



Universidad de Granada

decsai.ugr.es

Inteligencia Artificial en Telecomunicaciones

Máster en Ingeniería de Telecomunicaciones

Tema 3: Sistemas Expertos



**Departamento de Ciencias de la
Computación e Inteligencia Artificial**

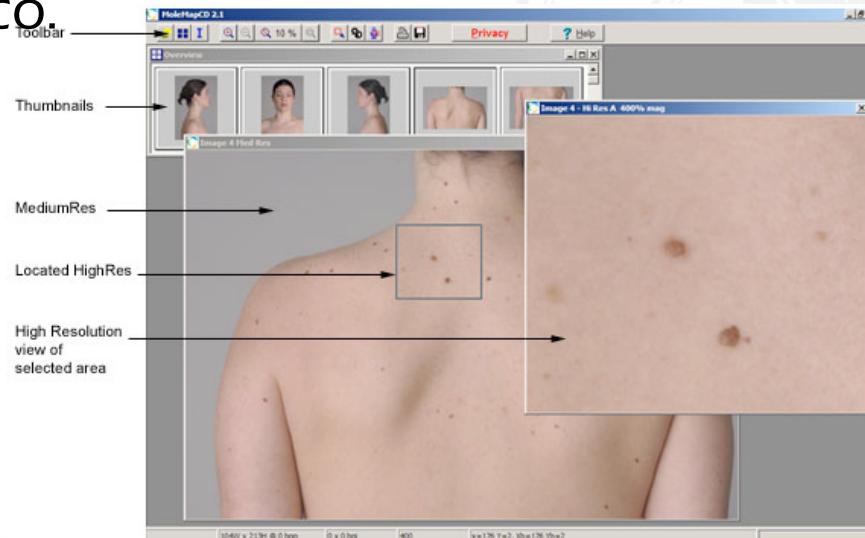
Introducción

- ▶ Los métodos de resolución de problemas que hemos visto son de aplicación general y para su correcto funcionamiento se fundamentan en una heurística para mejorar la búsqueda de soluciones.
- ▶ No obstante, la capacidad expresiva de las funciones heurísticas es reducida y una única función no puede representar todas las decisiones de exploración en el problema
- ▶ Con conocimiento más específico se podrían tomar mejores decisiones y analizar mejor cada paso de la exploración y acercar la exploración a la forma en la que un experto soluciona un problema.



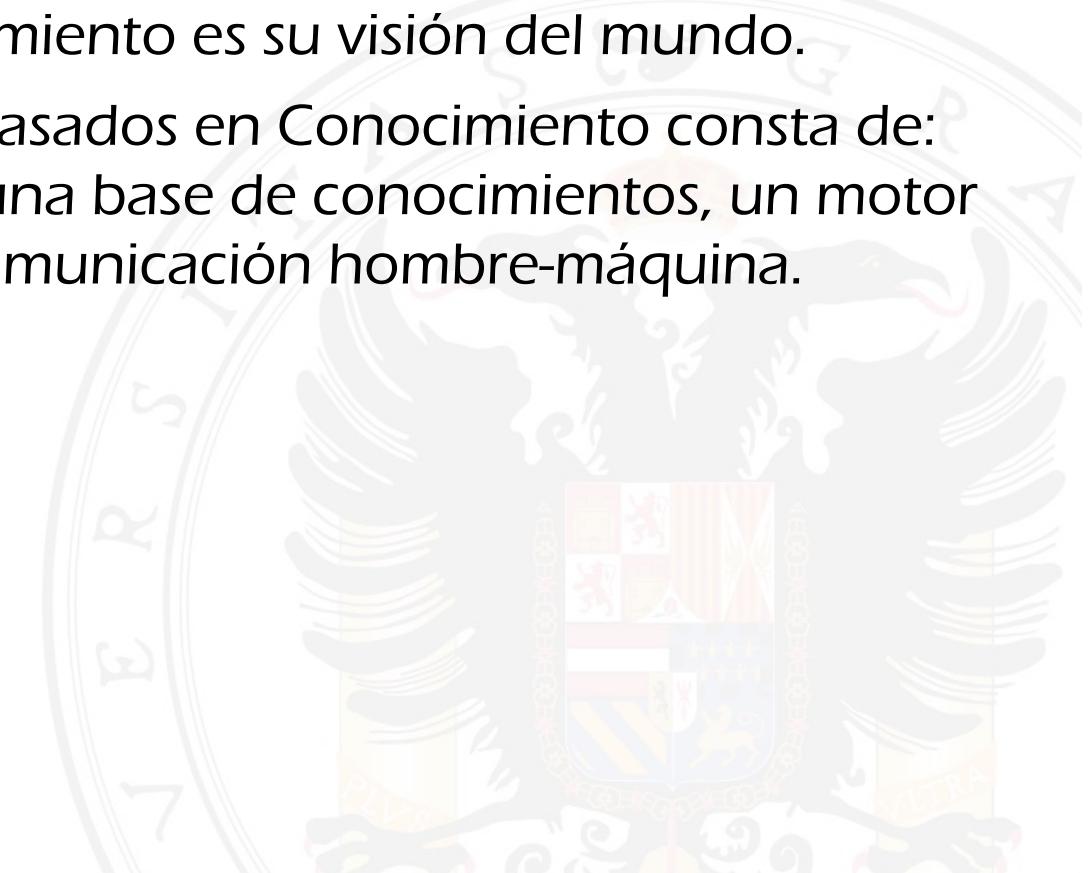
Sistemas Basados en el Conocimiento

- ▶ Un **Sistema Basado en el Conocimiento** es un sistema informático que utiliza conocimiento sobre un dominio concreto para encontrar solución a problemas sobre ese dominio.
- ▶ Si un Sistema Basado en el Conocimiento aplica un conocimiento extraído de un experto, conocimiento que tiene muy poca gente, entonces estamos ante un **Sistema Experto**.
- ▶ Los Sistemas Basados en el Conocimiento deben ser capaces de describir y justificar sus pasos de razonamiento, por ejemplo, un sistema de diagnóstico médico.



Sistemas Basados en el Conocimiento

- ▶ Los Sistemas basados en Conocimiento pretender representar funciones cognitivas del ser humano como el **aprendizaje y el razonamiento**.
- ▶ Un sistema basado en el conocimiento puede verse como un agente deliberativo cuya base de conocimiento es su visión del mundo.
- ▶ La composición de los Sistemas basados en Conocimiento consta de: Un mecanismo de aprendizaje, una base de conocimientos, un motor de razonamiento, y medios de comunicación hombre-máquina.



Sistemas Expertos

Dendral ["Dendritic Algorithm"]

Universidad de Stanford, 1965-1975

- ▶ Primer sistema experto, programado en LISP para obtención de la estructura de las moléculas de química orgánica a través de espectrografía de masas y otros datos.
- ▶ El sistema tuvo cierto éxito entre químicos y biólogos, ya que facilitaba enormemente la inferencia de estructuras moleculares

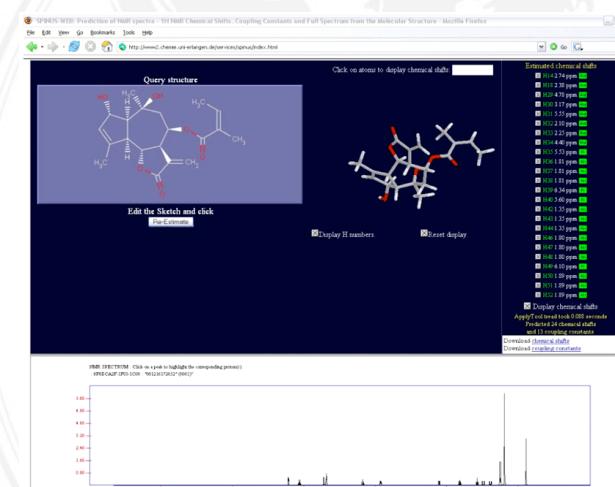
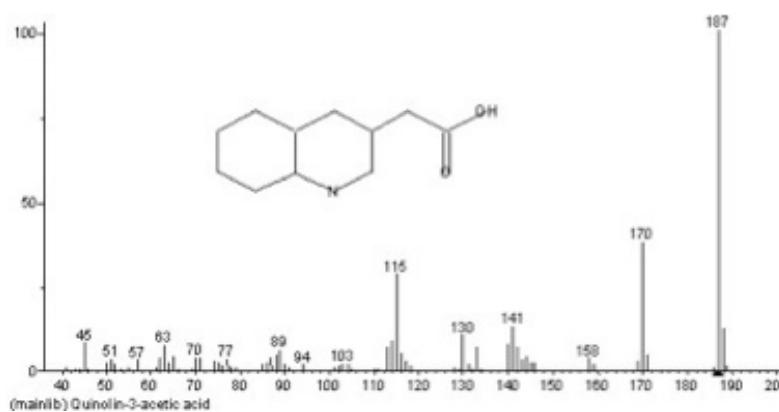


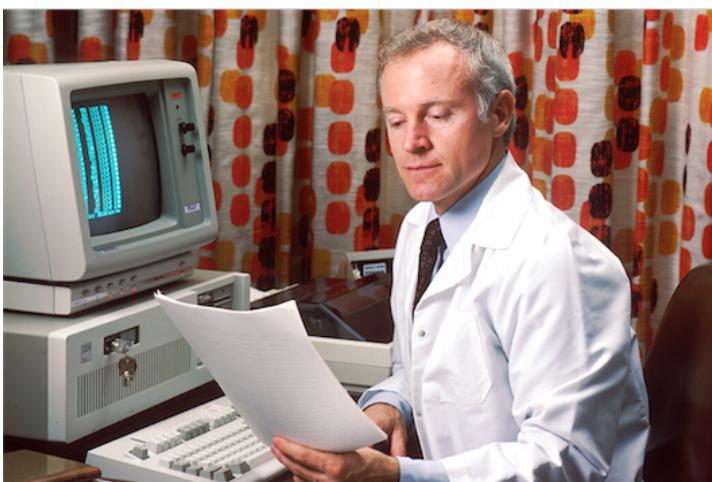
Figura 15b. SPINUS-WEB. Tela de entrada com uma estrutura 2D (acima, à esquerda) com deslocamentos químicos de RMN ^1H previstos (tabela à direita) e o respectivo espectro de RMN ^1H simulado (abaixo).

Sistemas Expertos

MYCIN

Stanford Research Institute, 1970s

- ▶ Diseñado en LISP para identificar las bacterias causantes de infecciones en la sangre y recomendar antibióticos, con una dosis ajustada al peso del paciente [NOTA: el nombre de muchos antibióticos termina con el sufijo “-mycin”].
- ▶ Incorpora un generador de explicaciones.
- ▶ Separación entre datos y conocimiento (500 reglas).
- ▶ Manejo de incertidumbre mediante factores de certeza

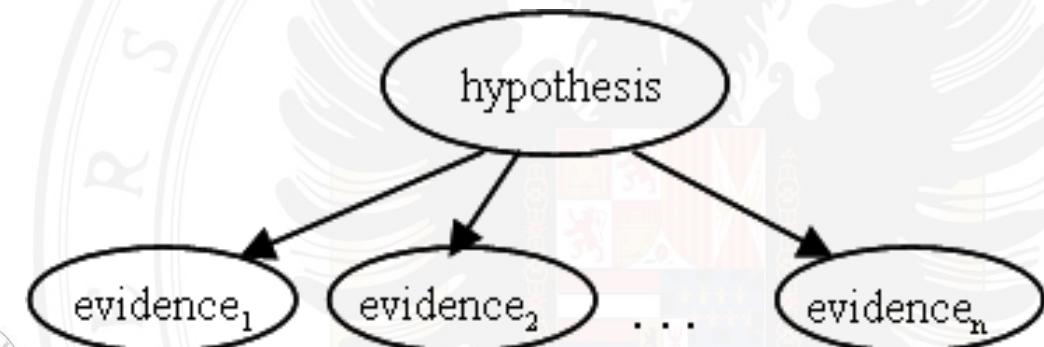
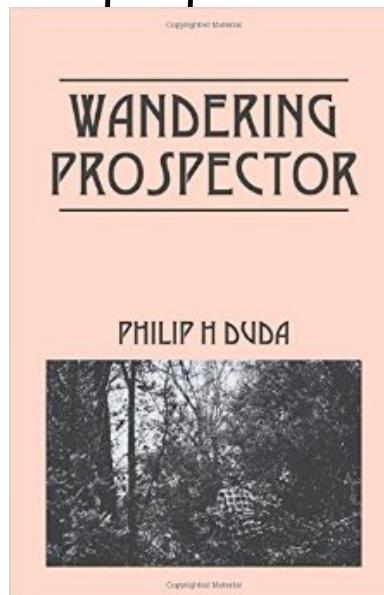


Sistemas Expertos

PROSPECTOR

Stanford Research Institute, 1974-1983

- ▶ Evaluación del potencial minero de una localización geológica (lugares de exploración o prospección).
- ▶ Representación del conocimiento del experto (mediante una red de inferencia) y de su proceso de razonamiento (mediante el uso de técnicas de tipo probabilístico).



Sistemas Expertos

R1 / XCON [eXpert CONfigurer]

Carnegie Mellon University, 1978

- ▶ Escrito en OPS5 para ayudar en la selección de componentes para la configuración de máquinas VAX, de DEC (Digital Equipment Corporation, adquirida por Compaq en 1998, que se fusionó con HP en 2002).
- ▶ Antes de XCON, cuando se pedía una VAX de DEC, cada cable, conexión y bit del software tenía que pedirse por separado (las computadoras y periféricos no se vendían completas en cajas como hoy en día). El personal de ventas no siempre tenía idea de lo que venia ...
- ▶ Puesto en marcha en 1980, en 1986 había procesado 80,000 pedidos y se estima que le ahorraba a DEC más de \$40M al año.



Sistemas Expertos

CLIPS

NASA Johnson Space Center, 1985-

<http://clipsrules.sourceforge.net/>



- CLIPS es una nos permite desarrollar y ejecutar (shell) sistemas expertos.
- CLIPS probablemente es la shell de sistemas expertos más utilizada debido a que es rápida, eficiente y de fuente abierta (gratuita).
- Otros “expert system shells”, descendientes de CLIPS:
 - Jess [Java Expert System Shell] <http://www.jessrules.com/>
 - FuzzyCLIPS, <https://github.com/rorchart/FuzzyCLIPS>

Sistemas Expertos

Algunos ejemplos sistemas expertos “clásicos”

- ▶ Medicina: MYCIN, PUFF, ABEL, AI/COAG, AI/RHEUM, CADUCEUS, ANNA, BLUE BOX, ONCOCIN, VM, INTERNIST-I, CASNET,...
- ▶ Química: CRYSTALIS, DENDRAL, TQMSTUNE, CLONER, MOLGEN, SECS, SPEX...
- ▶ Matemáticas: AM (Automated Mathematician), EURISKO, SMP, MATHPERT, CCH-ES, ExperTAX ...
- ▶ Informática: PTRANS, BDS, R1/XCON, XSEL, XSITE, DART, SNAP, YES/MVS, TIMM...
- ▶ Electrónica: ACE, IN-ATE, NDS, EURISKO, PALLADIO, IDEA, REDESIGN, CADHELP, SOPHIE...
- ▶ Ingeniería: REACTOR, DELTA (GE), JETA, STEAMER, SACON, CALLISTO, G2, SHARP, MARVEL, Pile Selection...
- ▶ Geología: DIPMETER, LITHO, MUD, PROSPECTOR...

Sistemas Expertos

Algunos shells para sistemas expertos

- ▶ E-MYCIN ("Essential/Empty MYCIN"), Stanford Research Institute, 1973-1980.
- ▶ OPS ("Official Production System"), Carnegie Mellon University, 1977.
- ▶ KEE ("Knowledge Engineering Environment") para máquinas Lisp, IntelliCorp, 1983
- ▶ CLIPS ("C Language Integrated Production System"], NASA Johnson Space Center, 1985
- ▶ ESDE ("Expert System Development Environment"), para máquinas MVS y VM, IBM, 1986
- ▶ JESS ("Java Expert System Shell") Sandia National Labs, 1995
- ▶ Drools (business rules engine) JBoss, 2001 <http://www.jboss.org/drools/>

Sistemas Expertos

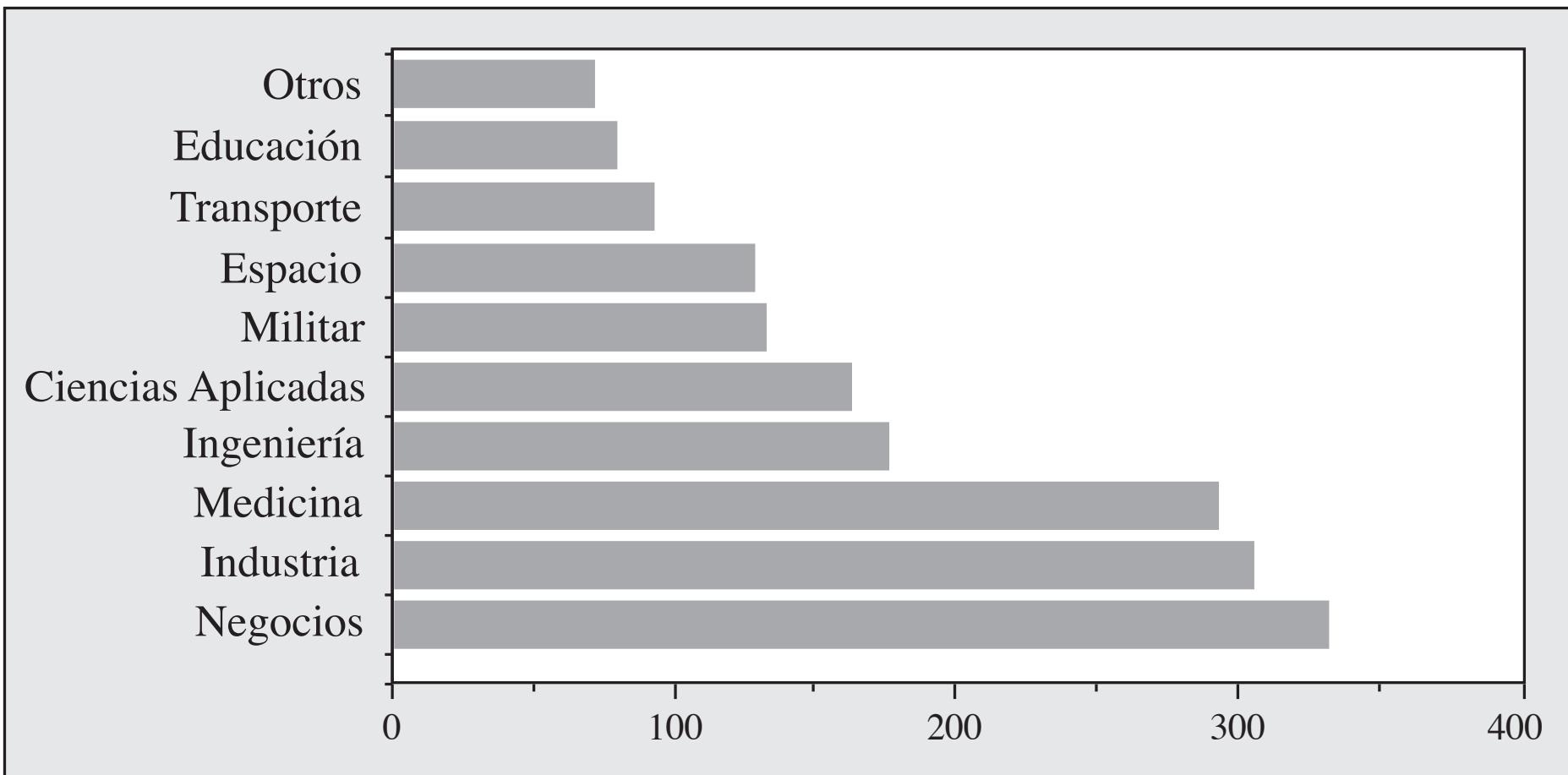


FIGURA 1.1. Campos de aplicación de los sistemas expertos. Adaptado de Durkin (1994) y Castillo, Gutiérrez, y Hadi (1995a).

¿Por qué usar Sistemas Expertos?

- ▶ Gente sin experiencia/conocimiento pueden resolver problemas propios de expertos. Especialmente importante cuando hay pocos expertos disponibles.
- ▶ Hace que el conocimiento esté más disponible.
- ▶ Se puede combinar el conocimiento de varios expertos.
- ▶ Son más rápidos. Especialmente en problemas complejos.
- ▶ Los humanos no son buenos en operaciones monótonas, aburridas o incontrolables.
- ▶ Ahorro económico. Los Sistemas Expertos pueden ser caros de crear pero son bastante baratos de mantener.
- ▶ Tienen que ser áreas en las que haya expertos humanos que nos pueden proporcionar el conocimiento necesario.

Sistemas Expertos como evolución del software

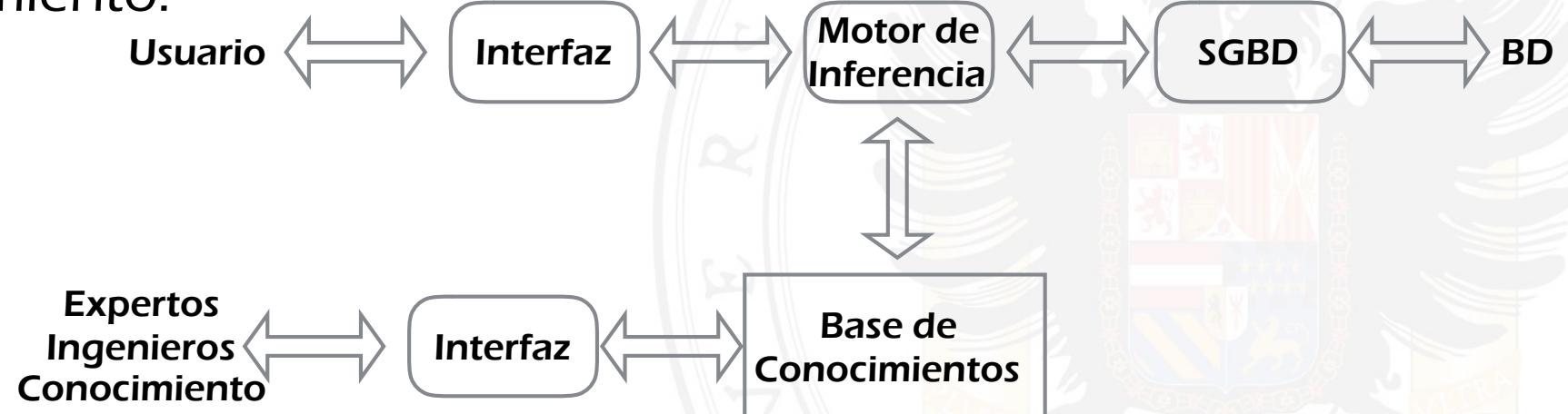
- ▶ Sistema primitivo:



- ▶ Independencia de datos:



- ▶ Independencia del conocimiento:



Sistemas tradicionales vs S.E.

- ▶ Se separa el conocimiento de los mecanismos que permiten manipularlo.
- ▶ Apenas existen instrucciones en el sentido clásico. El conocimiento no se guarda en un programa (secuencia de instrucciones) que resuelve el problema.
- ▶ El “programa” consiste, básicamente, en declarar conocimiento (usualmente, en forma de reglas).
- ▶ Una “caja negra” (motor de inferencia) infiere nuevo conocimiento y determina el flujo de control.

Ejemplo funcionamiento S.E.

Datos

► En lenguaje natural:

- Los padres de Elena son Carlos y Belén.
- Los padres de Carlos son Juan y María.

► Declaración de hechos PROLOG:

- `padres('Carlos','Belén','Elena').`
- `padres('Juan','María','Carlos').`

Ejemplo funcionamiento S.E.

Conocimiento

► En lenguaje natural:

- Los padres de los padres son los abuelos.

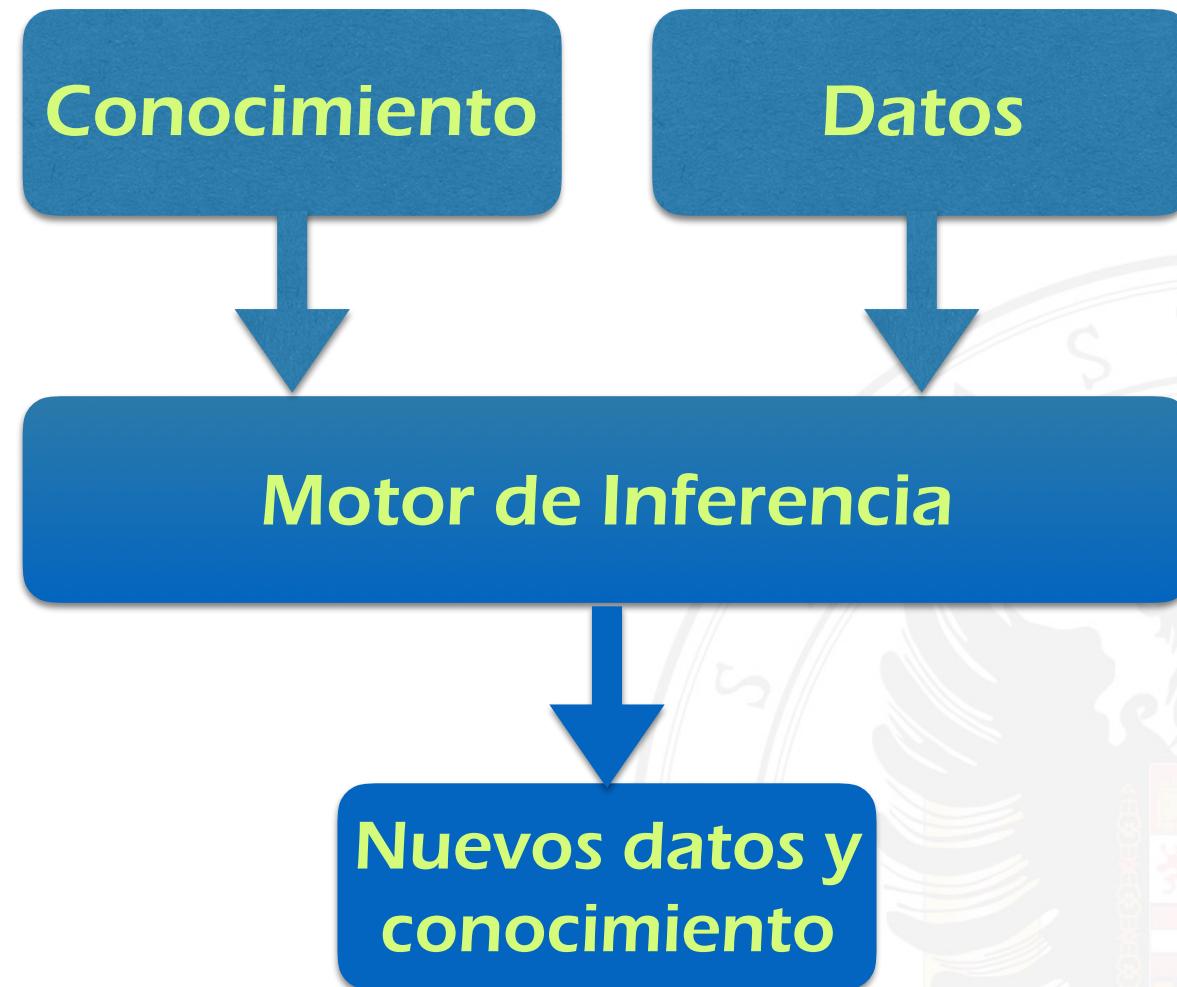
► Programa en PROLOG:

- `abuelos(Abuelo,Abuela,Nieto) if
padres (Abuelo, Abuela, Hijo) and
padres(Hijo, MujerHijo, Nieto).`
- `abuelos(Abuelo,Abuela,Nieto) if
padres (Abuelo, Abuela, Hija) and
padres(EsposoHija, Hija, Nieto).`

Datos vs. Conocimiento

Datos	Conocimiento
Afirmaciones puntuales	Afirmaciones Generales
Suelen ser dinámicos	Suele ser estático
Gran Volumen	Pequeño Volumen
Almacenamiento Secundario	Almacenamiento en RAM
Representación eficiente	Representación simbólica

Estructura de un Sistema Experto

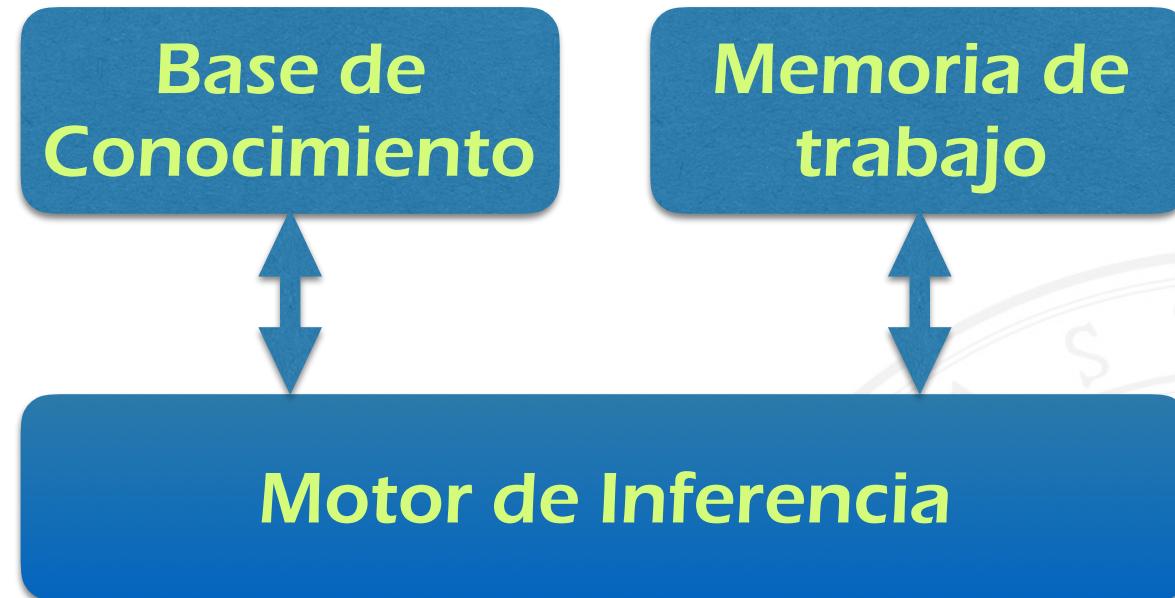


Términos habituales Psicología



- ▶ LTM (long-term memory): Memoria a largo plazo.
- ▶ STM (short-term memory): Memoria a corto plazo.

Arquitectura de un Sistema Experto



- ▶ Memoria a largo plazo ⇒ Base de Conocimiento
- ▶ Memoria a corto plazo ⇒ Memoria de Trabajo
- ▶ El Motor de Inferencia se encarga de seleccionar qué reglas se aplican en cada momento y se encarga de ejecutarlas.

Características de los Sistemas Expertos

- ▶ Separación de datos y conocimiento.
- ▶ Objetivo: Ayuda en la toma de decisiones (no sustituir al experto).
- ▶ Razonamiento simbólico debido a la representación del conocimiento
- ▶ Razonamiento heurístico debido a la naturaleza del conocimiento.
- ▶ Razonamiento con incertidumbre.
- ▶ Razonamiento con explicaciones.

Características de los Sistemas Expertos

Separación de datos y conocimiento.

- ▶ La separación de los datos y el conocimiento de su manipulación, permite actualizar fácilmente la base de datos o la base de conocimiento sin modificar el programa (motor de inferencia).
- ▶ Implementación del conocimiento explícito de un experto en un dominio concreto.

Características de los Sistemas Expertos

Objetivo: Ayuda en la toma de decisiones (no sustituir al experto).

► Consejos prácticos:

- No intentar cubrir un área excesivamente grande.
- Dividirla en subproblemas y construir, para cada uno de ellos, un sistema experto específico que lo resuelva.

Características de los Sistemas Expertos

Razonamiento simbólico

- ▶ Si una persona tiene fiebre y no es alérgica al ácido acetil salicílico (AAS) entonces suministrar aspirina 500mg
 - ▶ Pedro tiene fiebre
 - ▶ Pedro no es alérgico al AAS
-
- ▶ $\forall x \text{ Fiebre}(x) \wedge \neg \text{AlergiaAAS}(x) \rightarrow \text{Terapia}(x, \text{Aspirina500})$
 - ▶ $\text{Fiebre}(\text{Pedro})$
 - ▶ $\neg \text{AlergiaAAS}(\text{Pedro})$

Características de los Sistemas Expertos

Razonamiento heurístico.

- Reglas heurísticas basadas en la **experiencia** de los expertos (que puede fallar)
 - Ante un problema de arranque, descartar que sea un fallo de carburación y chequear primero el sistema eléctrico.
 - Si el tipo de interés está bajo, considerar invertir en acciones. Si el tipo de interés está alto, mejor invertir en bonos.
 - Las personas no suelen coger una gripe en verano.
 - Si se sospecha cáncer, comprobar el historial familiar.

Características de los Sistemas Expertos

Razonamiento con incertidumbre.

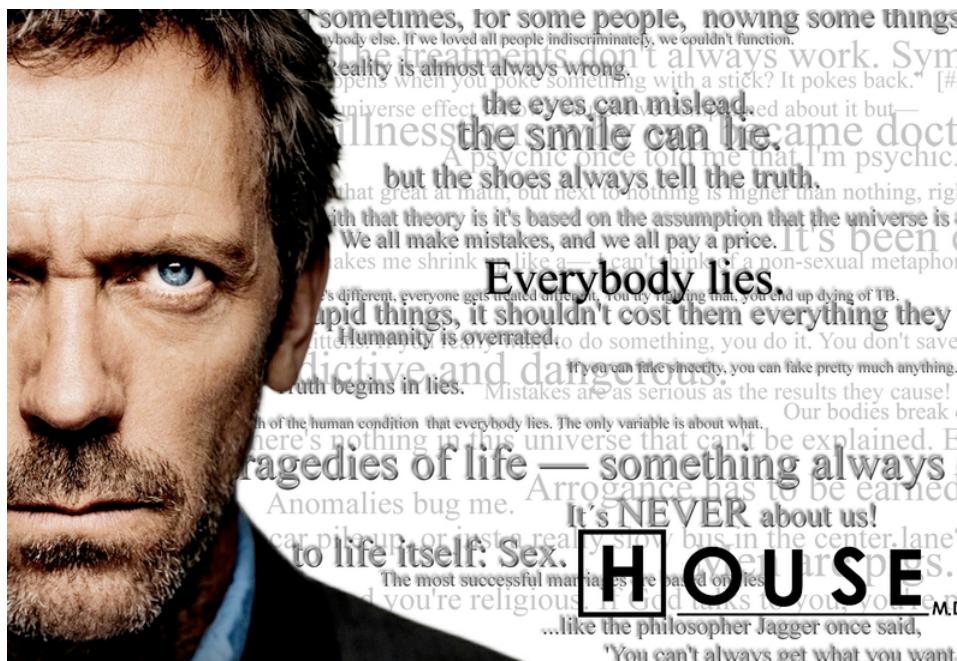
- ▶ Razonamiento inexacto y usando probabilidades.
 - ▶ PROSPECTOR usaba 'likelihoods' (verosimilitudes).
 - ▶ MYCIN usaba 'certainty factors' (factores de certeza).
-
- Si el paciente es un huésped de riesgo y existen reglas que mencionan a las pseudomonas y existen reglas que mencionan a las klebsiellas, entonces es plausible (0.4) que deban considerarse primero las segundas.

Características de los Sistemas Expertos

Programas Convencionales	Sistemas Expertos
Programación Imperativa	Programación Declarativa
Razonamiento Algorítmico	Razonamiento Heurístico
Control definido por el programador	Control definido por el motor de inferencia
Difíciles de Modificar	Fáciles de Modificar
Información Precisa	Información no Precisa
Solución como Resultado	Recomendación razonada
Solución “óptima”	Solución aceptable

Inconvenientes de los Sistemas Expertos

- ▶ Dificultad para adquirir el conocimiento.
- ▶ Dificultad para reutilizar el conocimiento.
- ▶ Casos nuevos o distintos.
- ▶ Dificultad para la adaptación.
- ▶ Dificultad en la validación de la correctitud/completitud del sistema.



Representación del Conocimiento

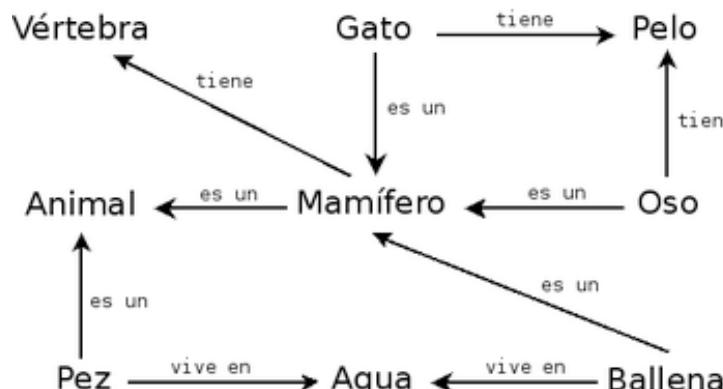
► Requisitos de los formalismos de representación del conocimiento:

- Potencia expresiva
- Facilidad de interpretación
- Eficiencia deductiva
- Posibilidad de explicación y justificación

► Algunos formalismos de representación:

- Reglas, redes semánticas, marcos, lógicas de descripción, lógica de primer orden, ontologías, etc.

► Cada formalismo de representación usa un método específico de inferencia.



```
R1: bueno(x) ∧ rico(y) ∧ quiere(x,y) → hereda-de(x,y)
R2: amigo(x,y) → quiere(x,y)
R3: antecesor(y,x) → quiere(x,y)
R4: progenitor(x,y) → antecesor(x,y)
R5: progenitor(x,z) ∧ progenitor(z,y) → antecesor(x,y)
H1: progenitor(padre(x),x)
H2: rico(Pedro)
H3: rico(padre(padre(Juan)))
H4: amigo(Juan,Pedro)
H5: bueno(Juan)
```

Sistemas Expertos basados en reglas

- ▶ El razonamiento basado en reglas es el enfoque más utilizado en los Sistemas Basados en el Conocimiento.
- ▶ **Producción:** Término utilizado en Psicología Cognitiva para describir relaciones entre situaciones y acciones.
- ▶ **Regla de producción:** Término utilizado en I. A. para denotar un mecanismo de representación del conocimiento que implementa una producción.

SI premisa ENTONCES acción.

- ▶ La **premisa** (condición ó antecedente) o conjunto de ellas establece las condiciones que se han de satisfacer en un momento dado para que la regla sea aplicable.
- ▶ La **acción** ó conseciente establece las acciones que se han de realizar cuando la regla “se active”:
 - Suprimir/añadir algún dato a la memoria de trabajo.
 - Ejecutar algún procedimiento.

Sistemas Expertos basados en reglas

- ▶ El motor de inferencia determina el orden en el que se aplican las reglas “activas” (aquéllas para las que se cumple su antecedente).
- ▶ El motor de inferencia se puede programar pero lo razonable es usar alguno existente (shell).
- ▶ Funcionamiento del Motor de Inferencia
 - Detección de reglas aplicables.
 - Elección de reglas (resolución de conflictos).
 - Aplicación de la regla.
 - Actualización de la memoria de trabajo
 - Repetir hasta que no haya reglas aplicables.

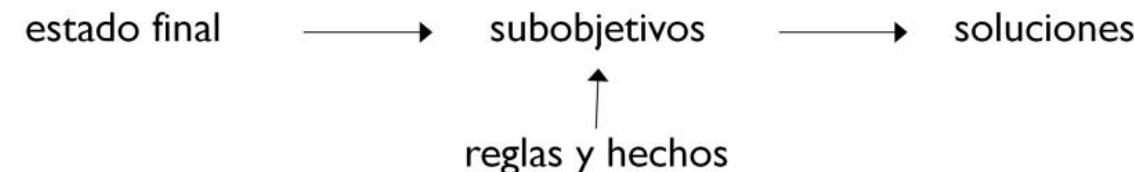
Sistemas Expertos basados en reglas

► En el motor de inferencia se pueden utilizar dos **mecanismos básicos de inferencia:**

- **Hacia adelante:** Adecuado para problemas de síntesis: configuración de sistemas, organización de tareas, etc. Es el tipo de razonamiento que usan lenguajes como CLIPS.



- **Hacia atrás:** Adecuado para problemas de diagnóstico. Este es el tipo de razonamiento que utiliza el lenguaje Prolog.



Sistemas Expertos basados en reglas

Resolución de conflictos: Cuando hay muchas reglas, hay que definir un sistema que indique cuál se aplica primero.

► Preferencia basada en reglas:

- Asignación de prioridades, orden de introducción (Prolog), reglas más/menos usadas, etc.

► Preferencia basada en premisas:

- Reglas que se apliquen a premisas más recientes, asignación de prioridades a antecedentes, etc.

► Preferencia basada en pruebas:

- Hacer un banco de pruebas, analizar los resultados y seleccionar la mejor.

Sistemas Expertos en Telecomunicaciones

- ▶ La gran mayoría de los problemas que encontramos en telecomunicaciones se pueden resolver mediante búsquedas en espacios de estados.
- ▶ No obstante una heurística codifica poca información para ser útil en algunos problemas.
- ▶ Las redes de telecomunicaciones han evolucionado rápidamente en los últimos años, consumiendo más ancho de banda y buscando una mayor calidad de servicio.
- ▶ La tecnología de redes han aumentado su complejidad y, por tanto, la complejidad de su gestión.
- ▶ Los Sistemas Expertos se han aplicado con éxito en tareas donde se necesita conocimiento especializado.

Gestión de Fallos

- ▶ En la gestión de redes, tareas relacionadas con la detección, diagnosis, recuperación y corrección de fallos.
- ▶ Max / Opti-Max (NYNEX): sistema experto para el mantenimiento de líneas telefónicas.
- ▶ Trouble Locator (Pacific Bell): para buscar fallos al nivel físico de red de telefonía local.
- ▶ ANSWER (AT&T): para la gestión de los conmutadores 4ESS de AT&T.
- ▶ Scout (AT&T): Para encontrar errores persistentes en la red.

Gestión de Fallos

- ▶ MAD (Northern Telecom): gestión de mensajes de diagnóstico de conmutadores DMS.
- ▶ Starkeeper Network Troubleshooter (AT&T): Busca fallos de red, basándose en el conocimiento que se tiene sobre fallos de componentes.
- ▶ ARTEX: identifica problema en redes de enrutamiento de audio.
- ▶ COMNET: Identificaba problemas en interconexiones de redes digitales y analógicas.
- ▶ FIESTA: busca errores en las comunicaciones por satélite.
- ▶ AUTOTEST-2: testea el funcionamiento de circuitos
- ▶ ExT, TERESA, IRA, LES, DANTEs, etc.

Gestión de la Configuración

- ▶ Los Sistemas Expertos también se usan en la gestión de la configuración de los recursos de las redes de comunicaciones. Se hacen cambios en la configuración, por ejemplo, para eliminar congestión de red.
- ▶ ECXpert (Lucent): sistema para la detección y reparación de fallos.
- ▶ ACE (AT&T): para la detección y diagnosis de fallos en cableado.
- ▶ NEMESYS (AT&T): Para evitar la congestión de redes.
- ▶ GTE's COMPASS; BELLCORE: Para monitorizar mensajes de los conmutadores de varios tipos.
- ▶ IAS (ITELPAC) ; DPN Monitor (Bell Labs Canada); DAD: Para la gestión de redes de comutación de paquetes.
- ▶ AMF (British Telecom): gestiona conmutadores usados en el enrutamiento de señales de audio.
- ▶ CENTAURE: Monitoriza la red de telecomunicaciones del sistema ferroviario francés.
- ▶ ICARO: Sistema experto para la gestión de canales comunicaciones de radio usando la ionosfera.
- ▶ NCAI: Gestión de redes militares de comutación de paquetes radio con los nodos en constante cambio.
- ▶ MAPCon: configuración de los parámetros usados en redes LAN con MAP (Manufacturing Automation Protocol).
- ▶ MES; ASSIGN: Gestiona los recursos solicitados por usuarios

Diseño de redes

- ▶ DesigNet (BBN Labs): diseño de redes con diferentes métricas (por ejemplo, retrasos medios en la red, carga en elementos individuales, costo).
- ▶ XTEL: diseño de redes para aplicaciones militares (criterios como la resistencia/supervivencia de nodos).
- ▶ CLASS: Genera predicciones de comportamiento de las redes por satélite de la NASA
- ▶ DATAcab (Univ. Sevilla): para el diseño de redes de fibra óptica y cable coaxial.
- ▶ KAT, System Configurator, LEIS, SLEEK, etc.

Otros S.E. usados en Telecomunicaciones

- ▶ Net/Advisor y NetCommand: para monitorizar el estados de las redes LAN en tiempo real.
- ▶ EXSYS (Pacific Bell): Sistema para supervisar LOMS (Loop Maintenance Operating System).
- ▶ NetHELP: Asistente para problemas de usuarios.
- ▶ ExSim: Ayuda en el enrutamiento.
- ▶ Service Definition Expert System; ENS (Bell Canada): Para buscar que productos o servicios son más conveniente para cada tipo de cliente.
- ▶ APRI (AT&T): sistema experto construido con redes bayesianas (aprendidas automáticamente) para la gestión de deudas incobrables.



Detección de Intrusiones

	Detection approach	Detection methodology ^a			Time series	Technology type ^b	Detection of attacks ^c	Performance ^d	Type of source	Other characteristics
		AD	SD	SP						
Statistics-based	Statistics (Axelsson, 2000; Debar et al., 2000; Patcha and Park, 2007; Garcia-Teodoro et al., 2009; Xie et al., 2011; Murali and Rao, 2005; Sabahi and Movaghhar, 2008; Lazarevic et al., 2005; Fragkiadakis et al., 2012; Mar et al., 2012)	✓	✓	-	○	H/N	B	M	Audit data, user profiles, usage of disk and memory	Simple but less accuracy
	Distance-based (Patcha and Park, 2007; Murali and Rao, 2005; Sabahi and Movaghhar, 2008; Lazarevic et al., 2005)	✓	-	-	○	N	U	M	Audit data, network packets	Real-time and active measurement
	Bayesian-based (Kabiri and Ghorbani, 2005; Patcha and Park, 2007; Garcia-Teodoro et al., 2009; Stavroulakis and Stamp, 2010; Lazarevic et al., 2005)	✓	✓	-	○	N	B	H	Audit data, Prior events, network traffic, user profiles	Optimal statistical (probabilistic) model
	Game Theory (Li et al., 2012; Paramasivan and Pitchai, 2011; Kantzavelou and Katsikas, 2010; Shena et al., 2011)	✓	-	-	○	H/N	U	L	System's events or incidents, Log events, byte sent	Self-study, control is poor
	Pattern Matching (Debar et al., 1999; Axelsson, 2000; Krugel and Toth, 2000; Debar et al., 2000; Murali and Rao, 2005; Sabahi and Movaghhar, 2008; Lazarevic et al., 2005; Kartit et al., 2012)	-	✓	-	✗	N	K	H	Audit records, signatures of known attacks	Simple but less flexible
	Perti Net (Debar et al., 1999; Axelsson, 2000; Dexbar et al., 2000; Murali and Rao, 2005; Lazarevic et al., 2005)	-	✓	-	○	H	K	M	Audit records, user defined known intrusion signatures	Simple concept and graphic depiction
	Keystroke monitoring (Krugel and Toth, 2000; Murali and Rao, 2005; Lazarevic et al., 2005)	-	✓	-	○	H	K	H	Audit records, user profiles, keystroke logs	Using user's typing pattern
	File system checking (Murali and Rao, 2005; Lazarevic et al., 2005)	✓	✓	-	✗	H	B	H	System// configuration/ User files, log files, applications	File integrity checking

Detección de Intrusiones

Rule-based	Rule-based (Axelsson, 2000; Krugel and Toth, 2000; Jones and Sielken, 2000; Xie et al., 2011; Stavroulakis and Stamp, 2010; Sabahi and Movaghfar, 2008; Lazarevic et al., 2005; Farooqi et al., 2012; Modi et al., 2012; Wang et al., 2011) Data Mining (Kabiri and Ghorbani, 2005; Patcha and Park, 2007; Xie et al., 2011; Murali and Rao, 2005; Lazarevic et al., 2005)	✓	✓	-	✗	H/N	B	H	Audit records, rule patterns from user profiles and policy	Not easily created and updated		
	Model/Profile-based (Krugel and Toth, 2000; Murali and Rao, 2005; Sabahi and Movaghfar, 2008; Lazarevic et al., 2005; Kartit et al., 2012)	✓	-	-	✗	H/N	U	M	Audit data, knowledgebase for association rule discovery Audit records, User profiles, Network packets, AP profiles	Automatically generated models	Varied modeling / profiling methods	
State-based	Support vector machine (SVM) (Modi et al., 2012; Kolias et al., 2011; Li et al., 2012; Horng et al., 2011) State-Transition Analysis (Debar et al., 1999; Axelsson, 2000; Krugel and Toth, 2000; Jones and Sielken, 2000; Debar et al., 2000; Stavroulakis and Stamp, 2010; Murali and Rao, 2005; Sabahi and Movaghfar, 2008; Lazarevic et al., 2005)	✓	✓	-	○	N	B	H	Limited sample data, binary data	Lower false positive rate, high accuracy	Flexibility, Detect across user sessions	
	User intention Identification (Debar et al., 1999; Debar et al., 2000; Murali and Rao, 2005; Lazarevic et al., 2005)	-	✓	-	○	H/N	K	H	Audit records, State-transition diagram of known attacks			
	Markov Process Model (Patcha and Park, 2007; Garcia-Teodoro et al., 2009; Murali and Rao, 2005; Lazarevic et al., 2005; Couture, 2012; Li et al., 2012)	✓	-	-	○	H/N	U	M	Audit date, Sequence of system calls or commands.	Probabilistic, Self-training		
	Protocol Analysis (Stavroulakis and Stamp, 2010; Murali and Rao, 2005; Sabahi and Movaghfar, 2008; Lazarevic et al., 2005)	✓	✓	✓	○	P	T	L	Audit records, Log file, Normal usage (Model) of a protocol	Low false positive rate, Less effective		

Detección de Intrusiones

Clase de Algoritmo	Algoritmo	Entrenamiento	Pruebas	Evaluación	Entorno	B	M	Auditoría	Características
Heuristic-based	Neural Networks (Axelsson, 2000; Patcha and Park, 2007; Stavroulakis and Stamp, 2010; Murali and Rao, 2005; Lazarevic et al., 2005; Mar et al., 2012; Modi et al., 2012; Wang et al., 2011) Fuzzy Logic (Kabiri and Ghorbani, 2005; Patcha and Park, 2007; Garcia-Teodoro et al., 2009; Stavroulakis and Stamp, 2010; Mar et al., 2012; Modi et al., 2012) Genetic algorithm (Patcha and Park, 2007; Garcia-Teodoro et al., 2009; Murali and Rao, 2005; Lazarevic et al., 2005; Modi et al., 2012; Li et al., 2012; Sen and Clark, 2011)	√	√	-	○	N	B	M	Audit data, Sequence of commands, Predict events
		√	-	-	×	H/N	U	H	Audit records, network traffic (TCP/UDP/ICMP)
		-	√	-	○	N	K	L	Audit data, known attacks
	Immune system (Debar et al., 1999; Debar et al., 2000; Stavroulakis and Stamp, 2010; Murali and Rao, 2005; Lazarevic et al., 2005) Swarm Intelligent (SI) (Kolias et al., 2011; Chung and Wahid, 2012; Alomari and Othman, 2012)	√	√	-	○	H	B	M	expressed as binary patterns
		√	-	-	○	N	U	H	Audit data, sequence of system calls Network connection data, log file data
									Heuristic and evolutionary learning Distributed, high overall security Bio-inspired computing intelligence