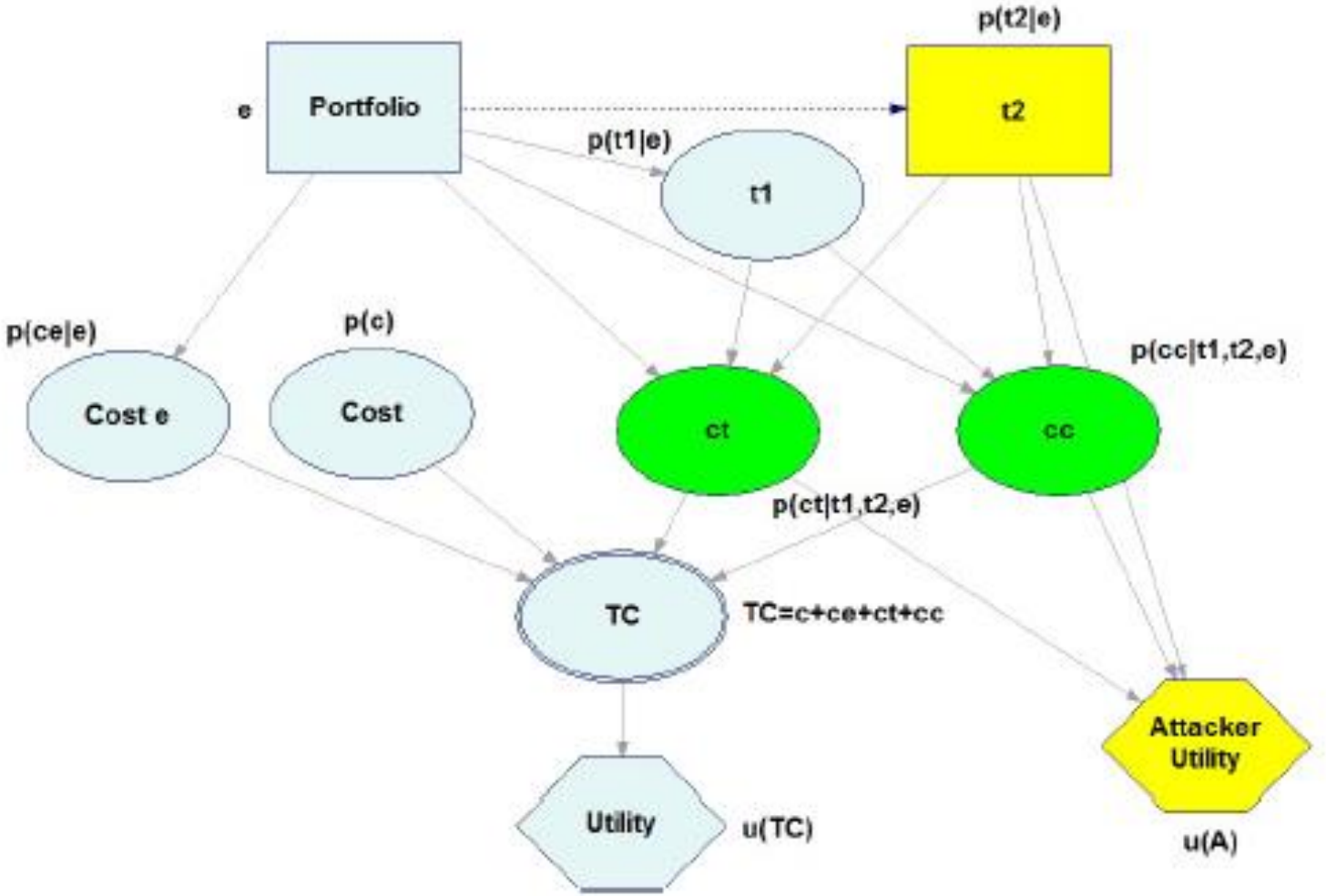
Análisis de riesgos en ciberseguridad



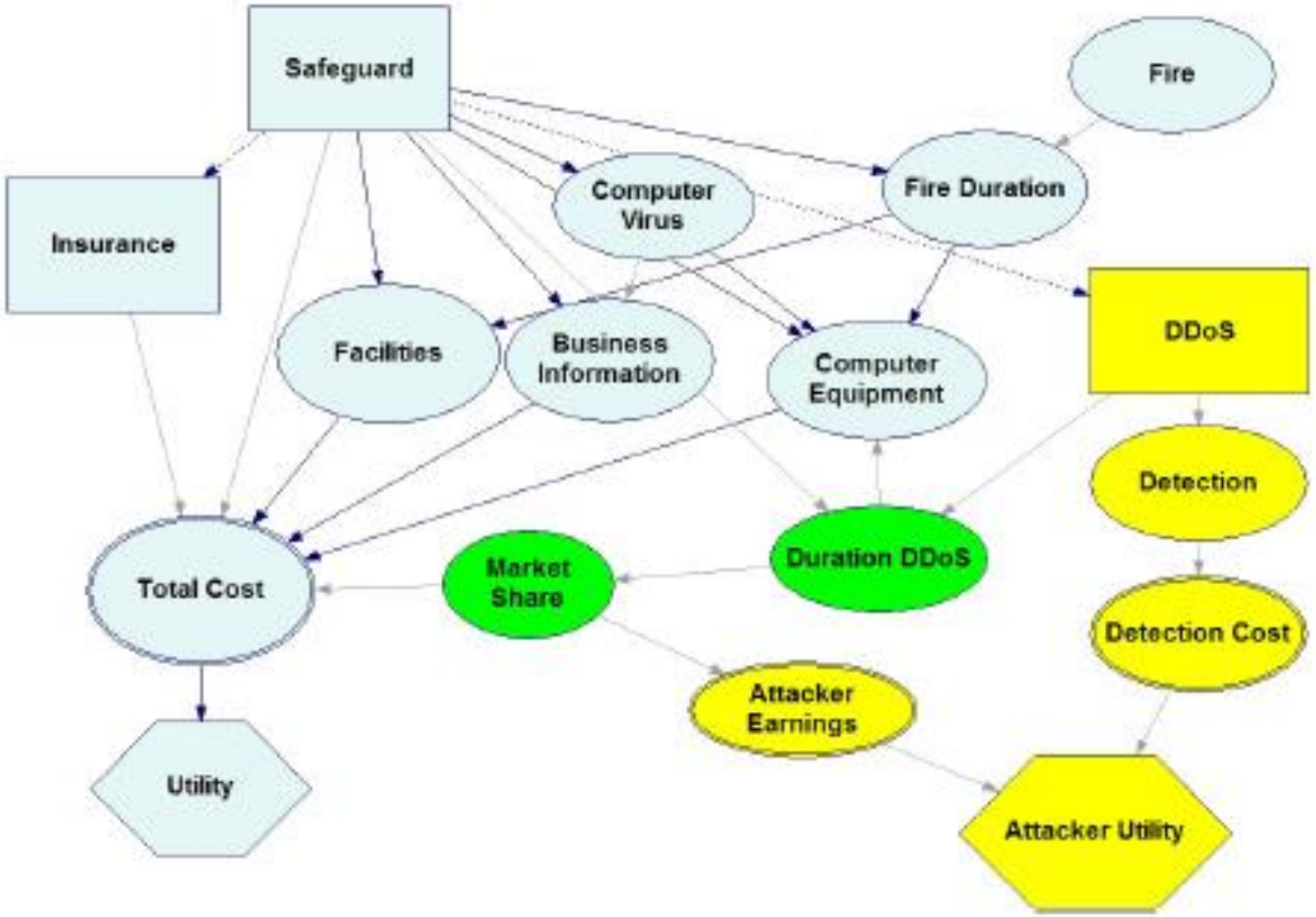




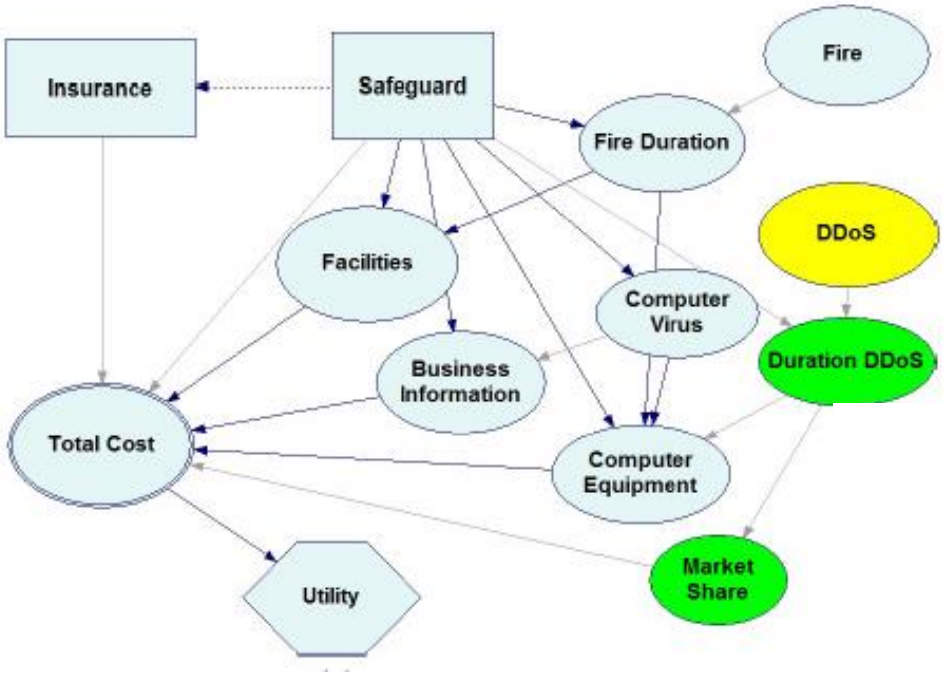
Análisis de riesgos adversarios en ciberseguridad

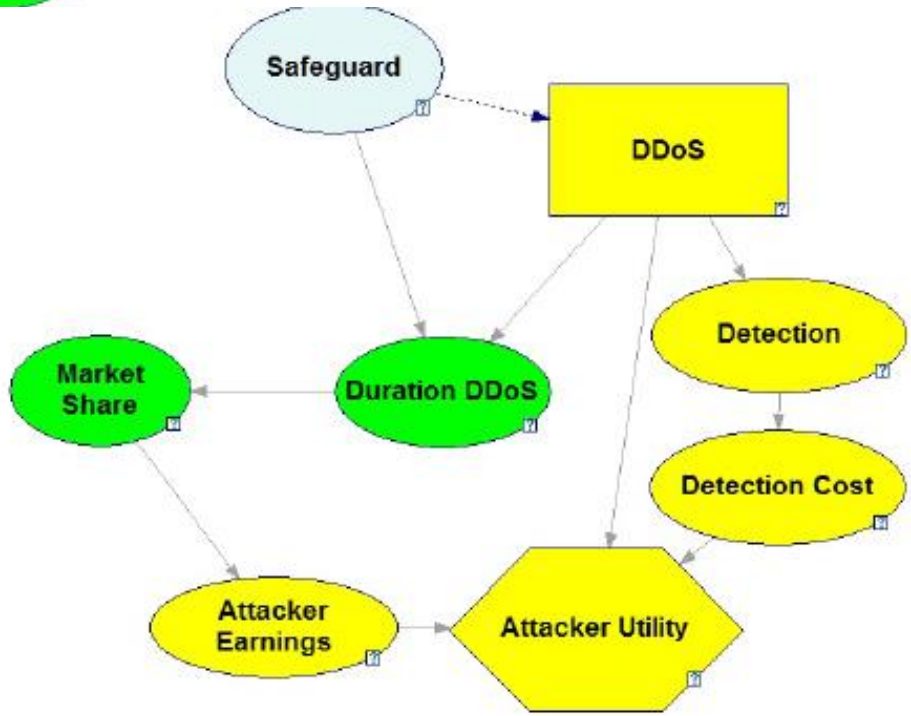


ARA ciberseguridad. Plantilla



ARA ciberseguridad plantilla





CYBECO
https://www.cybeco.eu/

Agenda

- Ciberseguridad
- Estándares de ciberseguridad
- Modelos para la ciberseguridad
- **Discusión**

Discusión

- Problema global: Ciberseguridad
- Perspectivas múltiples: Aquí modelos CD+IA (con ayuda de economistas, informáticos, psicólogos, hackers)

- Mejor tratamiento de la intencionalidad mediante Análisis de Riesgos Adversarios
- Mejores predicciones de ataques
- Integración de ciberseguros con contramedidas

- Big data. Automatizar modelos flexibles
- Small data. Juicios expertos estructurados
- Valoración de activos, reputación,….

Gracias

david.rios@icmat.es @davidrinsua

Amigos R. Acad. Ciencias. https://arac.rac.es/

SPOR-DataLab. https://www.icmat.es/datalab

Aisoy Robotics. https://www.aisoy.com