UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA
Y ADMINISTRACION

AUDIN: UN SISTEMA EXPERTO PARA AUDITORIA EN INFORMATICA

SEMINARIO DE INVESTIGACION INFORMATICA

Que en opción al grado de Licenciado en Informática presentan:

HERNANDEZ MONTALVO ARACELI
ROBLES ARRIOLA LAURA LETICIA
VELAZQUEZ MONTAÑO MARIO ARMANDO

MBA. JOSE ANTONIO ECHENIQUE GARCIA

1992

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

" A U D I N : UN SISTEMA EXPERTO PARA AUDITORIA EN INFORMATICA "

I N D I C E

PAGINAS

OBJETIVOS Y ALCANCE 1

INTRODUCCION 3

I. ANTECEDENTES 6

A) INTELIGENCIA ARTIFICIAL 7

B) SISTEMAS EXPERTOS 17

C) AUDITORIA EN INFORMATICA 31

- SEGURIDAD FISICA 37

II. SISTEMAS EXPERTOS 42

A) ARQUITECTURA 43

B) ANALISIS Y DESARROLLO 62

III. DESARROLLO DEL SISTEMA EXPERTO 73

A) SELECCION DEL PROBLEMA 74

B) MODELO DE CONSTRUCCION 84

PAGINAS

C) FORMALIZACION 89

D) IMPLEMENTACION 91

E) EVALUACION 107

CONCLUSIONES 109

BIBLIOGRAFIA 112

ANEXOS 115

1. CLASIFICACION DE LOS SHELLS 116

2. DEFINICION DETALLADA DEL PROBLEMA ... 118

3. PLANEACION DEL PRODUCTO 120

4. DISEÑO 122

5. PLANEACION DE LA PRUEBA 126

6. PLANEACION DE LA IMPLEMENTACION 128

7. RELACION DE RIESGOS Y REGLAS DE PRODUCCION 131

OBJETIVOS

Y

ALCANCE

AUDIN

OBJETIVO.

ELABORAR UN SISTEMA EXPERTO QUE REALICE LA EVALUACION DE UNA AUDITORIA EN INFORMATICA.

OBJETIVOS SECUNDARIOS.

- COMUNICAR LA EXPERIENCIA OBTENIDA EN LA CREACION DE UN SISTEMA EXPERTO.

- IDENTIFICAR LOS ASPECTOS BASICOS EN LOS QUE SE BASA LA AUDITORIA EN INFORMATICA DENTRO DE LA SEGURIDAD FISICA.

- DAR A CONOCER UNA HERRAMIENTA QUE APOYA EL DESARROLLO DE SISTEMAS EXPERTOS.

ALCANCE.

EL DESARROLLO DE ESTE SISTEMA SE ENFOCARA EXCLUSIVAMENTE AL AREA DE AUDITORIA EN SEGURIDAD FISICA.

INTRODUCCION

INTRODUCCION

En la actualidad se están dando grandes cambios tecnológicos en los que nos encontramos inmersos y para los cuales debemos estar preparados. Las computadoras son la base de estos cambios y han contribuido al aumento de la inteligencia humana, no sólo porque nos proporcionan información sino porque nos ayudan a analizarla, clasificarla y porque hacen que sin excesivo esfuerzo se pueda dar un salto de la información al conocimiento.

La introducción de las computadoras y robots inteligentes ha provocado un cambio radical en nuestra sociedad. Para entender la importancia de este hecho es conveniente comprender dos puntos fundamentales. El primero de ellos es que prácticamente todos los usos y aplicaciones de las computadoras y de la automatización, sobre todo en la industria, están estrechamente relacionados con los principios básicos en los que se fundó la revolución industrial: más especificamente, el uso de las computadoras y de la automatización ha reemplazado a aquellos trabajadores que desempeñan labores poco calificadas y repetitivas. El segundo punto a tener en cuenta es que la introducción de una automaización inteligente, provocará una segunda revolución industrial, sin embargo los trabajadores que serán reemplazados en esta ocasión pertenecen a un nivel de dirección media cuyo trabajo no requiere de una gran capacidad inventiva ni creativa, para soportar su toma de decisiones.

Por todo lo mencionando anteriormente, el motivo principal que nos mueve a dar los primeros pasos hacia el análisis, diseño e implementación de un Sistema Experto, está basado en una serie de espectativas sobre el control del conocimiento, así como el de utilizar un software para diseño de sistemas expertos que fuese lo suficientemente poderoso y didáctico para apoyo de los niveles directivos que se encargan de tomar decisiones basadas en una clasificación y análisis de información y que además nos permitiera obtener resultados satisfactorios, que en nuestro caso sería un dictamen de auditoría a un Centro de Cómputo.

El contenido de la presente Tesis se ha dividido en 3 capítulos comenzando con una introducción a la Inteligencia Artificial y a los Sistemas Expertos, así como dando un panorama general de la Auditoría en Informática.

Posteriormente se profundiza en la Arquitectura, en el Análisis y Desarrollo de los Sistemas Expertos, finalizando con el desarrollo del sistema experto "AUDIN".

El primer capítulo nos dá un esbozo general de la historia y evolución de la Inteligencia Artificial, así como de uno de sus principales campos de aplicación como lo son los Sistemas Expertos, así mismo contiene los principales conceptos de Auditoría en Informática, dándole un mayor énfasis a la Auditoría en "Seguridad Física".

Dentro del segundo capítulo se lleva a cabo un estudio detallado sobre la arquitectura de los sistemas expertos, sobre las diferentes formas de representación del conocimiento, así como de la metodología propuesta para el desarrollo del sistema experto.

En el tercer capítulo se utiliza la metodología planteada en el capítulo anterior, con el fin de diseñar un sistema experto que evalúe la seguridad física a un Centro de Cómputo.

Cabe aclarar que la metodología utilizada para el análisis y desarrollo del sistema experto "AUDIN", es tan sólo una más de las que existen actualmente en el medio de los sistemas expertos y en especial de los sistemas conchas(shells), y la cual fue tomada como una guía, ya que no es objetivo de esta Tesis, hacer un estudio comparativo entre metodologías de diseño de sistemas expertos, sino utilizar una como base para desarrollar nuestro trabajo.

CAPITULO 1.

ANTECEDENTES

INTELIGENCIA

ARTIFICIAL

AUDIN

INTELIGENCIA ARTIFICIAL

En la vida diaria existen palabras y expresiones que pueden decirse sin temor a ser interpretadas incorrectamente, tal es el caso de "dolor de muelas", "depresión", etc. Sin embargo hay otra como inteligencia, la cual , aunque la mayoría la aceptamos como una de las características más deseadas, no todos aludimos a lo mismo cuando hablamos de ella.

La inteligencia se refiere, evidentemente, a la capacidad para realizar con éxito operaciones mentales. Pero ¿qué operaciones?. No hay duda de que la memoria tiene algo que ver con la inteligencia y lo mismo sucede con la capacidad de razonar, con la inventiva y con otras habilidades del aparato psíquico.

En las siguientes líneas se planteará la evolución de una disciplina que se ocupa de simular todos aquellos actos que el hombre denomina inteligentes, llamada **inteligencia artificial (IA).**

El concepto inteligencia artificial describe el conocimiento que poseen las personas acerca de los acontecimientos diarios, introduciendo dicho conocimiento en computadoras de manera que estas puedan manejarlo. Este proceso conlleva una serie de preguntas : ¿cómo representamos la información para introducirla a la máquina?, ¿ de dónde y cómo extrae la máquina la información necesaria en sus interacciones con el mundo real?. El implementar el conocimiento y el proceso de racionalización en las computadoras es un problema cuyo desarrollo ha sido lento, debido entre otros motivos a la carencia de herramientas necesarias. Estas herramientas son los computadores digitales, así como los lenguajes de programación.

Hasta hace poco, mucha gente había observado el campo de la inteligencia artificial como el lado oscuro de la ciencia informática, pero en menos de 5 años, la inteligencia artificial ha pasado ha ser la aportación más importante a la informática. Este rápido cambio se basa en cuatro factores fundamentales : el éxito de los sistemas expertos, que fueron los primeros productos de la inteligencia artificial de auténtico impacto comercial, el bien conocido compromiso de los japoneses con la inteligencia artificial (5a. Generación de Computadoras)[1], la lenta pero firme integración de las técnicas de

[1] La comunicación entre el hombre y la computadora en nuestro propio lenguaje es uno de los aspectos clave para los japoneses en su proyecto de quinta generación.

inteligencia artificial en las aplicaciones existentes y, finalmente, el hecho que ha llegado la hora de la **Inteligencia Artificial.**

"Es difícil especificar una fecha exacta de comienzo de la inteligencia Artificial, quizá su nacimiento se deba a A.M. Turing y a su invención de la computadora de programas almacenados como datos en su memoria y ejecutados posteriormente"[2], o quizá se atribuye comunmente a la Conferencia de Dartmouth en el año de 1956, donde Newell, Shaw y Simon presentaron sus programas para demostrar las proposiciones lógicas.

Pero también existe otra opinión como la de A.L. Samuel quien señala que la inteligencia artificial comenzó en 1834 o poco después, cuando Charles Babbage sugirió la posibilidad de que su máquina analítica jugara ajedrez. Contrariamente, por la misma época, Ada Lovelace planteó una premisa que tanto oímos repetir: la computadora no puede hacer nada para lo que no haya sido programada.

Hasta 1940 renació el interés por la inteligencia artificial, más allá de lo teórico, con el surgimiento de las modernas computadoras digitales. En 1947 aparecieron los primeros "jugadores automáticos de damas".

El primer programa inteligente que se intentó crear en la historia de la computación fue el de A.L. Samuel, y tuvo el raro comienzo de las cosas importantes, ya que en ese tiempo no existía una computadora para ejecutarlo. Samuel se vio precisado a convertirlo en una notación simbólica escrita a mano, para de esta forma acelerar su progreso.

Sin embargo, lo que normalmente se conoce como inteligencia artificial empezó hacia 1960, cuando John McCarthy creó LISP, el primer lenguaje de investigación dentro de la inteligencia artificial.

"El término inteligencia artificial, suele atribuírsele a Marvin Minsky, quien en 1961 escribió un artículo titulado *Hacia la inteligencia artificial*. En 1963 apareció un libro titulado *Computers and Thought*, editado por Feigenhaum and Feldman.

[2] SCHILDT, Herbert, Utilización de C en la Inteligencia Artificial.

El volumen es la recopilación de veinte trabajos de veintiocho autores englobados dentro de la categoría de problemas de juego".[3]

No obstante después de haber mencionado la definición anterior de inteligencia artificial, señalaremos otras que nos parecen importantes:

"La inteligencia artificial es una nueva forma de resolver problemas, dentro de los cuales se incluyen los sistemas expertos, el manejo y control de robots y los procesadores de lenguaje natural".[4]

"La inteligencia artificial trata del diseño de sistemas inteligentes, esto es, sistemas que presentan las características asociadas con la inteligencia humana: entendimiento del lenguaje, aprendizaje, razonamiento, resolución de problemas, etc".[5]

"La inteligencia artificial es la solución de problemas complejos con el apoyo de la computadora mediante la aplicación de procesos que son similares al proceso de razonamiento humano".[6]

Los años sesenta fueron un período de intenso optimismo hacia la posibilidad de que una computadora pensase. Después de todo los sesenta contemplaron la primera computadora que jugaba ajedrez y el programa ELIZA, que fue escrito en 1964 por Joseph Weizenbaum, dicho programa actuaba como un psicoanalizador rogeriano. En su momento el programa causó conmoción, ya que la gente preguntaba si podría una máquina ser mejor que un ser humano, pero recuerden que este período fue de fuerte temor a la automatización.

En los años setenta los investigadores sintieron la necesidad de enriquecer el LISP y de diseñar lenguajes en los que el control del razonamiento deductivo fuese fácil de escribir y comprobar, siendo éste el período en el que surgen, entre otros los lenguajes: MICRO-PLANNER (1971), PLANNER (1972) y CONNIVER (1972). Al mismo tiempo se retorna al concepto de objeto en SIMULA-67 (1970).

[3] Información Científica y Tecnológica, VOL 7, NUM 109, pp 16.

[4] INGELEK, Inteligencia Artificial y Sistemas Expertos, pp 7, 12..

[5] Idem.

[6] ROLSTON, David W., Op. Cit., pp 15.

Hacia finales de los setenta, destacan algunos éxitos en el campo de la inteligencia artificial, como lo es el procesador del lenguaje natural (PNL), la representación del conocimiento (Redes Semánticas, Marcos, Guiones, etc), y la resolución de problemas. Estos éxitos formaron la base para la introducción de uno de los primeros productos comerciales de la inteligencia artificial: **el sistema experto.**

Uno de los más importantes acontecimientos dentro de la inteligencia artificial ocurrió en los años setenta, pero pasó virtualmente desapercibido en los Estados Unidos hasta la década de los ochenta. Este fue la creación de PROLOG(Programación Lógica), en 1972, obra de Alain Colmerauer en Marsella, Francia y perfeccionado en Inglaterra. Al igual que LISP, Prolog era un lenguaje diseñado para ayudar a resolver problemas relativos a la inteligencia artificial; al contrario de LISP poseía características especiales, tales como una base de datos incorporada, una sintaxis bastante simple y rutinas de retroseguimiento.[7]

En esencia, hacia 1980, LISP era el lenguaje de la inteligencia artificial elegido en los Estados Unidos, mientras que el Prolog tenía el mismo status en Europa. Sin embargo en 1981, esta situación cambio tras el anuncio de los japoneses de que usarían Prolog como base de sus computadoras de la "Quinta Generación".

Los aspectos claves en la historia de la inteligencia artificial se observan en la figura 1.1

PUEDEN LAS COMPUTADORAS PENSAR?

Determinar lo que se considera como programa inteligente implica conocer el significado de inteligencia. Se define el término inteligencia como "la capacidad de comprender hechos y proposiciones, sus relaciones y razonamientos".[8] Esta definición nos lleva a la

[7] La capacidad de retroseguimiento es importante para muchas de las rutinas de Inteligencia Artificial porque permite que un algoritmo busque la solución a un problema siguiendo varios caminos (lineas de razonamiento), si la ruttina encuentra un punto muerto simplemente vuelve hacia el punto más cercano del proceso e intenta otra vez.

[8] SCHILDT, Herbert, Op. Cit., pp 5.

pregunta "¿Qué significa razonar?". En este contexto significa pensar. Hace mucho tiempo se consideraba que la gente no podía explicar como pensaba, pero podía decir lo que pensaba. El hecho es que la gente realmente no puede entender cómo razona. Si lo hiciera, no sería pues tan difícil hacer a una computadora inteligente.

PERIODO	SUCESOS CLAVES
ANTES DE LA 2A GUERRA MUNDIAL	LOGICA FORMAL PSICOLOGIA DEL CONOCIMIENTO
LA POSTGUERRA 1945-1954, INICIO DE LA I.A.	DESARROLLO DE LA COMPUTADORA CONFERENCIAS SOBRE CIBERNETICA
AÑOS DE FORMACION 1955-1960	AUMENTA LA DISPONIBILIDAD DE LAS COMPUTADORAS LENGUAJE DE PROCESO DE INF.(IPL-1) PSICOLOGIA DEL PROCESO DE INF.
AÑOS DE DESARROLLO 1961-1970	LISP HEURISTICA ROBOTICA SOL. A PROBLEMAS DE AJEDREZ DENTRAL (STANFORD)
ESPECIALIZACION Y SISTEMAS EXPERTOS. 1970-1980	MYCIN (STANFORD) MACSYMA (MIT) INGENIERIA DEL CONOCIMIENTO EMYCIN (STANFORD) PROLOG
LA COMERCIALIZACION 1981	PROSPECTOR (SRI) PROYECTO JAPONES DE LA 5A. GEN. INTELLECT (A.I.C.) SISTEMAS INTELIGENTES DE RECUPERACION DE LA INFORMACION DIVERSAS COMPAÑIAS COMERCIALIZAN HERRAMIENTAS PARA LA CONSTR. DE SISTEMAS EXPERTOS

FIGURA 1.1.- ASPECTOS CLAVES EN LA HISTORIA DE LA INTELIGENCIA ARTIFICIAL

Debido a que la gran mayoría no entiende los procesos del pensamiento, incorrectamente se asume que cualquier mecanismo construido y dominado por el hombre no puede ser más inteligente que el hombre mismo.

Las dificultades estriban en un error de apreciación del concepto "inteligencia", ya que implícitamente se relaciona con "inteligencia humana". Esta asociación hace difícil admitir la posibilidad de que una máquina o un programa de computadora pueda ser inteligente, por el hecho de que los programas no realizan la misma labor igual que lo hace una persona, por eso cuando esta relación desaparece, es fácil decir que los programas inteligentes pueden existir.[9]

TEMAS FUNDAMENTALES DE LA INTELIGENCIA ARTIFICIAL

El campo de la inteligencia artificial se compone de varias áreas de estudio. Las más comunes e importantes son las siguientes:

- Búsqueda (de soluciones)
- Sistemas expertos
- Procesamiento del lenguaje natural.
- Reconocimiento de modelos.
- Robótica.
- Aprendizaje de las máquinas.
- Lógica.
- Incertidumbre y "lógica difusa".

Algunas de las áreas anteriores representan aplicaciones finales, tales como los sistemas expertos; otras como el procesamiento del lenguaje natural y la búsqueda de soluciones,

[9] Un programa inteligente es aquel que muestra un comportamiento similar al de un humano que se enfrenta a un mismo problema. No es necesario que el programa resuelva o intente resolver el problema de la misma manera que lo haría un humano.

son bloques de la inteligencia artificial que se añaden a otros programas para complementar su proceso.

Cuando hablamos de inteligencia artificial, el término búsqueda se refiere a la búsqueda de soluciones a un problema.

Los sistemas expertos son el primer producto de la inteligencia artificial viable comercialmente. Un sistema experto tiene dos atributos escencialmente: primeramente, le permite al usuario introducir información sobre un tema a la computadora, a esta información suele llamársele **base de conocimiento**; en segundo lugar, es capaz de responder a las interrogantes como si fuese un experto en la materia utilizando su base de conocimientos.

Para muchos investigadores en inteligencia artificial, el procesamiento del lenguaje natural (conocido con frecuencia como PNL Procesor Natural Languaje) es uno de los fines principales que la inteligencia artificial debe alcanzar porque permite a la computadora la entrada del lenguaje humano en forma directa. El mayor obstáculo para alcanzar esta meta es el tamaño y la complejidad de los lenguajes humanos.

El reconocimiento y relación de modelos es importante para varias aplicaciones incluidas la robótica y el procesamiento de imágenes, porque le permite a una computadora interrelacionarse con el mundo exterior.

Aplicado a la robótica la inteligencia artificial ayuda a que una computadora controle los movimientos usando un razonamiento especial. Para los robots industriales como los utilizados en el ensamble de automóviles, los problemas para la inteligencia artificial aparecen al tratar de suministrarles un movimiento natural y preciso dentro de un conjunto de posiciones concretas. Los robots autónomos tienen mayores problemas para desenvolverse ante sucesos inesperados o cambios de ambiente.

Una de las áreas más interesantes de la inteligencia artificial es la del aprendizaje mecánico. Esta área trata de hacer que los programas aprendan de sus propios errores, en base a la observación y a la autoevaluación. El aprendizaje mecánico significa simplemente hacer que la computadora sea capaz de beneficiarse de su propia experiencia.

De los muchos productos de la inteligencia artificial, de importancia práctica, están aquellos que pueden usarse para estudiar la corrección de un argumento aplicando reglas lógicas generales. El que la computadora pueda pensar de la misma manera implica el uso de la lógica incierta , es decir, la toma de decisiones basadas en una información incompleta o probable.

CONTRIBUCION DE LA INTELIGENCIA ARTIFICIAL A LOS SISTEMAS DE AYUDA PARA LAS DECISIONES (SIAD).

La inteligencia artificial se introduce en los SIAD de varias formas: primeramente, se impuso en el tratamiento de los datos cualitativos , aproximados o inciertos; en segundo punto, está relacionada al concepto de racionalidad limitada, ya que se han llegado a concebir sistemas que transcurran paralelamente al comportamiento humano. Finalmente la inteligencia artificial ha contribuido a la interfaz sobre todo en el diálogo hombre-máquina. Si el logro de tener pantallas claras, funcionales y agradables no es una función específica de la inteligencia artificial, digamos que han contribuido fuertemente, en particular los sistemas expertos.

La representación del conocimiento y sus materiales (taxonomía, jerarquía, prototipos y marcos), también han aportado ideas nuevas en el campo de los SIAD. En particular la descomposición de tareas complejas en problemas jerárquicos.

La idea de construir para un problema dado, *espacios de estado*, en el que por continuas tentativas el sujeto llega a progresar hacia una solución satisfactoria, es también otra contribución de la inteligencia artificial (Newell y Simon, 1972). Dentro de este campo los SIAD han utilizado procedimientos ya existentes como lo es MULTIDECISION, en el campo de la decisión en donde intervienen numerosos criterios de selección.

Finalmente se necesita hablar de un campo en plena efervescencia que es el de las bases de datos inteligentes. Se puede esperar en un futuro próximo introducir en la base de datos los conocimientos implícitos en forma de reglas para poder permitir la comprensión de cuestiones "no previstas". Dentro de la concepción y definición inteligente de base de datos se debe señalar una aplicación de sistemas expertos como lo es el sistema SECSI desarrollado por MASI e INRIE.

LAS PERSPECTIVAS DE LA INTELIGENCIA ARTIFICIAL

Aunque es difícil predecir en la actualidad lo que serán capaces de hacer los sistemas inteligentes dentro de sus múltiples aplicaciones, lo que observamos son sistemas basados en su conocimiento con el que son capaces de enfrentarse y resolver problemas dentro de un campo muy limitado, no tienen desarrollada la facultad de aprender, ni pueden razonar y esto se debe principalmente a dos factores: 1) la falta de sentido común y 2) sus razonamientos se deterioran rápidamente cuando el problema sale de su campo de solución.

El futuro de la inteligencia artificial depende en gran parte de los diferentes métodos de aprendizaje de las computadoras.

El procesamiento de imágenes humanas, es sin duda, la etapa más difícil de alcanzar en el desarrollo de la inteligencia artificial, porque implica la comunicación directa a través del habla y las imágenes con la computadora. El tratamiento efectivo de las señales eléctricas necesita en primer término, circuitos especializados para determinar los rasgos básicos de las palabras y de las imágenes. El tratamiento del lenguaje comprenderá el análisis fonético, sintáctico, semántico y pragmático. Para la traducción automática (inicialmente inglés y japonés), se pretende contar con un vocabulario de cien mil palabras y que el sistema almacene cuando menos cien mil símbolos.

SISTEMAS

EXPERTOS

AUDIN

SISTEMAS EXPERTOS

Como se mencionó anteriormente uno de los principales objetivos de los investigadores de la inteligencia artificial es la reproducción automática del razonamiento humano.

El razonamiento de un jugador de ajedrez no siempre es el mismo que el de un directivo que se pregunta la viabilidad de fabricar un nuevo producto. Hay muchos modos de razonar y de considerar situaciones complejas. La función asignada a los sistemas expertos es la de razonar. Podemos considerar la siguiente definición de un sistema experto: "es un programa de computadora capaz de almacenar información como si fuese una base de datos y utilizar dicha información para obtener nuevos resultados, empleando métodos de razonamiento e inferencia."[1]

Los sistemas expertos son programas que imitan el comportamiento de un humano. Utilizan la información que el usuario le proporciona para darle una opinión sobre cierta materia. Por tanto, el sistema experto le hace preguntas hasta que pueda identificar un objeto que se relacione con sus respuestas.

La década comprendida entre 1960 y 1970 vio sentar los principios básicos de la investigación en las estructuras de árbol así como el movimiento de ideas empleadas actualmente en la resolución de problemas y los sistemas expertos. Los textos de Newell y Simon (1972) y Nilsson (1971) marcan el final de este período. Los principales métodos de búsquedas en estructuras de árbol que todavía se emplean hoy en los sistemas expertos, estaban ya disponibles en aquel tiempo. Pero las realizaciones de los investigadores se concentraron especialmente en problemas fáciles de describir pero muy complejos de resolver, por ejemplo, el juego de ajedrez o la demostración de teoremas matemáticos (en estos comportamientos los programas quedaron -y siguen quedando -por debajo del rendimiento de los sistemas expertos humanos). Precisamente lo que ha llegado a ser el principal campo de aplicación de los sistemas expertos, es decir, los problemas "imprecisamente definidos" que constan de un gran número de reglas y de hechos pero con una complejidad estratégicamente limitada, no habían sido abordados en aquel tiempo, a excepción del programa DENDRAL, que apareció a mediados de los '60 bajo la dirección de Buchanan. Este programa determina la estructura desarrollada de una molécula a partir de su masa. DENDRAL, fue el primer programa en el que contribuyeron especialistas ajenos a la ciencia de la computación.

[1] INGELEK, Op. Cit., pp 21.

En los años setenta los programas e investigaciones se enfocan hacia la naturaleza del conocimiento. Investigadores de diferentes ramas (informática, psicología, filosofía, matemáticas, etc.) intentan determinar lo que es el conocimiento, es decir, la integración de todos aquellos factores internos, como lo son la capacidad de aprender y de razonar; así como factores externos, en este caso el medio ambiente que influye en la formación moral y psicológica de los individuos, que le permiten adquirir un sentido común para poder responder a las interrogantes diarias.

El desarrollo de las herramientas de programación, el estudio del conocimiento y el éxito de DENDRAL, permitieron en los años 1975-1980 el nacimiento de los **sistemas expertos.**

CARACTERISTICAS DE LOS SISTEMAS EXPERTOS

Como características de los sistemas expertos podemos considerar las siguientes:

- pueden almacenar información, como si fuese una base de datos, sobre el tema considerado.

- tiene la facultad de utilizar esa información para obtener unos resultados que no existían previamente en la computadora.

- tiene la capacidad de aprendizaje, la cual aunque parece una cualidad extravagante, resulta fácil de implantar, se convierte en una herramienta muy útil a la hora en que el sistema mejora con respecto del momento de su creación. El aprendizaje le permite al sistema utilizar nueva información que necesite para los procesos de inferencia.

- el poder de inducción, que no es otra cosa que la combinación de datos almacenados y de información que introduce el usuario, para producir nuevos elementos de juicio a un problema dado.

Las características mencionadas anteriormente quedan ejemplificadas en la figura 1.2.

Así mismo, los sistemas expertos permiten que una computadora ejecute una parte de un proceso de decisión inteligente o de solución a un problema. Este tipo de tecnología se puede aplicar cuando en un problema se presentan las siguientes condiciones generales :

a) Existen expertos humanos, que guiarán al ingeniero del conocimiento en la creación del sistema experto.

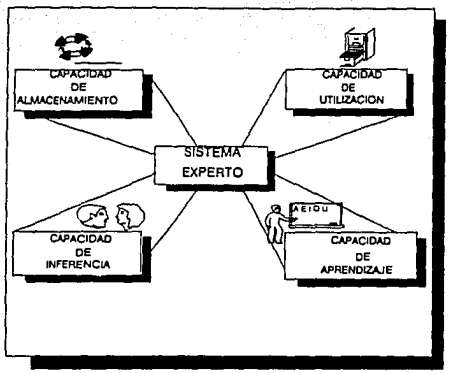


FIGURA 1.2.- CAPACIDADES DE LOS SISTEMAS EXPERTOS.

b) El problema tiene perfectamente enmarcado su dominio y la nomenclatura para su descripción está ya definida.

c) El problema no es reducible a un algoritmo numérico, ya que si no, no merecería la pena construir el sistema experto.

La construcción de sistemas expertos, es decir, la ingeniería del conocimiento se fundamenta en la estrecha colaboración entre un informático especializado y un experto humano cuyos conocimientos y experiencias sobre una materia determinada se tratan de transferir a un programa de computación, para que este sea capaz de resolver los problemas que se le plantean sobre esa materia de una manera similar a como lo hace el experto humano.

Un sistema experto se divide principalmente en la base de conocimientos, el método de solución de problemas, es decir, el motor de inferencias, y la forma de interaccionar con el usuario. Pero estos conceptos se tratarán más ampliamente en el Capítulo II Sistemas Expertos.

¿QUE PUEDE HACER UN SISTEMA EXPERTO?

Hay 2 formas de responder a ésta interrogante, una hablando de funciones que parecen pertenecer a los sistemas expertos, otra tratando de describir el contexto al cual va dirigida su construcción.

Comencemos hablando de funciones que se pueden confiar a un sistema experto. Entre estas funciones básicas, citaremos :

- *La interpretación:* traducción de señales en expresiones simbólicas que se utilizarán en los razonamientos;

- *El diagnóstico:* se establece una correlación entre características o síntomas y situaciones problema;

- *La formación :* transmisión de conocimientos a un alumno cuyo nivel y características han sido objeto de un diagnóstico; esta transmisión del saber o del saber hacer puede llevarse al diagnóstico, al mantenimiento, al diseño, etc.

- *La vigilancia :* el desencadenamiento de una alarma en las condiciones determinadas pudiendo evolucionar con el contexto o envío de un informe a partir de las señales interpretadas y utilizadas en un diagnóstico;

- *La previsión:* descripción de una situación anticipadamente, a partir de situaciones comunes y corrientes, generalmente para el modelo construido sobre base histórica o por aprendizaje;

- *La simulación :* deducción a partir de un modelo, de las consecuencias de las acciones o de acontecimientos, desencadenados por el sistema en el curso de la simulación.

- *La planificación :* definición en el tiempo y el espacio de las acciones, permitiendo esperar un estado final, comparando las consecuencias en curso y el estado deseado y previniendo los resultados de las acciones, respetando las reglas impuestas por el entorno y las consecuencias de las interacciones entre estados y acciones o entre estados sucesivos;

- *El mantenimiento*: plan de acción particular consistente de un diagnóstico en curso, iluminando las fallas de un sistema e identificando sus causas; de modo iterativo, la simulación permite confrontar los resultados de las pruebas, con los que daría un sistema en funcionamiento propiamente; el plan de acción consiste en crear las instrucciones necesarias para efectuar la reparación;

- *El diseño* : conjunto de elecciones y decisiones que permiten fijar eventualmente, puntos de control de rendimiento después de un diagnóstico, determinar en el manual de operaciones el objeto a cumplir en función de las necesidades expresadas en un instante dado y, de sugerir los medios para cumplir este objetivo, definiendo las especificaciones de un producto o de un proceso que concierne al manual de operaciones.

- *El control*: conjunto de acciones aplicadas a un sistema, después de la información resultante del monitoreo al mismo y de la anticipación de situaciones futuras, para asegurar através de un mantenimiento permanente y una respuesta adaptada a diversos acontecimientos casuales, un funcionamiento del sistema que se acerca lo más posible al funcionamiento normal.

A partir de estas funciones, ahora debemos definir los dominios de aplicación. Cada uno de estos dominios están cubiertos por un tipo de sistema experto. Se consideran dos tipos básicos : 1) Sistemas Expertos Generativos y 2) Sistemas Expertos Operativos.

Los primeros, realizan tareas de tipo "creativo", su función principal es el diseño (por ejemplo, industrial, de piezas mecánicas, etc), la resolución de problemas matemáticos, etc, utilizando su propia base del conocimiento.

Los segundos, son sistemas consultivos, manejan gran cantidad de información y su correcta utilización para la solución de un problema. Los principales campos de operación son: el mantenimiento de máquinas, la consulta médica especializada, etc.

A continuación mencionaremos en forma general el avance de las diversas ramas de aplicación de los Sistemas Expertos tomando en cuenta que la definición anterior nos permitirá ubicarlas dentro de un dominio específico.

Se encuentran en primer lugar, tanto desde el punto de vista histórico como en cantidad de sistemas desarrollados, las aplicaciones en medicina y biología destinadas a las funciones de diagnóstico y de propuestas terapéuticas. También las que se encuentran en el dominio de la agricultura y la economía.

El diagnóstico técnico y el mantenimiento(búsqueda de las causas de avería y para remediarlas) han dado lugar a numerosos sistemas encargados de la reparación de vehículos o de máquinas.

En el dominio económico y financiero, sus aplicaciones son en las funciones del diagnóstico de la empresa, de la formación de vendedores y los créditos a particulares, en las que se han interesado los diseñadores de Sistemas Expertos.

Las funciones de planificación, diagnóstico y simulación pueden combinarse para desarrollar aplicaciones en el dominio de ayuda a la decisión estratégica.

La función de la interpretación ha sido utilizada en química, bioquímica y en las aplicaciones militares.

En el campo de la enseñanza, las aplicaciones están en los programas tutoriales, los programas de simulación de modelos, así como los programas de material didáctico complementario para los cursos.

Resumiendo en lo que respecta a la industria, las funciones de diagnóstico y/o mantenimiento son las que ocupan el primer lugar, a continuación las de ayuda a la decisión, el control y vigilancia de procesos.

Lo que es inevitable es que los sistemas expertos están ampliando notablemente el ámbito de aplicación de la informática, ya que permiten resolver por métodos heurísticos problemas que hasta ahora habían resultado inabordables mediante procedimientos algorítmicos convencionales.

NUEVAS DIRECCIONES EN LA CONSTRUCCION DE SISTEMAS EXPERTOS

Un factor muy importante que demanda cada vez más de el mercado industrial es la integración. Un sistema experto debe ser capaz de integrarse en el entorno del hardware y software de la empresa que lo vaya a utilizar, de manera que pueda utilizar todos los recursos que esta dispone sin necesidad de renovar parte del sistema.

Otro factor muy importante es la interfase con el usuario. Las personas que utilicen estos sistemas expertos serán personas que no tengan conocimiento de informática, por ello necesitan un entorno fácil de manejar, de ser posible ayudado por gráficos. Siguiendo con las nuevas direcciones aparte de las dos anteriores, se encuentran otros aspectos muy importantes como:

- **La adquisición de conocimiento nuevo.** Quizá es el problema más grande al crear sistemas expertos, ya que se necesita como experto, al mejor del ramo y será prácticamente imposible retenerlo para poder actualizar el sistema al cabo del tiempo, por ello sería interesante que el sistema pudiese adquirir conocimiento nuevo y aprender a partir de experiencias pasadas.

- **¿Cómo extraer información de la manera más rápida posible?** No se puede tener al experto más calificado ocupado durante todo el proceso de desarrollo del sistema experto. ¿Cómo podemos conseguir la información que necesitamos de la manera más rápida?. Hay dos enfoques. En primer lugar, está el enfoque de sistemas de software, es decir de sistemas expertos cuyo objetivo es acelerar la codificación del conocimiento y verificar que está bien formalizado. Otro enfoque es que sea el propio experto quien produzca el conocimiento, pero esto tendría que ser a base de lenguaje natural, pues el experto no conoce los métodos de codificación y no tiene el tiempo para aprenderlos. La tarea del ingeniero del conocimiento (IC) no es tanto la de conocer la herramienta y saber codificar el conocimiento, como la de ser capaz de extraer el conocimiento necesario del experto humano y saber organizarlo y transportarlo a la base de conocimientos. Esta función es la de mayor dificultad en la construcción de Sistemas Expertos y se debe principalmente al hecho de que el proceso requiere comunicaciones estrechas entre el experto en el área y el IC.[2]

HERRAMIENTAS PARA LA CONSTRUCCION DE UN SISTEMA EXPERTO

Es lógico emplear la expresión *sistema experto* para designar un sistema completo con sus reglas y hechos, es decir, con el conocimiento que necesita para ser utilizable.

Emplearemos la palabra Shell, para designar un sistema con todas sus utilidades y que sólo necesita el conocimiento específico del dominio para ser un sistema experto. Los shells son desarrollados a partir de lenguajes de propósito general que proporcionan mayor potencia para la creación de los sistemas expertos incorporando muchas facilidades sobre inferencia y control, agilizando con esto enormemente, la creación del sistema.

Los lenguajes como LISP, PROLOG o SMALLTALK, son herramientas útiles capaces de simplificar la tarea de desarrollar los sistemas expertos.

[2] Bajo la denominación de Ingeniería del Conocimiento se conoce al proceso de adquirir el conocimiento del área específica y estructurarla en una base de conocimientos.

PIONEROS.

EMYCIN

Origen.-

EMYCIN se realizó bajo la dirección de Van Melle (1979); se trata de un sistema desarrollado por Shortliffe en la Universidad de Stanford (California) bajo el nombre de MYCIN (1976). El módulo de adquisición del conocimiento de MYCIN se debe a Davis (1976) y recibe el nombre de TEIRESIAS.

Máquinas y Lenguajes.-

MYCIN como TEIRESIAS, se escribieron en INTERLISP(dialecto de LISP) en una computadora DEC PDP-10.

Entornos y Utilidades.-

- Explicación de los razonamientos »por qué« y »cómo« (WHY y HOW).
- Explicación de las cuestiones, comentarios (WHAT) y ayudas(HELP).
- Módulo de admisión del conocimiento permitiendo introducción de nuevas reglas.

Aplicaciones.-

A causa de su origen EMYCIN está adaptado principalmente a problemas de diagnóstico en el campo de la medicina. Un sistema para el diagnóstico de averías de computadoras ha sido desarrollado por Bennet(DART, 1981), en geología se emplea LITHO para la determinación de litofacies (Bonnet,1982). Para la aplicación en diagnósticos financieros está siendo desarrollado por la Compagnie Bancaire.

Sistemas derivados y similares.-

Hay una versión de EMYCIN para computadoras personales llamada PERSONAL CONSULTANT, comercializada por Texas Instruments. Se ha anunciado una versión de PERSONAL CONSULTANT, que incluye macros.

KAS

Origen.-

KAS(knowledge Adquisition System) se derivó del PROSPECTOR por Duda, Gasching y Hart, para la exploración de depósitos minerales (1979). PROSPECTOR fue perfeccionado con la inclusión de restricciones de estado, por el SRI, empresa relacionada con la Universidad de Stanford.

Máquinas y Lenguajes.-

KAS está escrito en INTERLISP para el DECKL-10 y en MACLISP para el HB.DPS8 bajo sistema Multics.

Entornos y Utilidades.-

- Editor específico para la red semántica. Este editor evita los errores en la introducción o supresión de nodos en la red. El manipula tanto los hechos «preguntables» y los que no lo son.

- Explicación de los razonamientos, por qué y cómo (WHY y HOW).

- Explicación de las preguntas, comentarios (qué, WHAT) y ayuda.

- Modificación de las respuestas durante el proceso.

- Posibilidad de proveer y probar los factores de certeza, suficiencia y necesidad.

Aplicaciones.-

KAS, como su predecesor PROSPECTOR, está sobre todo adaptado al diagnóstico. Su lógica Bayesiana le hace apropiado en los dominios en donde es fácil establecer probabilidades a priori.

Sistemas derivados o similares.-

No existe ninguna versión de KAS para micros, pero dos sistemas del mismo tipo están disponibles para los micros: INFERENCE-MANAGER Y MICRO-EXPERT. Un shell relativamente similar a KAS es KES (Knowledge Engineering System), comercializado por Software Architecture and Engineering, al igual que KAS el sistema KES está basado en una red de inferencias y en el modelo bayesiano. KES se ha utilizado en el diagnóstico de averías y en la planificación de misiones militares.

HEARSAY-III

Origen.-

Hay una dinastía de HEARSAY. Los dos primeros fueron sistemas de comprensión del lenguaje natural. HEARSAY-III, fue diseñado por Ernan, London y Fickas.

Máquinas y Lenguajes.-

HEARSAY-III está escrito en INTERLISP para computadoras IBM Y DEC.

Entornos y utilidades.-

No hay utilidades en desarrollo; este shell se ha quedado en el prototipo. Es un sistema abierto de gran modularidad. El conocimiento y las reglas pueden tener -más o menos- cualquier forma.

Es una herramienta particularmente adaptada en los sistemas que tienen en cuenta el tiempo y las interacciones temporales complejas entre los subsistemas.

Aplicaciones.-

No existe ninguna aplicación fuera del dominio del reconocimiento del habla.

Sistemas derivados y similares.-

Ciertas ideas de HEARSAY-III han sido tomadas en AGE.

EXPERT

Origen.-

EXPERT surgió de la experiencia con CASNET(1977), que fue desarrollado en la Universidad de Rutgers en un ambiente médico comparable con el de MYCIN. EXPERT fue implantado por Weiss y Kulikowski (1979).

Máquinas y Lenguajes.-

Hay varias versiones escritas en FORTRAN para computadoras IBM Y DEC.

Entorno y Utilidades.-

- Existencia de un editor que permite escribir el programa.

- Explicación de los razonamientos por qué y cómo.

- Comentarios (qué).

- Acepta cambios en el curso de una sesión.

- Posibilidades de interfase con la base de datos.

Aplicaciones.-

Como KAS y EMYCIN, es un sistema de diagnóstico. La primera aplicación fue CASNET para el tratamiento de la glucoma y otras aplicaciones médicas.

Sistemas derivados y similares.-

No hay versión para micros.

AGE

Origen.-

Sistema desarrollado en la Universidad de Stanford por Nii y Aiello (1979). Es una herramienta que intenta proveer un entorno similar a los de EMYCIN, KAS, y HEARSAY.

Máquinas y Lenguajes.-

El sistema AGE se desarrolló en LISP para computadoras IBM y DEC.

Entorno y utilidades.-

- Pocas facilidades a nivel interfaz de entrada-salida.

- Un módulo de ayuda para construir uno mismo un sistema a partir de rutinas básicas.

- Posibilidad de incluir rutinas nuevas escritas en LISP.

Sobre aplicaciones y sistemas derivados no se tiene nada en desarrollo.

Dentro de la segunda generación encontramos sistemas orientados a los usuarios. En esta categoría se mencionan los sistemas : ART, S1, CRL y KEE.

Los sistemas más recientes son grandes sistemas proyectados para tener un uso más o menos universal: shells para micros, basados en los lenguajes de inteligencia artificial y particularmente los lenguajes orientados a objetos. De esta nueva oleada se tienen: ALOUETTE, que consideramos representativo de un sistema derivado de un lenguaje orientado a objetos SNARK, MP-LRO, seguido por ARGUMENT, INSIGHT e INTELLIGENCE SERVICE, que son sistemas desarrollados para micros y finalmente el sistema multiexperto DECIDEX.

Los párrafos anteriores se enfocan hacia las características de los sistemas expertos pioneros, pero para poder tener un punto de comparación con las herramientas modernas de diseño de sistemas expertos (shells), observemos la figura 1.3.

¿CUALES SON LAS VENTAJAS DE UN SISTEMA EXPERTO?

El atractivo de un sistema experto es fundamentalmente su disponibilidad y conveniencia. A diferencia de un humano que tiene que dormir, comer, descansar, etc... el sistema experto está disponible las 24 horas al día durante todos los días del año. Además pueden crearse muchos sistemas expertos, mientras que hay un número limitado de expertos humanos. Los conocimientos de un sistema experto pueden ser copiados y almacenados fácilmente, siendo muy difícil la pérdida de éstos.

SHELLS PARA SISTEMAS EXPERTOS

SHELL	SISTEMA BASICO	LENGUAJE	REFERENCIA	MODELO
AGE	HEARSAY II	LISP	Nii, 1979	REGLAS,TABLERO, FTES. INDEPEN. DE CONOC.
EMYCIN	MYCIN	LISP	BUCHANAN,1984	REGLAS,ENCADENAMIENTO HACIA ATRAS,CONS DE DIAGNOSTICO
EXPERT	CASNET	FORTRAN	WEISS, 1984	REGLAS, CLASIFICACION CONS. DE DIAGNOSTICO
KAS	PROSPECTOR	LISP	DUDA, 1984	REGLAS, REDES SEMANTICAS HACIA ADELANTE Y HACIA ATRAS.

HERRAMIENTAS PARA SISTEMAS EXPERTOS CON BASE EN PC

	FACTOR DECISORIO	INSIGTH2	M1	EXSYS	ESIP ADVISOR
ENCADENAMIENTO HACIA ADELANTE	X	X	X	NO	NO
ENCADENAMIENTO HACIA ATRAS	X	X	X	X	X
REPRESENTACION					
REGLAS	X	X	X	X	X
REDES SEMANTICAS	X	NO	NO	NO	NO
INCERTIDUMBRE INCORPORADA	NO	X	X	NO	X
INTERFAZ CON EL USUARIO					
EDITOR INCOPORADO	X	X	NO	X	NO
MENUS	X	X	NO	NO	X
INTERFAZ CON SOFTWARE					
DBASE	NO	X	X	X	NO
LOTUS 123	NO	NO	NO	X	NO
EXPLICACIONES INCORPORADAS	NO	NO	NO	X	NO

FIGURA 1.3.- SHELLS PARA SISTEMAS EXPERTOS

AUDITORIA

EN

INFORMATICA

AUDIN

AUDITORIA

La auditoría se puede definir como una investigación crítica sobre las operaciones de una organización.

La auditoría se basa en una revisión analítica del Control Interno, que es plasmado en un informe realizado por el auditor.

La auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados una vez llevados a cabo, son de carácter indudable, si no que requiere el ejercicio de un juicio profesional, sólido y maduro para juzgar los procedimientos que deben de seguirse, con el fin de estimar los resultados obtenidos.

OBJETIVOS DE LA AUDITORIA.

- Mejorar la situación de la empresa.
- Sugerir mejoras (en controles, procedimientos).
- Detectar fallas.
- Reunir elementos para la toma de decisiones.
- Reducir riesgos.
- Retroalimentar oportunamente a los encargados de la toma de decisiones.
- Optimizar el uso de recursos.
- Analizar imparcialmente el uso de recursos.
- Analizar imparcialmente las funciones.
- Estandarizar métodos y procedimientos.

TIPOS DE AUDITORIA.

La auditoría se puede clasificar en diferentes tipos dependiendo de:

- QUIEN LA REALIZA	Interna. Externa.
- TIPO DE RESULTADO	Financiera. Operacional. Administrativa. Crédito. Informática.
- POR SU PERIODO	Permanente Esporádica.
- POR SU ALCANCE	Exhaustiva Selectiva.

CONCEPTO DE CONTROL INTERNO.

El Control Interno es la verificación de la confiabilidad y exactitud de la información de una organización, promoviendo el uso de las políticas establecidas y la eficiencia operacional basada en la conjunción de métodos, procedimientos y planes.

"El control interno comprende el plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus activos, verificar la razonabilidad y confiabilidad de su información financiera, así como provocar la adherencia a las políticas prescritas por la administración".[1]

El estudio y evaluación del Control Interno se efectúa con el objeto de cumplir con la norma prevista de ejecución del trabajo que el auditor debe efectuar, a fin de que le permita determinar la naturaleza, extensión y oportunidad que va dar a los procedimientos de auditoría.

[1] ECHENIQUE, García José A., Auditoría en Informática.

ELEMENTOS DEL CONTROL INTERNO.

En general podemos definir los elementos del control interno en los siguientes:

- ORGANIZACION	Dirección. Cordinación. División de labores. Asignación de labores. Asignación de responsabilidades.
- PROCEDIMIENTOS	Planeación y Sistematización. Registros y formas. Informes.
- PERSONAL	Entrenamiento. Eficiencia. Moralidad. Retribución.
- SUPERVISION	Directa. Indirecta.

AUDITORIA ASISTIDA POR COMPUTADORA.

"En general, el auditor debe utilizar la computadora en la ejecución de la auditoría, ya que esta herramienta permite ampliar la cobertura del examen, reduciendo el tiempo/costo de las pruebas y procedimientos de muestreo, que de otra manera tendrían que efectuarse manualmente".[2]

En la actualidad, la auditoría se puede apoyar fuertemente con el uso de las computadoras reduciendo en gran parte el tiempo y costo de las pruebas efectuadas a las muestras seleccionadas, haciendo más eficiente la aplicación del examen.

[2] Idem.

Tomando en consideración que uno de los recursos más importantes de una empresa es su información, se deben tener absoluto cuidado con toda la documentación, paquetería, programas fuente y objeto utilizados en la auditoría, siendo esta área la responsable del mal uso que se les pudiera hacer a estos.

AUDITORIA INFORMATICA

La auditoría informática es el examen y validación de los controles y procedimientos utilizados en el área de sistemas a fin de verificar que se cumplan de manera satisfactoria y de acuerdo a las políticas de la empresa los objetivos siguientes:

- Continuidad en el servicio.

- Confidencialidad y seguridad de la información.

- Integridad y coherencia de la Información.

La auditoría en informática comprende un examen completo y constructivo de la unidad o área de informática en aspectos como Planeación, Organización, Control, Uso de recursos (Software, Hardware, Humanos, Técnicos y Financieros); con el fin de descubrir deficiencias e irregularidades y proporcionar las recomendaciones necesarias para mejorar su servicio, funciones, condiciones de operación y crecimiento.

La auditoría informática debe evaluar el todo con auxilio de los principios de la auditoría administrativa, interna, contable/financiera y a su vez proporcionar información a estos tipos de auditorías convirtiéndose en la herramienta automatizada capaz de realizar cualquiera de estas.

La diferencia entre los fines del control interno desde el punto de vista contable/financiero y el punto de vista informático es que el segundo, está orientado a todos los sistemas en general, al equipo de cómputo y al departamento de informática.

OBJETIVOS DE LA AUDITORIA INFORMATICA.

Después de revisar varios documentos de auditoría en informática podemos concluir que los objetivos son los siguientes:

- Garantizar la continuidad del servicio.

- Evitar el mal uso de la información.

- Garantizar que sea útil la información que se obtiene de la unidad de Informática.

- Verificar el cumplimiento de disposiciones legales y las actividades de la Unidad de Informática.

- Evaluar el control establecido en el uso y operación de los recursos de cómputo, así como su aprovechamiento.

El auditor informático debe establecer controles en:

- Aplicaciones (Programas de producción).

- Desarrollo de Sistemas.

- Instalaciones del Centro de Cómputo.

- Manual de uso de información.

- Manual de respaldo y recuperación de información.

SEGURIDAD

A fin de que dichos controles sean más eficaces, el auditor, debe tener un especial cuidado en la seguridad de los procedimientos, así como evaluar todo aquel aspecto que pueda interferir en su operación.

El objetivo de implantar controles de seguridad es el de establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio debido a posibles contingencias. Las contingencias se pueden presentar por diversos tipos de riesgos.

TIPOS DE RIESGOS.

- HUMANO	Modificación a los datos. Destrucción de los datos. Divulgación de Información.
- HARDWARE	Fallas de corriente eléctrica. Caídas de linea.

	Fallas de dispositivos.
- SOFTWARE	Errores de diseño y lógica. Pruebas deficientes Cambios no autorizados.
- ABUSOS	Espionaje Fraude Sabotaje Robo Material Recursos Información.
- CATASTROFES	Terremotos Incendios Inundaciones Motines o disturbios Interno Externo Explosiones.[3]

SEGURIDAD FISICA

La seguridad física no es otra cosa que el tener controles contra aquellas contingencias que puedan dañar el equipo de cómputo y por ende se provoque la discontinuidad del servicio, se altere la información o se dañe permanentemente.

Debemos considerar a los elementos de un centro de cómputo vitales para la empresa y cuya pérdida o daño puede ser de consecuencias imprevisibles para la organización. Es necesario que los aspectos de seguridad se extiendan a todo el centro de cómputo y áreas contiguas, ya que de nada serviría proteger solo las computadoras y la información, si el medio ambiente aledaño no es seguro.

[3] LAMBARRI, Alejandro, Apuntes de Auditoría en Informática.

Es comprensible que generalmente no se cubra al cien porciento los aspectos de seguridad física, pero cada empresa tiene la obligación de cubrirlos lo más pronto posible, con el fin de eliminar riesgos.

La seguridad física abarca los siguientes aspectos:

- CONSTRUCCION DEL CENTRO DE COMPUTO
- UBICACION
- SUMINISTRO DE ENERGIA
- RIESGOS NATURALES (catastrofes)
- MEDIO AMBIENTE
- ACCESO AL CENTRO DE COMPUTO
- PROTECCION CONTRA SABOTAJES
- OPERACION
- MANTENIMIENTO
- SEGUROS

CONSTRUCCION DEL CENTRO DE COMPUTO.

El centro de cómputo debe ser construido de acuerdo con especificaciones especiales del tipo de equipo a ser instalado, personal a laborar directamente asesorado por gente capacitada y con experiencia en la instalación de dicho equipo.

UBICACION.

Se sugiere que el centro de cómputo sea lo más inaccesible posible, fuera de áreas de gran actividad, alejado de zonas con alto índice de vandalismo y lejos de zonas con alto índice de fenómenos naturales.

SUMINISTRO DE ENERGIA.

Se debe tener una fuente de energía confiable y ademas contar con equipos de emergencia que entren en operación inmediatamente ante la falla de suministro normal de energía.

RIESGOS NATURALES.

El centro de cómputo debe estar instalado en una zona donde no se corra el peligro de que sufra inundaciones, sismos, tormentas eléctricas, tornados, etc..., que puedan ocasionar problemas en la operación del mismo.

MEDIO AMBIENTE.

El medio ambiente debe ser controlado lo humanamente posible tanto en el interior del centro de cómputo como en el exterior, para prevenir cualquier posible daño en el equipo con condiciones inapropiadas de operación.

ACCESO AL CENTRO DE COMPUTO.

Es necesario limitar el acceso a una única entrada en donde se tenga un control de personal autorizado y se evite el entrar con objetos que puedan dañar directa o indirectamente el equipo físico.

PROTECCION CONTRA SABOTAJES.

Esta protección se basa principalmente en el control de acceso, más es necesario que dentro del centro de cómputo las áreas vitales no estén al alcance de cualquier sabotaje voluntario o involuntario.

OPERACION.

La operación del centro de cómputo será llevada a cabo por personal altamente calificado para que minimicen los riesgos de dañar el equipo por falta de conocimientos o inexperiencia.

MANTENIMIENTO.

El mantenimiento se refiere al servicio técnico que se le da al equipo del centro de cómputo en períodos regulares de tiempo, con el fin de prevenir fallas en su funcionamiento que evitarían daños e interrupciones en el proceso de información.

SEGUROS.

Se debe contar con seguros que cubran el costo del equipo al momento en que ocurra un siniestro, así mismo los seguros que contrate la empresa deben de ser lo suficientemente amplios para cubrir daños ocasionados por fenómenos naturales ó negligencia del hombre.

Una de las formas más difundidas en el ambiente informático y a la vez más eficaz para prevenir cualquiera de los riesgos anteriores y cumplir con los aspectos de seguridad antes citados es el plan de contingencias.

PLAN DE CONTINGENCIAS.

El plan de contingencias, también conocido como planes de recuperación, es el proceso en donde se ven definidos, desarrollados y documentados planes de emergencia con el propósito de enfrentar cualquier tipo de desastre, que de una manera significativa altere el procesamiento de información.

En estos días, sólo algunas aplicaciones automatizadas pueden verse operadas por procesos manuales, con un alto costo y una gran pérdida de tiempo.

OBJETIVOS DEL PLAN DE CONTINGENCIAS.

- Minimizar los efectos financieros y operativos ante el problema.
- Evitar la interrupción de las funciones críticas del negocio.
- Definir posibles alternativas de solución.
- Proporcionar medidas de recuperación de daños.
- Orientar al reestablecimiento normal de operaciones.

IMPORTANCIA DE LA AUDITORIA INFORMATICA APLICADA A LA SEGURIDAD FISICA.

Es vital para cualquier empresa que todo tipo de contingencia sea resuelta sin o con el mínimo de efectos en la operación de los procesos del negocio, por ello, el aplicar métodos de auditoría no es sólo la verificación de los procedimientos de trabajo de acuerdo a las disposiciones legales y las políticas de la empresa, si no una forma eficaz de evaluar el estado en el que se encuentra la organización para hacer frente ante cualquier tipo de riesgo que amenace la estabilidad de los procesos de la empresa y por ende se vea afectado el nivel de calidad del servicio o producto, corriendo el riesgo de verse perjudicado el aspecto negocio y hasta poder ser desplazados por la competencia.

CAPITULO 2.

SISTEMAS EXPERTOS

ARQUITECTURA

AUDIN

ARQUITECTURA DE SISTEMAS EXPERTOS

Una vez explicada la teoría de los Sistemas Expertos así como sus características más importantes, nos queda por definir como está formado un Sistema Experto. Conocer la estructura general de un sistema de este tipo permite clarificar la comprensión de su funcionamiento.

Los Sistemas Expertos emplean una variedad de arquitecturas específicas en sus sistemas, principalmente porque una arquitectura es más utilizada que otra cuando se considera una aplicación dada. Actualmente se lleva a cabo una vasta investigación para estudiar diferentes aspectos de las arquitecturas de Sistemas Expertos y subsiste todavía un gran debate al respecto.

Anteriormente se pensaba que un Sistema Experto estaba formado únicamente por dos elementos, una base de conocimientos y un motor de inferencia, pero hoy en día ese enfoque ha ido evolucionando de tal manera que los elementos que conforman un Sistema Experto se han modificado a lo largo de su historia, agregándose otros tales como las facilidades de interfase con el usuario, o como el actualizador de conocimientos.

A pesar de que existen diferencias significativas en los diferentes enfoques, la mayoría de las arquitecturas tienen muchos componentes en común. La figura 2.1 muestra una arquitectura general con los componentes típicos, y que son descritos a continuación.

USUARIO

El usuario de un sistema experto puede seguir los siguientes modos de operación:

- Verificador. Intenta comprobar la validez y el desempeño del sistema.

- Tutor. Da información adicional al sistema o modifica el conocimiento que ya está presente en el sistema.

- Alumno. Busca rápidamente desarrollar pericia personal relacionada con el área específica mediante la recuperación de conocimientos organizados y condensados del sistema.

- Usuario. Aplica la pericia del sistema a tareas específicas reales.

El reconocimiento de las modalidades anteriores contrasta con la percepción del simple papel del usuario de los sistemas tradicionales de software.

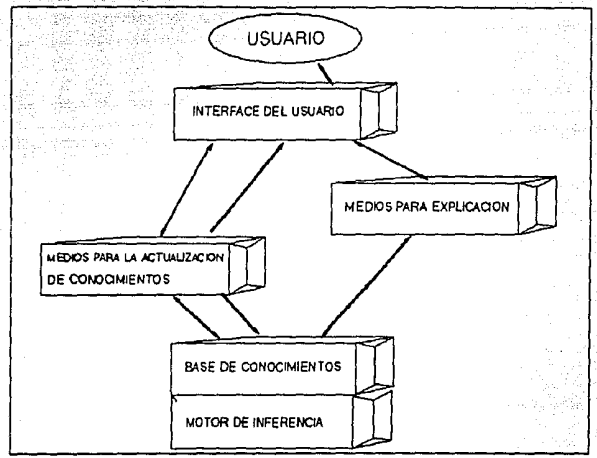


FIGURA 2.1

FACILIDADES DE INTERFASE CON EL USUARIO

Estas deben ser capaces de aceptar información por parte del usuario y traducirla a una forma compatible para el resto del sistema; o bien, recibir información del sistema y convertirla a una que el usuario pueda manipular.

Idealmente, esta facilidad se compone de un sistema procesador de lenguaje natural que acepta y devuelve esencialmente información en la misma forma como es aceptada u ofrecida por una persona experta. Aunque en la actualidad no existen sistemas que reproduzcan las capacidades del lenguaje humano, sí existen muchos otros que han producido impresionantes resultados mediante la utilización de subconjuntos restringidos del lenguaje.

Las facilidades de interfaz del usuario a menudo se diseñan para reconocer el modo en que el usuario está operando, su nivel de pericia, y la naturaleza de la transacción. Aunque el diálogo en lenguaje natural no es aún realizable, la comunicación con un Sistema Experto debe ser tan natural como sea posible, toda vez que el sistema trata de sustituir el desempeño del personal altamente calificado en la materia.

SISTEMA DE ALMACENAMIENTO Y GENERACION DE CONOCIMIENTO

Este actualmente abarca los elementos que constituían a un sistema experto en sus orígenes, pues consta de una base de conocimientos y un motor de inferencia. La función de este sistema consiste en almacenar confiablemente los conocimientos del experto, para recuperarlos e inferir nuevos conocimientos cuando se les requiera.

En el sistema de almacenamiento y generación de conocimiento, se almacena la información referente al tema tratado por el sistema. La información en dicho sistema está estructurada en tres niveles, que denotaremos como niveles de conocimiento, que es lo que la diferencía de una base de datos de un sistema tradicional de información. Estos tres niveles son conocidos como: Hechos Básicos, Reglas de Conocimiento y Reglas de Control.

NIVELES DE CONOCIMIENTO

Hechos Básicos de Información

Es el nivel más bajo dentro de la jerarquía de conocimientos, representan simplemente hechos básicos, es decir, los elementos lingüísticos más simples que poseen sentido por ellos mismos. Son la base de la información. Ejemplos de hechos básicos son:

- Juan esta en su casa
- Luis usa lentes
- Carlos es el presidente

Reglas de conocimiento

Son bloques lingüísticos que representan un determinado tipo de información en función de la forma en que se construyan. Están formados por hechos básicos, aunque puede ocurrir (de hecho ocurre en algunos sistemas expertos) que las reglas de conocimiento pueden por ellas mismas representar la unidad mínima de conocimiento con la que trabaje un determinado sistema experto. Una regla de conocimiento puede representar

lo que hay que hacer en caso de incendio; y solo representará eso. En caso de que ocurriera una inundación no podríamos aplicar esta regla.

Para crearla habrá que utilizar como mínimo dos hechos básicos: el primero representará que hacer realmente en caso de incendio; el segundo servirá para tener claro que la regla creada sólo se debe utilizar cuando hay un incendio y no cuando hay un terremoto.

Así formaríamos la siguiente regla de conocimiento:

SI hay un incendio ENTONCES corramos rápido

o la siguiente:

SI hay un incendio ENTONCES intentar apagarlo Y pedir ayuda

donde la propia regla esta formada por más de dos hechos.

Vemos como mediante la información de las reglas de conocimiento se constituye el conocimiento del sistema sobre un tema escogido, en este caso como actuar en un incendio.

Las palabras: "SI", "Y" y "ENTONCES" se llaman conectores y como vimos su función es unir diferentes hechos para crear una estructura (la regla de conocimiento) que posea sentido en su conjunto.

Se puede ver que la estructura básica de las reglas de conocimiento es:

SI [hechos-1] ENTONCES [hechos-2]

donde [hechos-1] es el primer conjunto de hechos, que recibe el nombre de antecedente, y [hechos-2] es el segundo, que se le llama consecuente.

Reglas de Control

Representan el último nivel de información en la estructura del sistema de almacenamiento y generación de conocimiento. Una vez constituídas las reglas de conocimiento sobre un tema, se almacenan todas ellas en la memoria del sistema. Sin

embargo, ante una pregunta habrá que responder con solo unas cuantas de las reglas que se poseen, no con todas.

El sistema necesita, por lo tanto, un instrumento capaz de elegir en cada caso la regla que corresponda. La elección de las reglas adecuadas para cada caso se realiza en el sistema por medio de otras reglas, llamadas reglas de control.

Las reglas de control, como su nombre lo indica, controlan la elección de las reglas de conocimiento. Por ejemplo una regla de control podría ser: "Cuando ocurra un hecho A entonces aplicar todas las reglas en que aparezca como antecedente el propio hecho A".

Así, en el caso de que ocurriera un incendio se aplicarían todas las reglas donde apareciese:

SI hay un incendio....

La estructura del sistema de almacenamiento y generación de conocimientos descrito anteriormente, se ilustra en la figura 2.2.

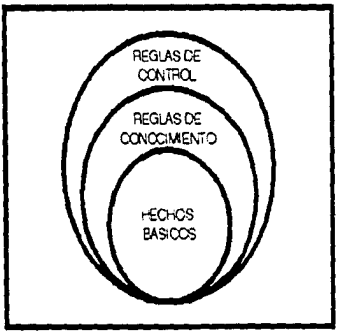


FIGURA 2.2

Una vez definidos los niveles de conocimiento, el siguiente paso es asignarles un lugar en la estructura del sistema experto.

Aquí existen diferencias de opinión entre los estudiosos del tema, ya que, para algunos dicha asignación es:

- Hechos básicos forman la base de datos asociada al sistema.

- Reglas de conocimiento forman la base de conocimiento.

- Reglas de control forman el motor de inferencia.

Es decir, crean una base de conocimientos formada por reglas y además, el sistema posee una base de datos asociada.

Para otro grupo de científicos la asignación se realiza de la siguiente manera:

- Hechos básicos y reglas de conocimiento forman la base de conocimientos.

- Reglas de control forman el motor de inferencia.

En esta asignación la base de conocimientos esta formada por los hechos básicos y las reglas de conocimientos. Estos dos enfoques se pueden representar mediante una canalización de tuberías, mostrada en el ejemplo de la figura 2.3.

BASE DE CONOCIMIENTOS.

La base de conocimientos representa un depósito de los conocimientos (por ejemplo, hechos fundamentales, reglas de conocimiento y heurísticas) disponibles para el sistema. En general, el conocimiento se almacena en forma de hechos y de reglas, pero los esquemas específicos empleados para almacenar la información varían grandemente. El diseño de este esquema de representación de conocimientos afecta el diseño del motor de inferencia, el proceso de actualización, el proceso de explicación y la eficiencia global del sistema.

Bajo la denominación de Ingeniería del Conocimiento se agrupan todas las áreas que intervienen en el desarrollo de los sistemas expertos. Dentro de estas áreas aparecen los siguientes campos: Adquisición del Conocimiento, Representación del Conocimiento y Métodos de Inferencia, que se explicarán más adelante.

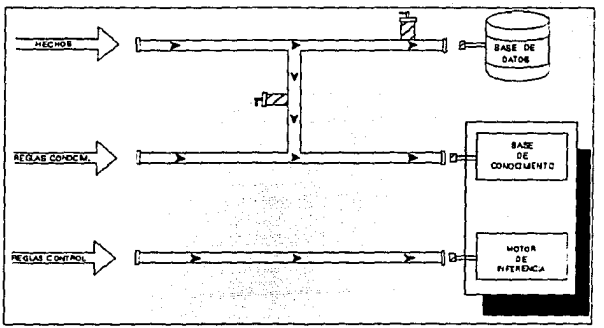


FIGURA 2.3

La Ingeniería de conocimientos, incluye por lo tanto, el proceso de adquirir el conocimiento del área específica y estructurarlo en la base de conocimientos, así como decidir cuales serán los métodos de inferencia a utilizar.

Adquisición del conocimiento.

Obtener el conocimiento necesario para la creación de un sistema experto no es una tarea sencilla. En algunos temas el sistema puede aprender a través de la experiencia, pero normalmente el experto y el llamado ingeniero del conocimiento, deben trabajar unidos para lograr condensar el saber en unas ciertas reglas lógicas. Actualmente se está trabajando sobre ciertos programas que reciben la sabiduría del experto mediante sesiones de enseñanza. El programa va preguntando, analizando las respuestas e incorporándolas a la base en forma de reglas lógicas. Aunque generalmente este trabajo es llevado a cabo por el ingeniero de conocimientos.

Un ingeniero de conocimientos es la persona que obtiene la información del área del experto y los transporta a la base de conocimientos. Debido a que un sistema experto requiere que dicha información se guarde en la base de conocimientos de acuerdo con las normas de representación, el ingeniero de conocimientos debe transformar la representación como parte del proceso de transportación de conocimientos.

La figura 2.4 muestra el proceso tal como se da típicamente.

Aunque los conocimientos pueden conseguirse de una variedad de fuentes, incluyendo la documentación y los sistemas de información existentes, la mayor parte de él, se debe de obtener de personas expertas. El conocimiento suministrado por el experto, en general estará en forma tal que sea orientado hacia el tema del área.

Para adquirir el conocimiento necesario, el ingeniero de conocimientos primero debe establecer una comprensión global del área, formar un diccionario mental de los términos y jerga esenciales del área y desarrollar una comprensión, básica de los conceptos claves.

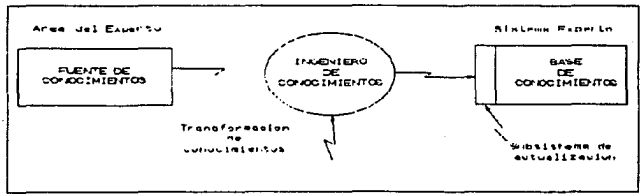


FIGURA 2.4

Luego debe condensar el conocimiento obtenido a partir de la información suministrada por el experto.

La función de adquisición de conocimientos es comúnmente, el aspecto de mayor dificultad en la construcción de un Sistema Experto. Esto se debe principalmente al hecho de que el proceso requiere comunicaciones humanas amplias, entre el experto en el área y el ingeniero de conocimientos y en consecuencia enfrenta los problemas asociados con esta actividad. Por tanto, el proceso de adquisición del conocimiento no está bien entendido ni bien definido. Si el proceso mismo de desarrollo de un sistema experto se visualizará como un área para expertos, el conocimiento asociado con el procedimiento de adquisición será considerado como heurístico.

Representación del Conocimiento

Uno de los puntos débiles de toda la teoría de sistemas expertos estriba en la forma de representar el conocimiento. Hay que buscar una forma capaz de representarlo suficientemente bien como para que resulte efectiva y aprovechable.

Se están desarrollando en la actualidad una gran variedad de métodos, todos ellos para facilitar el razonamiento simbólico y permitir la codificación y aplicación del sentido común. Sin embargo todos los métodos actuales de representación del conocimiento son aproximados y no encajan exactamente con lo que el hombre desea realmente transmitir.

Los modelos de representación de uso corriente hoy en día son principalmente, el resultado de grandes investigaciones y de análisis empíricos antes que resultados de consideraciones filosóficas de alguna teoría, que incluya todo lo relacionado con la representación. No existe ninguna técnica de representación que universalmente se acepte como la "mejor", y además un esquema será más aplicable que otro cuando se evalúe en términos relativos a un área específica.

Sin embargo, aún con la ausencia de una teoría lo suficientemente amplia, podemos evaluar cualquier esquema de representación, con algunos criterios generales. La evaluación entonces puede utilizarse para comparar y contrastar diferentes esquemas según su utilidad relativa a una aplicación específica. Algunos criterios generales importantes son los siguientes:

- Transparencia. Hasta qué punto podemos identificar fácilmente el conocimiento almacenado.

- Claridad. Hasta qué punto el conocimiento se puede representar directamente.

- Naturalidad. Hasta qué punto el conocimiento se puede representar en su forma original.

- Eficiencia. La facilidad relativa con la cual se puede acceder a conocimientos específicos durante la ejecución.

- Adecuación. Hasta qué punto una estructura dada se puede emplear para representar todos los conocimientos que requiere el sistema.

- Modularidad. Hasta que punto los fragmentos de conocimiento se pueden almacenar independientemente uno del otro.

Los esquemas más habituales de representación son: las redes semánticas, los marcos, los guiones y los sistemas de producción.

REDES SEMANTICAS.-

Una red semántica hace énfasis en la representación gráfica de las relaciones entre los elementos de un dominio. Los componentes básicos de una red semántica son los nodos y los enlaces. Los nodos se emplean para representar elementos del dominio, los cuales se muestran gráficamente como rectángulos y son rotulados con los nombres de los elementos representados. Los enlaces (o arcos) representan relaciones entre los elementos, éstos se muestran como un vector desde un nodo a otro; se rotulan con el nombre de las relaciones representadas. La red sencilla que se muestra a continuación, representa el enunciado " Caballo come Pasto".

CABALLO ------- come ------- PASTO

Un enlace se puede ver como algo que aseveramos sea cierto de un elemento con relación a otro. Debido a que la aseveración puede ser solamente veraz o falsa, un enlace es una relación binaria.

Dos de las relaciones binarias más comunmente empleadas en redes semánticas son *es un* (ISA) y *parte de* (PARTOF), el enlace ES-UN se emplea para representar el hecho de que un elemento es miembro de una clase de elementos que tienen un conjunto de propiedades distinguibles, en común. Un nodo que representa una ilustración de una clase es una *instancia* (ejemplo) de la clase. Por ejemplo la siguiente red representa el hecho de que un pájaro es un ave.

PAJARO ------- es-un ------- AVE

La siguiente red representa el hecho de que un pico es parte de un pájaro.

PICO ------- parte-de ------- PAJARO

Los dos fragmentos de redes se pueden combinar para formar una red:

PICO ----- parte-de ----- PAJARO ----- es-un ----- AVE

Cualquier característica calificativa, tal como color, tamaño y textura, se puede representar como una propiedad asociada con un nodo, y la herencia de propiedades nos dice que cualquier propiedad que atinemos a declarar como verdadera para una clase de elementos, debería ser cierta para cualquier ejemplo de la clase; las propiedades, por tanto, salen descendiendo a niveles más bajos conectados através de enlaces de herencia de propiedades. Este concepto hace las redes semánticas de particular interés para representar dominios que se pueden estructurar como taxonomías.

MARCOS.-

Un marco, introducido por primera vez, por Minsky en 1975, es una estructura para organizar el conocimiento poniendo énfasis en el conocimiento por omisión. Por ejemplo, con base en nuestras experiencias anteriores, esperamos que los automóviles tengan ruedas y un motor, que requieran de gasolina y corran. Estos elementos son las características definitorias que, cuando las tomamos como un todo, constituye nuestro entendimiento de un "automóvil", son nuestras expectativas con referencia a un automóvil; las cosas que a menos de que exista evidencia de lo contrario, esperamos que sean ciertas en todos los automóviles. Son todas esas expectativas nuestros valores por omisión para un automóvil.

Los marcos comparten varios conceptos en común con las redes semánticas. Cada marco representa una clase de elementos de la misma manera que un nodo de clase se emplea para representar tales elementos en una red semántica.

Un marco consiste de una serie de ranuras (slots) de las cuales cada una representa una propiedad estándar o atributo del elemento representado por un marco. Una ranura nos da un lugar para colocar sistemáticamente un componente de nuestras experiencias anteriores con relación a las clases de elementos representados.

Cada ranura se identifica, por el nombre del correspondiente atributo e incluye el valor, o rango de valores, que se pueden asociar con la ranura. Un valor por omisión puede indicarse también en la ranura. La figura 2.5 muestra un marco que ofrece una descripción parcial de la clase de objetos llamados "AUTOMOVILES".

Para dominios complejos, las ranuras se pueden dividir en subranuras cada vez más detalladas. Las ranuras se pueden llenar con marcos de bajo nivel. Un sistema de marcos se compone de marcos interrelacionados que se necesitan para representar un dominio.

FIGURA 2.5

El sistema de marcos se apoya ampliamente en el concepto de herencia en el mismo sentido que las redes semánticas. Cualquier clase de objetos se pueden incluir en muchos y variados marcos que representan objetos a diferentes niveles de especificación. Por ejemplo, la clase de automóviles se puede incluir en marcos denominados OBJETO FISICO, VEHICULO, Y AUTOMOVIL.

Un marco que representa una clase de objetos a cierto nivel dado de especificación, puede incluir ranuras y valores en ranuras que se heredan de marcos que representan mayor nivel de abstracción. El marco automóvil por ejemplo, hereda los atributos de "movilidad" y "mecanismo de movilidad" a partir del hecho de que constituye una especialización del marco VEHICULO. El uso de la opción de valor por omisión y de los valores de las ranuras heredadas posibilita el razonamiento eficiente debido a que tal utilización evita la necesidad de procesos costosos de razonamiento para descubrir hechos anteriores en situaciones nuevas.

GUIONES.-

Al igual que las expectativas con relación a objetos, tenemos ciertas expectativas acerca de las secuencias de eventos que probablemente ocurran en cualquier situación dada.

Estas expectativas se basan en nuestras observaciones de patrones recurrentes en los eventos de situaciones similares que hemos observado en el pasado.

Un Guión es una especialización del concepto general de un marco, es una estructura que se usa para guardar prototipos de secuencias de sucesos.

Muchos componentes diferentes se pueden emplear para construir un Guión. Algunos de los más comunes son:

- Condiciones de Entrada. Las condiciones que deben existir para que el Guión se pueda aplicar.
- Utilería. Ranuras que representan objetos que están involucrados en el Guión.
- Resultados del Guión. Condiciones que serán verdaderas después de que hayan ocurrido los eventos en el Guión.
- Papeles. Ranuras que representan gente o agentes que realizan acciones en el Guión.
- Escenas. Secuencias específicas de eventos que hacen el Guión.

La figura 2.6 muestra un Guión que representa el proceso de conducir hasta el centro comercial.

No existen reglas absolutas para definir el contenido genérico de un Guión para identificar las entradas especificas. Podemos, por ejemplo, decidir incluir entradas con relación a factores de tiempo, lugares de ocurrencia o puntos de vista.

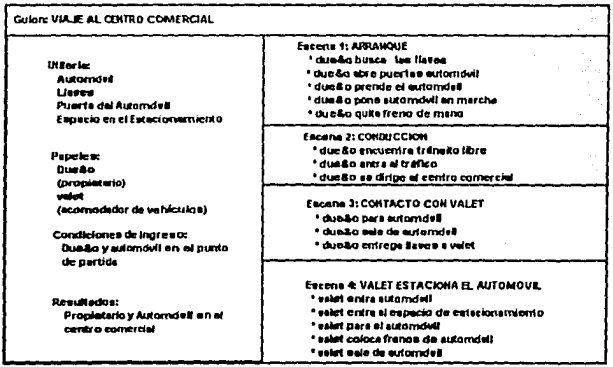


FIGURA 2.6

SISTEMAS DE PRODUCCION.-

Un sistema de producción, que es el esquema más comúnmente empleado en sistemas expertos, utiliza reglas para la representación del conocimiento. Un sistema de producción consta de:

- Una porción de memoria que se utiliza para rastrear el estado actual del universo en consideración.
- Un conjunto de reglas de producción (parejas condición-acción)
- Un interpretador que examine el estado actual y ejecute las reglas de producción aplicables.

Elementos de memoria global.

El área de memoria global que se emplea para rastrear el estado del sistema actual se compone de una serie de elementos individuales de memoria. Conceptualmente cada elemento de memoria describe el estado actual de un artículo de interés. Un elemento de memoria consiste de un símbolo que identifica el elemento descrito seguido de una serie de parejas atributo-valor, cada una de las cuales describe el valor actual del atributo asociado con el elemento (estado).

Como ejemplo la figura 2.7 muestra un elemento de memoria que describe un automóvil que pertenece a una persona llamada Juan.

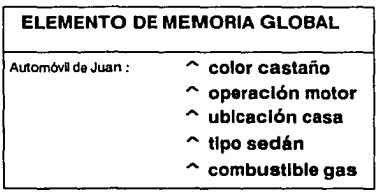


FIGURA 2.7

Reglas de producción.

La parte condicional de una regla a veces se llama LI, (o LHS en inglés) lado izquierdo, consiste de una serie de "elementos condición" que describen las condiciones que deben ser verdaderas para que la regla sea aplicable. Estas condiciones se describen mediante la identificación de los patrones requeridos de memoria global: *identificadores de elementos de memoria* junto con los *atributos y valores requeridos* asociados.

La parte de la acción de una regla, algunas veces conocida como LD (o RHS en ingles), el lado derecho, describe las acciones que se van a llevar a cabo cuando se dispara la regla. Las acciones posibles generalmente incluyen actividades tales como la entrada de descripciones de nuevos estados en la memoria global, modificar descripciones del estado existentes y realizar una actividad definida por el usuario que es única a la producción específica.

Interpretador.

El interpretador en un sistema de producción, en su forma más esencial, simplemente reconoce y ejecuta una producción cuyo LI se ha satisfecho. Para reconocer las reglas aplicables, el interpretador compara los patrones de atributo-valor con el estado actual de la memoria global. El proceso de razonamiento continúa debido a que la ejecución de una producción cambia normalmente el contenido de la memoria global y con eso activa las producciones adicionales.

MOTOR DE INFERENCIA.

Los Sistemas Expertos deben por su naturaleza tratar flexiblemente con situaciones cambiantes. La capacidad para responder ante situaciones cambiantes depende de la habilidad para inferir nuevos conocimientos a partir de conocimientos existentes. A manera de ejemplo sencillo, consideremos los dos hechos básicos siguientes:

1. Todos los animales respiran oxígeno.
2. Todos los perros son animales.

Se puede inferir un nuevo hecho, "todos los perros respiran oxígeno" a partir de los dos hechos anteriores. Para responder a una situación dada, un Sistema Experto debe aplicar el conocimiento apropiado.

El motor de inferencia es el sistema de software que ubica los conocimientos e infiere nuevos usando la base de conocimientos, su principal misión es seleccionar las reglas de conocimiento aplicables para resolver cada problema propuesto por el usuario.

El paradigma del motor de inferencia es la estrategia de búsqueda que se emplea para producir el conocimiento demandado. Varios paradigmas diferentes se emplean en un Sistema Experto, pero la mayoría de ellos se basan en dos conceptos fundamentales: encadenamiento hacia atrás (ó retroencadenamiento) que es un proceso de razonamiento descendente, que se inicia a partir de los objetivos deseados y trabaja hacia atrás en dirección de las condiciones pre-requisito; ó el encadenamiento hacia adelante (ó encadenamiento frontal) que es un procesamiento de razonamiento ascendente que se inicia con condiciones conocidas y trabaja hacia adelante para alcanzar los objetivos deseados.

MEDIOS PARA LA ACTUALIZACION DE CONOCIMIENTOS

Presumiblemente, la base de conocimientos es una reflexión cuidadosa del área en el momento en que el sistema se pone en servicio. Desafortunadamente en muchas áreas complejas el conocimiento crece y cambia constantemente por lo cual la base de conocimientos se debe modificar en el mismo sentido. Para llevar a cabo tales actualizaciones se emplea la facilidad para actualización de conocimientos. Este proceso puede tomar una de tres formas fundamentales, según se describe a continuación:

La primera forma es la "actualización manual de conocimientos". En este caso se lleva acabo por un ingeniero de conocimientos quien interpreta la información ofrecida por un experto en el área y actualiza la base de conocimientos mediante el uso de un sistema limitado de actualización.

La segunda forma, que representa el arte de los Sistemas Expertos, en donde el experto en el área ingresa directamente el conocimiento revisado sin la mediación de un ingeniero de conocimientos. En este caso el sistema de actualización debe ser mucho más elaborado.

En la tercera forma, "aprendizaje mecánico", el sistema genera nuevos conocimientos en forma automática y se basa en generalizaciones deducidas de experiencias anteriores. El sistema, en efecto, aprende nominalmente de la experiencia e idealmente el mismo sistema se actualiza. Este proceso que aún está en estado conceptual, es tema de mucha investigación. La habilidad para aprender es un componente importante de la inteligencia y al ofrecer completamente esta potencialidad mejoraría las capacidades de un Sistema Experto.

SISTEMA DE EXPLICACIONES

Además de lograr simplemente una conclusión cuando enfrenta un problema complicado, un experto es también capaz de explicar, hasta cierto punto, el razonamiento que conduce a dicha conclusión. Un Sistema Experto debe diseñarse para brindar una facultad semejante. Esta es una potencialidad que generalmente esta ausente en los sistemas tradicionales de computación.

Típicamente la explicación consiste en una identificación de los pasos en el proceso de razonamiento y de una justificación de cada uno de ellos. El proporcionar esta potencialidad para comunicar esta información, constituye esencialmente un subconjunto del problema del procesamiento de lenguaje natural. El sistema debe acceder a un registro de los conocimientos que se emplearon en el procesamiento, basándose en el esquema

de representación de la base de conocimientos y traducirlo a una forma que sea aceptable por el usuario.

Para proporcionar los niveles exactos de explicación, el sistema debe identificar el nivel de conocimientos del usuario y entender como adaptar la explicación para acoplarla apropiadamente. Las facilidades de explicación en varios sistemas actuales se limita a listar simplemente las reglas que se utilizaron durante la ejecución.

ANALISIS

Y

DESARROLLO

AUDIN

ANALISIS Y DESARROLLO DE SISTEMAS EXPERTOS

El desarrollo de un sistema experto no se puede considerar como un pensamiento aislado, ya que se encuentra íntimamente relacionado con el ciclo tradicional de vida de un sistema, de hecho surge como la necesidad de dar más flexibilidad a dicho ciclo.

El porqué de esto lo encontraremos si analizamos que en el "ciclo de vida tradicional de un sistema", no se puede comenzar una fase sin haber concluido totalmente la anterior.

A grandes rasgos podemos ilustrar este ciclo como sigue:

DEFINICION DE UN PROBLEMA

ANALISIS DE REQUERIMIENTOS

DISEÑO DEL SISTEMA PROPUESTO

PRUEBAS

IMPLEMENTACION

MANTENIMIENTO

Es necesario aclarar que en este capítulo se denominará "problema" a todos aquellos requerimientos ó necesidades que den origen al desarrollo de un sistema, ya sea de la forma tradicional ó através de un sistema experto y que pueden ser realmente problemas para la organización ó una idea que sin considerarse problema, le puede otorgar mayores beneficios.

Ahora bien, si tomamos en consideración que el usuario en la mayoría de las ocasiones detecta un problema que da inicio al desarrollo de un sistema, y a lo largo de dicho desarrollo, incluyendo en la fase de prueba, se da cuenta que otros de sus problemas se pueden solucionar con "ALGUNAS" modificaciones sobre el mismo sistema; por lo tanto, tenemos que retroceder hasta las primeras fases con el fin de hacer un buen desarrollo (incluyendo los nuevos requerimientos) y no es posible pasar a la siguiente etapa antes de concluir la anterior, ya que de lo contrario se puede estar dando mantenimiento a un sistema que todavía no se ha concluido.

CICLO DE VIDA DEL DESARROLLO DE UN SISTEMA EXPERTO (S.E.)

Cabe señalar en este punto que generalmente la aplicación de sistemas expertos esta relacionada con áreas en donde los problemas no son definidos correctamente desde el inicio. Se podría decir que el ciclo de vida de los sistemas expertos está basado en el ciclo tradicional, pero de un modo iterativo, contando con algunas características propias, tales como:

- El usuario está involucrado de principio a fin en el proceso. Esto es, desde la definición del problema, hasta que el sistema experto se concluye.

- Los resultados se van entregando poco a poco, conforme se van concluyendo, con el fin de que el usuario los revise y solicite los cambios que crea pertinentes.

- En contraposición con el ciclo tradicional, en el desarrollo de un sistema experto los cambios son benéficos y no se tienen que retroceder fases para implementarlo.

Con estas observaciones podemos entonces esquematizar el ciclo de vida de un sistema experto como se muestra en la figura 2.8.

Ahora estudiaremos un poco más a fondo cada una de las fases.

SELECCION DEL PROBLEMA.

Esta es una de las fases más críticas en el desarrollo de un sistema experto y por lo tanto una de las más importantes.

La selección del problema ó problemas que se pueden resolver através de sistemas expertos es divisible en los pasos descritos en la figura 2.9.

INVESTIGACION DEL PROBLEMA.

Dentro de esta tarea es necesaria una sesión de tormenta de ideas para generar una lista de problemas a considerar para ser resueltos por un sistema experto.

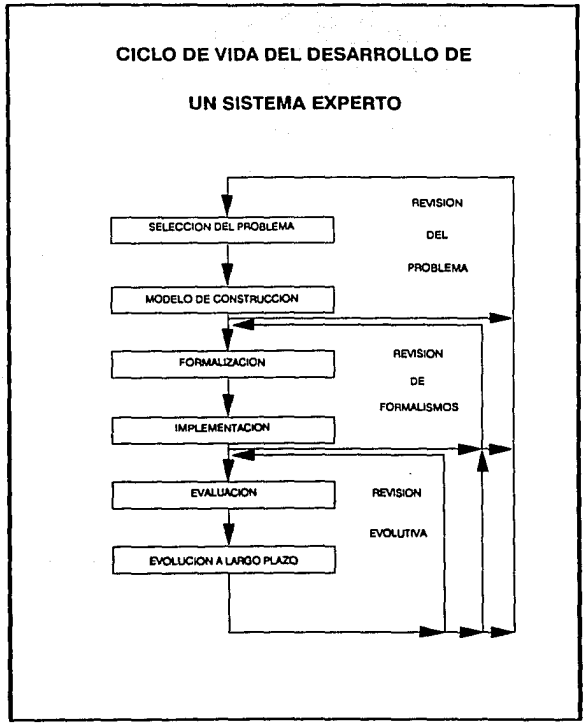

CICLO DE VIDA DEL DESARROLLO DE
UN SISTEMA EXPERTO
SELECCION DEL PROBLEMA
MODELO DE CONSTRUCCION
FORMALIZACION
IMPLEMENTACION
EVALUACION
EVOLUCION A LARGO PLAZO
REVISION
DEL
PROBLEMA
REVISION
DE
FORMALISMOS
REVISION
EVOLUTIVA

FIGURA 2.8

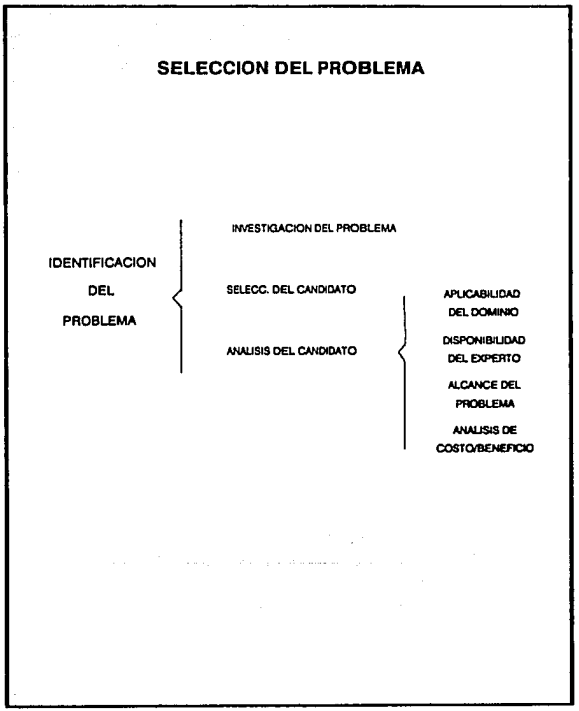

SELECCION DEL PROBLEMA
IDENTIFICACION
DEL
PROBLEMA
INVESTIGACION DEL PROBLEMA
SELECC. DEL CANDIDATO
ANALISIS DEL CANDIDATO
APLICABILIDAD
DEL DOMINIO
DISPONIBILIDAD
DEL EXPERTO
ALCANCE DEL
PROBLEMA
ANALISIS DE
COSTO/BENEFICIO

FIGURA 2.9

SELECCION DE CANDIDATOS.

Al decir "candidatos" nos referimos a los problemas con mayores posibilidades de tomarse en cuenta para el desarrollo de un sistemas expertos, por lo tanto, en esta fase se debe reducir la lista que nos arrojó la lluvia de ideas através de la aplicación de ciertos "criterios de filtración" como pueden ser los siguientes:[1]

- Requiere la tarea el empleo de conocimiento experto ?

- Es escasa la pericia (o es probable que se torne escasa pronto ?

- Están disponibles los expertos quienes saben cómo realizar la tarea ?

- Existen razones para creer que la solución algorítmica tradicional sería difícil de implementar ?

- Requiere la tarea una cantidad razonable de conocimientos de juicio o enfrenta algún grado de incertidumbre ?

- Requiere la tarea habilidades verbales primeramente (como opuestas a las físicas ?

- Es muy valiosa una solución del problema para la organización; esto es, el problema definitivamente vale la pena resolverlo ?

- Una solución que sea valiosa el día de hoy permanecerá útil durante los próximos años?

- Es aceptable para el sistema que ocasionalmente falle en encontrar una solución; esta bien que produzca una respuesta subóptima por lo menos en algunos casos ?

- Hay disponibilidad de una gran cantidad de tiempo para construir el sistema (por lo menos 6 meses) ?

ANALISIS DEL CANDIDATO.

Esta fase se divide en las siguientes actividades:

[1] ROLSTON, David W., Op. Cit., pp 140.

APLICABILIDAD DEL DOMINIO.

En este punto se hace un análisis más a detalle con respecto a la aplicación del sistemas expertos, por ejemplo, se estudia cuantos expertos se tienen para elaborar ese trabajo en comparación con todos los empleados (Pocos empleados hacen más trabajo), se revisa la necesidad de formalizar para preservar el conocimiento de dichas personas.

Un rasgo inequívoco de que el problema forma parte del dominio de los sistemas expertos es el hecho de que el trabajo es más bien mental que físico.

DISPONIBILIDAD DEL EXPERTO.

Esta actividad se refiere a que es indispensable contar con la disponibilidad de la persona que posea la mayor expertez para apoyar en todo momento el desarrollo del sistemas expertos, pues de lo contrario se corre el riesgo de que éste no sea del todo óptimo. Es comprensible el grado crítico de este punto en virtud de que son escasos los expertos en la materia, pero la organización debe tomar ésta responsabilidad si en verdad quiere obtener buenos resultados.

Ahora, es necesario que la persona que asigne la organización "done parte de sus conocimientos" para el nuevo sistema, además de contar con el reconocimiento de los usuarios ya que de ello depende la aceptación del futuro sistema por las personas que lo van a explotar.

Otro de los puntos en los que se debe hacer una aclaración en esta fase, se refiere al hecho de tratar de resolver, con el nuevo sistema, problemas que los actuales expertos no han sabido solucionar; esto es una grave idea que se tiene que poner en claro desde el principio del desarrollo.

ALCANCE DEL PROBLEMA.

Se debe trabajar con un problema bien delimitado (específico), tomando en cuenta el tamaño del sistema. Si el dominio del problema es muy extenso, es recomendable dividirlo en fases de desarrollo.

ANALISIS DE COSTO/BENEFICIO.

Antes de tomar cualquier decisión sobre la construcción de un sistema experto, la organización debe llevar a cabo un estudio de costo/beneficio con el objetivo de evaluar

y estimar los desembolsos necesarios contra los beneficios que se van a obtener con el sistema, a fin de tener un punto de comparación y de determinación para el desarrollo del Sistema Experto.

MODELO DE CONSTRUCCION.

Una vez que se ha seleccionado el problema, su dominio y alcance; se debe iniciar la construcción de un prototipo, el cual tendrá como objetivos principales obtener más datos acerca del dominio, así como demostrar a nivel general la forma en que va a funcionar el sistema, dando oportunidad al usuario de evaluarlo para determinar si se sigue sobre el planteamiento inicial, si hay cambios al diseño o definitivamente se suspende.

Dentro de esta etapa la persona encargada de desarrollar el sistema experto se comienza a involucrar con el experto de la organización para recabar información y aprender lo más posible acerca del área, con el fin de desarrollar un modelo de consulta general, y la forma en la que se va a generar la base del conocimiento; después de esto se selecciona la herramienta con la que se va a implementar el prototipo. Una vez que se ha desarrollado el prototipo se hacen pruebas con los problemas más frecuentes o aquellos con los que el usuario determina que se pueden probar diferentes situaciones a las que se enfrentará el experto, en éstas pruebas, tanto la persona de sistemas como el experto de la empresa llevan a cabo validaciones y evaluaciones para determinar si son necesarios algunos cambios, los cuales pueden ser sencillos o tan grandes que sea necesario realizar otro prototipo.

FORMALIZACION.

Una vez que un modelo de demostración ha sido totalmente satisfactorio, se pasa al desarrollo completo y formal del sistema, en esta fase se debe tener mucho cuidado de no adelantarse a llevar a cabo un formalismo prematuro.

Los objetivos fundamentales en esta etapa son:

- Asimilar el conocimiento adquirido durante el desarrollo prototipo.

- Llevar a cabo la planeación y estrategias para las siguientes fases.

- Explicar los puntos de verificación de una manera tan clara que permita a más gente (en particular al usuario) involucrarse cercanamente en el proyecto.

- Efectuar pruebas periódicas.

Dentro de la formalización se debe hacer un análisis detallado del problema. Una vez que ya se desarrolló el prototipo, estamos en condiciones de hacer una definición detallada, en la cual se describan más claramente los objetivos y restricciones que se tienen para delimitar el alcance del proyecto y lo que el usuario espera del sistema.

Después de concluida la descripción anterior, proseguimos con el diseño, en el que se realiza una investigación más profunda de los puntos que se tomaron como base para la elaboración del modelo. Posteriormente se observan las discrepancias entre las conclusiones obtenidas por el prototipo y el diseño; si fuese necesario en este punto se volvería a replantear el prototipo.

Una vez que concuerdan los resultados del modelo con el diseño se realiza la planeación del proyecto, en la cual se toman en cuenta los elementos necesarios para el desarrollo, tales como: presupuestos, hardware, software, tiempo requerido tanto del experto de la organización como para concluir lo planeado.

Ya determinada la planeación del proyecto se lleva a cabo la planeación de las pruebas. En esta etapa se evaluarán diferentes condiciones por las que puede atravesar el sistema, incluyendo aquí elementos que forcen al sistema a trabajar; para esto es necesario que se establezcan procedimientos de prueba a fin de mantener el control.

Posteriormente se realiza la planeación para la presentación del producto ante los usuarios más cercanos al manejo del mismo, para que, después de que el sistema se gane la confianza de los expertos humanos, se les haga la entrega del sistema para que lleven a cabo pruebas Post-instalación, haciendo una evaluación sobre el comportamiento del sistema experto ante situaciones reales; seguido de esto, se efectúa la planeación del soporte, en donde se especificarán cuales serán los conductos para desarrollar modificaciones, personal requerido, evaluación de las afectaciones al Sistema Experto, etc.

La última parte de la planeación se refiere al plan de implantación, en donde se describirán las actividades necesarias para la fase de la implementación, tales como: la forma en la que el sistema será alimentado de conocimientos, controles, partes en las que se dividirá el total del sistema, etc.

IMPLEMENTACION.

Para esta fase se puede aplicar la frase de "Divide y vencerás", ya que es recomendable (al igual que cualquier otro sistema) separar el TODO en pequeñas partes manejables y definitivamente más controlables.

Los principales puntos a desarrollar durante esta fase son:

Implementación:

- Revisión del prototipo
- Desarrollo de la infraestructura del sistema
- Adquisición de conocimientos esenciales
- Desarrollo de software
- Integración interna
- Verificación interna

Revisión Del Prototipo.

Evaluación de pruebas y funcionalidad del Sistema Experto.

Desarrollo De La Infraestructura Del Sistema.

Determinación del motor de inferencia, base del conocimiento, software, interfase con el usuario.

Adquisición De Conocimientos Escenciales.

Complementación de los casos de prueba através de la adquisición, integración, verificación (casos nuevos), actualización de casos de prueba y almacenamiento del conocimiento.

Desarrollo Del Software.

Implementación del software capaz de soportar el desarrollo del proyecto en especial la base de conocimientos.

Integración Interna.

Eliminar discrepancias entre módulos en los que se dividió el sistema.

Verificación Interna.

Revisión del sistema experto por parte del experto de la organización y de la persona de sistemas encargada de desarrollarlo.

EVALUACION.

En esta etapa se debe poner a prueba el sistema con casos o situaciones que al mismo tiempo sean analizados por el experto en la materia y que posteriormente serán estudiados por un conjunto de expertos reconocidos, a fin de evaluar la confiabilidad del nuevo sistema.

EVOLUCION A LARGO PLAZO.

Una vez que el sistema queda implantado, comienza la etapa en la cual se puede complementar la base de conocimientos, ampliar el dominio del sistema experto, y en general hacer correcciones necesarias para el óptimo funcionamiento del sistema.

CAPITULO 3.

DESARROLLO DEL

SISTEMA EXPERTO

SELECCION

DEL

PROBLEMA

AUDIN

SELECCION DEL PROBLEMA

Dentro de este capítulo seguiremos las fases de desarrollo de un sistema experto, para lo cual únicamente nos enfocaremos al sistema experto en auditoría en informática en seguridad física.

Tomando en consideración que las fases para el desarrollo de un sistema experto se explicaron en el capítulo anterior, y dentro de éste, se mencionó la forma en la cual se debe seleccionar un problema a desarrollar en el supuesto caso de que hubiese varios, a nosotros no nos corresponde llevar a cabo este punto, en virtud de que el problema ya esta seleccionado y fue la clave que dió origen a ésta tesis.

SELECCION DEL CANDIDATO.

Ahora identificaremos si realmente el tema seleccionado es factible de desarrollarse através de un sistema experto, aplicando los criterios de filtración mencionados en el punto de selección del candidato, para lo cual contestaremos el siguiente cuestionario: [1]

- Requiere la tarea el empleo de conocimiento experto ? SI
- Es escasa la pericia (o es probable que se torne escasa pronto ? SI
- Están disponibles los expertos quienes saben cómo realizar la tarea ? NO
- Existen razones para creer que la solución algorítmica tradicional sería difícil de implementar ? SI
- Requiere la tarea una cantidad razonable de conocimientos de juicio o enfrenta algún grado de incertidumbre ? SI
- Requiere la tarea habilidades verbales primeramente (como opuestas a las físicas ? SI
- Es muy valiosa una solución del problema para la organización; esto es, el problema definitivamente vale la pena resolverlo ? SI

[1] **Fuente de las Preguntas del Cuestionario.**
ROLSTON, David W. Principios de Inteligencia Atificial y Sistemas Expertos. McGraw-Hill Colombia 1990. pp. 140.

- Una solución que sea valiosa el día de hoy permanecerá útil durante los próximos años? **SI**

- Es aceptable para el sistema que ocasionalmente falle en encontrar una solución; esta bien que produzca una respuesta subóptima por lo menos en algunos casos ? **SI**

- Hay disponibilidad de una gran cantidad de tiempo para construir el sistema (por lo menos 6 meses) ? **SI**

Como podemos observar, en nuestro caso la mayoría de las respuestas fueron afirmativas, razón por la cual nuestro proyecto es factible de llevarse a cabo através de un sistema experto.

ANALISIS DEL CANDIDATO.

A.- APLICABILIDAD DEL DOMINIO.

Después de un análisis más profundo se concluyó lo siguiente:

Debido a que el área de auditoría en informática en seguridad física es relativamente nueva, actualmente se cuenta con pocos expertos que poseen la mayor parte del co -- nocimiento para llevar a cabo dicha función. Cabe hacer notar que algunos expertos muchas veces son personas con un poco más de experiencia que el nivel promedio de las personas de una misma área.

Por otro lado la difusión del conocimiento experto se ve limitado por falta de herramientas que marquen pautas concretas, encaminadas a la eliminación de tareas repetitivas, de conocimientos difusos y a la evaluación, así como el control del gran volumen de información con la que se cuenta dentro de la auditoría en informática en seguridad física en un centro de cómputo.

Tomando en cuenta los puntos anteriores, se observa que la tecnología de vanguardia en inteligencia artificial y sistemas expertos nos brinda la posibilidad de cubrir al máximo las expectativas del proyecto.

B.- DISPONIBILIDAD DEL EXPERTO.

Como se ha venido mencionando a lo largo del presente trabajo, para poder desarrollar adecuadamente un sistema experto es necesario contar con un experto (humano) en la materia, el cual sea capaz de "donar" sus conocimientos para el buen término del sistema.

Para llevar a cabo el presente proyecto contamos con el apoyo de una persona, cuya trayectoria dentro de la auditoría en informática lo ha llevado a ocupar un lugar importante en esta área, a lo largo de su ejercicio ha desempeñado labores de docencia y consultoria en diversas empresas.

C.- ALCANCE DEL PROBLEMA

Inicialmente se planteó la posibilidad de desarrollar un sistema experto que cubriera el campo de la Auditoría en Informática en general. Este alcance primario tuvo que ser reconsiderado debido a el gran volumen de información que se manejaba.

Considerando las diferentes áreas de aplicación de la Auditoría en Informática, se redujo en primera instancia a la auditoría en informática para evaluar la seguridad. Pero viendo que desde este punto de vista, **seguridad** se considera como la protección de los recursos siendo estos los principales:

- Personas.
- Instalaciones y edificios.
- Datos.
- Equipos.
- Suministros.
- Muebles.

y tomando en cuenta que las principales áreas de protección son las siguientes:

- Física.
- Respaldo y Recuperación (back-up).
- Controles y procedimientos.
- Sistemas de computación.

la decisión se enfocó hacia trabajar sobre la auditoría en informática en seguridad física del equipo de cómputo.

Así mismo por la necesidad de contar con un problema bien delimitado y con un dominio reducido que nos permitiera llevar a cabo la creación de un prototipo que facilitara la implementación y enseñanza a principiantes con un concepto básico del objetivo del sistema experto.

Este mismo alcance nos facilitará implementar el desarrollo de módulos independientes que funcionen correctamente por separado , como lo fue en este caso el módulo de seguridad física del equipo del centro de cómputo, para poder integrarlos posteriormente, si así se desea en un sistema integral de auditoría en informática.

Las figuras 3.1 y 3.2 señalan cada una de éstas áreas de protección.

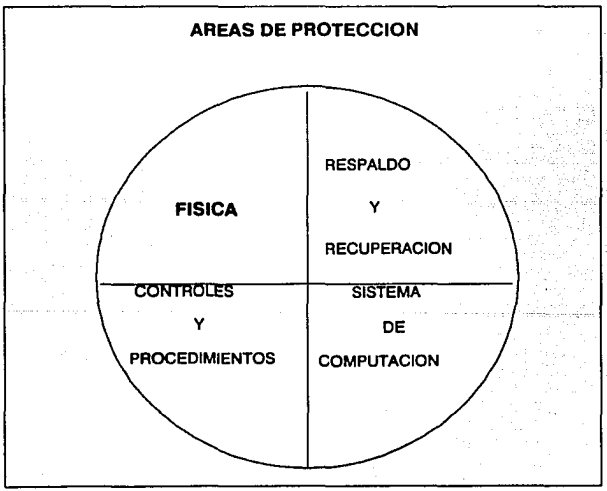


FIGURA 3.1

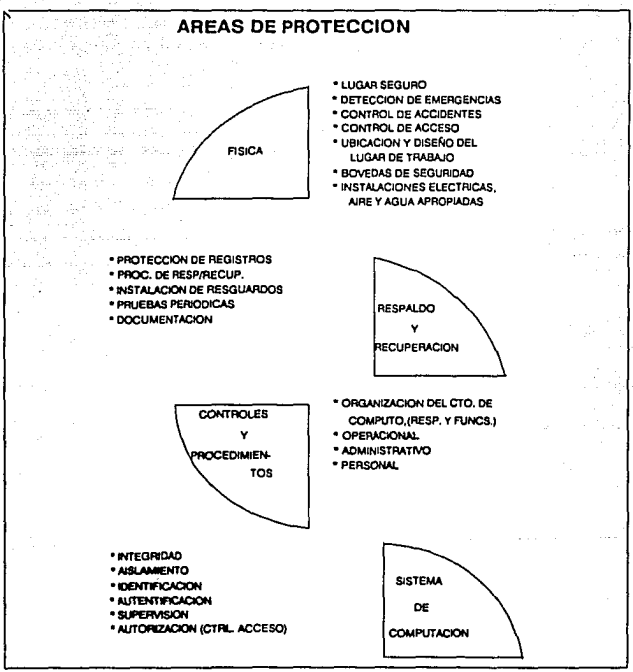


FIGURA 3.2.- AREAS DE PROTECCION

Los siguientes conceptos, son aquellos aplicables directamente a la verificación de la seguridad física. La definición de cada uno de éstos riesgos es la siguiente:

Control de Acceso al Centro de Cómputo.-

Señala el control del acceso de los individuos dentro y fuera del servicio de proceso de datos. Estos riesgos pueden implicar el permitir el acceso de algunos individuos a ciertas áreas y a otros el tener acceso a todas las áreas del servicio de proceso de datos.

Esta medida comprende a los programadores cuya tarea exclusiva es la de diseño, codificación, pruebas e implementación de productos y de ninguna manera deben tener acceso a las áreas operativas de captura y validación de datos en ambiente de producción, del área de ejecución de procesos, así como de la entrega y/o recepción de productos a usuarios finales.

De la misma forma el personal operativo del centro de procesamiento de datos no debe intervenir en la corrección o eliminación de productos finales si estos llegaran a presentar alguna falla en el momento de su ejecución, para este caso se deberá notificar al responsable de su mantenimiento actual o a el usuario final del mismo, para que se resuelva rápidamente sin impacto alguno.

Seguridad/Robo.-

Hace referencia a la seguridad o al robo de información, equipo, y software que debe conservarse confidencial debido a su naturaleza. En cierta manera, ésta es una forma de privacía, sólo que la información retirada de la organización no pertenece a un individuo.

La información puede ser dada accidentalmente (inadvertidamente), o puede ser el objeto de un robo. Este riesgo también incluye el robo de activos tales que pueden dar ocasión de fraude o desfalco.

Interrupciones y Desastres.-

Indica la interrupción del servicio de proceso de datos. Este riesgo incluye la destrucción total o parcial, intencional o no intencional (incendio o terremoto, etc), del servicio de proceso de datos, de manera que no pueda operar de modo normal.

Operación.-

Este punto se refiere a el conocimiento y experiencia del personal responsable de la operación diaria de los recursos del centro de cómputo (CPU, terminales, cintas, discos, etc). La cual debe ser necesaria y suficiente para poder responsabilizar a dicho personal de las operaciones de proceso de datos en los horarios fijados por los responsables del producto, así como de verificar que los dispositivos requeridos para la ejecución estén listos en el momento en que sean solicitados.

Generales.-

En este rubro enmarcamos todos los controles que quedaban fuera de los anteriormente planteados, pero que por su naturaleza necesitan ser evaluados primeramente por se parte de las políticas generales de la organización que es la que a fin de cuentas autorizará la implementación del sistema experto en la misma. Tales controles deberá contemplar la política de contratación de personal instruido en materia de seguridad, punto importante al comenzar a evaluar la seguridad física del centro de cómputo.

ANALISIS COSTO/BENEFICIO

Para evaluar la relación Costo/Beneficio del sistema AUDIN, se tomaron en cuenta los siguientes factores :

COSTOS POR:

RECURSOS HUMANOS.-

- Personal de Sistemas de Información (Analistas, Programadores, etc).
- Tiempo del experto humano.
- Personal usuario (Conversión, Carga de datos, etc).
- Personal otras divisiones (Organización, Auditoría, etc).

RECURSOS MATERIALES.-

- De cómputo (renta y/o compra de software de programación (EXSYS), paquete asesoría externa equipo de cómputo, renta y/o compra del hardware (Computadora Personal, mantenimiento, etc).

- De oficina (calculadoras, fotocopiadoras, otros).

- De proceso (pruebas parelelo, impresión, instalación, etc).

- Adecuaciones Físicas.

- Capacitación.

- Papelería (Formatos Preimpresos).

BENEFICIOS.-

Dentro de los principales beneficios que se aportarán con la implementación de dicho sistema dentro de una organización consideramos los siguientes:

BENEFICIOS ECONOMICOS.

- Recursos Humanos o Materiales.

- Reasignación o cancelación de puestos de recursos de áreas usuarias (Ahorro anual con prestaciones).

- Cancelación contratos de renta, mantenimiento.

- Venta de equipo de desecho.

- Depreciación equipo (Ahorro en impuestos).

- Reducción de Papelería.

- Reducción de tiempo de proceso, equipo utilizado, etc.

- Recuperación por cobro de comisiones, intereses, etc.

- Preservar el conocimiento institucional.

- Ampliar el nivel de pericia en virtud de poder guiar a cualquier auditor en la elaboración de un dictaminen sobre seguridad física, sin ningún problema.

- Proporcionar una retroalimentación al administrador del centro de cómputo sobre los puntos críticos a cubrir en la seguridad física del centro.

- Distribuir la pericia del sistema experto en las diversas áreas de oportunidad dentro de la empresa.

- Evitar que el experto humano realice tareas innecesarias que obstaculicen el realizar actividades realmente importantes en la elaboración de su auditoría.

- Disminución del costo de operación al reducir el tiempo de dictaminación de un informe de auditoría en informática.

La relación de beneficios mencionados anteriormente fueron superiores al costo del desarrollo del sistema experto, por lo cual consideramos que su implementación no tiene limitante en el costo del mismo y puede ser presentado el sistema para autorización sin el menor problema.

MODELO

DE

CONSTRUCCION

AUDIN

MODELO DE CONSTRUCCION

A través de esta fase daremos una idea del proceso real que se sigue en la construcción de un sistema experto pequeño, basado en la utilización de herramientas de inteligencia artificial como lo son los sistemas expertos.

Los pasos en los que dividiremos la construcción del sistema experto AUDIN son las siguientes:

1) SELECCION DE LA REPRESENTACION DEL CONOCIMIENTO.

2) SELECCION DE LA HERRAMIENTA.

3) IMPLEMENTACION DEL PROTOTIPO.

Con el problema ya delimitado, el siguiente paso se encaminará a la identificación y representación del conocimiento basándonos en las técnicas que tiene para ello, como lo son las reglas de producción.

Así mismo, una vez concluido el paso anterior, se determinará el tipo de herramienta necesaria para representar dicho conocimiento. La elección de una u otra no sólo depende de aspectos técnicos, sino también de recursos humanos y recursos económicos.

La última etapa pasa forzosamente por la construcción de un modelo reducido del sistema que se quiere implantar; con dicho modelo a escala se experimentará y resolverán las primeras dificultades, sirviendo de campo de pruebas del desarrollo final. Una vez suficientemente probado se van aumentando sus funciones y por tanto su complejidad y sufrirá diversos procesos de retroalimentación y mejora hasta su instalación final.

PASO 1.-REPRESENTACION DEL CONOCIMIENTO.

Como ya hemos dicho en anteriores capítulos, la base fundamental para que funcione un Sistema Experto es el conocimiento, representado de tal forma que sea reconocido por la computadora. Existen en la actualidad varias formas de representar el conocimiento, cada una con sus ventajas y desventajas, por lo que la selección de una de esas formas se vuelve complicada.

En nuestro caso decidimos utilizar los sistemas de producción como forma de representación del conocimiento por las siguientes razones:

- Se asemeja al lenguaje natural por lo que son fáciles de leer y entender.

- Las sentencias "SI-ENTONCES" son de uso cotidiano en los sistemas de programación lo que hace más fácil el convertir el conocimiento en dichas sentencias.

- La mayoría de las herramientas de apoyo para el desarrollo de Sistemas Expertos utilizan los sistemas de producción.

Ahora bien, en la construcción de **AUDIN**, el conocimiento se dividió en: Interrupción, Robo, Acceso, Operación, Sabotaje y Preguntas Generales, ya que de ésta manera se facilitará la aplicación de la auditoría y sobre todo la interpretación que de ésta lleve a cabo el auditor.

En las siguientes páginas mostraremos cómo se agruparon las "reglas de producción" para la elaboración del prototipo de **AUDIN.**

PASO 2.- SELECCION DE LA HERRAMIENTA

Para la selección de la herramienta que se aproximara a todas las expectativas sobre diseño de sistemas expertos que teníamos, se consideraron diversos factores de evaluación como a continuación se describen:

1) Primeramente por el número de reglas que se definirían para alimentar el conocimiento del sistema experto, se le ubicó como un sistema experto pequeño, la base de esta selección se puede observar en el Anexo 1- "Clasificación de los shells", que habla sobre las características de los sistemas de acuerdo a cada tipo.

2) Las herramientas pequeñas se adaptan bien y fácilmente a cualquier problema siempre que sean del tipo de diagnosis y prescripción como lo es en este caso la auditoría en informática.

Las herramientas de M1 o Personal Consultant, hubieran podido ser utilizadas, ya que ambas representan el conocimiento mediante reglas IF-THEN llamadas también Reglas de Producción, su motor de inferencia se basa en el encadenamiento hacia atrás, es decir, partiendo del propósito general o la meta (Diagnóstico de falla en el Centro de Cómputo), se infieren las reglas que diagnostican las fallas dentro de cada factor de elección considerado.

Pero en este caso la herramienta que cubrió con los puntos anteriormente mencionados pero que además nos ofreció una versatilidad en el manejo de interfaces en Dbase y Lotus, así como la posibilidad de contar con un editor, fue EXSYS.

EXSYS.-

Este Shell ofrece un nuevo nivel de sofisticación para el desarrollo de sistemas expertos a los ingenieros del conocimiento. Los Sistemas Expertos diseñados con EXSYS son fáciles de desarrollarse y relativamente rápidos independientemente de la complejidad del problema.

EXSYS fue escrito en C, para una mayor velocidad y una utilización eficiente de la memoria.

EXSYS incluye su propio compilador que permite editar y crear las reglas con un procesador de palabras. No son necesarios lenguajes especiales para editar las reglas.

Los sistemas expertos que se desarrollan con EXSYS son compatibles entre las computadoras IBM PC/XT/AT/ con 640k RAM, disco duro o disco flexible de alta densidad, un sistema operativo mayor a 2.0; DEC VAX/VMS en discos RX-50 o cintas y UNIX para cualquier configuración.

Una vez seleccionada la herramienta y la estrategia de resolución, esto implica que se debe confirmar que nuestro problema reúne las características de:

- El tiempo que debemos tardar en resolverlo debe estar normalmente entre los 15 o 30 minutos. Si es menos de 10 el problema es muy sencillo y si se tarda más de 30 implica demasiado conocimiento y se volvería muy lento.

- El proceso de resolución se podrá llevar a cabo mediante una serie de reglas y pocos cálculos. Si la solución requiere muchos cálculos, sería mejor la programación tradicional.

- El conjunto de soluciones finales deben ser menos de 50 en caso contrario, habrá probablemente otras herramientas más aptas que las de IA.

PASO 3.- IMPLEMENTACION DEL PROTOTIPO.

Para el desarrollo de **AUDIN** decidimos llevar a cabo un prototipo con 21 preguntas, las cuales serán incrementadas dentro de la fase de implementación a 80 ó 100 aproximadamente para contar con elementos suficientes a fin de poder dar un dictamen veraz sobre la auditoría efectuada.

Para asignar el peso correspondiente a cada pregunta, decidimos otorgar puntos malos a cada respuesta incorrecta, esto es, si la respuesta a una pregunta dada no cumple con los requerimientos para que un centro de cómputo sea seguro, se le asigna una puntuación X, la cual se va sumando al rubro al que afecte con el fin de determinar las codiciones inseguras y de alto riesgo en las que se encuentra el área evaluada.

Considerando que utilizaremos el encadenamiento hacia atrás, nuestra meta será "detectar fallas en el centro de cómputo", razón por la cual nuestras preguntas se enfocarán a la acumulación de fallas de la forma que se mencionó anteriormente.

FORMALIZACION

AUDIN

FORMALIZACION

Una vez que se ha revisado el prototipo y no se detectaron fallas de conceptualización se comienza a trabajar formalmente el sistema experto.

Para representar cada uno de los pasos dentro de esta fase se identificaron los siguientes puntos:

- DEFINICION DETALLADA DEL PROBLEMA.
- PLANEACION DEL PRODUCTO.
- DISEÑO.
- PLANEACION DE LA PRUEBA.
- PLANEACION DE LA IMPLEMENTACION.

La explicación de cada uno de estos puntos se observa de los anexos 2 al 6.

IMPLEMENTACION

AUDIN

IMPLEMENTACION

REVISION DEL PROTOTIPO.

Una vez terminada la primera versión del prototipo, se le pidió al experto que lo revisara; el resultado obtenido no fué muy satisfactorio, ya que la evaluación de las respuestas no arrojaba un dictamen correcto, por lo que se decidió retomar el diseño del prototipo antes de pasar a la siguiente fase.

En la segunda versión se aumentaron las preguntas a 50, y la forma de la evaluación se llevó a cabo tomando la relación que existía de cada pregunta con todos los rubros (Interrupción, Robo, Acceso, Operación, Sabotaje y Preguntas Generales), manejados como puntos de control para el sistema, la forma en la que se relacionaron se mostrará en la parte de desarrollo de la infraestructura del sistema. Terminada la segunda versión, se hizo la revisión correspondiente, obteniendo el visto bueno del experto para proseguir con el diseño de AUDIN.

DESARROLLO DE LA INFRAESTRUCTURA DEL SISTEMA.

La implementación del sistema experto se llevó a cabo mediante la elaboración de 87 preguntas, con 220 reglas de producción, que dieron origen a una base del conocimiento de 105 calificadores, de los cuales los primeros 79 se tomaron como riesgos independientes, a partir del riesgo 80 y hasta el 99 estos riesgos se agruparon y relacionaron dependiendo a la parte de la seguridad que afectaran.

Una vez generada dicha base del conocimiento se definió un riesgo en particular para cada rubro y se tomaron los subgrupos para llegar a la evaluación de cada punto de control.

Para tener un conocimiento más profundo sobre cuales fueron las reglas y riesgos utilizados, referirse al anexo 7.

Ahora bien, en las siguientes gráficas mostraremos cómo se llevó a cabo la evaluación de los riesgos.

RIESGO / RUBRO	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
INCENDIO	*						*			*				*		*	*		*	*
FALLAS EN EQUIPOS		*		*	*							*								
USO FALSO			*								*									
CONTAMINACION						*			*											
VISITAS																				
RELACIONES PERSONALES										*										
ACCESO												*								
EVACUACION													*							
DAÑO EQUIPO			*						*						*					
CAMBIO																		*		
AIRE ACONDICIONADO																				
SUMINISTRO DE ENERGIA																				
TEMBLOR																				
FALLAS																				
DOCUMENTACION																				
ADMINISTRACION																				
CONTINGENCIA																				
OTROS																				

MATRIZ DE EVALUACION DE RIESGOS (1)

RIESGO / HUMO	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
INCENDIO				X	X	X	X			X	X		X			X	X	X		
PENETRABLES																				
PISO FALSO	X																			
INUNDACION																				
VISITAS																				
INSTALACION ELECTR.								X					X					X		X
ACCESO																				
EVACUACION												X								
DAÑO EQUIPO		X	X															X		
SABOTAJE																				X
AIRE ACONDICIONADO			X											X						
SUMINISTRO DE ENERGIA										X					X				X	
LIMPIEZA																				
PAPELES																				
DOCUMENTACION																				
ADMINISTRACION																				
CONTINGENCIA																				
SEGUROS																				

MATRIZ DE EVALUACION DE RIESGOS (2)

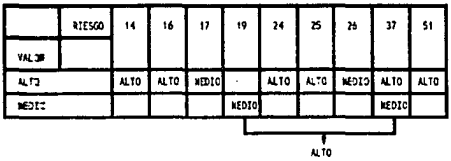
RIESGO / RUBRO	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
INCENDIO											*									
PENETRABLES					*															
PISO FALSO																				
INUNDACION																				
VISITAS													*	*		*		*	*	*
INSTALACION ELCTR.	*																			
ACCESO												*		*						
EVACUACION									*	*										
DAÑO EQUIPO								*												*
SABOTAJE				*	*															*
AIRE ACONDICIONADO		*	*																	
SUMISTRO DE ENERGIA																				
TEMBLOR						*	*													
GAFETES															*		*			
DOCUMENTACION																				
ADMINISTRACION																				
CONTINGENCIA																				
SEGUROS																				

MATRIZ DE EVALUACION (3)

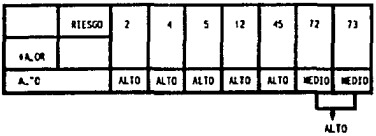
RIESGO / RUBRO	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
INCENDIO																			
PENETRABLES												*	*						
PISO FALSO																			
INUNDACION																			
VISITAS																			
INSTALACION ELCTR.																			
ACCESO	*													*					
EVACUACION																			
DAÑO EQUIPO														*					
SABOTAJE												*	*	*					
AIRE ACONDICIONADO																			
SUMISTRO DE ENERGIA																			
TEMBLOR																			
GAFETES																			
DOCUMENTACION		*	*		*	*				*									
ADMINISTRACION				*						*	*								
CONTINGENCIA							*	*											
SEGUROS															*	*	*	*	*

MATRIZ DE EVALUACION (4)

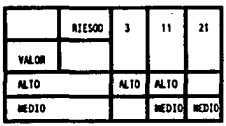
COMBATIR INCENDIO



PENETRACION



PISO FALSO



PREVENCION-INCENDIO

	RIESGO	1	7	10	20	27	30	31	33	36	38
VALOR											
ALTO		ALTO	ALTO	ALTO	MEDIO	MEDIO	ALTO	ALTO	ALTO	MEDIO	ALTO
MEDIO		MEDIO					MEDIO	MEDIO	MEDIO	MEDIO	

ALTO

INUNDACION

	RIESGO	6	9
VALOR			
ALTO		ALTO	MEDIO

VISITAS

	RIESGO	53	54	56	58	59	60	74
VALOR								
ALTO		MEDIO	ALTO	ALTO	ALTO	ALTO	MEDIO	MEDIO
MEDIO			MEDIO		MEDIO			

ALTO

ALTO

ALTO

INSTALACIONES ELECTRICAS

	RIESGO	10	28	33	38	40	41
VALOR							
ALTO		ALTO	ALTO	MEDIO	ALTO	ALTO	ALTO

ACCESO

	RIESGO	12	52	54	61	74
VALOR						
ALTO		ALTO	ALTO	ALTO	ALTO	MEDIO
MEDIO			MEDIO		MEDIO	

ALTO ALTO

EVACUACION

	RIESGO	13	32	49	58
VALOR					
ALTO		ALTO	ALTO	MEDIO	MEDIO
MEDIO			MEDIO		

ALTO

DAÑO EQUIPO MATERIAL

	RIESGO	3	9	15	23	38
VALOR						
ALTO		ALTO	MEDIO	ALTO	ALTO	ALTO

DAÑO EQUIPO HUMANO

	RIESGO	22	48	60	74
VALOR					
ALTO		ALTO	MEDIO	MEDIO	MEDIO

ALTO

GENERALES SABOTAJE

	RIESGO	40	44	45	60	72	73	74
VALOR								
ALTO		ALTO	ALTO	ALTO	MEDIO	MEDIO	MEDIO	MEDIO

ALTO

ALTO

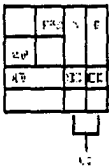
AIRE ACONDICIONADO

	RIESGO	23	34	42	43
VALOR					
ALTO		ALTO	MEDIO	ALTO	MEDIO
MEDIO					

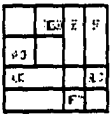
SUMINISTRO ENERGIA

	RIESGO	29	35	39
VALOR				
ALTO		ALTO	MEDIO	ALTO
MEDIO				MEDIO

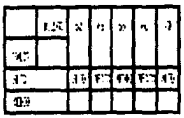
TEMBLOR



GAFETES



DOCUMENTACION



INTERRUPCION Y DESTASTRE

	RIESGO	80	81	82	83	84	85	86	87	89	90	91	92	93	94
VALOR															
ALTO		ALTO	ALTO	MEDIO	MEDIO	ALTO	ALTO	ALTO	ALTO	ALTO	MEDIO	MEDIO	ALTO	ALTO	ALTO
MEDIO		MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO

OPERACION

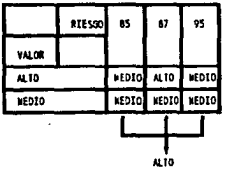
	RIESGO	96	97
VALOR			
ALTO		ALTO	ALTO
MEDIO		MEDIO	

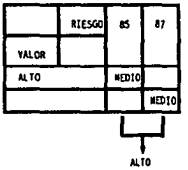
GENERALES

	RIESGO	88	90	95	96	97	98	99
VALOR								
ALTO		ALTO	MEDIO	MEDIO	MEDIO	ALTO	ALTO	ALTO
MEDIO		MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO

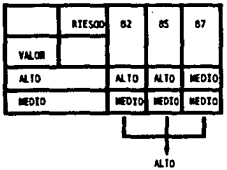
ALTO

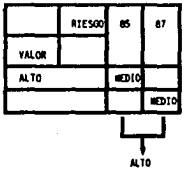
ACCESO CENTRO COMPUTO



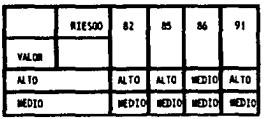


ROBO





SABOTAJE



ADMINISTRACION

	RIESGO	64	70	71
VALOR				
ALTO		ALTO	ALTO	ALTO

CONTINGENCIA

	RIESGO	67	68
VALOR			
ALTO		ALTO	ALTO
MEDIO			MEDIO

SEGUROS

	RIESGO	75	76	77	78	79
VALOR						
ALTO		ALTO	ALTO	MEDIO	ALTO	ALTO
MEDIO			MEDIO			

ALTO

Para asignar el peso correspondiente a cada pregunta, decidimos otorgar una valorización en cuestión del riesgo inherente, es decir, de acuerdo a la respuesta de cada una de ellas se le asignó un calificador de riesgo alto, medio o bajo en lugar de sumar puntos malos como en un principio se había contemplado.

Una ves que se tuvo para cada una de las preguntas el riesgo correspondiente, estos se agruparon en riesgos aún más generales, con los cuales se diseñaron diferentes matrices de evaluación para cada uno de los factores en los que se dividió el estudio del Centro de Cómputo, lo cual nos permitirá emitir un dictamen en términos de riesgo alto, medio o bajo dependiendo de las condiciones en las que se encuentre el Centro en cuestión.

Una vez concluído el desarrollo del sistema experto, se hicieron pruebas con respuestas controladas y aleatorias, a fin de conocer el comportamiento de **AUDIN** ante diferentes circunstancias, estas pruebas sirvieron para depurarlo antes de entregárselo al auditor que llevaría a cabo las pruebas finales.

EVALUACION

AUDIN

EVALUACION

Las pruebas iniciales fueron realizadas por los ingenieros del conocimiento, en las que se tuvieron que modificar varias preguntas que no estabaqn siendo bien elaboradas y evaluadas. Una vez concluida esta etapa se entregó el sistema al experto para su revisión.

Después de dos semanas de revisión el experto nos hizo algunas observaciones con respecto a la estructura de algunas las preguntas hechas a través de AUDIN, mencionándonos que se aumentara la facilidad para poder imprimir directamente en papel los resultados de la evaluación, la cual estaba correcta.

Terminada dicha facilidad, se le dió nuevamente el sistema al experto para una revisión final, concluyendo así el desarrollo.

CONCLUSIONES

AUDIN

CONCLUSIONES.

En la actualidad no se tiene bien definida una metodología para el desarrollo de sistemas expertos, es por eso que a lo largo de la presente tesis se ha demostrado una forma de analizar, desarrollar e implementar un sistema experto utilizando una herramienta que nos facilita este trabajo.

Ahora explicaremos a grandes rasgos la forma en la que se dessarrolló nuestra tesis.

Una vez que cubrimos la necesidad de delimitar el problema y su alcance, seleccionamos la herramienta de trabajo. Ya con estos elementos, el estudio se enfocó en identificar los aspectos básicos de la auditoría en informática dentro de la seguridad física, de los cuales la investigación se concentró en factores como: Robo, Operación, Acceso, Interrupción y Desastre, Sabotaje y Aspectos Generales; por ser éstos los de mayor importancia para la seguridad física.

Definidos estos rubros, proseguimos a determinar cuáles serían las condiciones ideales para que un centro de cómputo esté protegido ante estas situaciones, para llevar a cabo la evaluación se trabajó con el método de matrices de control, el cual nos arrojó los datos necesarios con los que generamos las reglas de producción que conformaron el Sistema Experto; ya con dichas reglas se comenzó la programación y pruebas del mismo. Para esto aclararemos que antes de llegar al diseño final de **AUDIN** se trabajó con varios prototipos cuyos métodos de evaluación no cubrían las expectativas.

Una vez concluído el desarrollo de **AUDIN**, se comenzaron las pruebas y depuraciones conjuntamente con el experto humano hasta tenerlo listo y depurado.

Esperamos que la presente exposición sirva como apoyo a las personas que se inician en los estudios de computación, y en especial en el campo de los sistemas expertos.

Cabe mencionar que **AUDIN** es un sistema que se puede aplicar a cualquier empresa en la que exista un centro de cómputo, teniendo como beneficio la disminución de tiempo para obtener el dictamen; para llevar a cabo una auditoría con **AUDIN**, no es necesario que la realice un experto en la materia, sino que cualquier auditor (aun sin experiencia) la puede aplicar y aprender al mismo tiempo.

Por último, haremos notar algunos de los problemas con los que nos enfrentamos (con el fin de darles a conocer las experiencias adquiridas) y con los que probablemente se pueden presentar las personas que quieran desarrollar un sistema experto.

- Los experimentos e investigaciones en el campo de la Inteligencia Artificial y de los sistemas expertos, no han tenido la difusión suficiente que nos permita tener un conocimiento más amplio sobre dichos temas.

- Se careció del apoyo necesario para el aprendizaje y aplicación de la herramienta utilizada para el diseño del sistema experto, por lo que algunos de los problemas tuvieron que ser resueltos de manera autodidacta.

No obstante lo antes mencionado, el trabajo cumple con el objetivo planteado al haber desarrollado un sistema experto que lleve a cabo la dictaminación de la Seguridad Física a un Centro de Cómputo, enfocándose el desarrollo del mismo a evaluar los aspectos de mayor interés para un auditor al momento de llevar a cabo la dictaminación que le fue asignada.

BIBLIOGRAFIA

AUDIN

BIBLIOGRAFIA

BENCHIMOL, Guy. et Al., Los Sistemas Expertos en la Empresa. Ed Macrobit-Rama. México 1988.

ECHENIQUE, G. José A., Auditoría en Informática. Ed. McGraw-Hill. México 1991.

ELISE, G. Jancura & BERGER, H. Arnold, Computers, Auditing & Control. Ed. Auerbach Publishiers, Inc.

EXSYS INC, Exsys Professional. Tomo I y II. Albuquerque N.M. 1988.

FINE, Leonard H., Seguridad en Centros de Cómputo. Políticas y Procedimientos. Ed. Trillas. México 1988.

FITZEGERALD, Jerry., Controles Internos para Sistemas de Computación. Ed. Limusa. México 1983. Primera Reimpresión.

KELLER, Robert, Expert System Technology. Ed. Yourdon Press. Estados Unidos 1987.

LAMBARRI, Alejandro, Apuntes de Auditoría en Informática. Ed. UPIICSA. México, 1990.

LI, David H., Auditoría en Centros de Cómputo. Objetivos, Lineamientos y Procedimientos. Ed. Trillas. México 1990.

RICH, Elaine., Artificial Intelligence. Ed. McGraw-Hill. Singapore 1984. Segunda Reimpresión.

ROLSTON, David W., Principios de Inteligencia Artificial y Sistemas Expertos. Ed. McGraw-Hill. Colombia 1990.

SCHILDT, Herbert. Utilización de C en Inteligencia Artificial. Ed. McGraw-Hill. España 1988.

VANCE, L. Lawrence, Auditoría. Ed Interamericana. México 1988.

Publicaciones:

Biblioteca Básica. VOL. INFORMATICA. Ed. Ingelek.

Instituto Mexicano de Contadores Públicos ,A.C., La Auditoría y el Procesamiento Electrónico de Información. México 1990.

Revista BYTE. Vol 16. Enero 1991.

Revista PC WORLD. COMUNICACIONES. Num. 17. Octubre 1988.

ANEXOS

AUDIN

ANEXO 1.

CLASIFICACION DE

LOS SHELLS

AUDIN

CLASIFICACION DE LOS SHELLS

Comercialmente los shells se dividen en tres categorías:

- **Herramientas para pequeños sistemas:** Pueden trabajar sobre computadoras personales. Son diseñadas para hacer más fácil el desarrollo de sistemas que contengan menos de 400 reglas.

- **Herramientas para grandes sistemas:** Pueden trabajar sobre máquinas LISP (computadoras especiales) o en grandes equipos y están diseñadas para crear sistemas expertos que contengan entre 100 y varios miles de reglas, aunque estén restringidos hacia la resolución de un único tipo de problemas.

- **Herramientas para grandes sistemas:** Pueden trabajar sobre máquinas LISP o en grandes equipos de cómputo y están diseñadas para crear sistemas que contengan entre 500 y varios miles de reglas; pueden incluirlas características necesarias para la resolución de distintos tipos de problemas.

ANEXO 2.

DEFINICION DETALLADA

DEL PROBLEMA

AUDIN

DEFINICION DETALLADA DEL PROBLEMA

En un centro de cómputo es necesario tener los controles indispensables para asegurar que los procesos se ejecuten sin ningún riesgo, el problema es que la mayor parte de las empresas no cuentan con una evaluación eficiente de la seguridad física o de una persona capacitada para señalar las deficiencias del centro de cómputo.

Tomando en cuenta que es difícil contar con personas que tengan la disponibilidad para elaborar un dictamen en auditoría en informática y considerando los puntos críticos que debe tomar en cuenta un auditor para llevar a cabo la evaluación de controles en seguridad física, surgió la posibilidad de desarrollar una herramienta que apoyara, facilitara y agilizara el trabajo en esta área.

DECLARACION DE OBJETIVOS.

- Agilizar los procedimientos para evaluar la Seguridad Física.
- Generar información veraz y oportuna de la Seguridad Física para establecer controles en áreas clave de un Centro de Cómputo.
- Proporcionar información comparativa para posteriores evaluaciones.

RESTRICCIONES.

Entre algunas de las restricciones que presenta en su diseño el Sistema Experto **AUDIN** tenemos su área de aplicación, ya que sólo evaluará la seguridad física de un centro de cómputo; en lo que se refiere a aprendizaje, **AUDIN** no cuenta con la capacidad de aprender de experiencias pasadas, por lo que, si se desea evaluar alguna otra condición que no este considerada en el diseño inicial, será necesaria incluirla através de nuevas opciones a fin de establecer sus controles y reglas de inferencia.

ANEXO 3.

PLANEACION DEL

PRODUCTO

AUDIN

PLANEACION DEL PRODUCTO

PRESENTACION INICIAL

Una vez terminadas las pruebas iniciales del Sistema Experto, este se presentará a los usuarios durante una reunión en la cual se le pedirá a uno de los asistentes efectúe una prueba del sistema y conteste en base al Centro de Computo del cual es responsable. Una vez que el sistema emita un dictamen este se pondrá a consideración de los presentes, de tal forma que se concluya sobre la confiabilidad del Sistema Experto, de los posibles errores, correcciones y sugerencias.

PRESENTACION DE EXPOSICION LIMITADA

Toda vez que se haya desarrollado un razonable nivel de confianza (75%), el Sistema Experto se entregara a unos cuantos auditores entre los que se incluirán los de la empresa y algunos externos, para que utilicen el sistema en base a casos reales y nuevamente indiquen el nivel de confianza que le darían al sistema y realimentar, con esto, al equipo de desarrollo para obtener al menos un 90 % de confiabilidad, y una vez alcanzado, poder entregarse para uso de todos los usuarios en general.

EVALUACION DEL PRODUCTO

Cuando el Sistema Experto haya sido entregado para uso general, se deberá realizar una evaluación semestral del mismo, acudiendo con todos los usuarios para que estos propongan posibles correcciones, adiciones o indiquen fallas del sistema, ademas de poder controlar el nivel de confianza actual contra el de la introducción inicial. Todo esto con la finalidad de orientar las modificaciones del sistema e influir en proyectos futuros.

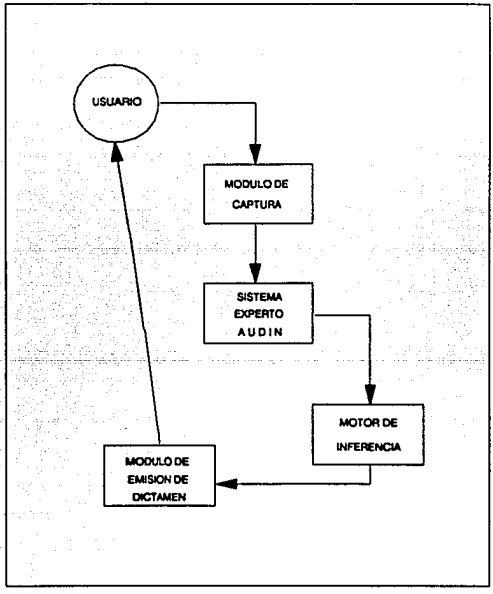
ANEXO 4.

DISEÑO

DISEÑO

USUARIO.

Dentro de la operación del sistema experto con casos reales, el usuario tiene tres funciones principales:



ARQUITECTURA DEL SISTEMA EXPERTO AUDIN

La primera es proporcionar datos através de un cuestionario que deberá responder, con dicha información, **AUDIN** aplicará las reglas necesarias para emitir un dictamen através de un reporte.

La segunda es dar seguimiento a las recomendaciones que emita el sistema experto por medio del dictamen.

La tercera y menos común, es la de informar al ingeniero de conocimientos si existe alguna nueva opción a evaluar ó falla dentro del sistema actual, con el fin de que **AUDIN** sea complementado ó modificado para considerarla.

AUDIN (AUDITORIA EN INFORMATICA).

Sistema Experto encargado de utilizar la información del usuario para evaluarla en base al motor de inferencia, compuesto de una serie de reglas de producción (IF-THEN), que evalúan cada uno de los factores de interés dentro de la seguridad física.

MODULO DE CAPTURA.

Integrado dentro de EXSYSP (herramienta seleccionada), que tiene como finalidad obtener la información proporcionada por el usuario através del cuestionario.

MODULO DE EXPLICACION.

También integrado en EXSYSP, en el cual el usuario puede visualizar las reglas que se están aplicando a cada pregunta del cuestionario en el momento de la ejecución.

MOTOR DE INFERENCIA.

Compuesto de todas las reglas de inferencia por medio de las cuales se evaluará la seguridad física del centro de cómputo. Dichas reglas fueron seleccionadas en base a los puntos más importantes dentro de la seguridad, con las que se establece la capacidad de **AUDIN** para actuar como un experto.

MODULO DE EMISION DEL DICTAMEN.

Reporte en donde el usuario podrá visualizar los resultados de la auditoría efectuada al centro de cómputo, el cual constará de observaciones y sugerencias para corregir las desviaciones encontradas; la generación de reportes se llevará a cabo en los períodos que establezca el auditor y le servirán para evaluar el status actual.

ANEXO 5.

PLANEACION DE

LA PRUEBA

AUDIN

PLANEACION DE LA PRUEBA

PROCEDIMIENTOS DE PRUEBA

Para la realización de las pruebas iniciales del Sistema Experto se seleccionaran 3 auditorías históricas, procurando que estas abarquen o sean representativas de los casos más comunes. Los encargados directos de seleccionar estos casos serán el Experto Humano y el Ingeniero de Conocimientos, y de igual manera ambos serán responsables de llevar a cabo estas pruebas y realizar la evaluación de las mismas.

Una vez que se haya concluído el desarrollo inicial del Sistema Experto, este se pondrá a prueba con los tres casos seleccionados y se hará una comparación para ver si se llega a los mismos resultados entre el Sistema Experto y el caso de prueba de tal manera que se corrijan los errores del sistema o se le añadan controles. Este proceso se repetirá tantas veces como sea necesario hasta que el Sistema Experto llegue a conclusiones razonables o semejantes a la de los tres casos de prueba.

IDENTIFICACION DE CASOS DE PRUEBA

Para seleccionar los tres casos de prueba del sistema el Experto Humano las obtendrá de auditorías realizadas por el mismo y en base a su experiencia, de tal forma que conozca a fondo los casos y pueda alimentar en todo momento al sistema con la información necesaria.

ANEXO 6.

PLANEACION DE LA

IMPLEMENTACION

AUDIN

PLANEACION DE LA IMPLEMENTACION

Una vez que las pruebas han sido consideradas exitosas, el siguiente paso consiste en implementar el sistema experto.

La implementación es un momento crítico, ya que nos encontramos con un reto, pues hay que romper o cambiar patrones de hábitos de la gente. Además si no se logra ese cambio, pronto se encontrará una confusión entre la forma de trabajar tradicionalmente una auditoría en informática y la propuesta por el nuevo sistema experto auditor.

Es muy importante definir a cada persona lo que debe hacer en la operación del sistema experto, y que además será beneficioso si entiende las otras partes del mismo, o sea, ¿qué pasa antes de que él haga su trabajo, y qué pasa después?.

Tomando en cuenta lo anterior se definieron los puntos más importantes que se deben contemplar en la implementación:

- El sistema fue desarrollado para evaluar todos los factores en conjunto, las pruebas de subconjunto no se recomiendan cuando los elementos se encuentran inter-relacionados como en este caso lo son el robo, con la interrupción y el acceso.

- La implementación se efectuará de acuerdo a los siguientes requerimientos:

- Estudio de Mercado para seleccionar los posibles usuarios potenciales del sistema experto.
- Seleccionar en cada organización al responsable de la evaluación de la seguridad física en el centro de cómputo, para inducirlo en el nuevo sistema.
- Asignar responsables del sistema y equipo de proceso una vez que se haya efctuado la adquisición del mismo.
- Verificar la adquisición e instalaciones físicas de software (módulos ejecutables), comunicaciones y equipo.
- Distribución del sistema a personas clave dentro de la organización.
- Establecer una estrategia de capacitación en la que se fijen niveles de entrenamiento, áreas a capacitar, metodología, documentación, etc.

- Capacitación a usuarios en captura, validación, interpretación de reportes.

  Dentro del plan de implementación la capacitación del usuario debe ser considerada tan importante como las anteriores, no obstante se haya desarrollado el sistema más completo, si no se logra transmitir los conocimientos y características principales, dicho sistema corre el peligro de fracasar, por el sólo hecho de falta de conocimiento.

  Así mismo se debe hacer notar que en ésta etapa se pueden presentar algunas desviaciones por la forma de trabajar de cada organización, por lo que es necesario aclarar en la implementación, que dichas particularidades pueden afectar el desarrollo satisfactorio del sistema, lo que implica definir un esquema específico del cual partir y desarrollar ajustes necesarios para se logre una mayor consolidación del nuevo sistema con el usuario quien finalmente interactúa con él.

- Documentación de datos.

- Fijar estándares en fechas, horarios y responsables en el soporte.

- Establecer con los usuarios periodos de uso y obtención de reportes.

ANEXO 7.

RELACION DE RIESGOS

Y

REGLAS DE PRODUCCION

AUDIN

REGLAS DE PRODUCCION DE "AUDIN"

REGLA: REGLA-1.1
IF:
LAS PUERTAS DEL CENTRO DE COMPUTO SON: {COMBUSTIBLES}
and: LOS PISOS DEL CENTRO DE COMPUTO SON: {COMBUSTIBLES}
THEN:
RIESGO INCENDIO 1 {ALTO}
ELSE:
RIESGO INCENDIO 1 {BAJO}

REGLA: REGLA-1.2
IF:
RIESGO INCENDIO 1 NOT {ALTO}
and: LAS PAREDES DEL CENTRO DE COMPUTO SON: {COMBUSTIBLES}
THEN:
RIESGO INCENDIO 1 {ALTO}
ELSE:
RIESGO INCENDIO 1 {BAJO}

REGLA: REGLA-1.3
IF:
RIESGO INCENDIO 1 NOT {ALTO}
and: LOS PISOS DEL CENTRO DE COMPUTO SON: {COMBUSTIBLES}
and: LAS PAREDES DEL CENTRO DE COMPUTO SON: {NO COMBUSTIBLES}
and: LAS PUERTAS DEL CENTRO DE COMPUTO SON: {NO COMBUSTIBLES}
THEN:
RIESGO INCENDIO 1 {MEDIO}
ELSE:
RIESGO INCENDIO 1 {BAJO}

REGLA: REGLA-2
IF:
LAS PAREDES ADYACENTES A LOS ARCHIVOS O AL EQUIPO SON:
{ ^ ^PENETRABLES^ ^ }
THEN:
RIESGO PENETRABLES 1 {ALTO}
ELSE:
RIESGO PENETRABLES 1 {BAJO}

REGLA: REGLA-3.1
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: SE CUENTA CON PISO FALSO ? {NO}
THEN:
RIESGO PISO FALSO {ALTO}
and: RIESGO MTO PISO FALSO {BAJO}

and: RIESGO ALTURA PISO {BAJO}
ELSE:
RIESGO PISO FALSO {BAJO}

REGLA: REGLA-3.2
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: SE CUENTA CON PISO FALSO ? {SI}
THEN:
RIESGO PISO FALSO {BAJO}

REGLA: REGLA-4
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO PISO FALSO {BAJO}
and: LAS PAREDES COMIENZAN A PARTIR DEL PISO FALSO ? {SI}
THEN:
RIESGO ENTRADA SUBREPTICIA {ALTO}
ELSE:
RIESGO ENTRADA SUBREPTICIA {BAJO}

REGLA: REGLA-5
IF:
EXISTE UNA BARRERA FISICA QUE SEPARE EL CENTRO DE COMPUTO DE LAS DEMAS AREAS DENTRO DE LA EMPRESA ? {SI}
THEN:
RIESGO PENETRABLE 2 {BAJO}
ELSE:
RIESGO PENETRABLE 2 {ALTO}

REGLA: REGLA-6
IF:
EL CENTRO DE COMPUTO SE ENCUENTRA EN PLANTA BAJA O SOTANOS ? {SI }
THEN:
RIESGO INUNDACION {ALTO}
ELSE:
RIESGO INUNDACION {BAJO}

REGLA: REGLA-7
IF:
EXISTE UNA AREA INTERNA DE ALMACENAMIENTO DE LA INFORMACION ? {SI}
and: EXISTE EQUIPO, ALARMAS Y LA PROTECCION ADECUADA CONTRA INCENDIO EN LAS AREAS INTERNAS DE ALMACENAMIENTO DE INFORMACION {NO}
THEN:
RIESGO INCENDIO 2 {ALTO}
ELSE:

RIESGO INCENDIO 2 {BAJO}

REGLA: REGLA-9
IF:
ESTAN PROTEGIDOS LOS TECHOS PARA EVITAR FILTRACION DE AGUA ? {NO}
THEN:
RIESGO FILTRACION {ALTO}
ELSE:
RIESGO FILTRACION {BAJO}

REGLA: REGLA-10
IF:
LOS CABLES QUE SUMINISTRAN ENERGIA AL CENTRO DE COMPUTO SE ENCUENTRAN AL DESCUBIERTO ? {SI}
THEN:
RIESGO CABLEADO {ALTO}
ELSE:
RIESGO CABLEADO {BAJO}

REGLA: REGLA-11.1
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO ALTURA PISO NOT {ALTO}
and: RIESGO PISO FALSO {BAJO}
and: A QUE ALTURA ESTA SITUADO APROXIMADAMENTE EL PISO FALSO ? {MENOS DE 25 cm.}
THEN:
RIESGO ALTURA PISO {MEDIO}

REGLA: REGLA-11.2
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO PISO FALSO {BAJO}
and: A QUE ALTURA ESTA SITUADO APROXIMADAMENTE EL PISO FALSO ? {ENTRE 25 Y 35 cm.}
THEN:
RIESGO ALTURA PISO {BAJO}

REGLA: REGLA-11.3
IF: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO PISO FALSO {BAJO}
and: A QUE ALTURA ESTA SITUADO APROXIMADAMENTE EL PISO FALSO ? {MAS DE 35 cm.}
THEN:

RIESGO ALTURA PISO {ALTO}
ELSE:
RIESGO ALTURA PISO {BAJO}

REGLA: REGLA-12
IF:
EXISTE UN UNICO ACCESO AL CENTRO DE COMPUTO ? {SI }
THEN:
RIESGO ACCESO 1 {BAJO}
ELSE:
RIESGO ACCESO 1 {ALTO}

REGLA: REGLA-13
IF:
SE CUENTA CON SALIDAS DE EMERGENCIA EN EL CENTRO DE COMPUTO ? {SI}
THEN:
RIESGO SALIDA EMERGENCIA {BAJO}
ELSE:
RIESGO SALIDA EMERGENCIA {ALTO}
and: RIESGO FALLA SAL EMER {BAJO}

REGLA: REGLA-14
IF:
DE LOS SIGUIENTES EQUIPOS CONTRA EL FUEGO, CON CUAL CUENTA EL CENTRO DE COMPUTO : {EXTINGIDORES MANUALES}
or: DE LOS SIGUIENTES EQUIPOS CONTRA EL FUEGO, CON CUAL CUENTA EL CENTRO DE COMPUTO : {GAS HALONE}
THEN:
RIESGO INCENDIO 3 {BAJO}
and: RIESGO DETEC SEÑALAM {BAJO}
and: RIESGO DAÑO EQUIPO {BAJO}
ELSE:
RIESGO INCENDIO 3 {ALTO}
and: RIESGO DAÑO EQUIPO {ALTO}
and: RIESGO DETEC SEÑALAM {BAJO}
and: RIESGO ASFIXIA {BAJO}

REGLA: REGLA-14.1
IF:
DE LOS SIGUIENTES EQUIPOS CONTRA EL FUEGO, CON CUAL CUENTA EL CENTRO DE COMPUTO : {OTRO}
THEN:
RIESGO DAÑO EQUIPO {ALTO}
ELSE:
RIESGO DAÑO EQUIPO {BAJO}

REGLA: REGLA-15.1
IF:
LOS DETECTORES DE HUMO Y FUEGO SE ENCUENTRAN INSTALADOS EN : {NO SE TIENEN}

THEN:
RIESGO PREV INCENDIO {ALTO}
and: RIESGO DETECCION INCENDIO {BAJO}
ELSE:
RIESGO PREV INCENDIO {BAJO}

REGLA: REGLA-15.2
IF:
LOS DETECTORES DE HUMO Y FUEGO SE ENCUENTRAN INSTALADOS EN : {AMBOS}
THEN:
RIESGO PREV INCENDIO {BAJO}

REGLA: REGLA-15.3
IF:
RIESGO PREV INCENDIO NOT {ALTO}
and: LOS DETECTORES DE HUMO Y FUEGO SE ENCUENTRAN INSTALADOS EN : {PISO FALSO}
or: LOS DETECTORES DE HUMO Y FUEGO SE ENCUENTRAN INSTALADOS EN : {TECHO}
THEN:
RIESGO PREV INCENDIO {MEDIO}

REGLA: REGLA-16
IF:
DE LOS SIGUIENTES EQUIPOS CONTRA EL FUEGO, CON CUAL CUENTA EL CENTRO DE COMPUTO : NOT {NO SE TIENE}
and: EN CASO DE FALSA ALARMA EXISTE UN INTERRUPTOR PARA DESACTIVAR LOS MECANISMOS DE EXTINCION DEL FUEGO ? {NO}
THEN:
RIESGO FALSA ALARMA {ALTO}
ELSE:
RIESGO FALSA ALARMA {BAJO}
and: RIESGO SABOTAJE 1 {ALTO}

REGLA: REGLA-17.1
DE LOS SIGUIENTES EQUIPOS CONTRA EL FUEGO, CON CUAL CUENTA EL CENTRO DE COMPUTO : {EXTINGIDORES MANUALES}
and: LA UBICACION DE LOS EXTINGUIDORES SE ENCUENTRA SEÑALADA ? {SI}
THEN:
RIESGO DETEC SEÑALAM {BAJO}

REGLA: REGLA-17.2
IF:
DE LOS SIGUIENTES EQUIPOS CONTRA EL FUEGO, CON CUAL CUENTA EL CENTRO DE COMPUTO : {EXTINGIDORES MANUALES}
and: LA UBICACION DE LOS EXTINGUIDORES SE ENCUENTRA SEÑALADA ? {NO}
THEN:
RIESGO DETEC SEÑALAM {MEDIO}

REGLA: REGLA-18

IF: EL MOBILIARIO DEL CENTRO DE COMPUTO ESTA FABRICADO DE MATERIALES NO COMBUSTIBLES O RETARDANTES DEL FUEGO ? {SI}
THEN:
RIESGO PROPAGACION INCENDIO {BAJO}
ELSE:
RIESGO PROPAGACION INCENDIO {ALTO}

REGLA: REGLA-19.1
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO PISO FALSO {BAJO}
and: SE DA MANTENIMIENTO CONSTANTE AL PISO FALSO ? {SI}
THEN:
RIESGO MTO PISO FALSO {BAJO}

REGLA: REGLA-19.2
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO PISO FALSO {BAJO}
and: SE DA MANTENIMIENTO CONSTANTE AL PISO FALSO ? {NO}
THEN:
RIESGO MTO PISO FALSO {MEDIO}

REGLA: REGLA-20
IF:
SE PROHIBE FUMAR, COMER Y BEBER EN EL CENTRO DE COMPUTO ? {SI}
THEN:
RIESGO DAÑO EQUIPO 2 {BAJO}
ELSE:
RIESGO DAÑO EQUIPO 2 {ALTO}

REGLA: REGLA-21.1
IF:
SE CUENTA CON AIRE ACONDICIONADO ? {SI}
and: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
THEN:
RIESGO AIRE ACOND {BAJO}

REGLA: REGLA-21.2
IF:
SE CUENTA CON AIRE ACONDICIONADO ? {NO}
and: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}

THEN:
RIESGO AIRE ACOND {ALTO}
and: RIESGO INCENDIO 4 {BAJO}
and: RIESGO FALLA AIRE ACOND {BAJO}
and: RIESGO CTRL TEMP HUM {BAJO}
and: RIESGO FILTRO AIRE {BAJO}
and: RIESGO DAÑO DUCTOS {BAJO}
ELSE:
RIESGO AIRE ACOND {BAJO}
and: RIESGO CTRL TEMP HUM {BAJO}

REGLA: REGLA-22.1
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO AIRE ACOND {BAJO}
and: EN CASO DE INCENDIO SE APAGA AUTOMATICAMENTE EL AIRE ACONDICIONADO ? {SI}
THEN:
RIESGO INCENDIO 4 {BAJO}

REGLA: REGLA-22.2
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO AIRE ACOND {BAJO}
and: EN CASO DE INCENDIO SE APAGA AUTOMATICAMENTE EL AIRE ACONDICIONADO ? {NO}
THEN:
RIESGO INCENDIO 4 {ALTO}
ELSE:
RIESGO INCENDIO 4 {BAJO}

REGLA: REGLA-23
IF:
SE CUENTA CON ALARMA CONTRA INCENDIO ? {SI}
THEN:
RIESGO ALARMA INCENDIO {BAJO}
ELSE:
RIESGO ALARMA INCENDIO {ALTO}
and: RIESGO DETECCION INCENDIO {BAJO}
and: RIESGO FALLA ALARM INCENDIO {BAJO}

REGLA: REGLA-24.1
IF:
RIESGO ALARMA INCENDIO {BAJO}
and: LA ALARMA CONTRA INCENDIO TIENE LA CAPACIDAD DE TRANSMITIR SEÑALES A UN ^ ^ PUNTO REMOTO ^ ^ ? {SI}

THEN:
RIESGO DETECCION INCENDIO {BAJO}

REGLA: REGLA-242
IF:
RIESGO ALARMA INCENDIO {BAJO}
and: LA ALARMA CONTRA INCENDIO TIENE LA CAPACIDAD DE TRANSMITIR SEÑALES A UN ^ ^ PUNTO REMOTO ^ ^ ? {NO}
THEN:
RIESGO DETECCION INCENDIO {ALTO}
ELSE:
RIESGO DETECCION INCENDIO {BAJO}

REGLA: REGLA-25
IF:
LA PAPELERIA EN GENERAL SE ALMACENA FUERA DEL CENTRO DE COMPUTO ? {SI}
THEN:
RIESGO INCENDIO 5 {BAJO}
ELSE:
RIESGO INCENDIO 5 {ALTO}

REGLA: REGLA-26
IF:
SE CUENTA CON ^ ^PANELES DE DISTRIBUCION ELECTRICA ^ ^ {SI}
THEN:
RIESGO DIST ELECTRICA {BAJO}
ELSE:
RIESGO DIST ELECTRICA {ALTO}
and: RIESGO PANEL EQUIPO {BAJO}
and: RIESGO OPERACION DIST ELECT {BAJO}

REGLA: REGLA-27
IF:
SE CUENTA CON SUMINISTROS DE POTENCIA ININTERRUMPIBLE ? {SI}
THEN:
RIESGO SUMIN ENERGIA {BAJO}
ELSE:
RIESGO SUMIN ENERGIA {ALTO}
and: RIESGO FALLA SUMIN ENERGIA {BAJO}
and: RIESGO INTERRUP EQUIPO {BAJO}
and: RIESGO EQUIPO COM {NO }

REGLA: REGLA-281
IF:
RIESGO PREV INCENDIO NOT {ALTO}
and: CADA CUANDO SE LE DA MANTENIMIENTO A LOS DETECTORES DE INCENDIO ? {TRIMESTRAL}
THEN:
RIESGO FALLA DETEC INCENDIO {BAJO}

REGLA: REGLA-28.3
IF:
RIESGO PREV INCENDIO NOT {ALTO}
and: CADA CUANDO SE LE DA MANTENIMIENTO A LOS DETECTORES DE INCENDIO ? {ANUAL}
or: CADA CUANDO SE LE DA MANTENIMIENTO A LOS DETECTORES DE INCENDIO ? {NO SE DA MANTENIMIETO}
THEN:
RIESGO FALLA DETEC INCENDIO {ALTO }
ELSE:
RIESGO FALLA DETEC INCENDIO {BAJO}

REGLA: REGLA-28.2
IF:
RIESGO FALLA DETEC INCENDIO NOT {ALTO }
and: RIESGO PREV INCENDIO NOT {ALTO}
and: CADA CUANDO SE LE DA MANTENIMIENTO A LOS DETECTORES DE INCENDIO ? {SEMESTRAL}
THEN:
RIESGO FALLA DETEC INCENDIO {MEDIO}

REGLA: REGLA-29.1
IF:
RIESGO ALARMA INCENDIO {BAJO}
and: CON QUE FRECUENCIA SE REVISA EL FUNCIONAMIENTO DE LA ALARMA CONTRA INCENDIO ? {TRIMESTRAL}
THEN:
RIESGO FALLA ALARM INCENDIO {BAJO}

REGLA: REGLA-29.3
IF:
RIESGO ALARMA INCENDIO {BAJO}
and: CON QUE FRECUENCIA SE REVISA EL FUNCIONAMIENTO DE LA ALARMA CONTRA INCENDIO ? {NO SE REVISA}
or: CON QUE FRECUENCIA SE REVISA EL FUNCIONAMIENTO DE LA ALARMA CONTRA INCENDIO ? {ANUAL}
THEN:
RIESGO FALLA ALARM INCENDIO {ALTO}
ELSE:
RIESGO FALLA ALARM INCENDIO {BAJO}

REGLA:REGLA-29.2
IF:
RIESGO FALLA ALARM INCENDIO NOT {ALTO}
and: RIESGO ALARMA INCENDIO {BAJO}
and: CON QUE FRECUENCIA SE REVISA EL FUNCIONAMIENTO DE LA ALARMA CONTRA INCENDIO ? {SEMESTRAL }
THEN:
RIESGO FALLA ALARM INCENDIO {MEDIO}

REGLA: REGLA-30.1
IF:
RIESGO SALIDA EMERGENCIA {BAJO}
and: CON QUE PERIODICIDAD SE REVISA EL FUNCIONAMIENTO DE LAS SALIDAS DE EMERGENCIA : {TRIMESTRAL}
THEN:
RIESGO FALLA SAL EMER {BAJO}

REGLA: REGLA-30.3
IF:
RIESGO SALIDA EMERGENCIA {BAJO}
and: CON QUE PERIODICIDAD SE REVISA EL FUNCIONAMIENTO DE LAS SALIDAS DE EMERGENCIA : {ANUAL}
or: CON QUE PERIODICIDAD SE REVISA EL FUNCIONAMIENTO DE LAS SALIDAS DE EMERGENCIA : {NO SE REVISA}
THEN:
RIESGO FALLA SAL EMER {ALTO}
ELSE:
RIESGO FALLA SAL EMER {BAJO}

REGLA: REGLA-30.2
IF:
RIESGO FALLA SAL EMER NOT {ALTO}
and: RIESGO SALIDA EMERGENCIA {BAJO}
and: CON QUE PERIODICIDAD SE REVISA EL FUNCIONAMIENTO DE LAS SALIDAS DE EMERGENCIA : {SEMESTRAL}
THEN:
RIESGO FALLA SAL EMER {MEDIO}

REGLA: REGLA-31.1
IF:
RIESGO DIST ELECTRICA {BAJO}
and: EL MANTENIMIENTO A LOS ^ ^ PANELES DE DISTRIBUCION ELECTRICA ^ ^ SE DA : {TRIMESTRALMENTE}
THEN:
RIESGO FALLA DIST ELECT {BAJO}

REGLA: REGLA-31.3
IF:
RIESGO DIST ELECTRICA {BAJO}
and: EL MANTENIMIENTO A LOS ^ ^ PANELES DE DISTRIBUCION ELECTRICA ^ ^ SE DA : {ANUALMENTE}
or: EL MANTENIMIENTO A LOS ^ ^ PANELES DE DISTRIBUCION ELECTRICA ^ ^ SE DA : {NO SE DA MANTENIMIENTO}
THEN:
RIESGO FALLA DIST ELECT {ALTO}
ELSE:
RIESGO FALLA DIST ELECT {BAJO}

REGLA: REGLA-31.2

IF: RIESGO FALLA DIST ELECT NOT {ALTO}
and: RIESGO DIST ELECTRICA {BAJO}
and: EL MANTENIMIENTO A LOS ^ ^ PANELES DE DISTRIBUCION ELECTRICA ^ ^ SE DA : {SEMESTRALMENTE}
THEN:
RIESGO FALLA DIST ELECT {MEDIO}

REGLA: REGLA-32.1
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO AIRE ACOND {BAJO}
and: CON QUE FRECUENCIA SE DA MANTENIMIENTO AL AIRE ACONICIONADO {TRIMESTRALMENTE}
THEN:
RIESGO FALLA AIRE ACOND {BAJO}

REGLA: REGLA-32.3
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO AIRE ACOND {BAJO}
and: CON QUE FRECUENCIA SE DA MANTENIMIENTO AL AIRE ACONICIONADO {ANUALMENTE}
or: CON QUE FRECUENCIA SE DA MANTENIMIENTO AL AIRE ACONICIONADO {NO SE DA MANTENIMIENTO}
THEN:
RIESGO FALLA AIRE ACOND {ALTO}
ELSE:
RIESGO FALLA AIRE ACOND {BAJO}

REGLA: REGLA-32.2
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO FALLA AIRE ACOND NOT {ALTO}
and: RIESGO AIRE ACOND {BAJO}
and: CON QUE FRECUENCIA SE DA MANTENIMIENTO AL AIRE ACONICIONADO {SEMESTRALMENTE}
THEN:
RIESGO FALLA AIRE ACOND {MEDIO}

REGLA: REGLA-33.1
IF:
RIESGO SUMIN ENERGIA {BAJO}
and: LA PERIDICIDAD EN EL MANTENIMIENTO A LOS EQUIPOS DE SUMINISTRO DE POTENCIA ININTERRUMPIBLE ES : {TRIMESTRAL}

THEN:
RIESGO FALLA SUMIN ENERGIA {BAJO}

REGLA: REGLA-33.1
IF:
RIESGO SUMIN ENERGIA {BAJO}
and: LA PERIDICIDAD EN EL MANTENIMIENTO A LOS EQUIPOS DE SUMINISTRO DE POTENCIA ININTERRUMPIBLE ES : {ANUAL}
or: LA PERIDICIDAD EN EL MANTENIMIENTO A LOS EQUIPOS DE SUMINISTRO DE POTENCIA ININTERRUMPIBLE ES : {NO SE DA MANTENIMIENTO}
THEN:
RIESGO FALLA SUMIN ENERGIA {ALTO}
ELSE:
RIESGO FALLA SUMIN ENERGIA {BAJO}

REGLA: REGLA-33.2
IF:
RIESGO FALLA SUMIN ENERGIA NOT {ALTO}
and: RIESGO SUMIN ENERGIA {BAJO}
and: LA PERIDICIDAD EN EL MANTENIMIENTO A LOS EQUIPOS DE SUMINISTRO DE POTENCIA ININTERRUMPIBLE ES : {SEMESTRAL}
THEN:
RIESGO FALLA SUMIN ENERGIA {MEDIO}

REGLA: REGLA-34.1
IF:
CADA CUANDO SE RETIRA LA BASURA COMBUSTIBLE DEL CENTRO DE COMPUTO: ' OTRO}
THEN:
RIESGO BASURA {ALTO}
ELSE:
RIESGO BASURA {BAJO}

REGLA: REGLA-34.2
IF:
RIESGO BASURA NOT {ALTO}
and: CADA CUANDO SE RETIRA LA BASURA COMBUSTIBLE DEL CENTRO DE COMPUTO : {CADA TERCER DIA}
THEN:
RIESGO BASURA {MEDIO}

REGLA: REGLA-34.3
IF:
CADA CUANDO SE RETIRA LA BASURA COMBUSTIBLE DEL CENTRO DE COMPUTO : {DIARIAMENTE}
or: CADA CUANDO SE RETIRA LA BASURA COMBUSTIBLE DEL CENTRO DE COMPUTO : {MAS DE UNA VEZ AL DIA}
THEN:
RIESGO BASURA {BAJO}

REGLA: REGLA-35.1
IF: EN CASO DE INCENDIO EL CENTRO DE COMPUTO CUENTA CON : {PLAN DA LUCHA CONTRA EL FUEGO}
or: EN CASO DE INCENDIO EL CENTRO DE COMPUTO CUENTA CON : {BRIGADA DE EVACUACION}
THEN:
RIESGO ACCION FUEGO {BAJO}

REGLA: REGLA-35.3
IF:
EN CASO DE INCENDIO EL CENTRO DE COMPUTO CUENTA CON : {NINGUNA}
THEN:
RIESGO ACCION FUEGO {ALTO}
ELSE:
RIESGO ACCION FUEGO {BAJO}

REGLA: REGLA-35.2
IF:
RIESGO ACCION FUEGO NOT {ALTO}
and: EN CASO DE INCENDIO EL CENTRO DE COMPUTO CUENTA CON : {OTRA}
THEN:
RIESGO ACCION FUEGO {MEDIO}

REGLA: REGLA-36
IF:
ESTA EL EQUIPO EN GENERAL PROTEGIDO CONTRA VARIACIONES DE VOLTAJE ? {SI}
THEN:
RIESGO VOLTAJE {BAJO}
ELSE:
RIESGO VOLTAJE {ALTO}

REGLA: EQUIPO-COMPUTO
IF:
TIENE INSTALADO EQUIPO DE COMUNICACIONES EN EL CENTRO DE COMPUTO ? {SI}
THEN:
RIESGO EQUIPO COM {SI }
ELSE:
RIESGO EQUIPO COM {NO }

REGLA: REGLA-37.1
IF:
RIESGO SUMIN ENERGIA {BAJO}
and: QUE EQUIPO(S) ESTA(N) CONECTADO(S) AL SUMINISTRO DE POTENCIA ININTERRUMPIDA : {CPU's}
THEN:
RIESGO INTERRUP EQUIPO {BAJO}
ELSE:
RIESGO INTERRUP EQUIPO {ALTO}

REGLA: REGLA-37.2
IF: RIESGO INTERRUP EQUIPO NOT {ALTO}
and: RIESGO EQUIPO COM {SI }
and: EQUIPO COMUNICACION CONECTADO {SI}
THEN:
RIESGO INTERRUP EQUIPO {BAJO}

REGLA: REGLA-37.3
IF: RIESGO INTERRUP EQUIPO NOT {ALTO}
and: RIESGO EQUIPO COM {SI }
and: EQUIPO COMUNICACION CONECTADO {NO}
THEN:
RIESGO INTERRUP EQUIPO {MEDIO}

REGLA: INTERNA-1
IF:
RIESGO SUMIN ENERGIA {BAJO}
and: QUE EQUIPO(S) ESTA(N) CONECTADO(S) AL SUMINISTRO DE POTENCIA ININTERRUMPIDA : {EQUIPO DE COMUNICACIONES}
THEN:
EQUIPO COMUNICACION CONECTADO {SI}
ELSE:
EQUIPO COMUNICACION CONECTADO {NO}

REGLA: REGLA-38
IF:
RIESGO DIST ELECTRICA {BAJO}
and: CUALQUIER PERSONA TIENE ACCESO A LOS ^ ^PANELES DE DISTRIBUCION ELECTRICA^ ^ ? {SI}
THEN:
RIESGO OPERACION DIST ELECT {ALTO}
ELSE:
RIESGO OPERACION DIST ELECT {BAJO}

REGLA: REGLA-39
IF:
RIESGO DIST ELECTRICA {BAJO}
and: ESTAN RELACIONADOS LOS INTERRUPTORES DE LOS ^ ^PANELES DE DISTRIBUCION ELECTRICA^ ^ CON EL EQUIPO CONECTADO A LOS MISMOS ? {SI}
THEN:
RIESGO PANEL EQUIPO {BAJO}
ELSE:
RIESGO PANEL EQUIPO {ALTO}

REGLA: REGLA-40.1
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO AIRE ACOND {BAJO}

and: SE CONTROLA LA HUMEDAD Y EL AIRE DENTRO DEL CENTRO DE COMPUTO ? {NO}
THEN:
RIESGO CTRL TEMP HUM {ALTO}
ELSE:
RIESGO CTRL TEMP HUM {BAJO}

REGLA: REGLA-40.2
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO AIRE ACOND {BAJO}
and: SE CONTROLA LA HUMEDAD Y EL AIRE DENTRO DEL CENTRO DE COMPUTO ? {SI}
THEN:
RIESGO CTRL TEMP HUM {BAJO}

REGLA: REGLA-41
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO AIRE ACOND {BAJO}
and: ES FILTRADO EL AIRE ACONDICIONADO ANTES DE LLEGAR AL CENTRO DE COMPUTO ? {NO}
THEN:
RIESGO FILTRO AIRE {ALTO}
ELSE:
RIESGO FILTRO AIRE {BAJO}

REGLA: REGLA-NUEVA1
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO AIRE ACOND {BAJO}
and: EXISTEN DUCTOS DE AIRE ACONDICIONADO FUERA DEL EDIFICIO ? {SI}
THEN:
DUCTOS EXTERNOS {SI }
ELSE:
DUCTOS EXTERNOS {NO }
and: RIESGO DAÑO DUCTOS {BAJO}
and: RIESGO ACCESO DUCTOS {BAJO}

REGLA: REGLA-42.1
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO AIRE ACOND {BAJO}
and: DUCTOS EXTERNOS {SI }

and: LOS DUCTOS DE AIRE ACONDICIONADO FUERA DEL EDIFICIO SON VULNERABLES ? {SI}
THEN:
RIESGO DAÑO DUCTOS {ALTO}
ELSE:
RIESGO DAÑO DUCTOS {BAJO}

REGLA: REGLA-42.2
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO AIRE ACOND {BAJO}
and: DUCTOS EXTERNOS {SI }
and: LOS DUCTOS DE AIRE ACONDICIONADO FUERA DEL EDIFICIO SON VULNERABLES ? {NO}
THEN:
RIESGO DAÑO DUCTOS {BAJO}

REGLA: REGLA-43.1
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO AIRE ACOND {BAJO}
and: DUCTOS EXTERNOS {SI }
and: LOS DUCTOS DE AIRE ACONDICIONADO FUERA DEL EDIFICIO SON SUFICIENTEMENTE GRANDES QUE PERMITEN EL ACCESO DE PERSONA ATRAVES DE ELLOS ? {SI}
THEN:
RIESGO ACCESO DUCTOS {ALTO}
ELSE:
RIESGO ACCESO DUCTOS {BAJO}

REGLA: REGLA-43.2
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO AIRE ACOND {BAJO}
and: DUCTOS EXTERNOS {SI }
and: LOS DUCTOS DE AIRE ACONDICIONADO FUERA DEL EDIFICIO SON SUFICIENTEMENTE GRANDES QUE PERMITEN EL ACCESO DE PERSONA ATRAVES DE ELLOS ? {NO}
THEN:
RIESGO ACCESO DUCTOS {BAJO}

REGLA: REGLA-44
IF: EL CENTRO DE COMPUTO SE ENCUENTRA UBICADO EN UNA ZONA CONSIDERADA SISMICA ? {SI}
THEN:
RIESGO TEMBLOR {ALTO}

ELSE:
RIESGO TEMBLOR (BAJO)
and: RIESGO GRALES TEMBLOR (BAJO)

REGLA: REGLA-45.1
IF:
RIESGO TEMBLOR (ALTO)
and: EN CASO DE MOVIMIENTO TELURICO SE TIENE PROTEGIDO EL EQUIPO PARA PROTEGER SU CAIDA O DESLIZAMIENTO ? (SI)
THEN:
RIESGO TEMBLOR EQUIPO (BAJO)
and: RIESGO GRALES TEMBLOR (BAJO)

REGLA: REGLA-45.2
IF:
RIESGO TEMBLOR (ALTO)
and: EN CASO DE MOVIMIENTO TELURICO SE TIENE PROTEGIDO EL EQUIPO PARA PROTEGER SU CAIDA O DESLIZAMIENTO ? (NO)
THEN:
RIESGO TEMBLOR EQUIPO (ALTO)
and: RIESGO GRALES TEMBLOR (ALTO)
ELSE:
RIESGO TEMBLOR EQUIPO (BAJO)

REGLA: REGLA-46.3
IF:
CON QUE FRECUENCIA SE DA ^ ^SERVICIO DE LIMPIEZA^ ^ AL CENTRO DE COMPUTO : NOT (DIARIO)
and: CON QUE FRECUENCIA SE DA ^ ^SERVICIO DE LIMPIEZA^ ^ AL CENTRO DE COMPUTO : NOT (CADA TERCER DIA)
and: CON QUE FRECUENCIA SE DA ^ ^SERVICIO DE LIMPIEZA^ ^ AL CENTRO DE COMPUTO : NOT (SEMANAL)
THEN:
RIESGO DAÑO EQUIPO 3 (ALTO)

REGLA: REGLA-46.1
IF:
CON QUE FRECUENCIA SE DA ^ ^SERVICIO DE LIMPIEZA^ ^ AL CENTRO DE COMPUTO : (DIARIO)
or: CON QUE FRECUENCIA SE DA ^ ^SERVICIO DE LIMPIEZA^ ^ AL CENTRO DE COMPUTO : (CADA TERCER DIA)
THEN:
RIESGO DAÑO EQUIPO 3 (BAJO)

REGLA: REGLA-46.2
IF:
CON QUE FRECUENCIA SE DA ^ ^SERVICIO DE LIMPIEZA^ ^ AL CENTRO DE COMPUTO : (SEMANAL)
THEN:
RIESGO DAÑO EQUIPO 3 (MEDIO)

REGLA: REGLA-47
IF:
EXISTEN CORREDORES LO SUFICIENTEMENTE AMPLIOS PARA FACILITAR UNA EVACUCION EN CASO DE SINIESTRO ? {SI}
THEN:
RIESGO EVACUACION 1 {BAJO}
ELSE:
RIESGO EVACUACION 1 {ALTO}

REGLA: REGLA-48
IF:
SE HAN COLOCADO PLANOS DE EVACUACION EN LUGARES VISIBLES DENTRO Y FUERA DEL CENTRO DE COMPUTO ? {SI}
THEN:
RIESGO EVACUACION 2 {BAJO}
ELSE:
RIESGO EVACUACION 2 {ALTO}

REGLA: REGLA-49.1
IF:
DE LOS SIGUIENTES EQUIPOS CONTRA EL FUEGO, CON CUAL CUENTA EL CENTRO DE COMPUTO : {EXTINGIDORES MANUALES}
and: LOS EXTINGUIDORES SON DE DIOXIDO DE CARBONO ? {SI}
and: SE CUENTA CON BOLSAS DE OXIGENO ? {SI}
THEN:
RIESGO ASFIXIA {BAJO}

REGLA: REGLA-49.2
IF:
DE LOS SIGUIENTES EQUIPOS CONTRA EL FUEGO, CON CUAL CUENTA EL CENTRO DE COMPUTO : {EXTINGIDORES MANUALES}
and: LOS EXTINGUIDORES SON DE DIOXIDO DE CARBONO ? {SI}
and: SE CUENTA CON BOLSAS DE OXIGENO ? {NO}
THEN:
RIESGO ASFIXIA {ALTO}
ELSE:
RIESGO ASFIXIA {BAJO}

REGLA: REGLA-50.1
IF:
EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : NOT {VIGILANTE DE ACCESO}
or: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {NO EXISTE CONTROL}
THEN:
RIESGO ACCESO PER INT {ALTO}
and: VAR CONTROL ACCESO 1 {NO}
and: VAR CONTROL ACCESO 2 {NO}
and: VAR CONTROL ACCESO 3 {NO}
and: VAR CONTROL ACCESO 4 {NO}

and: VAR CONTROL ACCESO 5 {NO}
ELSE:
RIESGO ACCESO PER INT {BAJO}
and: VAR CONTROL ACCESO 4 {SI}

REGLA: REGLA-50.2
IF: VAR CONTROL ACCESO 4 {SI}
and: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {IDENTIFICACION PERSONAL}
and: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {GAFETES}
or: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {TARJETA MAGNETICA}
or: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {CLAVES VERBALES}
or: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {HOJAS DE REGISTRO}
THEN:
RIESGO ACCESO PER INT {BAJO}
and: VAR CONTROL ACCESO 1 {NO}
ELSE:
VAR CONTROL ACCESO 1 {SI}

REGLA: REGLA-50.6
IF:
VAR CONTROL ACCESO 4 {SI}
and: VAR CONTROL ACCESO 1 {SI}
and: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {HOJAS DE REGISTRO}
and: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {TARJETA MAGNETICA}
or: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {CLAVES VERBALES}
THEN:
RIESGO ACCESO PER INT {BAJO}
and: VAR CONTROL ACCESO 5 {NO}
ELSE:
VAR CONTROL ACCESO 5 {SI}

REGLA: REGLA-50.3
IF:
VAR CONTROL ACCESO 4 {SI}
and: VAR CONTROL ACCESO 1 {SI}
and: VAR CONTROL ACCESO 5 {SI}
and: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {IDENTIFICACION PERSONAL}
or: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {TARJETA MAGNETICA}
THEN:
RIESGO ACCESO PER INT {MEDIO}

and: VAR CONTROL ACCESO 2 {NO}
ELSE:
VAR CONTROL ACCESO 2 {SI}

REGLA: REGLA-50.4
IF: VAR CONTROL ACCESO 4 {SI}
and: VAR CONTROL ACCESO 1 {SI}
and: VAR CONTROL ACCESO 5 {SI}
and: VAR CONTROL ACCESO 2 {SI}
and: RIESGO ACCESO PER INT NOT {BAJO}
and: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {GAFETES}
and: EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {HOJAS DE REGISTRO}
THEN:
RIESGO ACCESO PER INT {MEDIO}
and: VAR CONTROL ACCESO 3 {NO}
ELSE:
VAR CONTROL ACCESO 3 {SI}

REGLA: REGLA-50.5
IF:
VAR CONTROL ACCESO 1 {SI}
and: VAR CONTROL ACCESO 5 {SI}
and: VAR CONTROL ACCESO 2 {SI}
and: VAR CONTROL ACCESO 3 {SI}
THEN:
RIESGO ACCESO PER INT {ALTO}

REGLA: REGLA-51
IF:
SE PERMITE EL ACCESO A VISITANTES AL CENTRO DE COMPUTO ? {SI}
THEN:
RIESGO ACCESO VISITAS {ALTO}
and: RIESGO CTRL ACC VISITAS {BAJO}
ELSE:
RIESGO ACCESO VISITAS {BAJO}
and: RIESGO CTRL ACC VISITAS {BAJO}
and: RIESGO AUTORIZACION VIS {BAJO}
and: RIESGO FREC VISITAS {BAJO}
and: RIESGO VIGILANCIA VISITAS {BAJO}

REGLA: REGLA-52.1
IF:
RIESGO ACCESO VISITAS {ALTO}
and: EL ACCESO AL CENTRO DE COMPUTO PARA VISITANTES SE CONTROLA ATRAVES DE: {NO HAY CONTROL}
or: EL ACCESO AL CENTRO DE COMPUTO PARA VISITANTES SE CONTROLA ATRAVES DE: NOT {VIGILANTE DE ACCESO}
THEN:

RIESGO CTRL ACC VISITAS {ALTO}

REGLA: REGLA-52.2
IF:
RIESGO ACCESO VISITAS {ALTO}
and: RIESGO CTRL ACC VISITAS NOT {ALTO}
and: EL ACCESO AL CENTRO DE COMPUTO PARA VISITANTES SE CONTROLA ATRAVES DE: {GAFETES}
and: EL ACCESO AL CENTRO DE COMPUTO PARA VISITANTES SE CONTROLA ATRAVES DE: {IDENTIFICACION PERSONAL}
THEN:
RIESGO CTRL ACC VISITAS {BAJO}

REGLA: REGLA-52.3
IF:
RIESGO ACCESO VISITAS {ALTO}
and: RIESGO CTRL ACC VISITAS NOT {ALTO}
and: EL ACCESO AL CENTRO DE COMPUTO PARA VISITANTES SE CONTROLA ATRAVES DE: {IDENTIFICACION PERSONAL}
and: EL ACCESO AL CENTRO DE COMPUTO PARA VISITANTES SE CONTROLA ATRAVES DE: {HOJAS DE REGISTRO}
THEN:
RIESGO CTRL ACC VISITAS {BAJO}

REGLA: REGLA-52.4
IF:
RIESGO ACCESO VISITAS {ALTO}
and: RIESGO CTRL ACC VISITAS NOT {ALTO}
and: RIESGO CTRL ACC VISITAS NOT {BAJO}
and: EL ACCESO AL CENTRO DE COMPUTO PARA VISITANTES SE CONTROLA ATRAVES DE: {IDENTIFICACION PERSONAL}
THEN:
RIESGO CTRL ACC VISITAS {MEDIO}

REGLA: REGLA-52.5
IF:
RIESGO ACCESO VISITAS {ALTO}
and: RIESGO CTRL ACC VISITAS NOT {ALTO}
and: RIESGO CTRL ACC VISITAS NOT {BAJO}
and: EL ACCESO AL CENTRO DE COMPUTO PARA VISITANTES SE CONTROLA ATRAVES DE: {GAFETES}
and: EL ACCESO AL CENTRO DE COMPUTO PARA VISITANTES SE CONTROLA ATRAVES DE: {HOJAS DE REGISTRO}
THEN:
RIESGO CTRL ACC VISITAS {MEDIO}

REGLA: REGLA-52.6
IF:
RIESGO ACCESO VISITAS NOT {MEDIO}
and: RIESGO CTRL ACC VISITAS NOT {ALTO}

and: RIESGO CTRL ACC VISITAS NOT {BAJO}
THEN:
RIESGO CTRL ACC VISITAS {ALTO}

REGLA: REGLA-NUEVA2
IF:
EL ACCESO AL CENTRO DE COMPUTO PARA PERSONAL INTERNO SE CONTROLA ATREVES DE : {GAFETES}
or: EL ACCESO AL CENTRO DE COMPUTO PARA VISITANTES SE CONTROLA ATRAVES DE : {GAFETES}
THEN:
HAY GAFETES {SI }
ELSE:
HAY GAFETES {NO }
and: RIESGO GAFETES 1 {BAJO}
and: RIESGO GAFETES 2 {BAJO}

REGLA: REGLA-53.1
IF:
HAY GAFETES {SI }
and: SE INDICA EN LOS GAFETES EL NOMBRE DE LA EMPRESA ? {SI}
THEN:
RIESGO GAFETES 1 {MEDIO}

REGLA: REGLA-53.2
IF: HAY GAFETES {SI }
and: SE INDICA EN LOS GAFETES EL NOMBRE DE LA EMPRESA ? {NO}
THEN:
RIESGO GAFETES 1 {BAJO}

REGLA: REGLA-54.1
IF:
RIESGO ACCESO VISITAS {ALTO}
and: SE REQUIERE AUTORIZACION ESPECIAL DE ACCESO AL CENTRO DE COMPUTO PARA VISITANTES ? {SI}
THEN:
RIESGO AUTORIZACION VIS {BAJO}

REGLA: REGLA-54.2
IF:
RIESGO ACCESO VISITAS {ALTO}
and: SE REQUIERE AUTORIZACION ESPECIAL DE ACCESO AL CENTRO DE COMPUTO PARA VISITANTES ? {NO}
THEN:
RIESGO AUTORIZACION VIS {ALTO}

REGLA: REGLA-55
IF:
HAY GAFETES {SI }

and: SE DIFERENCIAN LOS GAFETES DE ACCESO AL CENTRO DE COMPUTO DEPENDIENDO DE LAS PERSONAS QUE LO PORTAN ? {SI}
THEN:
RIESGO GAFETES 2 {BAJO}

REGLA: REGLA-55.2
IF:
HAY GAFETES {SI }
and: SE DIFERENCIAN LOS GAFETES DE ACCESO AL CENTRO DE COMPUTO DEPENDIENDO DE LAS PERSONAS QUE LO PORTAN ? {NO}
THEN:
RIESGO GAFETES 2 {BAJO}

REGLA: REGLA-56.1
IF:
RIESGO ACCESO VISITAS {ALTO}
and: CON QUE FRECUENCIA SE REALIZAN RECORRIDOS POR EL CENTRO DE COMPUTO : {MENSUAL}
or: CON QUE FRECUENCIA SE REALIZAN RECORRIDOS POR EL CENTRO DE COMPUTO : {TRIMESTRAL}
THEN:
RIESGO FREC VISITAS {ALTO}

REGLA: REGLA-56.2
IF:
RIESGO ACCESO VISITAS {ALTO}
and: RIESGO FREC VISITAS NOT {ALTO}
and: CON QUE FRECUENCIA SE REALIZAN RECORRIDOS POR EL CENTRO DE COMPUTO : {SEMESTRAL}
THEN:
RIESGO FREC VISITAS {MEDIO}

REGLA: REGLA-56.3
IF:
RIESGO ACCESO VISITAS {ALTO}
and: RIESGO FREC VISITAS NOT {ALTO}
and: RIESGO FREC VISITAS NOT {MEDIO}
and: CON QUE FRECUENCIA SE REALIZAN RECORRIDOS POR EL CENTRO DE COMPUTO : {NUNCA}
THEN:
RIESGO FREC VISITAS {BAJO}
and: RIESGO VIGILANCIA VISITAS {BAJO}

REGLA: REGLA-57.1
IF:
CON QUE FRECUENCIA SE REALIZAN RECORRIDOS POR EL CENTRO DE COMPUTO : NOT {NUNCA}
and: COMO SE MANTIENEN VIGILADOS A LOS VISITANTES DURANTE EL RECORRIDO : {NO SON VIGILADOS}
THEN:

RIESGO VIGILANCIA VISITAS {ALTO}

REGLA: REGLA-57.2
IF:
CON QUE FRECUENCIA SE REALIZAN RECORRIDOS POR EL CENTRO DE COMPUTO : NOT {NUNCA}
and: COMO SE MANTIENEN VIGILADOS A LOS VISITANTES DURANTE EL RECORRIDO : NOT {NO SON VIGILADOS}
THEN:
RIESGO VIGILANCIA VISITAS {BAJO}

REGLA: REGLA-58
IF:
SE PERMITE INTRODUCIR OBJETOS PERSONALES(BOLSAS, PORTAFOLIOS, PAQUETES, ETC) AL CENTRO DE COMPUTO ? {SI}
THEN:
RIESGO OBJETOS PERS {ALTO}
ELSE:
RIESGO OBJETOS PERS {BAJO}

REGLA: REGLA-59
IF:
SE MANTIENE UN GUARDIA A LA ENTRADA DEL CENTRO DE COMPUTO LAS 24 HORAS? {SI}
THEN:
RIESGO CC VIGILADO {BAJO}
ELSE:
RIESGO CC VIGILADO {ALTO}

REGLA: REGLA-60
IF:
SE CUENTA CON PROCEDIMIENTOS, GUIAS O DOCUMENTOS DE SEGURIDAD ? {SI}
THEN:
RIESGO MANUALES SEG {BAJO}
ELSE:
RIESGO MANUALES SEG {ALTO}
and: RIESGO MANUALES ESTANDAR {BAJO }

REGLA: REGLA-61.1
IF:
RIESGO MANUALES SEG {BAJO}
and: SE ENCUENTRAN ESTANDARIZADOS ? {SI}
THEN:
RIESGO MANUALES ESTANDAR {BAJO }

REGLA: REGLA-61.2
IF:
RIESGO MANUALES SEG {BAJO}
and: SE ENCUENTRAN ESTANDARIZADOS ? {NO}
THEN:

RIESGO MANUALES ESTANDAR {ALTO}

REGLA: REGLA-62
IF: EXISTE UNA PERSONA RESPONSABLE DE TODO LO RELACIONADO CON LA SEGURIDAD DEL CENTRO DE COMPUTO ? {SI}
THEN:
RIESGO PERS RESP {BAJO}
ELSE:
RIESGO PERS RESP {ALTO}

REGLA: REGLA-63
IF:
EXISTE UNA PUBLICACION RELATIVA A LA SEGURIDAD ? {SI}
THEN:
RIESGO INF PERSONAL {BAJO}
ELSE:
RIESGO INF PERSONAL {ALTO}
and: RIESGO FREC PUBLICACION {BAJO}

REGLA: REGLA-64.1
IF:
RIESGO INF PERSONAL {BAJO}
and: CON QUE FRECUENCIA SE EMITE : {SEMESTRAL}
or: CON QUE FRECUENCIA SE EMITE : {ANUAL}
THEN:
RIESGO FREC PUBLICACION {ALTO}
ELSE:
RIESGO FREC PUBLICACION {BAJO}

REGLA: REGLA-64.2
IF:
RIESGO INF PERSONAL {BAJO}
and: RIESGO FREC PUBLICACION NOT {ALTO}
and: CON QUE FRECUENCIA SE EMITE : {AL INGRESO}
THEN:
RIESGO FREC PUBLICACION {MEDIO}
ELSE:
RIESGO FREC PUBLICACION {BAJO}

REGLA: REGLA-65
IF:
EXISTE UN PLAN EN DONDE SE SEÑALEN LOS PROCEDIMIENTOS A SEGUIR EN CASO DE DESASTRE ? {SI}
THEN:
RIESGO CONTINGENCIA {BAJO}
ELSE:
RIESGO CONTINGENCIA {ALTO}
and: RIESGO MEDIOS RECUPERACION {BAJO}

REGLA: REGLA-66.1
IF:
RIESGO CONTINGENCIA {BAJO}
and: QUE INCLUYE ESTE PLAN : NOT {PROCEDIMIETOS DE RECUPERACION PARA LA REPRODUCCION DE LA INFORMACION }
or: QUE INCLUYE ESTE PLAN : NOT {UBICACION DE LOS MEDIOS DE RESPALDO Y QUIEN CONTACTA LOS MEDIOS DE RESPALDO}
or: QUE INCLUYE ESTE PLAN : NOT {QUE ARCHIVOS O BASES DE DATOS DEBEN SER RECUPERADOS PRIMERO}
or: QUE INCLUYE ESTE PLAN : NOT {EN DONDE PUEDE SER ENCONTRADO EL EQUIPO DE REEMPLAZO Y CUAL ES SU CONFIGURACION}
or: QUE INCLUYE ESTE PLAN : NOT {EN DONDE PUEDE ENCONTRARSE EL SOFTWARE DE REEMPLAZO }
or: QUE INCLUYE ESTE PLAN : NOT {LA LOCALIZACION DE OTRO EQUIPO DE APOYO, TAL COMO GENERADORES, AIRE ACONDICIONADO, ETC}
or: QUE INCLUYE ESTE PLAN : NOT {LA ACCION A SER TOMADA EN CASO DE UN DAÑO PARCIAL INESPERADO}
THEN:
RIESGO MEDIOS RECUPERACION {ALTO}

REGLA: REGLA-66.2
IF:
RIESGO CONTINGENCIA {BAJO}
and: RIESGO MEDIOS RECUPERACION NOT {ALTO}
and: QUE INCLUYE ESTE PLAN : NOT {LA AYUDA QUE SE PUEDE ESPERAR DEL PROVEEDOR DEL EQUIPO }
or: QUE INCLUYE ESTE PLAN : NOT {PROCEDIMIENTOS PARA LA IMPOSICION DE CONTROLES EXTRAORDINARIOS DURANTE EL DESASTRE Y HASTA QUE REGRESEN LOS SISTEMAS A LA NORMALIDAD}
THEN:
RIESGO MEDIOS RECUPERACION {MEDIO}
ELSE:
RIESGO MEDIOS RECUPERACION {BAJO}

REGLA: REGLA-68
IF: LA EMPRESA HA ESTABLECIDO POLITICAS Y PROCEDIMIENTOS CON RESPECTO A LA SEGURIDAD FISICA ? {SI}
THEN:
RIESGO POLITSEG {BAJO}
ELSE:
RIESGO POLITSEG {ALTO}

REGLA: REGLA-69
IF:
LA EMPRESA DESTINA TIEMPO Y PRESUPUESTO A LOS ESFUEZOS Y ENTRENAMIENTO CON RESPECTO A LA SEGURIDAD FISICA ? {SI}
THEN:
RIESGO APOYO SEG {BAJO}
ELSE:
RIESGO APOYO SEG {ALTO}

REGLA: REGLA-70.1
IF:
LAS VENTANAS DEL CENTRO DE COMPUTO SE MANTIENEN CERRADAS LAS 24 Hrs. DEL DIA ? {NO}
THEN:
RIESGO VENTANAS {ALTO}
and: RIESGO VENTANAS ABIERTAS {ALTO}
and: PENETRACION VENTANAS {SI}

REGLA: REGLA-70.2
IF:
LAS VENTANAS DEL CENTRO DE COMPUTO SE MANTIENEN CERRADAS LAS 24 Hrs. DEL DIA ? {SI}
THEN:
RIESGO VENTANAS {ALTO}
and: RIESGO VENTANAS ABIERTAS {BAJO}
and: PENETRACION VENTANAS {NO}

REGLA: REGLA-70.3
IF:
LAS VENTANAS DEL CENTRO DE COMPUTO SE MANTIENEN CERRADAS LAS 24 Hrs. DEL DIA ? {NO HAY VENTANAS}
THEN:
RIESGO VENTANAS {BAJO}
and: RIESGO VENTANAS ABIERTAS {BAJO}
and: PENETRACION VENTANAS {NO}

REGLA: REGLA-71
IF:
SE CUENTA CON UN DETECTOR DE METALES A LA ENTRADA DEL CENTRO DE COMPUTO ? {SI}
THEN:
RIESGO DETEC METALES {BAJO}
ELSE:
RIESGO DETEC METALES {ALTO}

REGLA: REGLA-72
IF:
EL EQUIPO DE PROCESAMIENTO DE DATOS ESTA ASEGURADO ? {SI}
THEN:
RIESGO SEGURO EQUIPO {BAJO}
and: RIESGO COBERTURA SEGUROS {BAJO}
ELSE:
RIESGO SEGURO EQUIPO {ALTO}
and: RIESGO COBERTURA SEGUROS {BAJO}
and: RIESGO VENCIM POLIZAS {BAJO}
and: RIESGO COSTO SEG EQUIPO {BAJO}
and: RIESGO AMPARO CAUSA SINIESTRO {BAJO}

REGLA: REGLA-73.1
IF:
RIESGO SEGURO EQUIPO {BAJO}
and: QUE CUBRE EL SEGURO : NOT {EQUIPO DE PROCESAMIENTO DE DATOS.}
THEN:
RIESGO COBERTURA SEGUROS {ALTO}

REGLA: REGLA-73.2
IF:
RIESGO SEGURO EQUIPO {BAJO}
and: RIESGO COBERTURA SEGUROS NOT {ALTO}
and: QUE CUBRE EL SEGURO : NOT {SOFTWARE}
THEN:
RIESGO COBERTURA SEGUROS {MEDIO}
ELSE:
RIESGO COBERTURA SEGUROS {BAJO}

REGLA: REGLA-74.1
IF:
RIESGO SEGURO EQUIPO {BAJO}
and: SE VERIFICAN CONTINUAMENTE LAS FECHAS DE VENCIMIENTO DE LAS POLIZAS ? {SI}
THEN:
RIESGO VENCIM POLIZAS {BAJO}

REGLA: REGLA-74.2
IF:
RIESGO SEGURO EQUIPO {BAJO}
and: SE VERIFICAN CONTINUAMENTE LAS FECHAS DE VENCIMIENTO DE LAS POLIZAS ? {NO}
THEN:
RIESGO VENCIM POLIZAS {ALTO}

REGLA: REGLA-75.1
IF:
RIESGO SEGURO EQUIPO {BAJO}
and: LA POLIZA DEL EQUIPO CUBRE SU COSTO : {AL PRECIO DEL EQUIPO CUANDO SE ADQUIERE EL SEGURO}
THEN:
RIESGO COSTO SEG EQUIPO {ALTO}

REGLA: REGLA-75.2
IF:
RIESGO SEGURO EQUIPO {BAJO}
and: LA POLIZA DEL EQUIPO CUBRE SU COSTO : {AL PRECIO DE COMPRA DEL MISMO, AL MOMENTO DEL SINIESTRO}
THEN:
RIESGO COSTO SEG EQUIPO {BAJO}

REGLA: REGLA-76.1
IF:
RIESGO SEGURO EQUIPO {BAJO}
and: LA POLIZA AMPARA AL EQUIPO EN CASO DE DAÑOS CAUSADOS POR: {AMBOS}
THEN:
RIESGO AMPARO CAUSA SINIESTRO {BAJO}
ELSE:
RIESGO AMPARO CAUSA SINIESTRO {ALTO}

REGLA: ACUMULADO-1
IF:
ACCESO PREGUNTADO {SI}
and: ROBO PREGUNTADO {SI}
and: SABOTAJE PREGUNTADO {SI}
and: INTER Y DESAS PREGUNTADO {SI}
and: OPERACION PREGUNTADO {SI}
and: GENERALES PREGUNTADO {SI}
THEN:
SI - Confidence = 1
ELSE:
SI - Confidence = 0

REGLA: ACUMULADO-1.1
IF:
RIESGO ACCESO CENTRO COMPUTO {ALTO}
or: RIESGO ACCESO CENTRO COMPUTO {MEDIO}
or: RIESGO ACCESO CENTRO COMPUTO {BAJO}
THEN:
ACCESO PREGUNTADO {SI}
ELSE:
ACCESO PREGUNTADO {NO}

REGLA: ACUMULADO-1.2
IF:
RIESGO ROBO {ALTO}
or: RIESGO ROBO {MEDIO}
or: RIESGO ROBO {BAJO}
THEN:
ROBO PREGUNTADO {SI}
ELSE:
ROBO PREGUNTADO {NO}

REGLA: ACUMULADO-1.3
IF:
RIESGO SABOTAJE {ALTO}
or: RIESGO SABOTAJE {MEDIO}
or: RIESGO SABOTAJE {BAJO}

THEN:
SABOTAJE PREGUNTADO {SI}

ELSE:
SABOTAJE PREGUNTADO {NO}

REGLA: ACUMULADO-1.4
IF: RIESGO INTERRUPCIONES Y DESASTRES {ALTO}
or: RIESGO INTERRUPCIONES Y DESASTRES {MEDIO}
or: RIESGO INTERRUPCIONES Y DESASTRES {BAJO}
THEN:
INTER Y DESAS PREGUNTADO {SI}
ELSE:
INTER Y DESAS PREGUNTADO {NO}

REGLA: ACUMULADO-1.5
IF:
RIESGO OPERACION {ALTO}
or: RIESGO OPERACION {MEDIO}
or: RIESGO OPERACION {BAJO}

THEN:
OPERACION PREGUNTADO {SI}
ELSE:
OPERACION PREGUNTADO {NO}

REGLA: ACUMULADO-1.6
IF:
RIESGO GENERALES {ALTO}
or: RIESGO GENERALES {MEDIO}
or: RIESGO GENERALES {BAJO}
THEN:
GENERALES PREGUNTADO {SI}
ELSE:
GENERALES PREGUNTADO {NO}

REGLA: REGLA-77.1
IF:
RIESGO INCENDIO 1 {ALTO}
or: RIESGO INCENDIO 2 {ALTO}
or: RIESGO CABLEADO {ALTO}
or: RIESGO FALLA DETEC INCENDIO {ALTO }
or: RIESGO FALLA ALARM INCENDIO {ALTO}
or: RIESGO FALLA DIST ELECT {ALTO}
or: RIESGO VOLTAJE {ALTO}
THEN:
RIESGO PREVENIR INCEND {ALTO}
ELSE:
RIESGO PREVENIR INCEND {BAJO}

REGLA: REGLA-78
IF:
RIESGO INCENDIO 1 {MEDIO}

and: RIESGO PROPAGACION INCENDIO (ALTO)
THEN:
RIESGO PREVENIR INCEND (ALTO)
ELSE:
RIESGO PREVENIR INCEND (BAJO)

REGLA: REGLA-80
IF:
RIESGO PROPAGACION INCENDIO (ALTO)
and: RIESGO INCENDIO 5 (ALTO)
and: RIESGO BASURA (ALTO)
and: RIESGO VOLTAJE (ALTO)
THEN:
RIESGO PREVENIR INCEND (ALTO)
ELSE:
RIESGO PREVENIR INCEND (BAJO)

REGLA: REGLA-77.2
IF:
RIESGO PREVENIR INCEND NOT (ALTO)
and: RIESGO INCENDIO 1 (MEDIO)
or: RIESGO PROPAGACION INCENDIO (ALTO)
or: RIESGO INCENDIO 5 (ALTO)
or: RIESGO FALLA ALARM INCENDIO (MEDIO)
or: RIESGO FALLA DIST ELECT (MEDIO)
or: RIESGO BASURA (ALTO)
or: RIESGO BASURA (MEDIO)
THEN:
RIESGO PREVENIR INCEND (MEDIO)

REGLA: REGLA-79
IF:
RIESGO PREVENIR INCEND NOT (ALTO)
and: RIESGO FALLA DETEC INCENDIO (MEDIO)
and: RIESGO FALLA ALARM INCENDIO (MEDIO)
and: RIESGO FALLA DIST ELECT (MEDIO)
THEN:
RIESGO PREVENIR INCEND (ALTO)

REGLA: REGLA-81
IF:
RIESGO INCENDIO 3 (ALTO)
or: RIESGO PREV INCENDIO (ALTO)
or: RIESGO INCENDIO 4 (ALTO)
or: RIESGO ALARMA INCENDIO (ALTO)
or: RIESGO ACCION FUEGO (ALTO)
or: RIESGO ASFIXIA (ALTO)
THEN:
RIESGO COMBATIR INCEND (ALTO)
ELSE:

RIESGO COMBATIR INCEND (BAJO)

REGLA: REGLA-82
IF:
RIESGO DETEC SEÑALAM (MEDIO)
and: RIESGO ACCION FUEGO (MEDIO)
THEN:
RIESGO COMBATIR INCEND (ALTO)
ELSE:
RIESGO COMBATIR INCEND (BAJO)

REGLA: REGLA-81.2
IF:
RIESGO COMBATIR INCEND NOT (ALTO)
and: RIESGO FALSA ALARMA (ALTO)
or: RIESGO DETECCION INCENDIO (ALTO)
or: RIESGO DETEC SEÑALAM (MEDIO)
or: RIESGO ACCION FUEGO (MEDIO)
THEN:
RIESGO COMBATIR INCEND (MEDIO)

REGLA: REGLA-83
IF: RIESGO PENETRABLES 1 (ALTO)
or: RIESGO ENTRADA SUBREPTICIA (ALTO)
or: RIESGO PENETRABLE 2 (ALTO)
or: RIESGO ACCESO 1 (ALTO)
or: RIESGO ACCESO DUCTOS (ALTO)
or: RIESGO GRALES VISITAS (ALTO)
THEN:
RIESGO PENETRACION (ALTO)
ELSE:
RIESGO PENETRACION (BAJO)

REGLA: REGLA-84
IF:
PENETRACION VENTANAS (SI)
THEN:
RIESGO PENETRACION (ALTO)
ELSE:
RIESGO PENETRACION (BAJO)

REGLA: REGLA-85
IF:
RIESGO PENETRACION NOT (ALTO)
and: RIESGO VENTANAS (ALTO)
and: RIESGO VENTANAS ABIERTAS (BAJO)
or: RIESGO PENETRACION NOT (ALTO)
and: RIESGO VENTANAS (BAJO)
and: RIESGO VENTANAS ABIERTAS (ALTO)
THEN:

RIESGO PENETRACION {MEDIO}

REGLA: REGLA-87
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? NOT {PC's}
and: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? NOT {REDES}
and: RIESGO PISO FALSO {ALTO}
or: RIESGO ALTURA PISO {ALTO}
THEN:
RIESGO GRALES PISO FAL {ALTO}
ELSE:
RIESGO GRALES PISO FAL {BAJO}

REGLA: REGLA-86
IF:
QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MINIS}
or: QUE TIPO DE EQUIPO SE TIENE INSTALADO EN EL CENTRO DE COMPUTO ? {MAIN FRAMES}
and: RIESGO GRALES PISO FAL NOT {ALTO}
and: RIESGO ALTURA PISO {MEDIO}
or: RIESGO MTO PISO FALSO {MEDIO}
THEN:
RIESGO GRALES PISO FAL {MEDIO}

REGLA: REGLA-89
IF:
RIESGO INUNDACION {ALTO}
THEN:
RIESGO GRALES INUNDA {ALTO}
ELSE:
RIESGO GRALES INUNDA {BAJO}

REGLA: REGLA-88
IF: RIESGO GRALES INUNDA NOT {ALTO}
and: RIESGO FILTRACION {ALTO}
THEN:
RIESGO GRALES INUNDA {MEDIO}

REGLA: REGLA-91.1
IF:
RIESGO ACCESO VISITAS {ALTO}
and: RIESGO OBJETOS PERS {ALTO}
and: RIESGO DETEC METALES {ALTO}
THEN:
RIESGO GRALES VISITAS {ALTO}
ELSE:
RIESGO GRALES VISITAS {BAJO}

REGLA: REGLA-91.2
IF:
RIESGO CTRL ACC VISITAS {ALTO}
or: RIESGO AUTORIZACION VIS {ALTO}
or: RIESGO FREC VISITAS {ALTO}
or: RIESGO VIGILANCIA VISITAS {ALTO}

THEN:
RIESGO GRALES VISITAS {ALTO}
ELSE:
RIESGO GRALES VISITAS {BAJO}

REGLA: REGLA-92
IF:
RIESGO ACCESO VISITAS {MEDIO}
and: RIESGO CTRL ACC VISITAS {MEDIO}
THEN:
RIESGO GRALES VISITAS {ALTO}
ELSE:
RIESGO GRALES VISITAS {BAJO}

REGLA: REGLA-93
IF:
RIESGO CTRL ACC VISITAS {MEDIO}
and: RIESGO FREC VISITAS {MEDIO}
THEN:
RIESGO GRALES VISITAS {ALTO}
ELSE:
RIESGO GRALES VISITAS {BAJO}

REGLA: REGLA-90
IF:
RIESGO GRALES VISITAS NOT {ALTO}
and: RIESGO ACCESO VISITAS {ALTO}
or: RIESGO CTRL ACC VISITAS {MEDIO}
or: RIESGO FREC VISITAS {MEDIO}
or: RIESGO OBJETOS PERS {ALTO}
or: RIESGO DETEC METALES {ALTO}
THEN:
RIESGO GRALES VISITAS {MEDIO}

REGLA: REGLA-94
IF:
RIESGO CABLEADO {ALTO}
or: RIESGO DIST ELECTRICA {ALTO}
or: RIESGO VOLTAJE {ALTO}
or: RIESGO OPERACION DIST ELECT {ALTO}
or: RIESGO PANEL EQUIPO {ALTO}
THEN:
RIESGO GRALES ELECT {ALTO}

ELSE:
RIESGO GRALES ELECT {BAJO}

REGLA: REGLA-95
IF: RIESGO GRALES ELECT NOT {ALTO}
and: RIESGO FALLA DIST ELECT {ALTO}
THEN:
RIESGO GRALES ELECT {MEDIO}

REGLA: REGLA-97.1
IF:
RIESGO ACCESO 1 {ALTO}
or: RIESGO ACCESO PER INT {ALTO}
or: RIESGO CTRL ACC VISITAS {ALTO}
or: RIESGO CC VIGILADO {ALTO}
THEN:
RIESGO GRALES ACCESO {ALTO}
ELSE:
RIESGO GRALES ACCESO {BAJO}

REGLA: REGLA-97.2
IF:
RIESGO GRALES ACCESO NOT {ALTO}
and: RIESGO CTRL ACC VISITAS {MEDIO}
and: RIESGO DETEC METALES {ALTO}
THEN:
RIESGO GRALES ACCESO {ALTO}

REGLA: REGLA-97
IF:
RIESGO GRALES ACCESO NOT {ALTO}
and: RIESGO ACCESO PER INT {MEDIO}
and: RIESGO CTRL ACC VISITAS {MEDIO}
THEN:
RIESGO GRALES ACCESO {ALTO}
ELSE:
RIESGO GRALES ACCESO {BAJO}

REGLA: REGLA-96
IF:
RIESGO GRALES ACCESO NOT {ALTO}
and: RIESGO DETEC METALES {BAJO}
and: RIESGO ACCESO PER INT {MEDIO}
and: RIESGO CTRL ACC VISITAS {BAJO}
or: RIESGO GRALES ACCESO NOT {ALTO}
and: RIESGO DETEC METALES {BAJO}
and: RIESGO ACCESO PER INT {BAJO}
and: RIESGO CTRL ACC VISITAS {MEDIO}
or: RIESGO GRALES ACCESO NOT {ALTO}
and: RIESGO ACCESO PER INT {BAJO}

and: RIESGO DETEC METALES (ALTO)
and: RIESGO CTRL ACC VISITAS (BAJO)
THEN:
RIESGO GRALES ACCESO (MEDIO)

REGLA: REGLA-99
IF:
RIESGO SALIDA EMERGENCIA (ALTO)
or: RIESGO FALLA SAL EMER (ALTO)
THEN:
RIESGO GRALES EVACUACION (ALTO)
ELSE:
RIESGO GRALES EVACUACION (BAJO)

REGLA: REGLA-100
IF:
RIESGO FALLA SAL EMER (MEDIO)
and: RIESGO EVACUACION 2 (ALTO)
THEN:
RIESGO GRALES EVACUACION (ALTO)
ELSE:
RIESGO GRALES EVACUACION (BAJO)

REGLA: REGLA-98
IF:
RIESGO GRALES EVACUACION NOT (ALTO)
and: RIESGO FALLA SAL EMER (MEDIO)
or: RIESGO EVACUACION 2 (ALTO)
or: RIESGO EVACUACION 1 (ALTO)
THEN:
RIESGO GRALES EVACUACION (MEDIO)

REGLA: REGLA-102
IF:
RIESGO PISO FALSO (ALTO)
or: RIESGO DAÑO EQUIPO (ALTO)
or: RIESGO AIRE ACOND (ALTO)
or: RIESGO VOLTAJE (ALTO)
THEN:
RIESGO DAÑO EQ MAT (ALTO)
ELSE:
RIESGO DAÑO EQ MAT (BAJO)

REGLA: REGLA-103
IF:
RIESGO DAÑO EQ MAT NOT (ALTO)
and: RIESGO FILTRACION (ALTO)
THEN:
RIESGO DAÑO EQ MAT (MEDIO)

REGLA: REGLA-104.1
IF:
RIESGO DAÑO EQUIPO 2 {ALTO}
THEN:
RIESGO DAÑO EQ HUM {ALTO }
ELSE:
RIESGO DAÑO EQ HUM {BAJO}

REGLA: REGLA-104.2
IF:
RIESGO OBJETOS PERS {ALTO}
and: RIESGO DETEC METALES {ALTO}
THEN:
RIESGO DAÑO EQ HUM {ALTO }
ELSE:
RIESGO DAÑO EQ HUM {BAJO}

REGLA: REGLA-103
IF:
RIESGO DAÑO EQ HUM NOT {ALTO }
and: RIESGO DAÑO EQUIPO 3 {ALTO }
or: RIESGO OBJETOS PERS {ALTO}
or: RIESGO DETEC METALES {ALTO}
THEN:
RIESGO DAÑO EQ HUM {MEDIO}

REGLA: REGLA-106
IF:
RIESGO DAÑO EQ HUM {ALTO }
or: RIESGO OPERACION DIST ELECT {ALTO}
or: PENETRACION VENTANAS {SI}
or: RIESGO DAÑO DUCTOS {ALTO}
or: RIESGO ACCESO DUCTOS {ALTO}
THEN:
RIESGO GRALES SABOTAJE {ALTO}
ELSE:
RIESGO GRALES SABOTAJE {BAJO}

REGLA: REGLA-105
IF:
RIESGO GRALES SABOTAJE NOT {ALTO}
and: RIESGO PENETRACION {MEDIO}
or: RIESGO OBJETOS PERS {ALTO}
or: RIESGO DETEC METALES {ALTO}
THEN:
RIESGO GRALES SABOTAJE {MEDIO}

REGLA: REGLA-108
IF:
RIESGO AIRE ACOND {ALTO}

or: RIESGO CTRL TEMP HUM (ALTO)
THEN:
RIESGO GRALES AIRE (ALTO)
ELSE:
RIESGO GRALES AIRE (BAJO)

REGLA: REGLA-107
IF:
RIESGO GRALES AIRE NOT (ALTO)
and: RIESGO FALLA AIRE ACOND (ALTO)
or: RIESGO FILTRO AIRE (ALTO)
THEN:
RIESGO GRALES AIRE (MEDIO)

REGLA: REGLA-110
IF: RIESGO SUMIN ENERGIA (ALTO)
or: RIESGO INTERRUP EQUIPO (ALTO)
THEN:
RIESGO GRALES SUMINIST (ALTO)
ELSE:
RIESGO GRALES SUMINIST (BAJO)

REGLA: REGLA-109
IF:
RIESGO GRALES SUMINIST NOT (ALTO)
and: RIESGO FALLA SUMIN ENERGIA (ALTO)
or: RIESGO INTERRUP EQUIPO (MEDIO)
THEN:
RIESGO GRALES SUMINIST (MEDIO)

REGLA: REGLA-111
IF:
RIESGO GRALES TEMBLOR NOT (ALTO)
and: RIESGO TEMBLOR (ALTO)
and: RIESGO TEMBLOR EQUIPO (BAJO)
or: RIESGO GRALES TEMBLOR NOT (ALTO)
and: RIESGO TEMBLOR (BAJO)
and: RIESGO TEMBLOR EQUIPO (ALTO)
THEN:
RIESGO GRALES TEMBLOR (MEDIO)

REGLA: REGLA-114
IF:
RIESGO GAFETES 2 (ALTO)
THEN:
RIESGO GRALES GAFETES (ALTO)
ELSE:
RIESGO GRALES GAFETES (BAJO)

REGLA: REGLA-113
IF:
RIESGO GRALES GAFETES NOT {ALTO}
and: RIESGO GAFETES 1 {MEDIO}
THEN:
RIESGO GRALES GAFETES {MEDIO}

REGLA: REGLA-116
IF:
RIESGO MANUALES SEG {ALTO}
or: RIESGO POLIT SEG {ALTO}
THEN:
RIESGO GRALES DOCUM {ALTO}
ELSE:
RIESGO GRALES DOCUM {BAJO}

REGLA: REGLA-115
IF: RIESGO GRALES DOCUM NOT {ALTO}
and: RIESGO MANUALES ESTANDAR {ALTO}
or: RIESGO INF PERSONAL {ALTO}
or: RIESGO FREC PUBLICACION {ALTO}
THEN:
RIESGO GRALES DOCUM {MEDIO}

REGLA: REGLA-117
IF:
RIESGO PERS RESP {ALTO}
or: RIESGO POLIT SEG {ALTO}
or: RIESGO APOYO SEG {ALTO}
THEN:
RIESGO GRALES ADMIN {ALTO}
ELSE:
RIESGO GRALES ADMIN {BAJO}

REGLA: REGLA-119
IF:
RIESGO CONTINGENCIA {ALTO}
or: RIESGO MEDIOS RECUPERACION {ALTO}
THEN:
RIEGO GRALES CONTING {ALTO}
ELSE:
RIEGO GRALES CONTING {BAJO}

REGLA: REGLA-118
IF:
RIEGO GRALES CONTING NOT {ALTO}
and: RIESGO MEDIOS RECUPERACION {MEDIO}
THEN:
RIEGO GRALES CONTING {MEDIO}

REGLA: REGLA-121.1
IF:
RIESGO SEGURO EQUIPO {ALTO}
or: RIESGO COBERTURA SEGUROS {ALTO}
or: RIESGO COSTO SEG EQUIPO {ALTO}
or: RIESGO AMPARO CAUSA SINIESTRO {ALTO}
THEN:
RIESGO GRALES SEGUROS {ALTO}
ELSE:
RIESGO GRALES SEGUROS {BAJO}

REGLA: REGLA-121.2
IF:
RIESGO COBERTURA SEGUROS {MEDIO}
and: RIESGO VENCIM POLIZAS {ALTO}
THEN:
RIESGO GRALES SEGUROS {ALTO}
ELSE:
RIESGO GRALES SEGUROS {BAJO}

REGLA: REGLA-120
IF:
RIESGO GRALES SEGUROS NOT {ALTO}
and: RIESGO COBERTURA SEGUROS {MEDIO}
and: RIESGO VENCIM POLIZAS {BAJO}
or: RIESGO GRALES SEGUROS NOT {ALTO}
and: RIESGO COBERTURA SEGUROS NOT {MEDIO}
and: RIESGO VENCIM POLIZAS {ALTO}
THEN:
RIESGO GRALES SEGUROS {MEDIO}

REGLA: REGLA-124.1
IF:
RIESGO GRALES ACCESO {ALTO}
THEN:
RIESGO ACCESO CENTRO COMPUTO {ALTO}
and: GENERALES ACCESO ALTO {SI}
ELSE:
RIESGO ACCESO CENTRO COMPUTO {BAJO}
and: GENERALES ACCESO ALTO {NO}

REGLA: REGLA-124.2
IF:
RIESGO GRALES VISITAS {ALTO}
and: RIESGO GRALES ACCESO {MEDIO}
THEN:
RIESGO ACCESO CENTRO COMPUTO {ALTO}
and: 85 Y 87 {SI}
ELSE:
RIESGO ACCESO CENTRO COMPUTO {BAJO}

and: 85 Y 87 {NO}

REGLA: REGLA-124.1
IF:
RIESGO GRALES VISITAS {MEDIO}
and: RIESGO GRALES ACCESO {MEDIO}
and: RIESGO GRALES GAFETES {ALTO}
or: RIESGO GRALES GAFETES {MEDIO}
THEN:
RIESGO ACCESO CENTRO COMPUTO {ALTO}
ELSE:
RIESGO ACCESO CENTRO COMPUTO {BAJO}

REGLA: REGLA-122
IF:
RIESGO ACCESO CENTRO COMPUTO NOT {ALTO}
and: RIESGO GRALES VISITAS {ALTO}
or: RIESGO GRALES GAFETES {ALTO}
THEN:
RIESGO ACCESO CENTRO COMPUTO {MEDIO}
and: T RIESGO ACCESO MEDIO

REGLA: REGLA-123
IF:
RIESGO ACCESO CENTRO COMPUTO NOT {ALTO}
and: RIESGO GRALES VISITAS {MEDIO}
and: RIESGO GRALES ACCESO NOT {MEDIO}
and: RIESGO GRALES GAFETES NOT {MEDIO}
or: RIESGO ACCESO CENTRO COMPUTO NOT {ALTO}
and: RIESGO GRALES VISITAS NOT {MEDIO}
and: RIESGO GRALES ACCESO {MEDIO}
and: RIESGO GRALES GAFETES NOT {MEDIO}
or: RIESGO ACCESO CENTRO COMPUTO NOT {ALTO}
and: RIESGO GRALES VISITAS NOT {MEDIO}
and: RIESGO GRALES ACCESO NOT {MEDIO}
and: RIESGO GRALES GAFETES {MEDIO}
THEN:
RIESGO ACCESO CENTRO COMPUTO {MEDIO}

REGLA: REGLA-126.1
IF:
RIESGO PENETRACION {ALTO}
or: GENERALES ACCESO ALTO {SI}
THEN:
RIESGO ROBO {ALTO}
ELSE:
RIESGO ROBO {BAJO}

REGLA: REGLA-126.2
IF: 85 Y 87 {SI}

THEN:
RIESGO ROBO (ALTO)
ELSE:
RIESGO ROBO (BAJO)

REGLA: REGLA-126.3
IF:
RIESGO PENETRACION (MEDIO)
and: RIESGO GRALES ACCESO (MEDIO)
and: RIESGO GRALES VISITAS (ALTO)
or: RIESGO GRALES VISITAS (MEDIO)
THEN:
RIESGO ROBO (ALTO)
ELSE:
RIESGO ROBO (BAJO)

REGLA: REGLA-125.1
IF:
RIESGO ROBO NOT (ALTO)
and: RIESGO GRALES VISITAS (ALTO)
or: RIESGO GRALES VISITAS (MEDIO)
THEN:
RIESGO ROBO (MEDIO)

REGLA: REGLA-125.2
IF:
RIESGO ROBO NOT (ALTO)
and: RIESGO PENETRACION (MEDIO)
and: RIESGO GRALES ACCESO NOT (MEDIO)
or: RIESGO ROBO NOT (ALTO)
and: RIESGO PENETRACION NOT (MEDIO)
and: RIESGO GRALES ACCESO (MEDIO)
THEN:
RIESGO ROBO (MEDIO)

REGLA: REGLA-128
IF:
RIESGO PENETRACION (ALTO)
or: RIESGO GRALES VISITAS (ALTO)
or: RIESGO GRALES SABOTAJE (ALTO)
THEN:
RIESGO SABOTAJE (ALTO)
ELSE:
RIESGO SABOTAJE (BAJO)

REGLA: REGLA-127
IF:
RIESGO SABOTAJE NOT (ALTO)
and: RIESGO PENETRACION (MEDIO)
or: RIESGO GRALES VISITAS (MEDIO)

or: RIESGO GRALES ELECT {MEDIO}
or: RIESGO GRALES SABOTAJE {MEDIO}
or: RIESGO GRALES ELECT {ALTO}
THEN:
RIESGO SABOTAJE {MEDIO}

REGLA: REGLA-130
IF:
RIESGO PREVENIR INCEND {ALTO}
or: RIESGO COMBATIR INCEND {ALTO}
or: RIESGO GRALES INUNDA {ALTO}
or: RIESGO GRALES VISITAS {ALTO}
or: RIESGO GRALES ELECT {ALTO}
or: RIESGO DAÑO EQ MAT {ALTO}
or: RIESGO GRALES AIRE {ALTO}
or: RIESGO GRALES SUMINIST {ALTO}
or: RIESGO GRALES TEMBLOR {ALTO}
or: GENERALES ACCESO ALTO {SI}
THEN:
RIESGO INTERRUPCIONES Y DESASTRES {ALTO}
ELSE:
RIESGO INTERRUPCIONES Y DESASTRES {BAJO}

REGLA: REGLA-129.1
IF:
RIESGO INTERRUPCIONES Y DESASTRES NOT {ALTO}
and: RIESGO PENETRACION {ALTO}
or: RIESGO GRALES PISO FAL {ALTO}
or: RIESGO DAÑO EQ HUM {ALTO }
or: RIESGO GRALES SABOTAJE {ALTO}
THEN:
RIESGO INTERRUPCIONES Y DESASTRES {MEDIO}

REGLA: REGLA-129.2
IF:
RIESGO INTERRUPCIONES Y DESASTRES NOT {ALTO}
and: RIESGO PREVENIR INCEND {MEDIO}
or: RIESGO COMBATIR INCEND {MEDIO}
or: RIESGO PENETRACION {MEDIO}
or: RIESGO GRALES PISO FAL {MEDIO}
or: RIESGO GRALES INUNDA {MEDIO}
THEN:
RIESGO INTERRUPCIONES Y DESASTRES {MEDIO}

REGLA: REGLA-129.3
IF:
RIESGO INTERRUPCIONES Y DESASTRES NOT {ALTO}
and: RIESGO GRALES VISITAS {MEDIO}
or: RIESGO GRALES ELECT {MEDIO}
or: RIESGO DAÑO EQ MAT {MEDIO}

or: RIESGO DAÑO EQ HUM (MEDIO)
or: RIESGO GRALES SABOTAJE (MEDIO)
THEN:
RIESGO INTERRUPCIONES Y DESASTRES (MEDIO)

REGLA: REGLA-129.4
IF:
RIESGO INTERRUPCIONES Y DESASTRES NOT (ALTO)
and: RIESGO GRALES ACCESO (MEDIO)
or: RIESGO GRALES AIRE (MEDIO)
or: RIESGO GRALES SUMINIST (MEDIO)
or: RIESGO FILTRACION (MEDIO)
THEN:
RIESGO INTERRUPCIONES Y DESASTRES (MEDIO)

REGLA: REGLA-132.1
IF:
RIESGO GRALES DOCUM (ALTO)
or: RIESGO GRALES ADMIN (ALTO)
THEN:
RIESGO OPERACION (ALTO)
ELSE:
RIESGO OPERACION (BAJO)

REGLA: REGLA-134.1
IF:
RIESGO GRALES EVACUACION (ALTO)
or: RIESGO GRALES ADMIN (ALTO)
or: RIEGO GRALES CONTING (ALTO)
or: RIESGO GRALES SEGUROS (ALTO)
THEN:
RIESGO GENERALES (ALTO)
ELSE:
RIESGO GENERALES (BAJO)

REGLA: REGLA-135
IF:
RIEGO GRALES CONTING (MEDIO)
and: RIESGO GRALES SEGUROS (MEDIO)
THEN:
RIESGO GENERALES (ALTO)
ELSE:
RIESGO GENERALES (BAJO)

REGLA: REGLA-131
IF:
RIESGO OPERACION NOT (ALTO)
and: RIESGO GENERALES NOT (ALTO)
and: RIESGO GRALES DOCUM (MEDIO)
and: RIESGO GRALES ADMIN NOT (MEDIO)

or: RIESGO OPERACION NOT {ALTO}
and: RIESGO GENERALES NOT {ALTO}
and: RIESGO GRALES ADMIN {MEDIO}
and: RIESGO GRALES DOCUM NOT {MEDIO}
THEN:
RIESGO OPERACION {MEDIO}
and: RIESGO GENERALES {MEDIO}

REGLA: REGLA-133
IF:
RIESGO GENERALES NOT {ALTO}
and: RIESGO DAÑO EQ HUM {ALTO }
or: RIESGO GRALES GAFETES {ALTO}
or: RIESGO GRALES DOCUM {ALTO}
or: RIESGO GRALES EVACUACION {MEDIO}
or: RIESGO DAÑO EQ HUM {MEDIO}
or: RIESGO GRALES GAFETES {MEDIO}
or: RIEGO GRALES CONTING {MEDIO}
or: RIESGO GRALES SEGUROS {MEDIO}
THEN:
RIESGO GENERALES {MEDIO}

RELACION DE RIESGOS

RIESGOS PARA LA EVALUACION DE PREGUNTAS

NUM. DE RIESGO	NOMBRE DEL RIESGO
1	Riesgo-Incendio-1
2	Riesgo-Penetrables-1
3	Riesgo-Piso-Falso
4	Riesgo-Entrada-Subrepticia
5	Riesgo-Penetrables-2
6	Riesgo-Inundación
7	Riesgo-Incendio-2
8	Ductos-Externos
9	Riesgo-Filtración
10	Riesgo-de-Cableado
11	Riesgo-Altura-Piso
12	Riesgo-Acceso-1
13	Riesgo-Salida-Emergencia
14	Riesgo-Incendio-3
15	Riesgo-Daño-Equipo-1
16	Riesgo-Prev-Incendio
17	Riesgo-Falsa-Alarma
18	Riesgo-Sabotaje-1
19	Riesgo-Detec-Señalam
20	Riesgo-Propagación-Incendio
21	Riesgo-Mto-Piso-Falso
22	Riesgo-Daño-Equipo-2
23	Riesgo-Aire-Acond
24	Riesgo-Incendio-4
25	Riesgo-Alarma-Incendio
26	Riesgo-Detección-Incendio
27	Riesgo-Incendio-5
28	Riesgo-Dist-Eléctrica
29	Riesgo-Sumin-Energía
30	Riesgo-Falla-Detec-Incendio
31	Riesgo-Falla-Alarm-Incendio
32	Riesgo-Falla-Sal-Emer
33	Riesgo-Falla-Dist-Elect
34	Riesgo-Falla-Aire-Acond
35	Riesgo-Falla-Sumin-Energía
36	Riesgo-Basura
37	Riesgo-Acción-Fuego
38	Riesgo-Voltaje
39	Riesgo-Interrup-Equipo
40	Riesgo-Operación-Dist-Elect
41	Riesgo-Panel-Equipo

NUM. DE RIESGO	NOMBRE DEL RIESGO
42	Riesgo-Ctrl-Temp-Hum
43	Riesgo-Filtro-Aire
44	Riesgo-Daño-Ductos
45	Riesgo-Acceso-Ductos
46	Riesgo-Temblor
47	Riesgo-Temblor-Equipo
48	Riesgo-Daño-Equipo-3
49	Riesgo-Evacuación-1
50	Riesgo-Evacuación-2
51	Riesgo-Asfixia
52	Riesgo-Acceso-PI
53	Riesgo-Acceso-Visitas
54	Riesgo-Ctrl-Acc-Visitas
55	Riesgo-Gafetes-1
56	Riesgo-Autorización-Vis
57	Riesgo-Gafetes-2
58	Riesgo-Frec-Visitas
59	Riesgo-Vigilancia-Visitas
60	Riesgo-Objetos-Pers
61	Riesgo-CC-Vigilado
62	Riesgo-Manuales-Seg
63	Riesgo-Manuales-Estandar
64	Riesgo-Pers-Resp
65	Riesgo-Inf-Personal
66	Riesgo-Frec-Publicación
67	Riesgo-Contingencia
68	Riesgo-Medios-Recuperación
69	Riesgo-Equipo-Com
70	Riesgo-Polit-Seg
71	R iesgo-Apoyo-Seg
72	Riesgo-Ventanas
73	Riesgo-Ventanas-Abiertas
74	Riesgo-Detec-Metales
75	Riesgo-Seguro-Equipo
76	Riesgo-Cobertura-Seguros
77	Riesgo-Vencim-Polizas
78	Riesgo-Costo-Seg-Equipo
79	Riesgo-Amparo-Causa-Siniestro

RIESGOS DERIVADOS DE LA EVALUACION DE PREGUNTAS

NUM. RIESGO	NOMBRE RIESGO	RIESGOS DE LOS QUE SE DERIVA
80	Riesgo-Prevenir-Incend	1,7,10,20,27,30,31,33,36,38.
81	Riesgo-Combatir-Incend	14,16,17,19,24,25,26,37,51.
82	Riesgo-Penetración	2, 4,5,12,45,72,73.
83	Riesgo-Grales-Piso-Fal	3,11,21.
84	Riesgo-Grales-Inunda	6,9.
85	Riesgo-Grales-Visitas	53,54,56,58,59,60,74.
86	Riesgo-Grales-Elect	10,28,33,38,40,41.
87	Riesgo-Grales-Acceso	12,52,53,54,61,74.
88	Riesgo-Grales-Evacuación	13,32,49,50.
89	Riesgo-Daño-Eq-Mat	3,9,15,23,38.
90	Riesgo-Daño-Eq-Hum	22,48,60,74.
91	Riesgo-Grales-Sabotaje	40,44,45,60,72,73,74.
92	Riesgo-Grales-Aire	23,34,42,43.
93	Riesgo-Grales-Suminist	29,35,39.
94	Riesgo-Grales-Temblor	46,47.
95	Riesgo-Grales-Gafetes	55,57.
96	Riesgo-Grales-Docum	62,63,65,66,70.
97	Riesgo-Grales-Admin	64,70,71.
98	Riesgo-Grales-Conting	67,68.
99	Riesgo-Grales-Seguros	75,76,77,78,79.

RIESGOS GENERALES POR FACTOR DE EVALUACION

NUM. RIESGO	NOMBRE RIESGO	RIESGOS DE LOS QUE SE DERIVA
100	Riesgo-Acc-Centro-Cómputo	85,87,95.
101	Riesgo-Robo	82,85,87.
102	Riesgo-Sabotaje	82,85,86,90
103	Interrup-y-desa	81,82,83,84,86,90 91,92,93,94.
104	Riesgo-Operación	96,97.
105	Riesgo-Generales	88,90,95,96,97, 98,99.