Modelos
para
la ciberseguridad

David Ríos

Real Academia de Ciencias

Y

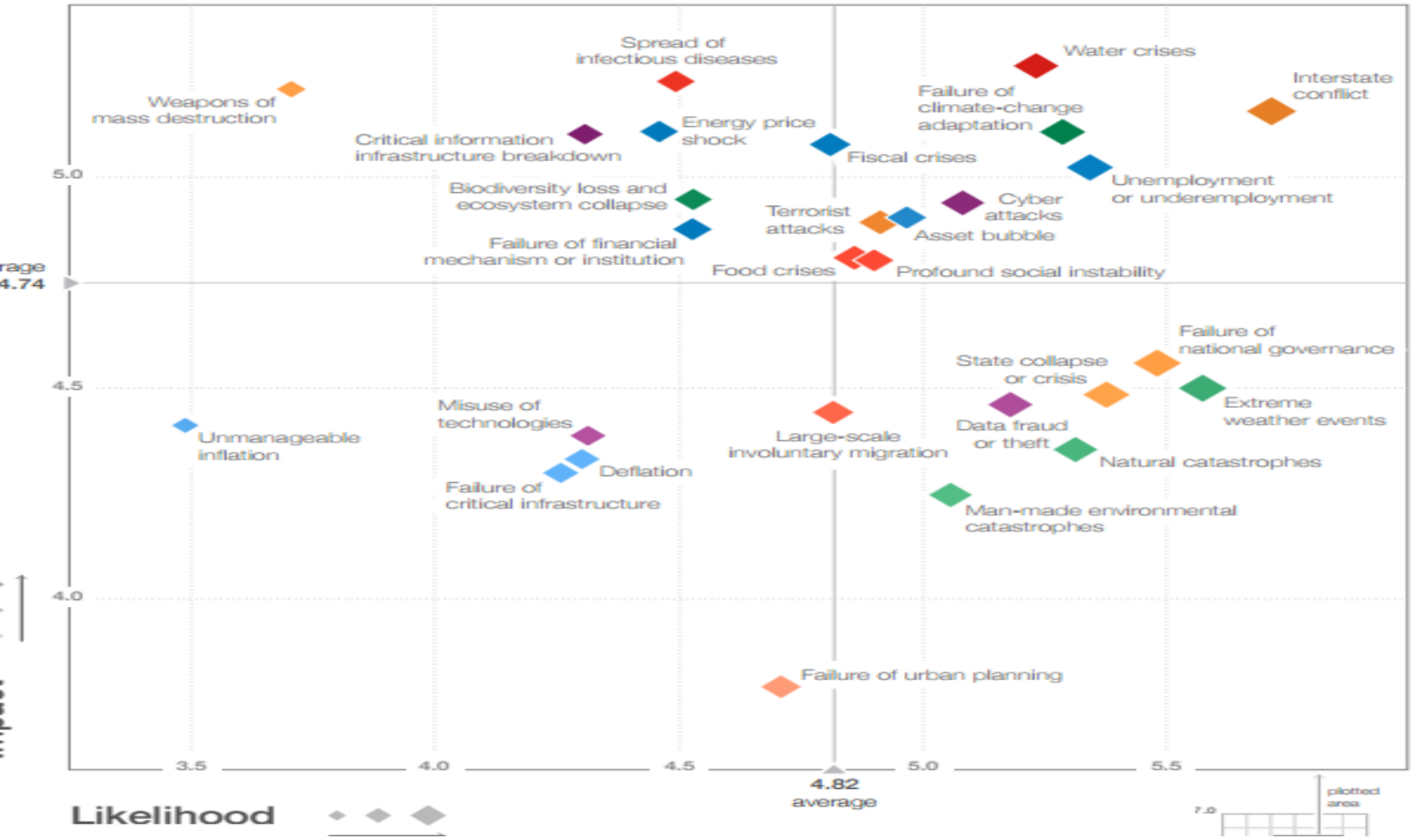
AXA-ICMAT Chair in Adversarial Risk Analysis, DataLab ICMAT, CSIC

PPCyT , Febrero 2018

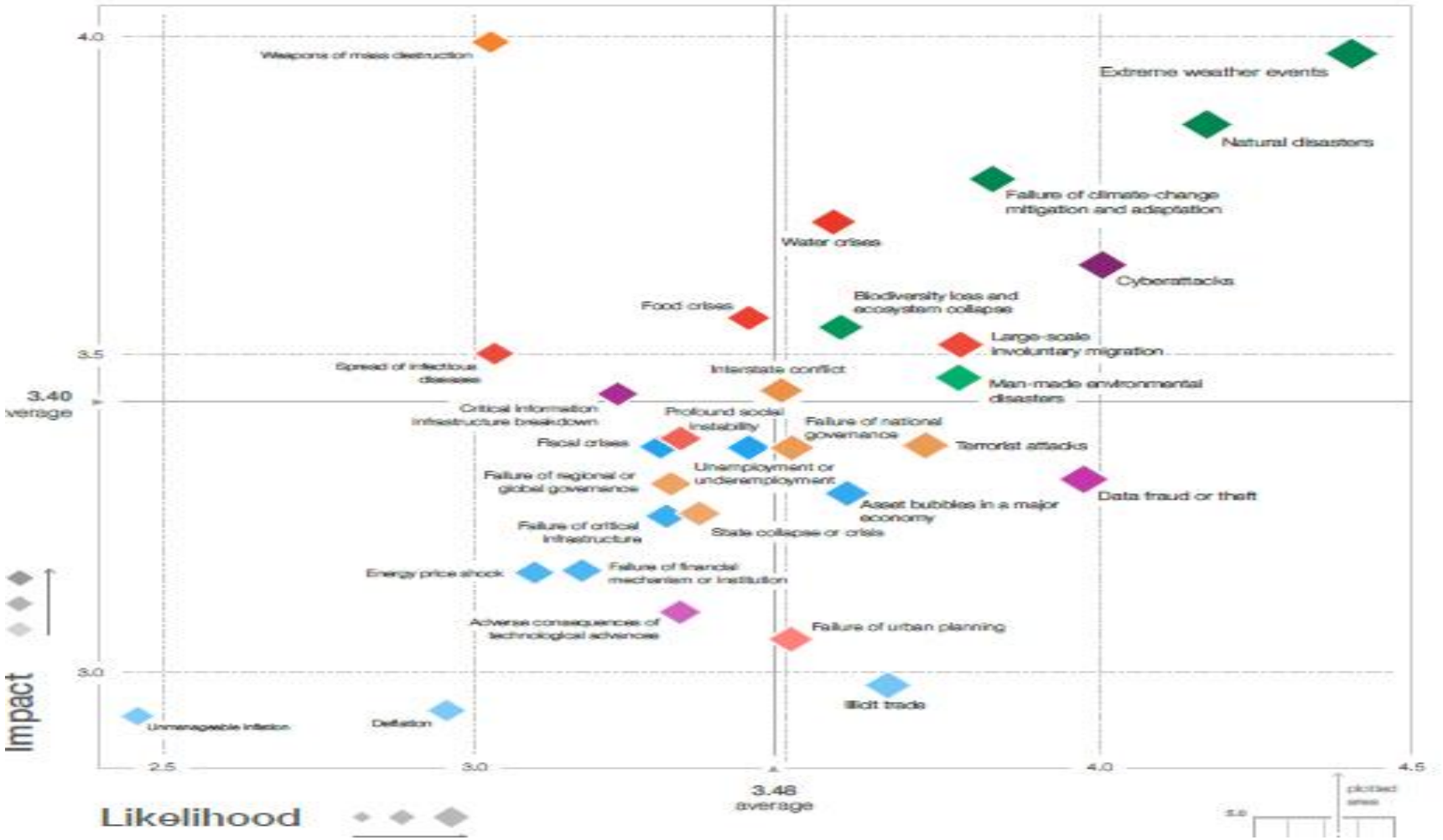
Agenda

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

World Economic Forum. Global Risks Map 2017



World Economic Forum. Global Risks Map 2018



Ciberseguridad en la prensa

Ciberseguridad. Dominios de Conocimiento

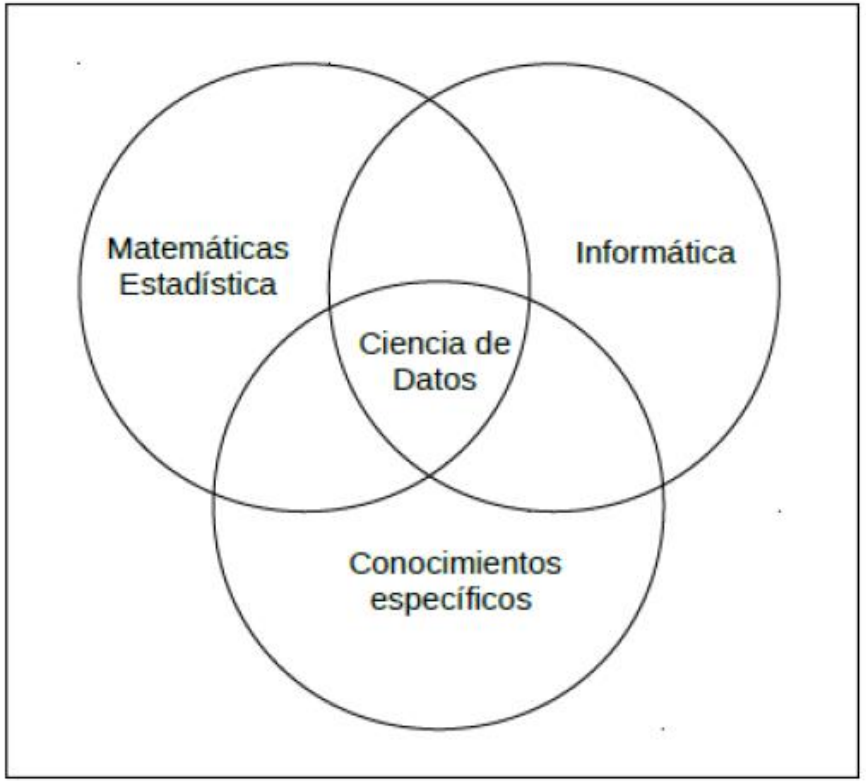
- Auditoría y Certificación
- Criptología
- Seguridad y Privacidad de datos
- Educación
- Gestión operativa y forense de incidentes
- Factor humano
- Gestión e identidad de accesos
- Gestión y gobernanza de la seguridad
- Redes y sistemas distribuidos
- Ingeniería de la seguridad del hardware y el software
- Medición de la seguridad
- Aspectos legales de la tecnología
- Fundamentos teóricos del análisis y diseño de la seguridad
- Gestión de la confianza, auditoría

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
  - MacAfee cataloga alrededor de 70 nuevas amenazas por minuto
- Crecientemente sofisticadas (no sólo tecnológicamente)
- Tiempo de respuesta es excesivo
- Causa inmensos daños económicos (ambientales, de salud,….) pero también en relación con la inteligencia competitiva, la seguridad nacional,…
- Coches, aviones, sistemas médicos, sistemas de inversión, infraestructuras críticas, sistemas de votación,… cada vez más influidos por TIC
- IoT. Cada vez más sistemas interconectados: 10000 M dispositivos conectados a Inet
- Países, ciberdelincuentes, ciberterroristas, actores internos,…..

Ciber riesgos

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

- Wannacry. **No dirigido**. Paró el servicio de salud de 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)
- España tercer país más atacado … principalmente desde Rusia y China

- Mercado negro
- El quinto espacio de operaciones
- Ciberreserva española con 2000 miembros

- 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,….

Catálogos

- Regulaciones

Nombre	Ambito
Directiva EU Protección de Datos 95/46/EC	EU
Directiva EU 16/1148 Seguridad de Redes y de la Información	EU
Regulación 2016/670 General sobre Protección de Datos	EU
LOPD 1999	España
´……	

Catálogos

- Vulnerabilidades. CVE

Código	Nombre	Descripción
CVE-2016-5195	Dirty COW	Vulnerabilidad en kernel Linux que permite a usuarios escalar privilegios
CVE-2017-6607	CISCO ASA DNS DoS	Permite recargar un dispositivo o cooromper su información
	,,,,,,,,,,,,,,	

Catálogos

- Actores

Etiqueta	Motivación
Hacker	Dinero, status, reto técnico,…
Crimen organizado	Dinero,…
Insider	Venganza,…
Competidor	Espionaje,…
País	Espionaje, control político,…
….	….

Catálogos

- Tipos de ataque

Etiqueta	Descripción
Ataque alteración	….
Botnet	…
Ataque fuerza bruta	….
DDoS	
……	
……	

Y otros catálogos

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

Cyber essentials. Recomendaciones UK

1. Descargar actualizaciones de software
2. Usar passwords fuertes
3. Borrar emails sospechosos
4. Usar anti-virus
5. Concienciar al personal

Aproximaciones

- Marcos para el análisis de riesgos
- Marcos para la evaluación del control y el cumplimiento
- 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 IS 1….. VIDEO 8

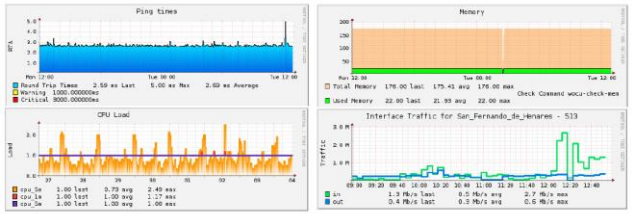
Pocos datos compartidos…..

Agenda

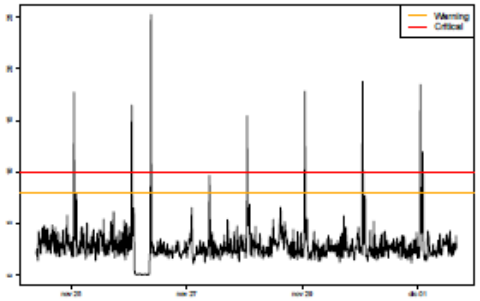
- Ciberseguridad
- Estándares de ciberseguridad
- **Modelos para la ciberseguridad**
- Discusión

Monitorización de la red para seguridad (safety and security)

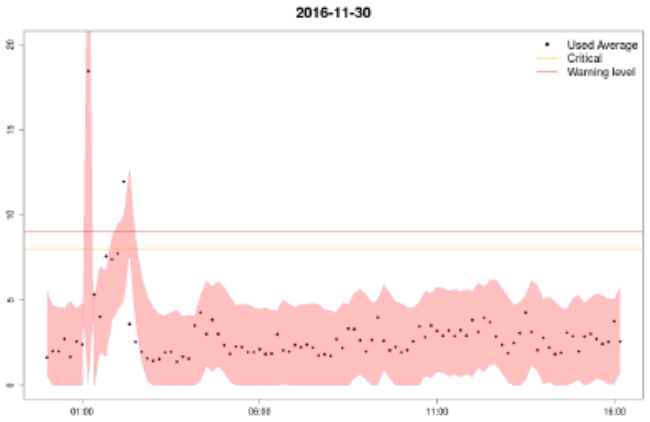
- Sistema recoge medidas de cientos de miles de dispositivos conectados a Internet!!!!
- Por cada dispositivo varias medidas cada muy poco tiempo (1 min, 5 min, 10 min)
- Big Data!!!
- Sistema de monitorización descriptivo: si se alcanzan valores críticos, alarma
- Capacidad predictiva???



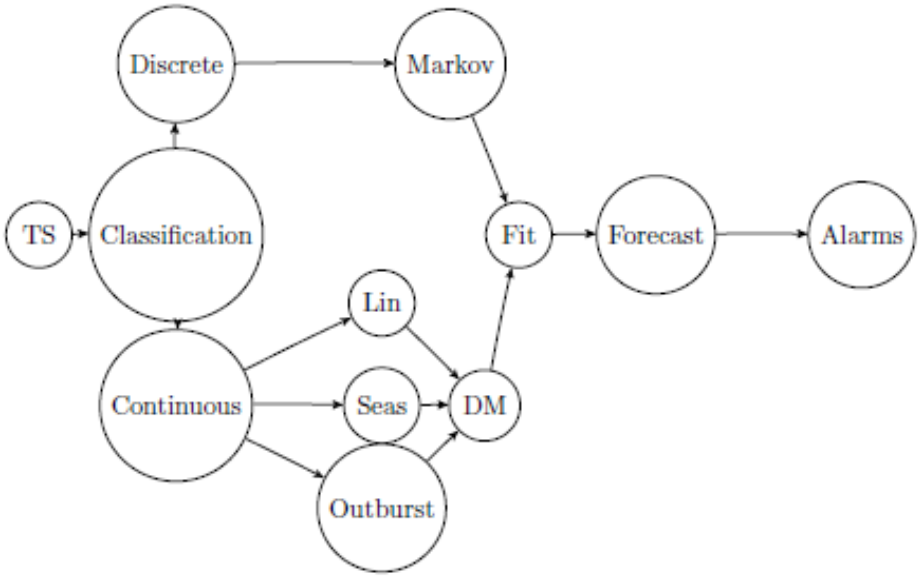
Monitorización de la red para seguridad

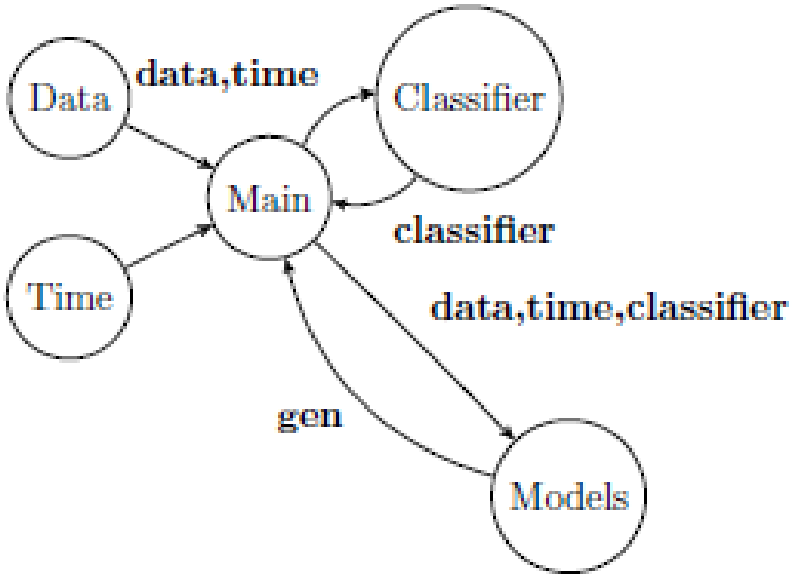


- Tres requisitos
  - Automático
  - Flexible y Versátil
  - Escalable (en tiempo y memoria). Tiempo real
- Diseñar una clase genérica de modelos de predicción Tendencia+estacional(s)+estallidos
- Procedimiento automatizado de identificación
- Alarmas (corto y largo plazo) si
  - Predicen niveles críticos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



Monitorización de la red para seguridad





Clasificación adversaria

- Problema de clasificación. Llega un objeto y debemos decidir a qué clase pertenece:

  spam/no spam; malware/ no malware; severidad 1-2-3-4-5; fraude/no fraude

- Muchos métodos estadísticos y de ML: Naive Bayes, Support Vector Machines, Deep Neural Nets,…
- Olvidan que hay malos dispuestos a atacar nuestro sistema

Clasificación adversaria

- Clasificación adversaria, Aprendizaje máquina adversaria,…
- Teoría de Juegos

  Defensor calcula su clasificador óptimo

  Atacante lo sabe, calcula su ataque óptimo

  Defensor lo sabe y calcula su defensa óptimo

  ….

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

Clasificación adversaria

- Análisis de riesgos adversarios
- Problema de decisión del clasificador. Recibe un objeto. A qué clase pertenece. Incertidumbre: Qué ataque ha utilizado el eventual atacante??
- Problema del atacante. Incertidumbres sobre sus elementos. Usamos toda la información disponible. Simulamos para predecir cual ha sido su ataque. Lo incorporamos al problema del decisor.
- Obtenemos mejoras espectaculares sobre el estándar actual NB
- Todavía muy lento para algunas aplicaciones en tiempo real….

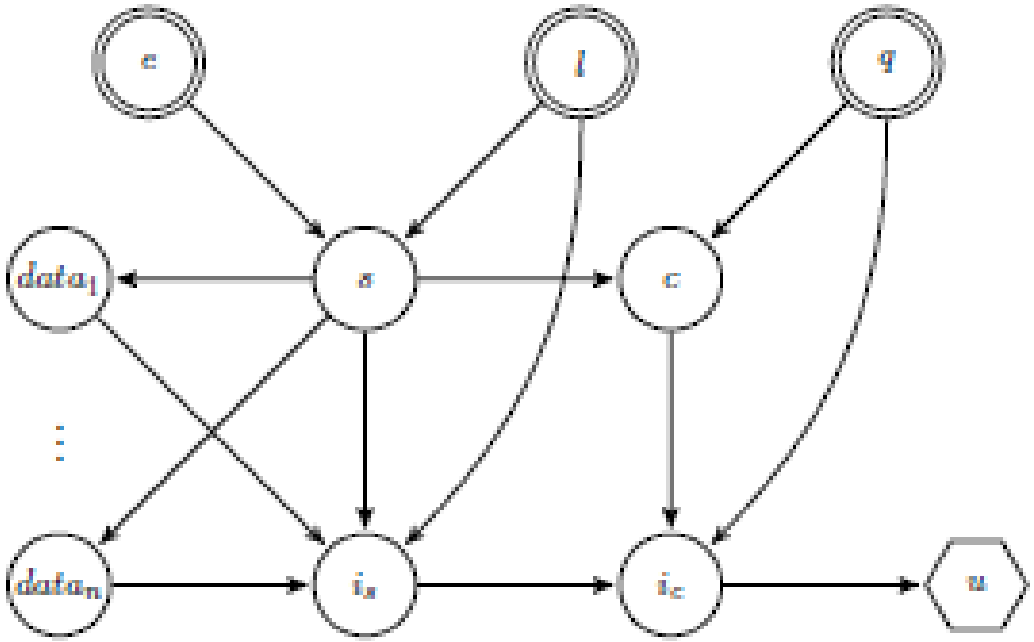
Gestión de ciber riesgos en la cadena de suministro

- Sistema de inteligencia de amenazas que captura en la red datos :
  - Incidentes (IPs de dispositivos contaminados por botnets, 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??
- Evaluación de riesgo predictivo??

Gestión de ciber riesgos en la cadena de suministro

- Big Data, pero juicios de expertos requeridos!!



Gestión de ciber riesgos en la cadena de suministro

- Cliente+Proveedores
- Modelo para predecir:
  - Si un proveedor será atacado (según los distintos vectores, de forma combinada, dados los datos del vector, el entorno y la postura…)
  - El impacto sobre el proveedor (disponibilidad, cuanto tiempo estará caido)
  - Si tal ataque se propagará al cliente
  - Si el cliente será atacado
  - El impacto sobre el cliente (caida de servicio, pérdida de reputación)
- Agregación de los impactos
- Actitud frente al riesgo

Gestión de ciber riesgos en la cadena de suministro

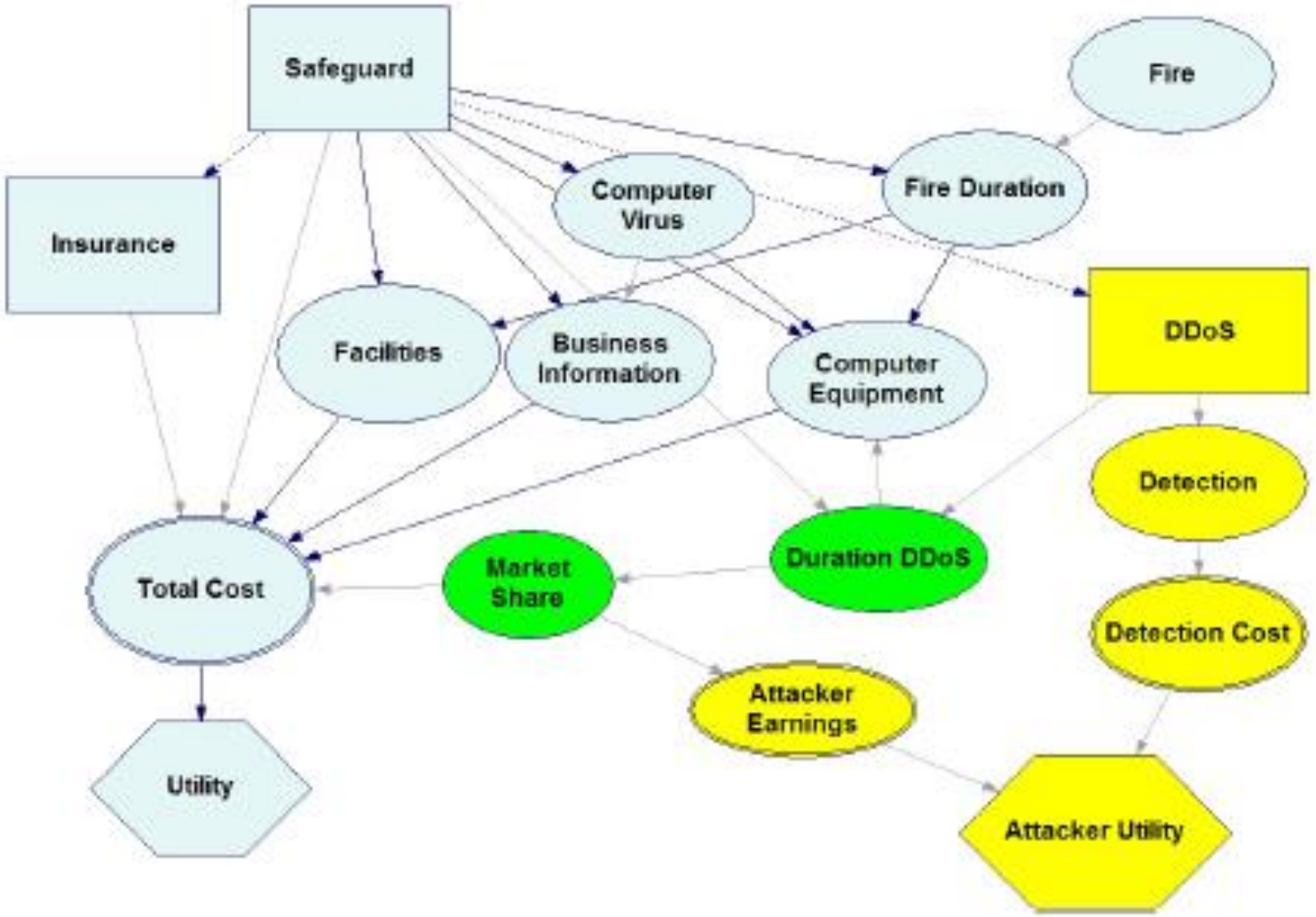
- Riesgo sobre el cliente
- Riesgo sobre el cliente debido al proveedor
- Riesgo total
- Predicción sobre esas medidas de riesgo

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

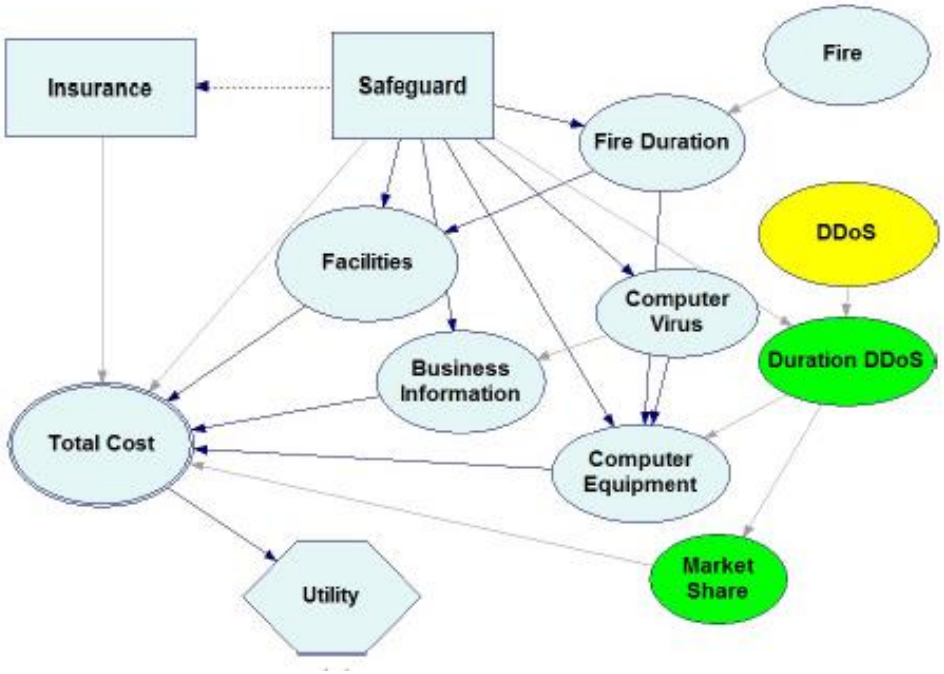
Gestión de ciber riesgos

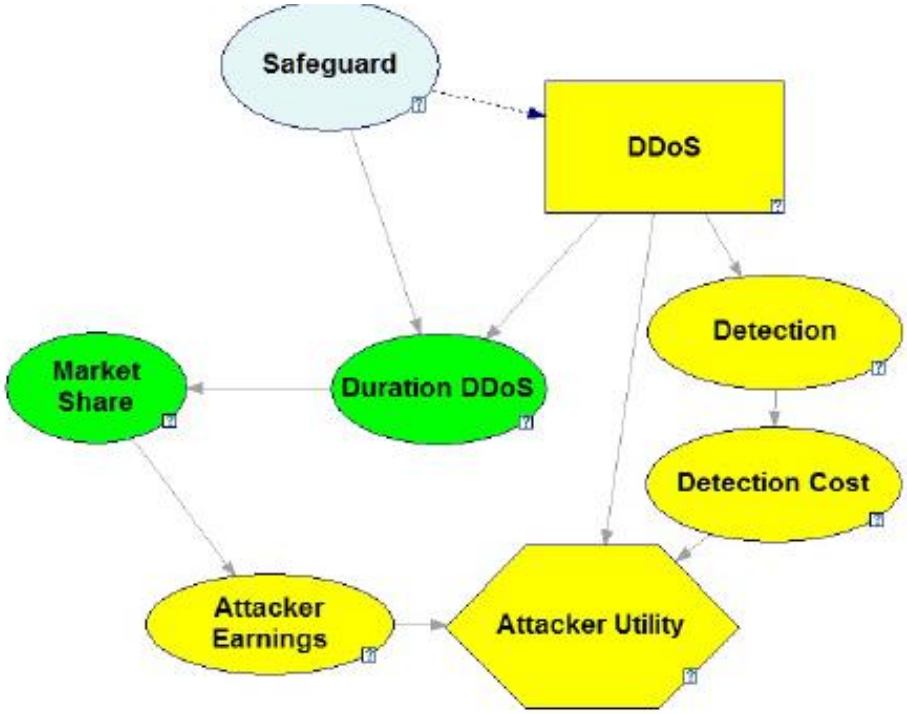
- Nivel Táctico/Estratégico
- Cuál es la mejor inversión en medidas de seguridad (incluyendo un ciberseguro) frente a los ciber riesgos?

ARA ciberseguridad. Plantilla



ARA ciberseguridad plantilla





CYBECO

Agenda

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

Discusión

- Un problema global: La ciberseguridad
- Perspectivas múltiples: Aquí modelos matemáticos (pero construidos con ayuda de economistas, informáticos, psicólogos, hackers)

- Nuevas matemáticas: ARA
- Mejor tratamiento de la intencionalidad
- Mejores predicciones de los ataques
- Integración de ciberseguros con contramedidas

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

Gracias

david.rios@icmat.es @davidrinsua

Vocabulario VCTRAC. https://vctrac.es/index.php?title=P%C3%A1gina_principal
Fondo bibliográfico y documental. http://www.rac.es/4/4_7.php
Viraliza a una científica. http://viraliza.fundaciontatianapgb.org/
Amigos de la Real Academia de Ciencias. https://arac.rac.es/

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

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

It's a Risky Life. Canal YouTube ICMAT

CYBECO https://www.cybeco.eu/