**REPÚBLICA BOLIVARIANA DE VENEZUELA**

**UNIVERSIDAD PRIVADA DR. RAFAEL BELLOSO CHACÍN**

**FACULTAD DE INGENIERÍA**

**ESCUELA DE INFORMÁTICA**

****

**SISTEMA EXPERTO PARA LA DETECCION DEL MALWARE**

**PRESENTADO POR**

ANDRADE SAÚL

FERNÁNDEZ LUIS

SEGOVIA JAVIER

URDANETA ALEJANDRO

VILLALOBOS ALEJANDRO

**MARACAIBO, JULIO DE 2013**

1. **Descripción de la situación o problema bajo estudio**

Se propone un sistema experto que determine la probabilidad de que una computadora esté infectada con malware. Se hace uso de la técnica de factores de certidumbre para determinar el estado de la máquina.

Se toman en cuenta 3 factores: (1) si la computadora es segura o no lo es, (2) la peligrosidad del comportamiento del usuario y (3), la fiabilidad del sistema.

1. **Tipo de conocimiento usados**

Para este proyecto se usaron 2 tipos de conocimiento el declarativo y procedimental, explicados a continuación:

* Conocimiento Declarativo: Este tipo se basa en los hechos existentes para sacar conclusiones y deducir lo que realizara el sistema experto en consecuencia a ello.

Para el proyecto en cuestión usamos este conocimiento debido a que hay reglas ya expuestas en la información suministrada, donde exponen hechos concretos y conclusiones concretas que no cambian a través del tiempo, sino se mantienen iguales

* Conocimiento Procedimental: Este tipo se basa en el cambio que puede tener el sistema experto a través del tiempo, incorporando nuevos estados y conclusiones, a medida que se encuentran nuevos hechos no acotados en la base de conocimientos.

Para nuestro sistema también usamos conocimiento procedimental, debido a que no están acotadas en la base de datos todos los casos posibles para la detección de malware, más bien tenemos un sistema de aprendizaje donde el usuario puede agregar nuevos estados y las conclusiones correspondientes a estos, por lo tanto el sistema va cambiando a través del uso del mismo y de los nuevos conocimientos adquiridos por los usuarios.

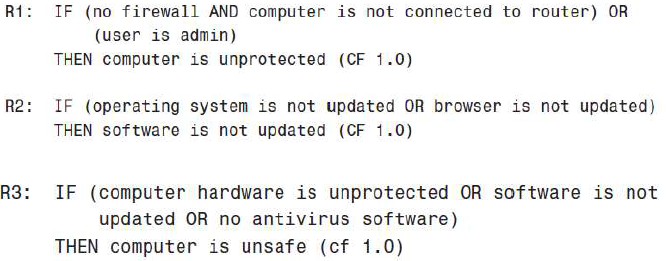
1. **Representación del conocimiento**

Utilizamos reglas de producción para representar el conocimiento, debido a que el sistema experto tiene muchas decisiones, y esta representación se amolda más al mismo.

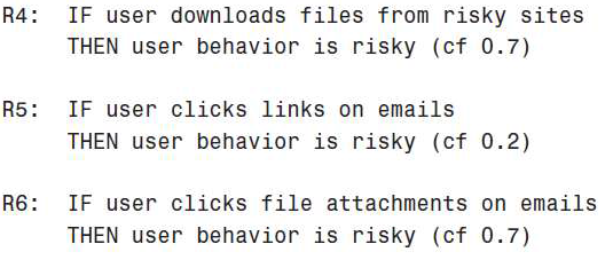
También como usamos conocimiento procedimental el sistema aprende a través de nuevos conocimientos que no han sido acotados en la base de datos, por esto la representación hay 2 tipos de reglas de producción:

* 1. Las que son del conocimiento declarativo.
  2. Las que son del conocimiento procedimental.

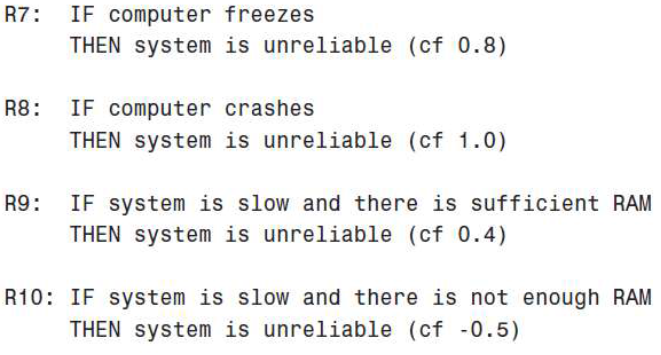
1. Cuestionario #1:



1. Cuestionario #2:



1. Cuestionario #3:

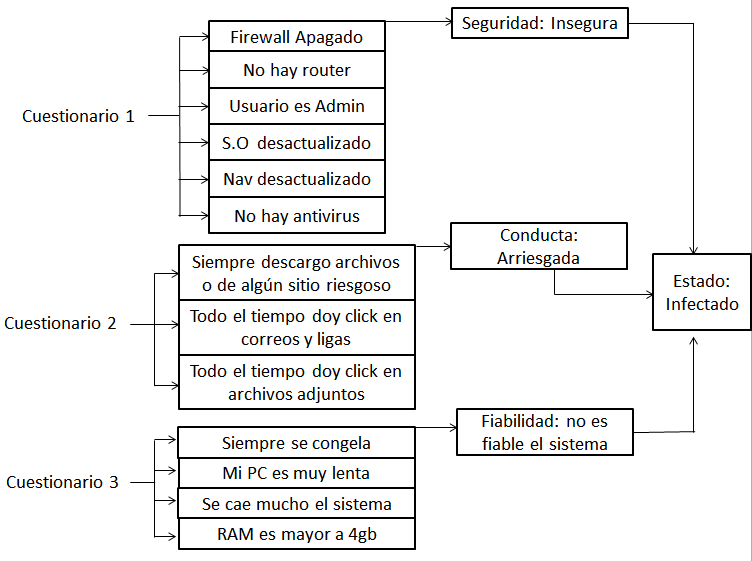


1. Aprendizaje del sistema:

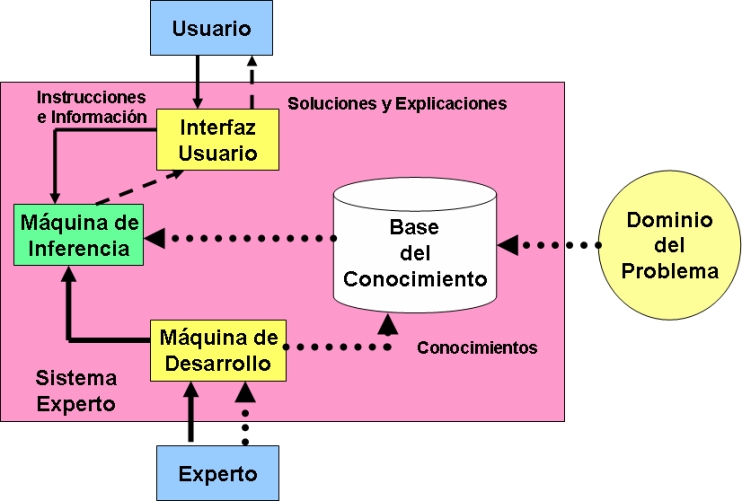
IF el sistema no da resultado a los estados seleccionados THEN agregar nuevo estado a la base de datos (\*)

(\*) = El sistema tiene un botón “Nomedesclick”, donde ingresara a la base de datos y se mostraran todas las tablas creadas y sus relaciones, allí se muestran todas las conclusiones y los estados que activan dichas conclusiones, para agregar una nueva conclusión con diferentes estados hacer click en “Agregar Regla” y a continuación se agregara una nueva fila a la base de datos, donde el usuario podrá realizar un nuevo estado, representando una nueva conclusión.

1. **Diseño lógico de la base conocimientos**

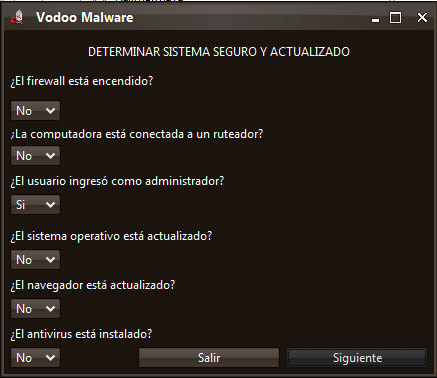
****

1. **Estructura del Sistema experto**

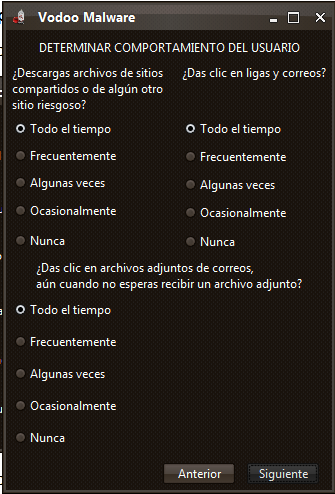


1. **Plan de pruebas**

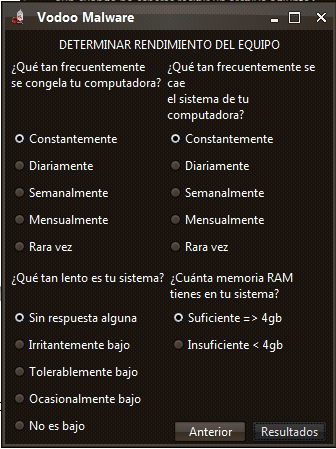
Cuestionario #1:

****

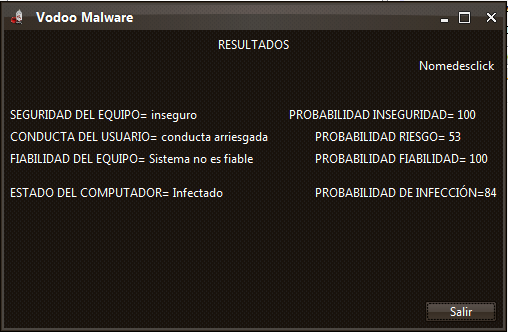
Cuestionario #2:



Cuestionario #3:



Resultados:



1. **Descripción de procedimientos requeridos para poner a funcionar la aplicación**

Simplemente con abrir NetBeans IDE y dar en click en File > New Proyect > (La ruta donde descomprimió el proyecto), y compilarlo correrá el programa sin problemas ya que la base de datos esta creada en SQLite que es un gestor donde tiene integrado el motor de SQL sin necesidad de estar creando las tablas, el las generas solo de acuerdo al código que contiene programado.