Controles Inteligentes sobre el SGSI de la Universidad del Cauca - Fase II Proyecto SGSI UNICAUCA

CARLOS ANDRES RODALLEGA OBANDO
OSCAR RICARDO VALENCIA AGUILAR

Director: SILER AMADOR DONADO

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE SISTEMAS
GRUPO DE I+D EN TECNOLOGÍAS DE LA INFORMACIÓN
LINEA DE INVESTIGACIÓN: SEGURIDAD INFORMÁTICA
POPAYÁN, ENERO DE 2013

Agradecimientos

A Dios, por permitirnos experimentar esta maravillosa sensación que llaman vida, por ser nuestro guía, por darnos la oportunidad de sacar adelante uno de nuestros proyectos.

A nuestros padres, por permitirnos ser una continuación de su vida, brindándonos protección, formación y ese amor único que es puro e incondicional.

A nuestras familias, que día tras día nos han acompañado y brindado su apoyo en cada uno de los logros de nuestras vidas.

A nuestros profesores y/o educadores, que mas que formarnos nos ofrecieron su amistad y nos brindaron sus conocimientos, personales de los cuales aunque no parezca siempre nos quedamos con un poco para seguir nuestro camino.

Al Ingeniero Siler Amador Donado, por darnos el honor de trabajar bajo su dirección, así como por descarriarnos y mostrarnos que no siempre lo que todos hacen es la mejor opción.

A nuestros amigos y compañeros, que con su presencia y ausencia también han aportado en el desarrollo de nuestras vidas.

Finalmente a nuestra alma mater la Universidad del Cauca, por abrirnos sus puertas, acogernos, formarnos y permitirnos alcanzar este tan anhelado logro.

Tabla de contenido

Índice de ilustraciones

Índice de tablas

Capítulo I

Introducción

1.1 Introducción

En la actualidad el incremento de dispositivos informáticos, así como la interconectividad que implican los mismos, ha permitido una mejor accesibilidad y distribución de la información; desafortunadamente a medida que se incrementan estos factores también se incrementan las brechas de seguridad, motivo por el cual es necesario que cada empresa implemente y/o maneje sus procesos siguiendo las normas correspondientes, como lo son en este caso ISO/IEC 27001 [1] e ISO/IEC 27002 [2]; las normas que se centran en el SGSI[1] y los controles.

Los controles y los procedimientos sobre los que estos actúan no siempre llevan un proceso lineal, motivo por el cual es muy probable que los mismos fallen o no respondan de la mejor manera; con base en lo anterior se eligieron los controles como el punto sobre el cual realizar el aporte, el cual consta de mejorar los procedimientos y aplicar técnicas de inteligencia artificial, todo esto buscando generar un gran impacto en la eficiencia y efectividad del SGSI.

1.2 Planteamiento del Problema

Con el constante uso de los sistemas de información utilizados por las diferentes personas o entidades en diferentes ámbitos como lo son, gubernamentales, militares, educativas entre otras, es inevitable que existan serias amenazas que ponen en peligro la integridad de la información y con ello la viabilidad de los negocios. En la actualidad es indispensable brindar robustez y seguridad para evitar el acceso de personal no autorizado a la red de telecomunicación de las empresas, y demás organizaciones que utilicen dichos medios para almacenar, procesar y modificar la información.

La seguridad de la información es de vital importancia en cualquier entidad,

[1]Sistema de Gestión de Seguridad de la Información.

especialmente en este proyecto, donde se establecen unas políticas tomando en cuenta las normas ISO/IEC 27001, ISO/IEC 27005 [3], para hacer una medición de los servicios con alto nivel de riesgo y realizar un mejor control y reajuste de la configuración en dichos servicios.

Es importante esclarecer la importancia de brindar soporte y seguridad a todos los medios de información y en especial los que nos rodean, por lo cual el presente trabajo plantea ¿Cómo implementar controles inteligentes orientados a disminuir el nivel de riesgo de un acceso ilegal a la información? En este caso haciendo referencia a la División de las TIC de la Universidad del Cauca, detectando, controlando e informando a los administradores encargados, por medio del SGSI-UNICAUCA haciendo uso de los controles inteligentes los cuales deben actuar en tiempo real frente a dicha situación.

Con el creciente descubrimiento de vulnerabilidades que afectan gravemente los sistemas operativos y aplicaciones sujetas a éstos, se toma como caso de estudio la División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca y con base al SISTEMA DE ALERTAS DE SEGURIDAD INFORMÁTICA PARA LOS SERVICIOS CRÍTICOS DE LA DIVISIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DE LA UNIVERSIDAD DEL CAUCA" (FASE I DEL PROYECTO SGSI-UNICAUCA), se propone desarrollar el trabajo de grado denominado Controles Inteligentes sobre el SGSI de la Universidad del Cauca - Fase II proyecto SGSI UNICAUCA.

Actualmente existen varios servicios implementados en la División de las TIC de la Universidad del Cauca como los son el servicio WEB, FTP, PROXY, DNS, CORREO ELECTRONICO, entre otros, cada uno con un nivel de riesgo específico, los cuales han sido evaluados y clasificados previamente en la FASE I del proyecto SGSI-UNICAUCA, esto con el fin de obtener los dos (2) servicios con mayor nivel de criticidad, sobre los cuales se desarrollarán los controles inteligentes respectivos, teniendo en cuenta las vulnerabilidades más explotadas por parte de los atacantes o en su defecto, errores internos de dicho servicio, ya sea por una incorrecta configuración por parte del administrador o por factores externos.

1.3 Justificación de la Investigación

La investigación realizada en el proyecto actual denominado Controles inteligentes sobre el SGSI de la Universidad del Cauca - Fase II Proyecto SGSI UNICAUCA, se realiza principalmente como un aporte al proyecto SGSI UNICAUCA, mediante el uso de controles que basen su funcionamiento en técnicas de inteligencia artificial, los cuales serán desarrollados para dos de los servicios críticos de la división de TIC de la Universidad del Cauca. Para su adecuado funcionamiento es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad, de la misma manera es necesario tener definido un conjunto de políticas de seguridad y sus respectivos procedimientos, de modo que los controles den soporte en la toma de decisiones de la organización, siguiendo los estándares ISO/IEC 27001, ISO/IEC 27005. En la actualidad la gestión de la seguridad de la información se ha convertido en un proceso necesario para todas las organizaciones, para abordar de manera adecuada este proceso es necesaria una planificación cuidadosa en función a la situación de cada organización.

El proyecto adicionalmente aportará de manera significativa a las empresas en el proceso de identificación y aplicación de los controles, los cuales son indispensables en su búsqueda de cumplir con la serie de normas ISO/IEC 27000. A demás teniendo en cuenta que en la actualidad los controles que se usan en este ámbito son aplicados mas como listas de chequeo o controles convencionales, este proyecto busca la aplicación de técnicas de inteligencia artificial en la automatización y el desarrollo de este tipo de controles.

1.4 Objetivos de la Investigación

1.4.1 Objetivo General

Implementar controles inteligentes sobre dos de los servicios críticos en la División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca.

1.4.2 Objetivos Específicos

- Caracterizar las técnicas más utilizadas en la inteligencia artificial que se adaptan mejor para el desarrollo de los controles inteligentes en el SGSI-UNICAUCA.
- Identificar los controles que permiten verificar los procedimientos definidos para el cumplimiento de las políticas de seguridad establecidas para los dos servicios críticos identificados previamente en la fase I del proyecto SGSI UNICAUCA.
- Diseñar y desarrollar controles inteligentes para dos de los servicios críticos de la División de Tecnologías de la información y la Comunicación de la Universidad del Cauca.
- Analizar el desempeño, eficiencia y el tiempo de respuesta de los controles inteligentes desarrollados en este proyecto.

Capítulo II

Marco Teórico y Estado del Arte

2.1 Marco Teórico

2.1.1 Sistema de Gestión de Seguridad de la Información

Un SGSI o Sistema de Gestión de Seguridad de la Información es un proceso sistemático basado en un conjunto de políticas y buenas prácticas, el cual se centra en la administración correcta de la información, esto buscando la mayor reducción del riesgo (hasta niveles residuales que sean gestionables o aceptables) de afectar la confidencialidad, la integridad y la disponibilidad de la información.

2.1.2 Controles

En la literatura actual se pueden encontrar diversos planteamientos sobre que es un control, según el experto Buró K. Scanlan "*El control tiene como objetivo cerciorarse de que los hechos vayan de acuerdo con los planes establecidos*". En ámbito de un SGSI y en especial para la familia de normas ISO/IEC 27001, los controles se centran en la identificación de la normativa y las medidas de cumplimiento (Cumplimiento de requerimientos legales), en la comprobación y/o verificación del cumplimiento de las medidas de seguridad definidas a nivel empresarial por parte del personal (Cumplimiento de políticas de seguridad, estándares y técnicas de buenas prácticas).

2.1.3 Lógica Difusa [4]

La lógica difusa se inició en 1965 por Lotfi A. Zadeh, profesor de la Universidad de California en Berkeley. Surgió como una herramienta importante para el control de sistemas y procesos industriales complejos, así como también para la electrónica de entretenimiento y hogar, sistemas de diagnóstico y otros sistemas expertos.

La lógica difusa en comparación con la lógica convencional permite trabajar con información que no es exacta para poder definir evaluaciones

convencionales, contrario con la lógica tradicional que permite trabajar con información definida y precisa.

La lógica difusa se puede aplicar en procesos demasiado complejos, cuando no existe un modelo de solución simple o un modelo matemático preciso. Es útil también cuando se necesite usar el conocimiento de un experto que utiliza conceptos ambiguos o imprecisos. De la misma manera se puede aplicar cuando ciertas partes de un sistema a controlar son desconocidas y no pueden medirse de forma confiable y cuando el ajuste de una variable puede producir el desajuste de otras. No es recomendable utilizar la lógica difusa cuando algún modelo matemático ya soluciona eficientemente el problema, cuando los problemas son lineales o cuando no tienen solución.

La lógica difusa se aplica principalmente en sistemas de control difuso que utilizan expresiones ambiguas para formular reglas que controlen el sistema. Un sistema de control difuso trabaja de manera muy diferente a los sistemas de control convencionales. Estos usan el conocimiento experto para generar una base de conocimientos que dará al sistema la capacidad de tomar decisiones sobre ciertas acciones que se presentan en su funcionamiento. Los sistemas de control difuso permiten describir un conjunto de reglas que utilizaría una persona para controlar un proceso y a partir de estas reglas generar acciones de control. El control difuso puede aplicarse tanto en sistemas muy sencillos como en sistemas cuyos modelos matemáticos sean muy complejos. La estructura de un controlador difuso se muestra en la ilustración 1.

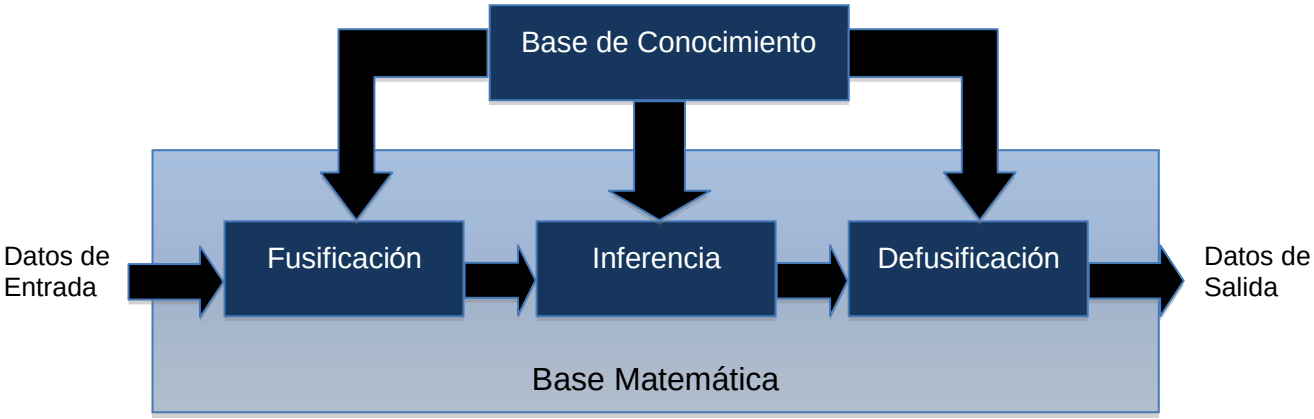

Ilustración 1 Estructura del modelo difuso [5]

Fusificación

La fusificación tiene como objetivo convertir valores crisp o valores reales en valores difusos. En la fusificación se asignan grados de pertenencia a cada una de las variables de entrada con relación a los conjuntos difusos previamente definidos utilizando las funciones de pertenencia asociadas a los conjuntos difusos.

2.1.3.1 Funciones de Pertenencia [5]

La función de pertenencia de un conjunto nos indica el grado en que cada elemento de un universo dado, pertenece a dicho conjunto. Es decir, la función de pertenencia de un conjunto A sobre un universo X será de la forma:

$$\mu A : X \rightarrow [0,1]$$

donde $\mu A\ (X) = r$, si r es el grado en que X pertenece a A.

Si el conjunto es nítido, su función de pertenencia tomará los valores en {0,1}, mientras que si es borroso, los tomará en el intervalo [0,1]. Si $\mu A(X) = 0$ el elemento no pertenece al conjunto, si $\mu A(X) = 1$ el elemento sí pertenece totalmente al conjunto.

2.1.3.2 Tipos de funciones de pertenencia

Función Triangular

Definida mediante el límite inferior a, el superior b y el valor modal m, tal que $a < m < b$.

$$\mu_A(x) = \begin{cases} 0, & \text{si } x \le a \\ \dfrac{x-a}{m-a}, & \text{si } a < x \le m \\ \dfrac{b-x}{b-m}, & \text{si } m < x < b \\ 0, & \text{si } x \ge b \end{cases}$$

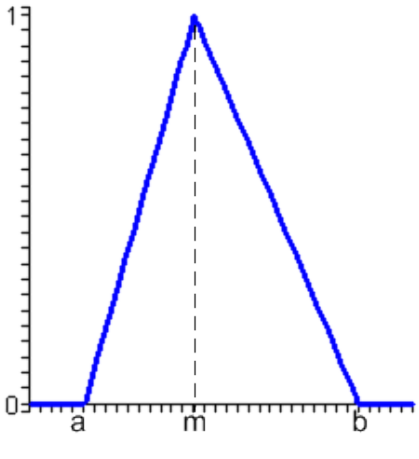

Ilustración 2 Función Triangular [6]

La ilustración 2 es un ejemplo de una función triangular de donde cabe resaltar que esta no necesariamente debe ser simétrica.

Función Trapezoidal

Definida por sus límites inferior a, superior d, y los límites de soporte inferior b y superior c, tal que $a < b < c < d$.

$$\mu_A(x) = \begin{cases} 0, & \text{si } (x < a) \text{ ó } (x > d) \\ \dfrac{x-a}{b-a}, & \text{si } a \le x \le b \\ 1, & \text{si } b \le x \le c \\ \dfrac{d-x}{d-c}, & \text{si } c \le x \le d \end{cases}$$

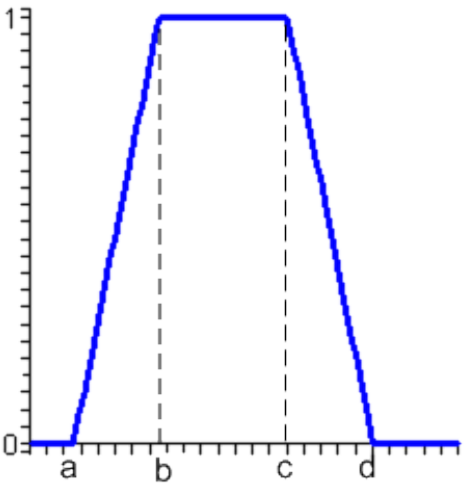

Ilustración 3 Función Trapezoidal [6]

La ilustración 3 es un ejemplo de una función trapezoidal que dado el caso de que si los valores de b y c son iguales, se obtiene una función triangular, además tiene dos casos especiales que ocurren cuando $a = b = -\infty$ y $c = d = +\infty$.

Función Gaussiana

Definida por su valor medio m y el parámetro $k > 0$. Esta función es la típica campana de Gauss y cuanto mayor es el valor de k, más estrecha es dicha campana.

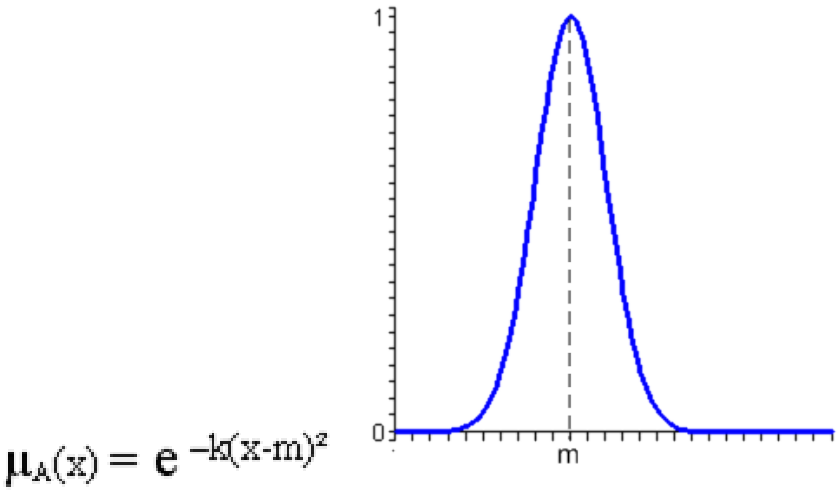

Ilustración 4 Función Gaussiana [6]

La ilustración 4 es un ejemplo de una función gaussiana.

Función Singleton [6]

Tiene un valor único cuando $x = a$.

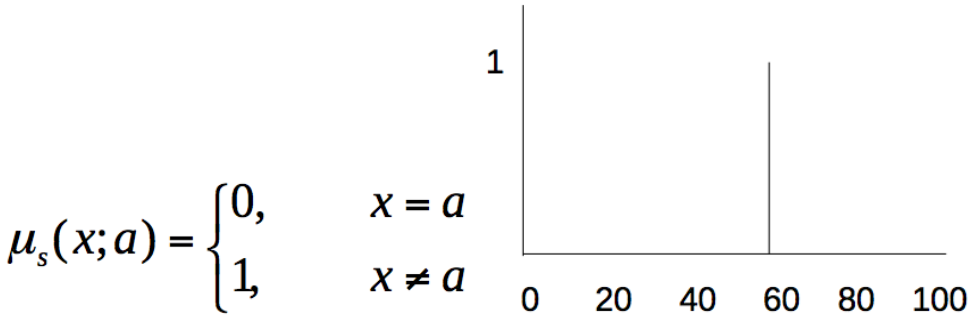

Ilustración 5 Función Singleton [6]

La ilustración 5 es un ejemplo de una función singleton.

2.1.3.3 Base de Conocimiento

La base de conocimiento contiene el conocimiento asociado con el dominio de la aplicación y los objetivos del control. En esta etapa se deben definir las

reglas lingüísticas de control que realizaran la toma de decisiones que decidirán la forma en la que debe actuar el sistema.

2.1.3.4 Inferencia

La inferencia relaciona los conjuntos difusos de entrada y salida para representar las reglas que definirán el sistema. En la inferencia se utiliza la información de la base de conocimiento para generar reglas mediante el uso de condiciones, por ejemplo: si caso1 y caso2, entonces acción1.

2.1.3.5 Defusificación

La defusificación realiza el proceso de adecuar los valores difusos generados en la inferencia en valores crisp, que posteriormente se utilizarán en el proceso de control. En la defusificación se utilizan métodos matemáticos simples como el método del Centroide, Método del Promedio Ponderado y Método de Membrecía del Medio del Máximo.

2.1.4 Herramientas para Lógica Difusa

Las herramientas que facilitan las distintas etapas del proceso de diseño de sistemas de inferencia basados en lógica difusa, desde su descripción inicial hasta la implementación final.

2.1.4.1 Xfuzzy 3.0 [7]

Xfuzzy 3.0 es un entorno de desarrollo para sistemas de inferencia basados en lógica difusa. Está formado por varias herramientas que cubren las diferentes etapas del proceso de diseño de sistemas difusos, desde su descripción inicial hasta la implementación final. Sus principales características son la capacidad para desarrollar sistemas complejos y la flexibilidad para permitir al usuario extender el conjunto de funciones disponibles. El entorno ha sido completamente programado en Java, de forma que puede ser ejecutado sobre cualquier plataforma que tenga instalado el JRE (Java Runtime Environment). La siguiente figura muestra el flujo de diseño de Xfuzzy 3.0.

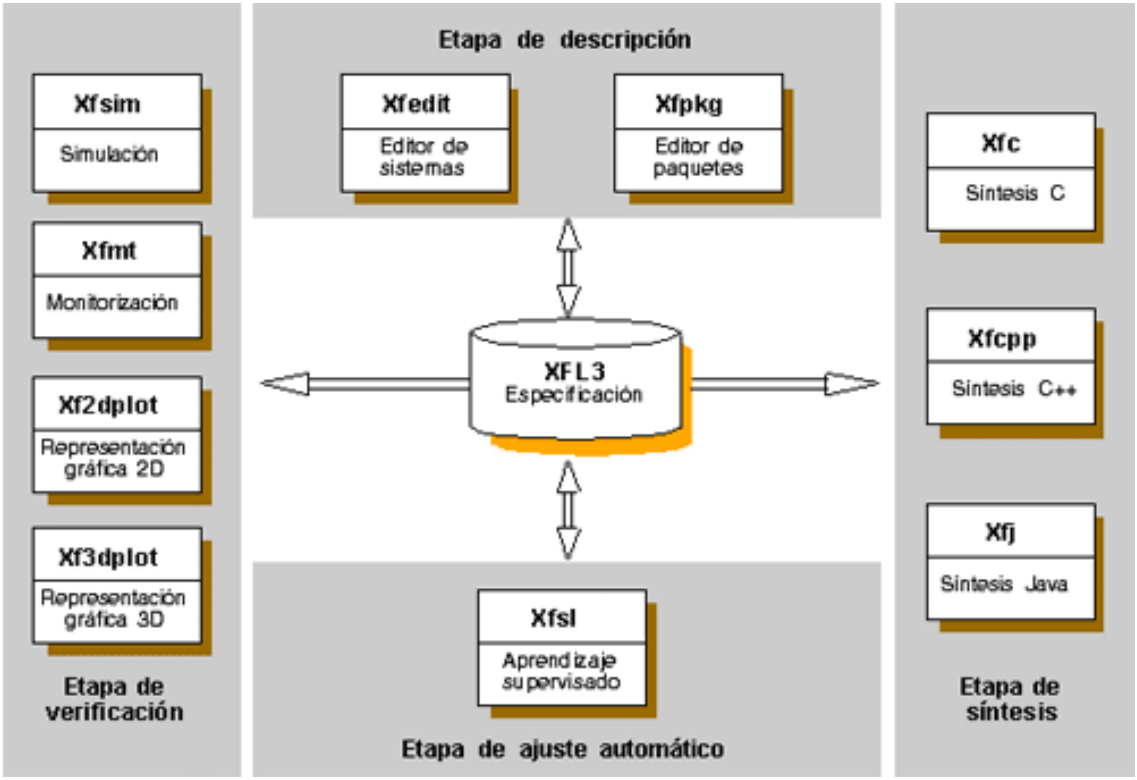

Ilustración 6 Flujo de Desempeño Xfuzzy[7]

La etapa de descripción incluye herramientas gráficas para la definición del sistema difuso. La etapa de verificación está compuesta por herramientas de simulación, monitorización y representación gráfica del comportamiento del sistema. La etapa de ajuste facilita la aplicación de algoritmos de aprendizaje. Finalmente, la etapa de síntesis incluye herramientas para generar descripciones en lenguajes de alto nivel para implementaciones software o hardware.

2.1.4.2 FuzzyCLIPS [8]

Esta es una versión ampliada de CLIPS, las modificaciones introducidas en CLIPS contienen la capacidad de manejar conceptos y razonamientos difusos. Permite a los expertos el dominio de las normas que utilizan términos difusos. FuzzyCLIPS permite cualquier combinación de términos difusos y normales, comparación numérica de controles lógicos e incertidumbres en las reglas y los hechos. Mejora el lenguaje CLIPS por medio de una capacidad de razonamiento difuso que está completamente integrado con el motor de hechos

e inferencias de CLIPS permitiendo representar y manipular hechos y reglas difusas.

2.1.4.3 FuzzyTECH [9]

FuzzyTECH proporciona por un lado todas las herramientas necesarias para diseñar y probar un sistema de lógica difusa. Una vez diseñado, FuzzyTECH almacena su trabajo como un archivo con formato FTL. FTL es sinónimo de "Lenguaje de Tecnología Fuzzy", y puede ser considerado como "el lenguaje de programación de la lógica difusa" FuzzyTECH proporciona una interfaz de usuario totalmente gráfica, por otra parte, FuzzyTECH convierte la descripción del sistema en FTL a código que pude ser usado en el hardware destino, que es donde la solución de lógica difusa va a ejecutarse finalmente.

El Diseño de un sistema de lógica difusa es diferente de la codificación convencional. FuzzyTECH cuenta con tres "asistentes de diseño inexacto" que guían paso a paso. Como un principiante, esto asegura que se han cubierto todos los pasos de diseño, como un desarrollador con experiencia será capaz de diseñar el prototipo de un sistema complejo en tan sólo unos minutos.

2.1.5 Web Services [10]

Un servicio Web es un componente software que se basa en las siguientes tecnologías:

- Un formato que describa la interfaz del componente (sus métodos y atributos) basado en XML[2]. Por lo general este formato es el WSDL[3].
- Un protocolo de aplicación basado en mensajes y que permite que una aplicación interaccione (use, instancia, llame, ejecute) al WebService. Por lo general este protocolo es SOAP[4].
- Un protocolo de transporte que se encargue de transportar los mensajes por internet. Por lo general este protocolo de transporte es HTTP[5] que es exactamente el mismo que usamos para navegar por la Web.

[2] Extensible Markup Language.
[3] Web Service Description Language.
[4] Simple Object Access Protocol.

Los servicios Web, no son por tanto aplicaciones con una interfaz gráfica con la que las personas puedan interaccionar, sino que son software accesible en internet (o en redes privadas que usen tecnologías internet) por otras aplicaciones. De esta forma podemos desarrollar aplicaciones que hagan uso de otras aplicaciones que estén disponibles en internet interaccionando con ellas.

2.2 Estado del arte

2.2.1 Plataformas SGSI

Elaborada la búsqueda de las diferentes plataformas SGSI disponibles en el mercado, a continuación se realiza una pequeña descripción de estas.

ISOTools [11]

ISOTools es la Solución Informática para los Sistemas de Gestión. Desarrollada en entorno Web con el objetivo de cumplir los requisitos de las normas ISO y de modelos de Excelencia, ISOTools resulta una herramienta ideal para implantar, mantener y mejorar continuamente los Sistemas de Calidad, Medio Ambiente o Riesgos Laborales entre otros. Es una herramienta flexible y adaptable a las necesidades de cada empresa u organización independientemente del tamaño y del sector que opere. Es una solución que favorece la conservación del know how[6] en la organización, la agilización y mejora de los procesos así como la accesibilidad y búsqueda rápida y fácil de la información.

e-PULPO [12]

e-PULPO es una herramienta software que permite que la gestión completa de un Departamento de Tecnologías de la Información (TI) sea más eficiente y efectiva, permitiendo además reportar a la Dirección los logros del departamento, lo que convierte a e-PULPO en una herramienta básica en cualquier Departamento de Tecnologías de la Información.

[5] Hiper-Text Transport Protocol.
[6] El como hacer.

Para ello, cubre las recomendaciones básicas de las mejores prácticas de ITIL[7].

Además, se le ha dotado de funcionalidades que permiten cubrir las que el negocio exige a un Departamento de Tecnologías de la Información hoy día, como:

Gestión de los requisitos legales (LOPD[8] -Ley 15/1999 y RD 1720/2007, ENS[9] -RD 3/2010).

Gestión de los requisitos normativos (SGSI[10] -ISO 27001 e ISO 27002-, SGTI[11] -ISO 20000).

GesConsultor [13]

GESConsultor proporciona una solución integral para consultores y empresas a la hora de implementar y gestionar un Sistema de Gestión. Es una herramienta para la implantación y el seguimiento del ciclo completo de Sistemas de Gestión en la que destacan las siguientes características:

- Implantación de normas.
- Gestión documental.
- Análisis de Riesgos
- Lugar de encuentro entre consultores, empresa, y los equipos de trabajo que se relacionan con los Sistemas de Gestión.
- Gestión a través de Web para acceso desde cualquier lugar por cualquier perfil.
- Portal personalizado según el perfil de acceso.

ECIJA | SGSI [14]

ECIJA | SGSI es una herramienta Web que permite la gestión integral de la seguridad de la información y el seguimiento centralizado de las obligaciones que establecen los estándares internacionales: ISO27001 e

[7] *ITIL: Biblioteca de Infraestructura de Tecnologías de la Información (Information Technology Infrastructure Library)*
[8] *LOPD: Ley Orgánica de Protección de Datos*
[9] *ENS: Esquema Nacional de Seguridad*
[10] *SGSI: Sistema de Gestión de la Seguridad de la Información*
[11] *SGTI: Sistema de Gestión de Servicios de Tecnologías de la Información*

ISO27002 en la gestión de la misma.

ECIJA | SGSI ayuda a medir el grado de eficacia de los sistemas de gestión de la seguridad de la información, valorando la seguridad de la información mediante los impactos producidos con base a los términos de confidencialidad, integridad y disponibilidad de la misma.

Facilita un sistema completo de gestión de la seguridad de la información, capaz de garantizar que los riesgos de los activos de la información sean conocidos, asumidos, gestionados y minimizados por la organización.

AGGIL [15]

AGGIL incluye un conjunto de herramientas para la implantación y mantenimiento de sistemas de gestión ISO (9001, 14001, 27001, etc.).
Los módulos de AGGIL incluyen una base común que facilita la integración de sistemas de gestión. Sobre esta base común, se dispone de herramientas que dan respuesta a los requerimientos de cada uno de los sistemas (Calidad, Seguridad de la Información, Gestión Medio Ambiental, etc.)
Las herramientas ISO de AGGIL son usadas por los responsables de sistemas de gestión de la empresa, los cuales pueden acceder al sistema de gestión, en un entorno colaborativo.
Con AGGIL, el mantenimiento de sistemas se simplifica y sistematiza evitando duplicidades y reduciendo el papel, optimiza las dedicaciones para el mantenimiento de tus sistemas de gestión, facilita la auditoría de tus sistemas agilizando la información.

S2GSI [16]

S2GSI ha sido diseñada para la gestión eficiente de las principales actividades derivadas de la implantación de un SGSI. S2GSI facilita el proceso de implantación y el mantenimiento del SGSI, con independencia del ámbito de la organización. Entre las principales características se encuentran:

- Soporte a la gestión del estado de cumplimiento de los controles.

- Posibilidad de gestionar diferentes marcos normativos de forma simultánea ISO/IEC 27001 ISO/IEC 27002, RD 1720/2007, PCI DSS, ENS (RD 3/2010), etc.
- Definición de procedimientos de verificación personalizados.
- Registro de auditorías y seguimiento de las no conformidades y acciones correctivas.
- Apoyo a la gestión documental.
- Importación automática de datos.
- Presentación de informes textuales y gráficos.

SECURIA SGSI [17]

Securia SGSI es una herramienta integral que cubre el proceso automático de implantación, puesta en funcionamiento, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma internacional ISO 27001.

Módulos funcionales de SecuriaSGSI:

- Módulo de Gestión de Incidencias y No Conformidades: Mediante la gestión de las incidencias, la entidad se asegura de que los eventos y los puntos débiles de la seguridad de la información, asociados con los sistemas de información, se comunican de forma que sea posible emprender su resolución mediante la aplicación de acciones correctivas.
- Módulo de Mejora Continua: Gestión de acciones preventivas y de mejora que se aplican al sistema de seguridad para adaptarlo a nuevas situaciones y en previsión de posibles fallos, situaciones de riesgo, etc.
- Módulo de Gestión Documental: Los documentos exigidos por el SGSI deben estar protegidos y controlados (4.3.2. ISO 27001).
- Módulo de Análisis y Gestión de Riesgos: Inventario de procesos y activos, valoración del impacto de activos, identificación de amenazas y vulnerabilidades, cálculo del riesgo, decisión de criterios de aceptación, toma de decisiones de actuación, generación y seguimiento de las contramedidas, evaluación del nivel de seguridad.

GlobalSGSI [18]

GlobalSGSI es una herramienta web que permite cubrir el ciclo completo de análisis, implantación, gestión y mantenimiento de la Norma ISO 27001. Dispone de un gestor documental que le ayudará a la hora de gestionar toda la documentación inherente a cualquier sistema de gestión, al tratarse de una plataforma web, hace que sea una herramienta colaborativa entre los integrantes del equipo de trabajo, o entre distintos usuarios del mismo sistema. El análisis de riesgos, una de las partes fundamentales en la implantación de la norma ISO 27001, puede realizarse de manera distribuida y colaborativa entre los diferentes responsables de unidades de negocio.

CALLIO SECURA 17799 [19]

La funcionalidad de Gestión de SGSI le permitirá definir un número ilimitado de SGSI. De esta manera, cada ambiente puede tener su propio perímetro de seguridad o el medio ambiente de seguridad, cada SGSI, junto con sus equipos de trabajo, se pueden crear, definir y administrar de forma independiente. Además, los usuarios pueden tener acceso a los diferentes SGSI, y los papeles asignados individualmente.

Esta funcionalidad también le permite:

- Gestión de amenazas, vulnerabilidades y los controles. Las amenazas, las vulnerabilidades y los controles contenidos en la norma ISO 13335 se incluyen por defecto, sin embargo, puede agregar muchos otros que usted considere apropiado.
- Manejar distintos tipos de criterios de evaluación, tales como la confidencialidad, disponibilidad, integridad y cumplimiento de la ley. También puede agregar otros criterios relacionados que se consideren oportunos, tales como la eficacia, la eficiencia, el cumplimiento, la confiabilidad de la información.
- Crear asociaciones entre los distintos tipos de activos, las amenazas, vulnerabilidades y los controles. Esto hará que sea más fácil de administrar y evaluar el SGSI y de implementar controles diseñados para mitigar los riesgos a los activos.

- Personalizar las escalas de la vulnerabilidad, la ocurrencia y el criterio utilizado durante los procesos de evaluación de los activos de la evaluación y el riesgo.

Sistema de alertas de seguridad informática para los servicios críticos de la división de tecnologías de la información y la comunicación de la Universidad del Cauca (Fase I del proyecto SGSI - UNICAUCA) [20]

La implementación del sistema de alarmas de seguridad informáticas está desarrollada en lenguaje de programación PHP, utiliza el sistema de monitoreo Nagios para verificar el estado de los servicios de información presentes de la División de TIC de la Universidad de Cauca, valor fundamental para completar en cálculo del valor de riesgo, siendo el valor de probabilidad de que una amenaza explote una o varias vulnerabilidades. Los estados son consultados en tiempo real de la base de datos MySQL, exportada con la ayuda de NDOUtils el cual permite exportar los sucesos y configuración de una o más instancias de Nagios.

El sistema mezcla la eficiencia de herramientas de monitoreo como Nagios y la aplicación de controles de seguridad como los propuestos en la norma ISO/IEC 27001:2005. El diseño y desarrollo de las fases de implantación de un Sistema de Gestión de Seguridad de la Información se basa en el ciclo PHVA[12], que permite al proyecto enfocarse correctamente en las necesidades de la División de TIC de la Universidad del Cauca. Los diferentes indicadores con los que cuenta la aplicación para medir la funcionalidad:

- Indicador de disponibilidad de los servicios.
- Indicador de conexiones bloqueadas

De los SGSI nombrados anteriormente se profundiza en dos de estos, con el fin de seleccionar sobre cuál de los SGSI se implantaran los controles inteligentes. Los SGSI sobre los cuales se profundizará son el SECURIA y el resultado de la fase I del proyecto SGSI-UNICAUCA.

El desarrollo de la fase I del proyecto SGSI, dejo como producto un sistema de

[12] Planificar, hacer, verificar y actuar.

alertas que funciona como una aplicación web desarrollada en PHP, la cual cuenta con una base de datos en MySQL, y además utiliza NAGIOS como sistema de monitoreo para verificar la información de los servicios. Este sistema permite la configuración de los riesgos, alertas y los controles que se encargan de estas siguiendo con los estándares ISO/IEC 27001:27005, toda esta información se analiza para mostrar los diferentes resultados en tiempo real.

El sistema SGSI SECURIA es una completa aplicación de escritorio desarrollada en Java, la cual soporta cada uno de sus módulos sobre una base de datos desarrollada en PostgreSQL. SECURIA permite la gestión de incidencias, gestión documental, el análisis y gestión de riesgos, todo esto siguiendo con el estándar ISO/IEC 27001; además se hace notar que él mismo controla o realiza la gestión de usuarios basada en perfiles de usuario. Cabe notar que una de las características además de sus múltiples funcionalidades, es que el mismo está bajo la licencia Creative Commons (CC).

Para el desarrollo del proyecto se utilizará el SECURIA SGSI debido a que de las plataformas comerciales anteriormente mencionadas es la única que se encuentra bajo la licencia Creative Commons (CC), lo cual facilita su estudio que es esencial para el desarrollo de este proyecto, además cuenta con un buen soporte, y a diferencia de la FASE I del proyecto SGSI Unicauca ofrece una variedad mayor de módulos, así como una la gestión de usuarios y privilegios más orientada al ámbito productivo, lo cual lo hace más aplicable a la división de TIC de la Universidad de Cauca.

2.2.2 Trabajos relacionados con controles inteligentes

Realizada la búsqueda de proyectos institucionales y externos en los cuales se hiciera referencia a controles inteligentes, se encontró que estos se enfocan más en el área de la automatización de procesos y la robótica; adicional a esto se pudo verificar que en esta área el concepto que se tiene de control cambia al punto que los controles referenciados en estos proyectos manejan gran parte del sistema, de modo que se pueden ver como sistemas de control y no como puntos de control que es el concepto que se maneja en este proyecto.

Inteligencia Artificial en el Sector Agropecuario [21]

Este trabajo de investigación presenta una visión global de la aplicación de las técnicas de inteligencia artificial en el sector agropecuario. El presente trabajo inicia realizando una breve descripción de algunas de las técnicas de inteligencia artificial, y posteriormente presenta la aplicación de algunas de estas en el sector como lo es un modelo de control de predicción para procesos industriales de evaporación por medio de redes neuronales, modelado de secado de granos basado en una red neuronal topológica, de la misma forma se nombra el uso de redes bayesianas, sistemas expertos y sistemas multiagente con diversos fines como lo son el control ambiental, el manejo de maquinaria agrícola, la producción vegetal, producción animal y la ingeniería de riegos, en cada uno de ellos se aplican los diversos controles y la inteligencia artificial, en algunos por aparte y en otros bajo el concepto mencionado anteriormente.

Control Inteligente de redes Urbanas de tráfico [22]

En este artículo se presenta y describe el sistema ITACA el cual ha sido desarrollado para el control de tráfico urbano, también se describen los elementos básicos del problema y se le da peso al hecho de que la disponibilidad de acciones óptimas o situaciones ideales no basta para garantizar el control óptimo de la red de tráfico; esto se da debido a que durante el proceso de desarrollo el modelo de control daba espacio a embotellamientos, puesto que se aplica individualmente por intersección; este problema llevó a los autores a mejorar el sistema mediante la introducción de un modelo de control con arquitectura distribuida.

2.2.3 Aplicación de técnicas de inteligencia artificial en seguridad informática.

A continuación se presentan diversos trabajos de investigación y desarrollo en el área de seguridad informática, sobre los cuales el estudio y la aplicación de diversas técnicas de técnicas de inteligencia artificial, han resultado muy

significativos en la mejora en sus procesos, así como la optimización de sus resultados.

Intrusion detection by machine learning [23]

Este artículo presenta las diferentes técnicas de aprendizaje automático, que ayudan a la detección de intrusos (IDS) en la tarea de tratar de resistir los ataques externos, técnicas tales como las redes neuronales, algoritmos genéticos, maquinas de vectores, entre otras. Algunas técnicas se basan en la combinación de diferentes técnicas de aprendizaje, híbridos o técnicas por conjuntos; estas técnicas se han desarrollado como clasificadoras, las cuales se centran en clasificar o reconocer si el acceso a Internet entrante es el acceso normal o un ataque.

Seguridad Inteligente [24]

Este articulo se centra en mostrar la gran relación existente entre la seguridad de la información y la inteligencia artificial, basándose en el estudio de diferentes proyectos los cuales aplican diferentes técnicas de IA en diferentes ámbitos de la seguridad de la información, como lo son el desarrollo de aplicaciones de auditoría, aplicaciones para el monitoreo de trafico sobre la red, herramientas de detección de intrusos, etc.

Intelligent System for Information Security Management: Architecture and Design Issues[25]

En este artículo se presenta el resultado del estudio de diversas técnicas de inteligencia artificial, con lo cual se logra definir una arquitectura para un SGSI-Inteligente. A partir de lo anterior se espera obtener un sistema que mejore los procesos de gestión de la seguridad, como lo son el seguimiento, control y toma de decisiones, esperando obtener un mayor efecto del que pudiera causar un experto en seguridad de la información, mediante la proporción de mecanismos para mejorar la construcción activa de conocimientos sobre las amenazas, políticas, procedimientos y riesgos.

InForce Technology [26]

Es un plataforma desarrollada en la universidad del cauca producto de una tesis de pregrado, la cual permite automatizar la planificación, dirección y cumplimiento de políticas de seguridad, centrándose en el ahorro de tiempo, esfuerzos y costos, lo anterior basándose en una arquitectura de agentes inteligentes para la gestión, desarrollo, implementación y control de las políticas de seguridad.

A partir del estudio de las diferentes soluciones SGSI relacionadas en este documento, así como los proyectos desarrollados que integran las áreas de inteligencia artificial y seguridad informática, se aprecia que estas dos áreas resultan ser muy compatibles, al punto que se podrían definir como complementarias. También se evidencian los diferentes enfoques de los proyectos, donde algunos están centrados en el monitoreo de los eventos en tiempo real (Antivirus, IDS, Firewall) y otros en la gestión documental y de políticas que pueden denominarse como procesos administrativos. Finalmente con base en el anterior estado del arte, es posible concluir que actualmente existe una variedad de soluciones en seguridad informática con aplicación de técnicas de inteligencia artificial, sin embargo no se encuentran soluciones que hagan uso de técnicas de inteligencia artificial en la definición y/o desarrollo de los controles establecidos en la norma ISO/IEC 27002.

Capítulo III

Caracterización de las técnicas de inteligencia artificial

La ejecución del presente trabajo está basada en el "Modelo Integral para el Profesional de Ingeniería" [27], el cual permitió un mejor entendimiento de los objetivos propuestos, haciendo uso como primera medida del "Modelo para la investigación científica" para generar conocimiento socialmente no existente y que sea útil en el campo de la seguridad informática.

Para la utilización del "Modelo para la investigación científica" se abarcan las siguientes fases:

- Fase I - Definición: Identificar las diferentes técnicas que potencialmente serán utilizadas en el posterior desarrollo de los diferentes controles.
- Fase II - Ejecución: Obtener las características más relevantes de las técnicas identificadas anteriormente.
- Fase III - Síntesis: A partir de una serie de criterios definidos encontrar las posibles técnicas de inteligencia artificial a aplicar en el desarrollo del proyecto.

3.1 Técnicas de Inteligencia Artificial

Siguiendo el "Modelo Integral para el Profesional de Ingeniería" y de la misma forma haciendo uso del "Modelo para la investigación científica" en su primera fase (fase I - Definición); A partir de la búsqueda de proyectos relacionados con el desarrollo de controles inteligentes, se seleccionaron las técnicas más aplicadas en los mimos. Las técnicas seleccionadas como posibles candidatas a usar en el desarrollo de este proyecto fueron.

3.1.1 Sistemas expertos:

Según Stivens [28] "*Los sistemas expertos son máquinas que piensan y razonan como un experto lo haría en una cierta especialidad o campo.*" Durkin [29] Plantea que "*Un sistema experto puede definirse como un sistema*

informático (hardware y software) que simula a los expertos humanos en un área de especialización dada."

Basado en las definiciones anteriores se puede decir que un sistema experto debería tener la capacidad de procesar la información mediante un conjunto de reglas adquiridas previamente con la ayuda de expertos en un determinado tema, además de razonar ante situaciones específicas.

3.1.2 Lógica difusa:

La lógica difusa nace con los conceptos propuestos por Lotfi Asker Zadeh [30] en su artículo titulado "Fuzzy Sets" en 1965. Con lo cual introduce la teoría de conjuntos difusos o lógica difusa. La lógica difusa es utilizada como una metodología para tratar de manera simple la resolución de problemas a partir de información vaga, ambigua, imprecisa con ruido o incompleta. Trata de imitar las decisiones de expertos, basada en información que cuenta con las características mencionadas anteriormente.

3.1.3 Redes neuronales:

Los primeros modelos de redes neuronales datan de 1943 por los neurólogos McCulloch y Pitts [31]. Las redes neuronales están basadas en la biología, ya que están formadas por elementos que se comportan de manera similar a las neuronas y están organizadas de forma similar a la del cerebro, emulando de esta forma ciertas características propias de los humanos.

3.1.4 Redes Bayesianas:

Los primeros conceptos de estos fueron propuestos por J. Pearl[32] en 1988. El cual con su enfoque probabilístico contribuyó al desarrollo de las redes bayesianas. Las redes bayesianas hacen uso de la teoría de probabilidad para modelar los diferentes fenómenos. Usan un conjunto de variables y las dependencias entre ellas como grafos dirigidos.

3.2 Características de las técnicas de inteligencia artificial

Para continuar con la fase II (ejecución) del "Modelo para la investigación"; Se procedió a seleccionar las características más relevantes de las técnicas de

inteligencia artificial nombradas anteriormente obteniendo los siguientes resultados:

Técnicas de Inteligencia	**Características**
Sistemas Expertos	• Requiere de los conocimientos de un grupo de expertos. • Método de inferencia deductiva mediante reglas con valores exactos. • Rapidez para dar respuesta. • Crecimiento dinámico. • Capacidad de emitir explicaciones sobre sus decisiones.
Lógica Difusa	• Soporta datos imprecisos. • Tolerancia a datos imprecisos. • Se basa en lenguaje humano. • Se basa en la experiencia de expertos. • Flexibilidad.
Redes Neuronales	• Topología. • Mecanismo de aprendizaje. • Representación de la información. • Velocidad de respuesta que depende del entrenamiento de la misma. • Robustez.
Redes Bayesianas	• Representación gráfica de las relaciones explicitas. • Compuestas por la parte cualitativa y subjetiva. • Inferencia bidireccional. • Permite valores con grados de incertidumbre. • Valor de salida es una probabilidad de distribución.

	• Fácil análisis de sensibilidad.

Tabla 1 Características de técnicas de inteligencia artificial

3.3 Criterios de selección

Culminado con el desarrollo de la fase III (Síntesis) del "Modelo para la investigación científica"; Se definen una serie de criterios para la selección de las técnicas candidatas que mejor se adapten a las necesidades del proyecto. Los criterios definidos son los siguientes:

- Dado que las necesidades del proyecto se centran en un sistema en el cual, se realizará la toma de decisiones a partir de ciertas características y basándose en manuales de buenas prácticas, se establece que es necesaria la utilización de técnicas basadas en conocimientos.

- Partiendo de la limitación de tiempo que se tiene para el desarrollo del presente proyecto, hace a las técnicas de inteligencia artificial clásicas como las principales candidatas a usar, gracias a que cuentan con una amplia documentación de aplicación en diversos ámbitos.

En este punto a partir del criterio que se centra en la limitación de tiempo actual, se descarta la aplicación de las redes bayesianas, debido a la necesidad de estas de un modelo probabilístico del cual no se dispone.

3.3.1 Pruebas de efectividad y eficacia sobre las técnicas IA

Adicional a los criterios de selección antes mencionados, se define un criterio selectivo basado en pequeñas pruebas (efectividad y eficacia).

Con el fin de realizar las pruebas de efectividad y eficacia se abordó un problema el cual consiste en determinar el tipo de una página web a partir de su contenido textual y sus enlaces[13].

Para la realización de las pruebas se desarrolló un robot que recorría las páginas realizando un conteo de palabras y enlaces claves, a partir de lo cual

[13] Problema abordado en la materia Inteligencia artificial orientada por Ing. Ember Ubeimar Martínez

se obtenía la información que posteriormente se pasaría a procesar con las diferentes técnicas de inteligencia artificial; en el caso de las redes neuronales se desarrolló una red neuronal que consta de 1 capa de entrada (lineal), 2 capas ocultas (sigmoid) y 1 capa de salida (sigmoid). Para el sistema de lógica difusa se desarrolló un sistema con sus respectivos tipos de datos, funciones de pertenencia y de 2 niveles de reglas, en el caso del sistema experto se presentó una limitación debido a que estos tipos de sistemas como se evidencia en su caracterización, basan su funcionamiento en la evaluación de valores específicos [33] (sobre estos se definen sus variables y bases de conocimientos), valores que por las características de las paginas y el método de recolección de información (buscando las mismas condiciones para las pruebas) no se pudieron identificar, hallando de esta manera una limitante en sistemas expertos. Sin embargo en documentación encontrada se denominan muchos de los sistemas del tipo fuzzy como sistemas expertos difusos, debido a que estos también requieren de una definición de reglas sobre sus funciones miembro.

En este punto, se descartan los sistemas expertos a partir de la limitación presentada a la hora de trabajar con valores no específicos, por lo tanto se definieron como las técnicas candidatas a usar en el desarrollo del proyecto, redes neuronales y lógica difusa, sin embargo buscando la ejecución de todas las actividades acordadas, se continuó con el desarrollo de las pruebas en este caso solo sobre las dos técnicas finales.

A partir de los resultados obtenidos en las diferentes pruebas se realizó la siguiente tabla, en la cual el tiempo de respuesta fue promediado a partir del número de pruebas que se realizó por cada escenario en este caso 4.

Pág. Analizar	RNA Salida	RNA Tiempo	Fuzzy Salida	Fuzzy Tiempo
PG1	PG	1 ms	PG	0 ms
PE1	PE	0 ms	PE	0 ms
PN1	PN	0 ms	PN	0 ms
PG2	PG	0 ms	PG	0 ms
PE2	PE	0 ms	PE	0 ms

PN2	PN	0 ms	PN	0 ms
PG3	PG	0 ms	PG	0 ms
PE3	PE	0 ms	PE	0 ms
PN3	PN	0 ms	PN	0 ms

Tabla 2 Resultado pruebas identificación Paginas

PGx: Página gubernamental número x
PG: Página gubernamental
PEx: Página de educación numero x
PE: Página de educación
PNx: Página de Noticias numero x
PN: Página de Noticias

En la tabla anterior se puede apreciar que las dos técnicas de inteligencia que estaban siendo evaluadas, fueron efectivas en la identificación de del tipo de las paginas, también se puede apreciar que los tiempos de respuesta son bastante bajos, al punto que solo en 1 de los casos las redes neuronales se tomaron 1 milisegundo.

De la misma manera se plantearon algunos escenarios un poco más difíciles de identificar, lo anterior con el fin de obtener un posible resultado erróneo de alguna de las técnicas, los resultados de estas pruebas se plasman en la siguiente tabla.

Pág. Analizar	RNA Salida	RNA Tiempo	Fuzzy Salida	Fuzzy Tiempo
PN-SE1	PN	0 ms	PN	0 ms
PN-SE2	PN	0 ms	PN	0 ms
PN-SE3	PN	0 ms	PN	0 ms
PN-SE4	PN	0 ms	PN	0 ms
PN-SG1	PN	0 ms	PN	0 ms
PN-SG1	PN	0 ms	PN	0 ms
PE-SN1	PE	0 ms	PE	0 ms
PE-SN2	PE	0 ms	PE	0 ms
PG-SN1	PG	0 ms	PG	0 ms

Tabla 3 Resultado pruebas identificación Paginas confusas

PN-SEx: Página noticias sección educación número x
PN-SGx: Página de noticias sección gobierno numero x
PE-SNx: Página de educación sección noticias numero x

PG-SNx: Página del gobierno sección noticias numero x
PG: Página gubernamental PE: Página de educación
PN: Página de Noticias

Como se puede observar en la tabla anterior, en estos escenarios cuyos datos en el momento de la caracterización podían tornarse ambiguos, las técnicas evaluadas, una vez más fueron eficientes en la identificación del tipo de páginas, con tiempos de respuesta mínimos.
A partir de los resultados obtenidos y plasmados en las tablas 2 y 3 se puede apreciar que las técnicas evaluadas presentan un alto grado de eficiencia y efectividad, incluso en entornos que aparentemente provocarían resultados erróneos.

Con base en los criterios de selección anteriormente definidos, incluyendo los resultados de la aplicación de los mismos, las características de cada técnica y las pruebas realizadas, se definen como las técnicas candidatas a usar en el desarrollo de los controles, las técnicas de redes neuronales y lógica difusa. A partir de las cuales, la técnica que se use en cada control dependerá únicamente de las necesidades y condiciones propias de cada control.

Capítulo IV

Identificación de controles

Inicialmente se presenta la lista de resumen de la ISO/IEC 27002:2005 que será el punto inicial y el eje para el desarrollo del presente proyecto. Este listado contenido en el Anexo A contempla 11 Dominios, 39 Objetivos de Control y 133 Controles, los cuales en este punto inicial se pueden considerar en su totalidad como candidatos a ser el objetivo de trabajo.

4.1 Selección de los Servicios Críticos

Con el objetivo de encontrar los dos servicios críticos que se utilizarán para la realización del proyecto, se realizó un primer encuentro con el representante de la división de TIC de la Universidad del Cauca con el fin de listar los servicios más críticos para la división de TIC inicialmente los servicios candidatos a servicios críticos son:

- Portal Institucional.
- Correo Electrónico.
- SIMCA[14] y SIMCAS.
- LDAP[15].
- DNS[16].

Posterior a esto con el objetivo de seleccionar solo dos servicios críticos de la anterior lista se construye un instrumento de medición basándose en la FASE I Proyecto SGSI-UNICAUCA el cual consta de diferentes listas de chequeo anexo B (Tabla B.1, B.2, B.3, B.4, B.5) las cuales son fueron diligenciadas mediante diferentes entrevistas con los dos representantes de la división de TIC de la Universidad del Cauca, a partir de lo cual se construyo una matriz de valoración para los servicios críticos.

[14] Sistema Integrado de Matricula y Control Academico
[15] Protocolo Ligero de Acceso a Directorios
[16] Sistema de Nombres de Dominio

Servicios Críticos / **Criterios de Evaluación**	SIMCA (11.11%)	Servidores LDAP (11.11%)	Servicios de DNS (11.11%)	Portal Institucional (11.11%)	Correo electrónico (11.11%)
¿Si el servicio falla afecta el funcionamiento de otros servicios?	Si	Si	Si	Si	Si
¿Existen servicios que dependen del servicio seleccionado?	Si	Si	Si	Si	Si
¿Existen políticas claras para el servicio seleccionado?	No	No	No	No	Si
¿Existe algún proceso de organización interna para este servicio?	No	No	No	No	No
¿Existe información de alta confidencialidad en ese servicio?	Si	Si	No	No	Si
¿Este servicio es capaz de trabajar de modo independiente?	No	Si	Si	No	Si
¿Existen controles, alarmas o algún seguimiento de administración sobre este servicio crítico?	Si	Si	Si	Si	Si
¿Existe un procedimiento documentado sobre cómo se debe llevar a cabo el servicio?	No	No	No	Si	Si
¿Se genera algún registro por la prestación o no del servicio crítico?	Si	Si	Si	Si	Si
Peso Total:	55,5%	66,66%	55,55%	55,55%	88,88%

Tabla 4 Matriz de valoración para los servicios críticos

La tabla 4 indica los resultados luego de aplicar las diferentes entrevistas al representante de la división de TIC sobre los diferentes servicios considerados como críticos, método que arrojó como resultado la selección de los dos servicios críticos a utilizar en la realización del proyecto, siendo estos los siguientes; el servicio de LDAP con un 66,66% y el servicio de correo electrónico con un 88,88% porcentaje equivalente al nivel de riesgo para la Universidad del Cauca.

4.2 Procedimientos Relacionados con los Controles Inteligentes

Los procedimientos sobre los cuales se desarrolló el presente proyecto, se obtuvieron con base al documento de políticas con el que cuenta la división de TIC, del cual cabe resaltar que se encuentra en proceso de aprobación pero fue el que se seleccionó como guía a seguir durante el proyecto.

Trabajando a partir del documento antes mencionado se identificaron tres procedimientos sobre los cuales se podría realizar el desarrollo de los controles inteligentes, estos procedimientos son:

- PU1p1: Procedimiento para la creación de una cuenta de correo electrónico institucional individual. En este procedimiento se aplica el control de validez de carnet y el de contraseña segura.

- PU2p1: Procedimiento para la creación de una cuenta de correo electrónico de grupo institucional. En este procedimiento se aplica el control de validez de carnet y el de contraseña segura.

- PU3p1: Procedimiento para la creación de una lista de correo electrónico institucional. En este procedimiento se aplica el control de validez de carnet y el de contraseña segura.

Analizando los procedimientos anteriormente mencionados y tratando de unificarlos debido a que son similares, se propuso un procedimiento que incluyera los tres procedimientos anteriores y a la vez mejorara algunos de los pasos a seguir, logrando de esta manera la optimización de los mismos.

Actualmente la mayoría de servicios de la Universidad de Cauca se autentican a través del servidor LDAP principalmente el servicio de correo electrónico institucional; partiendo de las condiciones anteriores es claro que los procedimientos de creación de cuentas de correo electrónico institucional influyen directamente sobre los dos servicios críticos, razón por la cual el desarrollo del proyecto se centro en el procedimiento de creación de cuentas de correo electrónico. Proceso definido en el siguiente diagrama de flujo de datos (seccionado para no perder calidad de imagen).

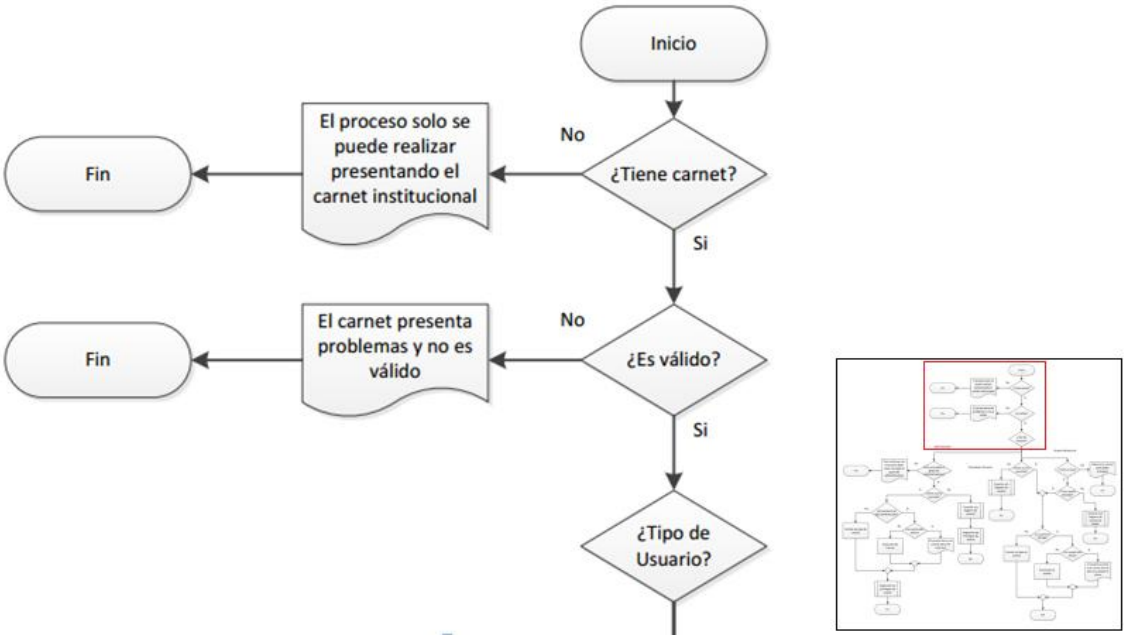

Ilustración 7 Procedimiento planteado Sección 1/3

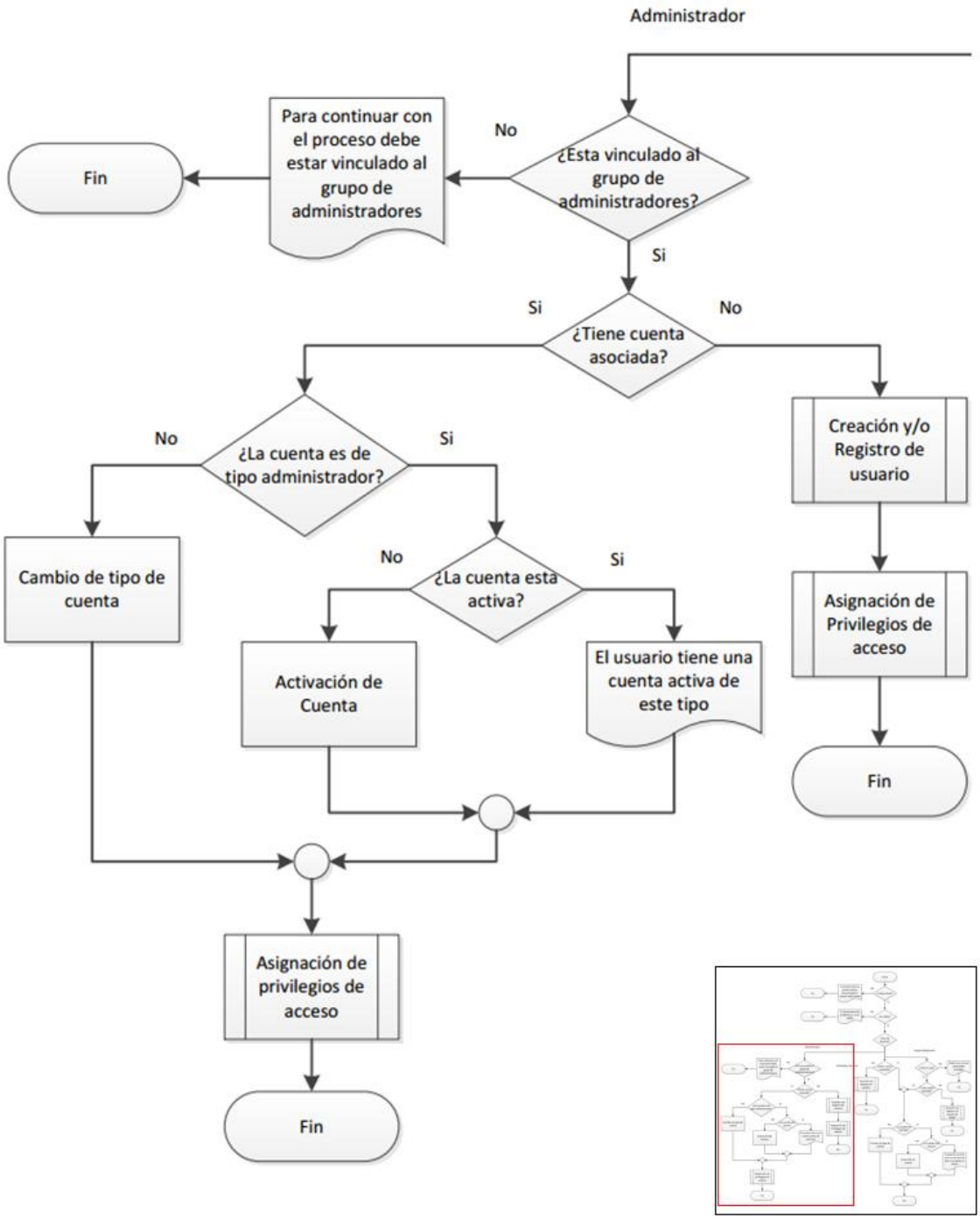

Ilustración 8 Procedimiento planteado Sección 2/3

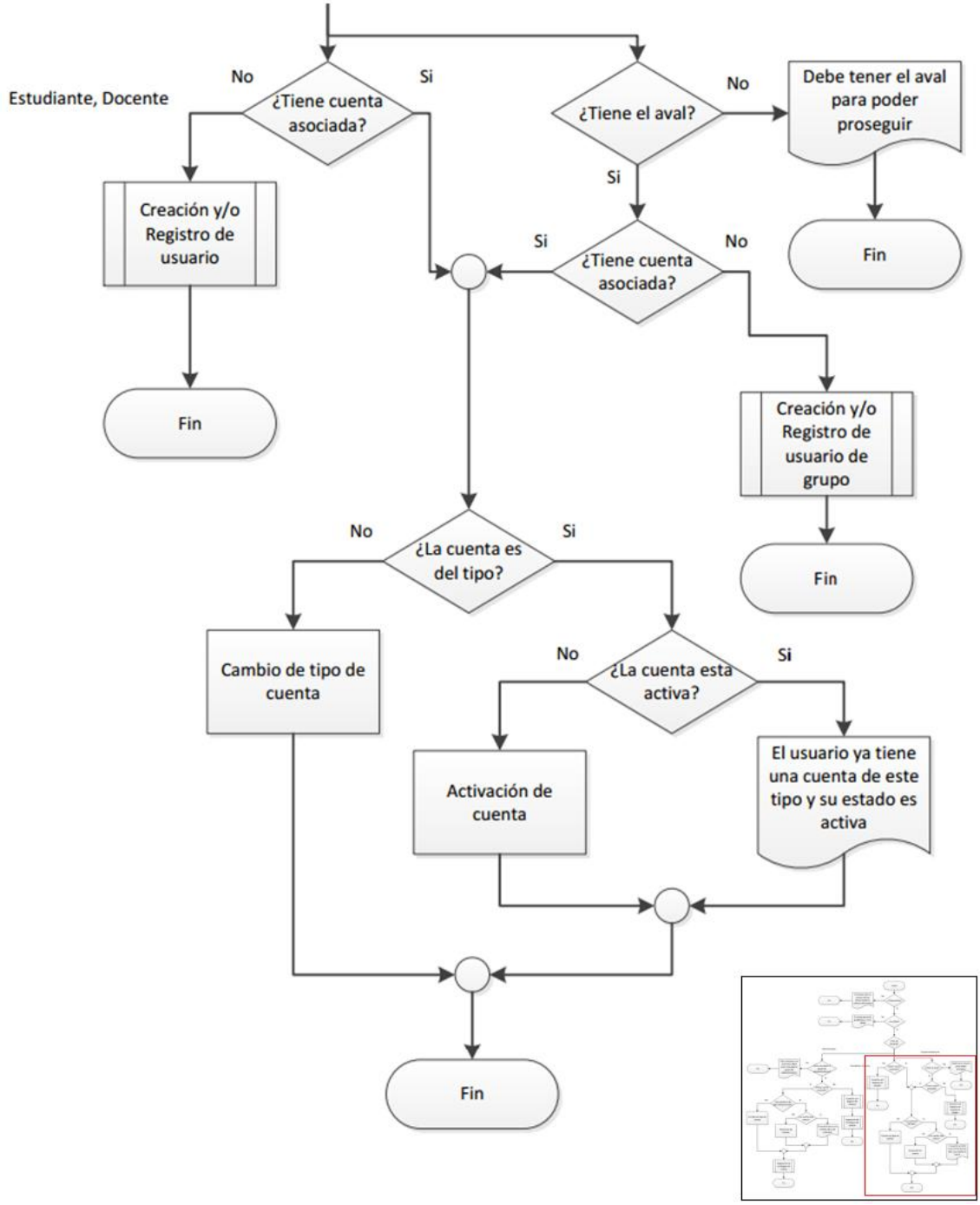

Ilustración 9 Procedimiento planteado Sección 3/3

4.3 Selección de Controles

Con base en el diagrama de flujo de datos de la definición del procedimiento que se realizó, se encontraron los diferentes puntos del mismo en los cuales era posible aplicar controles, esto se plasmo sobre el mismo diagrama dando como resultado el diagrama de flujo contenido en el anexo D sobre el cual se

pueden apreciar los siguientes controles:

- Control de verificación del carnet institucional.
- Control de verificación de cuentas asociadas.
- Control de verificación del tipo de cuenta.
- Control de relación de nombre de usuario con datos personales.
- Control de uso de papel.
- Control de asignación de privilegios.
- Control de administración de servidor.
- Control de robustez de contraseña.
- Control de realización de proceso.

Una vez identificados los controles sobre el diagrama de flujo mencionado anteriormente se procedió a verificar cuáles de estos eran candidatos y necesitaban la aplicación de alguna de las técnicas de inteligencia artificial, en este caso para cada control se realizó un estudio detallado de las entradas, los procesos y las salidas, a partir de lo cual se pudo seleccionar y/o descartar los controles sobre los cuales aplicar o no las técnicas de inteligencia artificial anexo E, con la evaluación anterior y buscando que los controles a desarrollar pudiesen ser aplicables en otros procedimientos de los diferentes servicios de la división de TIC, se seleccionaron como los controles a desarrollar el control de verificación del carnet institucional y el control de robustez de la contraseña, los cuales a partir de este punto se nombrados como control de validez del carnet y control de seguridad de la contraseña respectivamente; Teniendo en cuenta que el desarrollo del presente trabajo se centra en la familia de normas ISO 27000, se consultó el resumen de la norma ISO27002:2005 (Anexo A) y se pudo apreciar que con lo definido hasta el momento se está trabajando sobre:

Dominio: *11 Control de Acceso*

Objetivo de control: *11.2 Gestión de acceso de usuario*

Controles: *11.2.1 Registro de usuario*

11.2.3 Gestión de contraseñas de usuario.

Debido a que en la elección de controles se tuvo en cuenta que los mismos pudieran ser usados en diversos procedimientos y servicios, se puede identificar la influencia sobre los controles *9.1.2 Controles físicos de entrada* y el *11.3.1 Uso de Contraseñas,* logrando de esta forma un mayor impacto de los controles*.*

Capítulo V

Diseño y desarrollo de controles

El diseño y desarrollo del proyecto estará basado en el “Modelo Integral para el Profesional de Ingeniería” tomando el “Modelo para la construcción de soluciones”, cuyo propósito es el diseño y desarrollo de los controles inteligentes.

Para la utilización del “Modelos para la construcción de soluciones” se abarcan las siguientes fases:

- **Fase I** - Estructura para descripción del sistema: Diseño de los controles inteligentes para los dos servicios críticos encontrados en la División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca.

- **Fase II** - Modelo del proceso de desarrollo: Para el proceso de desarrollo del proyecto se aplicará una metodología ágil y activa, que permita resultados prácticos y concisos de una manera efectiva, por eso se acude a la metodología “Extreme Programming” ó “Metodología XP” [34], [35].

5.1 Fase I – Estructura para la descripción del sistema

Para realizar el proceso de diseño del los controles para dos de los servicios críticos, se efectuaron la siguiente serie de actividades:

- División por niveles.
- Definición de los sensores.
- Definición de las reglas de la forma si P y Q entonces R.

5.1.1 División por niveles

Se definió por cada control un diagrama el cual se ha llamado división en niveles, que consiste en encontrar la relación de la salida esperada del control

con un conjunto de características que ayudan al control a realizar una determinada evaluación. A partir de la división en niveles se logró una visualización más clara de cada uno de los elementos internos que hacen parte de los controles a desarrollar.

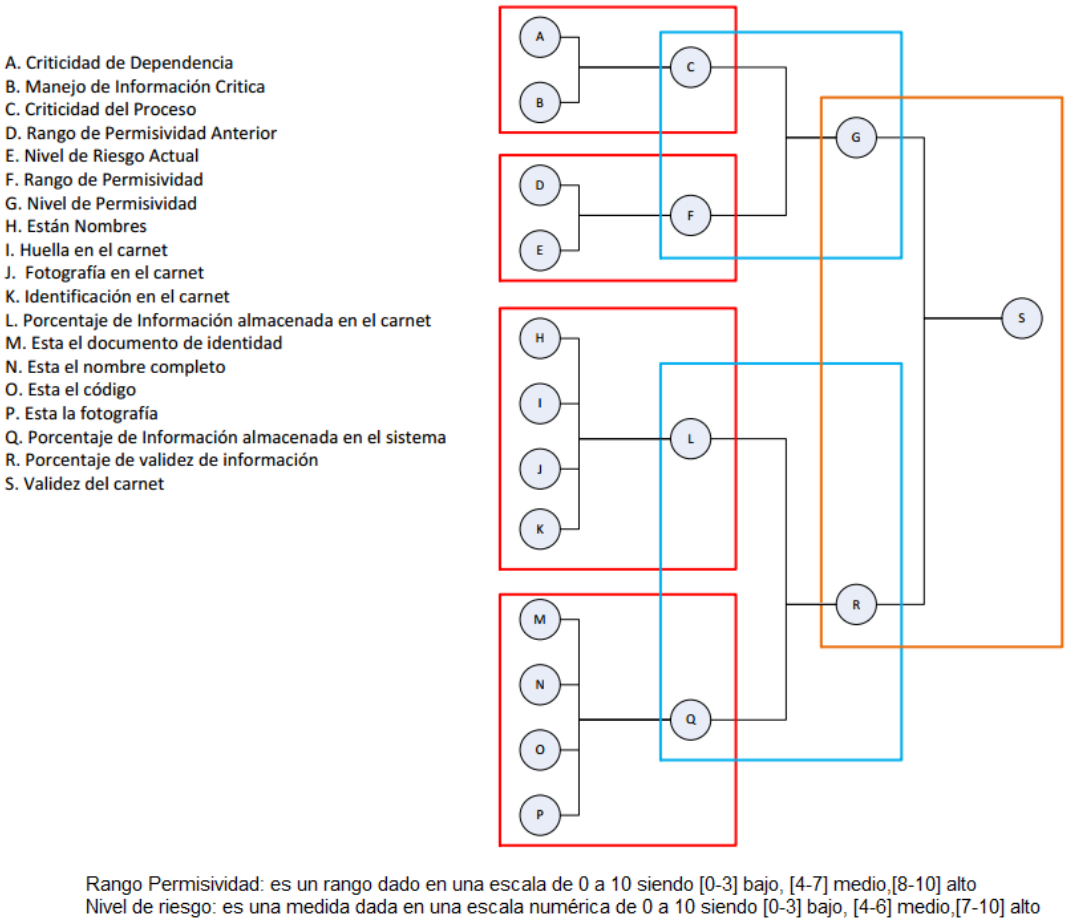

Ilustración 10 Diagrama de Control de Validez del Carnet

En el diagrama anterior, control de validez del carnet institucional, encontramos los diferentes bloques que nos sirven para visualizar la relación entre los elementos de cada categoría y de la misma forma visualizar como las entradas de una sección son resultado de la salida en la anterior y viceversa. Adicional a esto permite diferenciar la forma en la cual se establece cada categoría y de quien depende, esto con el fin de entender mejor la relación existente en cada una de las reglas a definir. Este diagrama está compuesto por dieciséis elementos que juntos definen el cumplimiento o no del objetivo del diagrama que es el control de validez del carnet institucional.

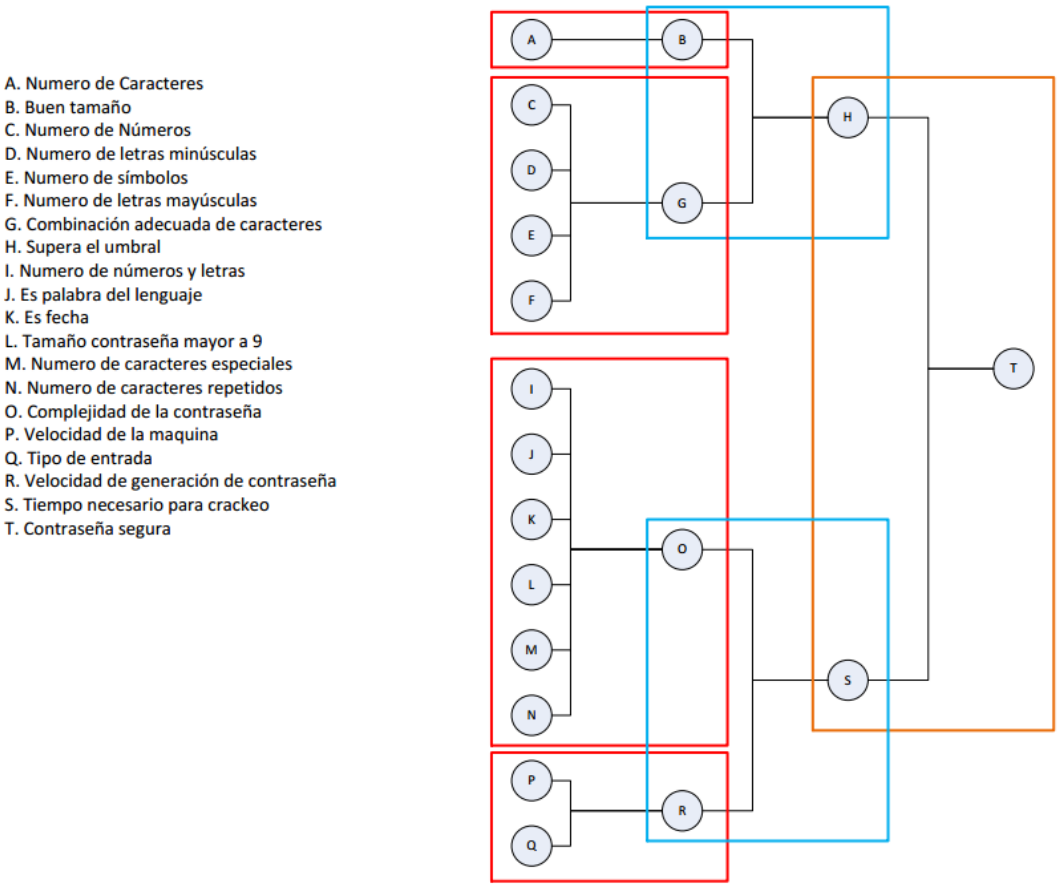

Ilustración 11 Diagrama de Control de Contraseña Segura

En el diagrama de control de contraseña segura, al igual que en el diagrama de control de validez del carnet, encontramos los diferentes bloques que nos sirven para visualizar la relación entre los elementos de cada categoría y de la misma forma visualizar como las entradas de una sección pueden llegar a ser el resultado de la anterior; este diagrama está compuesto por diecinueve elementos que juntos definen el cumplimiento o no del objetivo del control que es la verificación de si una contraseña es segura o no.

5.1.2 Definición de sensores:

Al ser un proyecto que se basa en técnicas de inteligencia artificial necesita de diferentes tipos de percepciones y acciones que son obtenidas o producidas por los diferentes sensores los cuales a su vez pueden ser físicos, mecánicos, pulsos eléctricos u ópticos en computadoras, o a la vez entradas y/o salidas de bits de un software y su entorno.

En la realización del proyecto se utilizaran alrededor de 24 sensores los cuales alimentaran el sistema de inferencia, estos sensores fueron escogidos y definidos haciendo uso de la división en niveles centrada únicamente en las especificaciones propias de cada control, los cuales como se evidencio anteriormente, surgieron a partir de los procedimientos que fueron planteados usando como referencia el documento de políticas de la división de TIC de la Universidad del Cauca. Los sensores usados para el desarrollo de este proyecto son:

Sensores para el control de validez del carnet:

- Criticidad de Dependencia: Teniendo en cuenta la dependencia actual indica que tan crítica es esta dependencia.
- Manejo de información crítica: Es la medida que nos indica que tan crítica es la información que se está manejando, en el proceso sobre el cual es necesario el uso del control de validez del carnet.
- Rango de permisividad anterior: Es la medida que indica que tan estricto es el sistema al verificar los datos en un punto anterior.
- Nivel de riesgo actual: Indica la probabilidad actual que ocurra un evento que afecte un determinado proceso.
- Identificación en el carnet: Indica si la identificación de la persona se encuentra almacenada en el carnet.
- Nombres en el carnet: Indica si los nombres de la persona se pueden obtener mediante la información almacenada en el carnet.
- Huella en el carnet: Indica si la huella de la persona se encuentra almacenada en el carnet.
- Fotografía en el carnet: Indica si la fotografía de la persona se pueden obtener mediante la información almacenada en el carnet.
- Identificación en el sistema: Indica si la identificación de la persona se encuentra almacenada en el sistema.
- Nombres en el sistema: Indica si los nombres de la persona se encuentran almacenados en el sistema.
- Código en el sistema: Indica si el código de la persona se encuentra almacenado en el sistema.

- Fotografía en el sistema: Indica si la fotografía se encuentra almacenada en el sistema.

Sensores para el control de contraseña segura:

- Número de caracteres: Indica el número de caracteres que tiene una contraseña este se considera bueno si es mayor a 9 caracteres.
- Cantidad de Números: Indica la cantidad de números que están contenidos en la contraseña.
- Letras Minúsculas: Indica la cantidad de letras minúsculas que están contenidas en la contraseña.
- Símbolos: Indica la cantidad de símbolos que están contenidos en la contraseña.
- Letras mayúsculas: Indica la cantidad de letras mayúsculas que están contenidas en la contraseña.
- Cantidad de letras: Indica el número de letras que están contenidos en una contraseña.
- Palabra del Lenguaje: Medida que determina si la contraseña es una palabra convencional que se encuentra en un lenguaje.
- Fecha: Determina si la contraseña es una fecha.
- Cantidad de caracteres especiales: Determina el número de caracteres especiales que contiene una contraseña.
- Cantidad de caracteres repetidos: Determina el número de caracteres repetidos dentro de una contraseña.
- Velocidad de la maquina: Indica la velocidad de procesamiento que tiene el equipo.
- Tiempo de crackeo: Indica el tiempo necesario para crackear una contraseña.
- Tipo de entrada: indica la forma como se va a realizar el crackeo que puede ser incremental o diccionario.

Con estos sensores se espera poder cumplir con el objetivo de cada control y lograr de esta manera el cumplimiento de los objetivos del proyecto.

5.1.3 Definición de las reglas si P y Q entonces R

Para continuar con el proceso de diseño de los controles inteligentes se procedió a partir de la división por niveles, a definir todas las reglas de la forma si P y Q entonces R, las cuales en un caso determinado podrían convertirse en la base de conocimiento de los controles inteligentes, un ejemplo de las reglas obtenidas es:

“Si tiempo de crakeo alto y contraseña supera el umbral entonces contraseña segura”

Tc Alto ∧ Uc Supera el umbral -> Ns Segura

“Si tiempo de crackeo medio y contraseña supera el umbral entonces contraseña aceptable.”

Tc Medio ∧ Uc Supera el umbral -> Ns Aceptable

En el anexo E se encuentra todo el conjunto de reglas que fueron definidas para los dos controles; lo anterior se realizó siguiendo las recomendaciones de uno de los expertos en inteligencia artificial. Vale la pena aclarar que la definición de reglas además de centrarse en la división en niveles de los controles también tuvo en cuenta los documentos de buenas prácticas que aplicaban en cada caso, todo esto debido a que más adelante las mismas podrían transformarse en la base de conocimiento para el sistema.

A partir de las definiciones anteriores y las características de las técnicas de inteligencia artificial candidatas (seleccionadas en la sección de caracterización), se descarta la técnica de redes neuronales debido a que no se cuenta con los escenarios suficientes para un correcto entrenamiento de las mismas, además de esto se necesita una técnica que permita la integración de reglas basadas en documentos de buenas prácticas y/o criterios de evaluación de expertos, motivo por el cual se selecciona a la lógica difusa como la técnica a aplicar en el desarrollo de los controles.

5.2 Fase II – Modelo del proceso de desarrollo:

Una vez realizado el diseño de los controles se procede a realizar su desarrollo, aplicando la metodología de desarrollo ágil “Extreme Programming” ó “Metodología XP” que cuenta con las siguientes fases:

- Fase de exploración.
- Fase de planificación.
- Fase de iteraciones.
- Fase de evaluación.

5.2.1 Fase de exploración

En la fase de exploración se realizaron las diferentes historias de usuario que ayudaron a tener una idea a un nivel muy alto de los controles en general. Las Historias de usuario realizadas son las siguientes:

Historia de Usuario	
Número: 001	**Nombre:** Monitoreo de nivel de riesgo
Usuario:	Administrador
Modificación de Historia Número:	**Iteración Asignada:**
Prioridad en Negocio: Alta	
Descripción:	El usuario administrador podrá a través de un dashboard o tablero de control monitorizar el nivel de riesgo actual del sistema.
Observaciones:	

Tabla 5 Historia de usuario monitoreo de nivel de riesgo

Historia de Usuario	
Número: 002	**Nombre:** Control de Validez del carnet Institucional
Usuario:	Funcionario
Modificación de Historia Número:	**Iteración Asignada:**
Prioridad en Negocio: Media	
Descripción:	En cada proceso que lo requiera se deberá de manera automática e inteligente realizar la verificación de la validez del carnet institucional

Observaciones:	

Tabla 6 Historia de usuario control de validez de carnet

Historia de Usuario	
Número: 003	**Nombre:** Control de Nivel de seguridad de contraseña
Usuario:	Funcionario
Modificación de Historia Número:	**Iteración Asignada:**
Prioridad en Negocio: Media	
Descripción:	En cada proceso que lo requiera se deberá de manera automática e inteligente verificar el nivel de la contraseña a ingresar (registro, cambio)
Observaciones:	

Tabla 7 Historia de usuario control de nivel de seguridad de contraseña

5.2.2 Fase de planificación

En esta fase se acordó el orden en el cual se desarrollarán las historias de usuario presentadas anteriormente asociando a estas un tiempo de entrega de máximo una semana para cada una de ellas; tiempo que fue estimado mediante la realización de un conjunto de reuniones grupales con los implicados en el proyecto que para este caso los desarrolladores y director.

Tarjeta de ingeniería	
Número de Tarea: 01	**Historia de Usuario:** 003
Nombre de Tarea: Implementación del control de nivel de seguridad de contraseña.	
Tipo de Tarea: Desarrollo	
Fecha Inicio:	**Fecha Fin:**
Programador Responsable: Carlos A. Rodallega, Oscar R. Valencia.	
Descripción:	

Tabla 8 Tarjeta de Ingeniería Control de Nivel de Seguridad de Contraseña

Tarjeta de ingeniería	
Número de Tarea: 02	**Historia de Usuario:** 002
Nombre de Tarea: Implementación del control de validez de carnet.	
Tipo de Tarea: Desarrollo	
Fecha Inicio:	**Fecha Fin:**
Programador Responsable: Carlos A. Rodallega, Oscar R. Valencia.	
Descripción:	

Tabla 9 Tarjeta de Ingeniería Control de Validez de Carnet

Tarjeta de ingeniería	
Número de Tarea: 03	**Historia de Usuario:** 001
Nombre de Tarea: Implementación del dashboard.	
Tipo de Tarea: Desarrollo	
Fecha Inicio:	**Fecha Fin:**
Programador Responsable: Carlos A. Rodallega, Oscar R. Valencia.	
Descripción: La implementación de este dashboard debe hacerse sobre cualquier plataforma web.	

Tabla 10 Tarjeta de Ingeniería DashBoard

5.2.3 Fase de iteraciones

Para esta fase con el fin del desarrollo de las diferentes historias de usuario presentadas anteriormente, se realizan cuatro iteraciones de la siguiente forma:

5.2.3.1 Iteración 1

Análisis y desarrollo de la historia de usuario Nro. 003, según la tarjeta de ingeniería 001, en donde se definió la tarjeta CRC de la clase palabra junto con el prototipo funcional de esta.

Nombre de la clase: palabra	

Responsabilidades
desglosar();
buscarDiccionario();
contarMayusculas();
ContarMinisculas();
contarNumeros();
contarSimbolos();
contarRepetidos();
esPalabra();
esFecha();
	Colaboradores

Tabla 11 CRC palabra

Como parte del proceso de análisis y desarrollo del control de nivel de seguridad de la contraseña, inicialmente fue necesaria la definición formal del modelo de lógica difusa correspondiente.

Para este modelo se definen las diferentes funciones de pertenencia usadas en el así como también las variables lingüísticas y el método de defusificación utilizado.

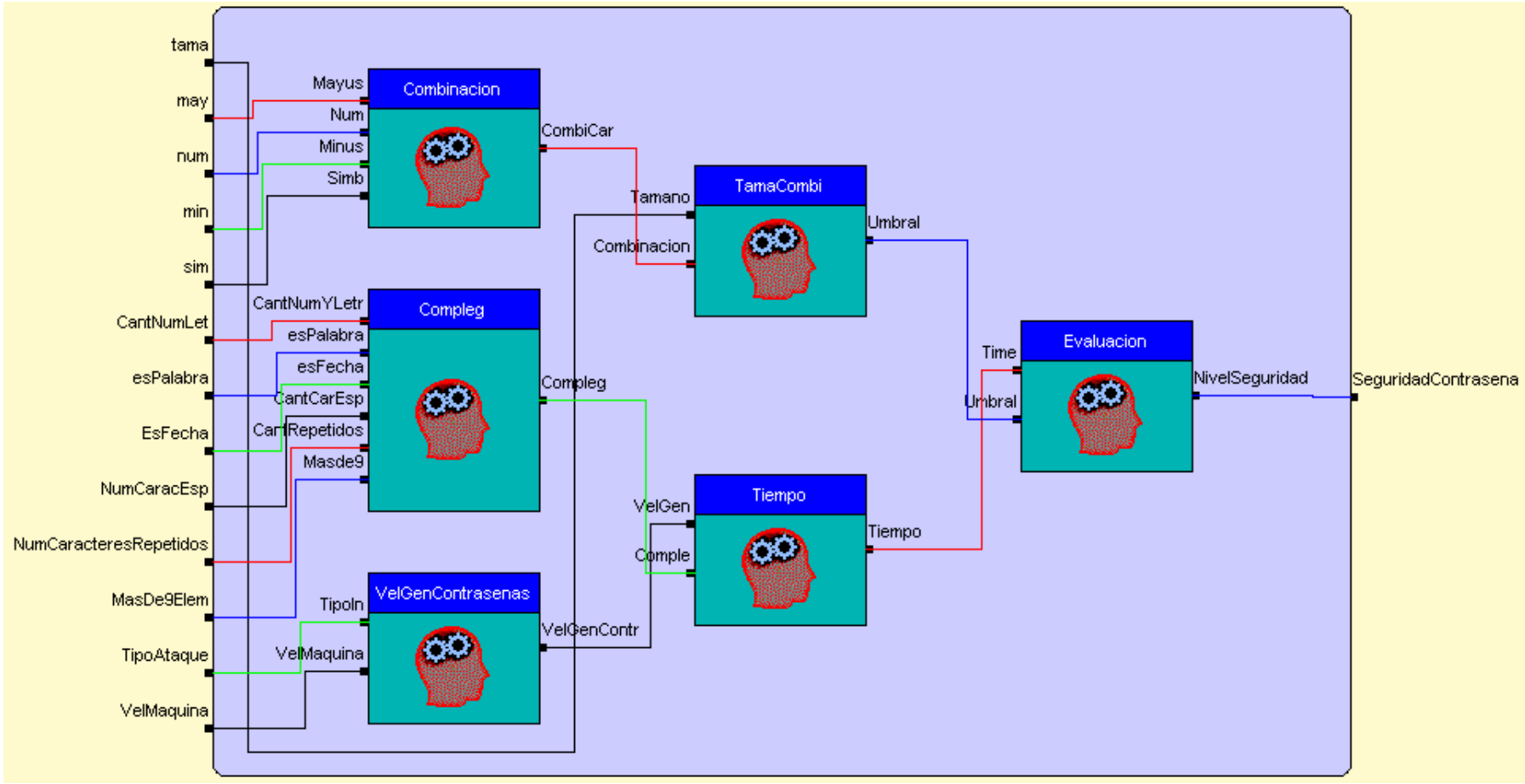

Ilustración 12 Diagrama Xfuzzy Control Seguridad Contraseña

La ilustración 12 presenta el diagrama del modelo de lógica difusa realizado (herramienta usada Xfuzzy) para el control de seguridad contraseña, el cual consta de 13 sensores los cuales se encargan de recibir la información que después es procesada por cada módulo (una llamada a una base de reglas) que junto con el mecanismo de inferencia obtiene la salida específica. Cada módulo representa una base de reglas con su respectiva función de pertenencia la cual depende únicamente de la información a evaluar.

A continuación se listan los diferentes módulos presentes en el diagrama:

- Combinación: Este módulo consta de cuatro entradas (mayúsculas, números, minúsculas, símbolos) y una salida (combinación de caracteres)

  La variable de entrada mayúsculas (may) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -6.0, 0.0, 2.0, 4.0) y alto (x: 3.0, 1.0).

  La variable de entrada números (num) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -6.0, 0.0, 2.0, 4.0) y alto (x: 3.0, 1.0).

  La variable de entrada minúsculas (min) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -6.0, 0.0, 2.0, 4.0) y alto (x: 3.0, 1.0).

  La variable de entrada símbolos (sim) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -6.0, 0.0, 2.0, 4.0) y alto (x: 3.0, 1.0).

  La variable de salida combinación de caracteres (CombiCar) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -0.5, 0.0, 0.5, 1.5), media (x: 0.5, 1.5, 2.5, 3.5) y alta (x: 3.0, 3.2, 4.0, 4.5).
- Compleg: Este módulo costa de seis variables de entrada (cantidad de números y letras, es palabra, es fecha, cantidad de caracteres especiales, cantidad de repetidos, longitud mayor a nueve) y una salida (complejidad de contraseña).

La variable de entrada cantidad de números y letras (CantNumYLetr) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas baja (x: -10.0, 0.0, 6.0, 10.0) y alta (x: 6.0, 10.0, 50.0, 60.0).

La variable de entrada es palabra (esPalabra), esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas, no con un valor de 0 y si con un valor de 1.

La variable de entrada es fecha (EsFecha) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas, no con un valor de 0 y si con un valor de 1.

La variable de entrada cantidad de caracteres especiales (NumCaracEsp) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas baja (x: -10.0, 0.0, 1.0, 5.0) y alta (x: 1.0, 5.0, 50.0, 60.0).

La variable de entrada cantidad de repetidos (NumCaracteresRep) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas baja (x: -10.0, 0.0, 1.0, 5.0) y alta (x: 1.0, 5.0, 50.0, 60.0).

La variable de entrada longitud mayor a nueve (Masde9eleme) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas no con un valor de 0 y si con un valor de 1.

La variable de salida complejidad de contraseña (CompC) esta expresada mediante una función de tipo campana de gauss (bell) y tiene como variables lingüísticas baja (x: 0.0, 1.99999999999), media (x: 4.0, 1.9999999999999998) y alta (x: 6.0, 1.7999999999999998).

- VelGenContrasenas: Este módulo costa de dos variables de entrada (tipo ataque, velocidad de maquina) y una salida (velocidad generación de contraseña).

  La variable de entrada tipo ataque (TipoAtaque) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas incremental con un valor de 0 y diccionario con un valor de 1.

La variable de entrada velocidad de la máquina (VelMaquina) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas lenta (x: -125.0, 0.0, 250.0, 375.0), media (x: 250.0, 375.0, 625.0, 750.0) y rápida (x: 625.0, 750.0, 1000.0, 1125.0).

La variable de salida velocidad generación de contraseña (VelGenContr) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -1.25, 0.0, 2.5, 3.75), media (x: 2.5, 3.75, 6.25, 7.5) y alto (x: 6.25, 7.5, 10.0, 11.25).

- TamaCombi: Este módulo consta de dos variables de entrada (tamaño y combinación) y una salida (umbral).

  La variable de entrada tamaño (tama) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas maloTamano (x: -10.0, 0.0, 8.0, 10.0) y buenTamano (x: 8.0, 10.0, 30.0, 40.0).

  La variable de entrada combinación (combinacion) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas baja (x: -0.5, 0.0, 0.5, 1.5), media (x: 0.5, 1.5, 2.5, 3.5) y alta (x: 3.0, 3.2, 4.0, 4.5).

  La variable de salida umbral (Umbral) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas inferiorUmbral (x: -2.0, 0.0, 1.5, 2.5), umbralMedio (x: 1.5, 2.5, 4.5, 5.5) y superaUmbral (x: 4.5, 5.5, 6.0, 8.0).

- Tiempo: Este módulo costa de dos variables de entrada (velocidad de generación y complejidad) y una salida (tiempo generación).

  La variable de entrada velocidad de generación (VelGen) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -1.25, 0.0, 2.5, 3.75), media (x: 2.5, 3.75, 6.25, 7.5) y alto (x: 6.25, 7.5, 10.0, 11.25).

  La variable de entrada complejidad (Comple) esta expresada mediante una función de tipo campana de Gauss (bell) y tiene como variables lingüísticas baja (x: 0.0, 1.99999999999), media (x: 4.0, 1.9999999999999998) y alta (x: 6.0, 1.7999999999999998).

La variable de salida tiempo (tiempo) esta expresada mediante la función de tipo trapezoidal y triangular y tiene como variables lingüísticas bajo (x: -10800.0, 10800.0, 21600.0), medio (x: 10800.0, 21600.0, 32400.0) y alto (x: 21600.0, 32400.0, 43200.0, 54000.0).

- Evaluación: Este módulo costa de dos variables de entrada (tiempo y umbral) y una salida (nivel de seguridad).

  La variable de entrada tiempo (time) esta expresada mediante la función de tipo trapezoidal y triangular y tiene como variables lingüísticas bajo (x: -10800.0, 10800.0, 21600.0), medio (x: 10800.0, 21600.0, 32400.0) y alto (x: 21600.0, 32400.0, 43200.0, 54000.0).

  La variable de entrada umbral (Umbral) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas inferiorUmbral (x: -2.0, 0.0, 1.5, 2.5), umbralMedio (x: 1.5, 2.5, 4.5, 5.5) y superaUmbral (x: 4.5, 5.5, 6.0, 8.0).

  La variable de salida nivel de seguridad (NivelSeguridad) esta expresada mediante la función de tipo trapezoidal y tiene como variables lingüísticas insegura (x: -1.25, 3.5, 4.75), aceptable (x: 3.5, 4.0, 8.0, 9.0) y segura (x: 8.0, 9.0, 10.0, 11.25).

Este diagrama usa los operadores por defecto es decir que utiliza el operador T-Norma, además para el proceso de defusificación se utilizó el método de FuzzyMean, cabe resaltar este ajuste del sistema fue realizado mediante pruebas no formales con cada uno de los métodos hasta encontrar uno que se ajustara al comportamiento esperado. Finalmente se procedió a exportar el código del modelo a java y crear el prototipo funcional del mismo.

5.2.3.2 Iteración 2

Análisis y desarrollo de la historia de usuario Nro. 002, según la tarjeta de ingeniería 002, definición de tarjeta CRC Carnet perteneciente a esta iteración junto con el prototipo funcional de esta.

Nombre de la clase: carnet	
Responsabilidades obtenerElementos();	**Colaboradores**

Tabla 12 CRC Carnet

Como parte del proceso de análisis y desarrollo del control de validez del carnet, inicialmente fue necesaria la definición formal del modelo de lógica difusa correspondiente.

Para este modelo se definen las diferentes funciones de pertenencia usadas en el así como también las variables lingüísticas y el método de defusificación utilizado.

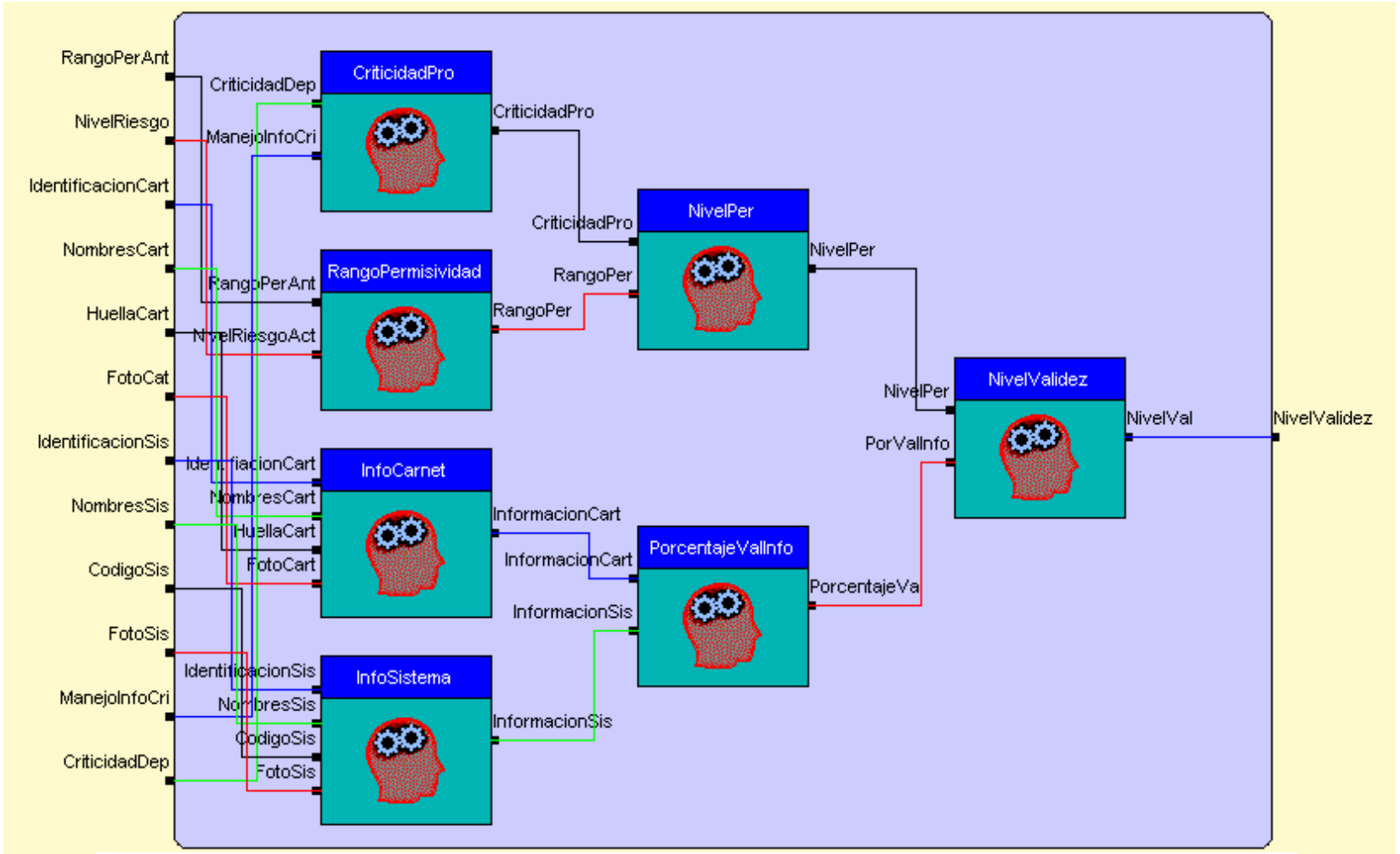

Ilustración 13 Diagrama Xfuzzy Control Validez Carnet

En la ilustración 13 se puede apreciar el diagrama hecho en Xfuzzy para el control de validez del carnet el cual consta de 12 sensores los cuales se encargan de recibir la información que después es procesada por cada módulo (una llamada a una base de reglas), que junto con el mecanismo de inferencia obtiene la salida específica. Cada módulo representa una base de reglas con su respectiva función de pertenencia la cual depende únicamente de la información a evaluar, a continuación se listan los diferentes módulos presentes en el diagrama:

- CriticidadPro: Este módulo consta de dos entradas (criticidad de la dependencia y el manejo de información crítica) y una salida (criticidad del proceso).

  La variable de entrada criticidad de la dependencia (CriticidadDep) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -1.25, 0.0, 2.5, 3.75), medio (x: 2.5, 3.75, 6.25, 7.5) y alto (x: 6.25, 7.5, 10.0, 11.25).

  La variable de entrada manejo de información critica (ManejoInfoCri) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -1.25, 0.0, 2.5, 3.75), medio (x: 2.5, 3.75, 6.25, 7.5) y alto (x: 6.25, 7.5, 10.0, 11.25).

  La variable de salida criticidad del proceso (CriticidadPro) esta expresada mediante una función singleton y tiene como variables lingüísticas bajo con el valor de 0 y alto con el valor de 1.
- RangoPermisividad: Este módulo consta de 2 entradas (rango de permisividad anterior y nivel de riesgo actual) y una salida (rango de permisividad).

  La variable de entrada rango de permisividad anterior (RangoPerAnt) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -1.25, 0.0, 2.5, 3.75), medio (x: 2.5, 3.75, 6.25, 7.5) y alto (x: 6.25, 7.5, 10.0, 11.25).

  La variable de entrada nivel de riesgo actual (NivelRiegoAct) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -1.25, 0.0, 2.5, 3.75), medio (x: 2.5, 3.75,

6.25, 7.5) y alto (x: 6.25, 7.5, 10.0, 11.25).

La variable de salida rango de permisividad (RangoPer) esta expresada mediante una función de tipo trapezoidal y tienen como variables lingüísticas bajo (x: -1.25, 0.0, 2.5, 3.75), medio (x: 2.5, 3.75, 6.25, 7.5) y alto (x: 6.25, 7.5, 10.0, 11.25).

- InfoCarnet: Este módulo consta de cuatro variables de entrada (identificación carnet, nombres carnet, huella carnet y foto carnet) y una salida (información carnet).

  La variable de entrada identificación carnet (IndentificacionCart) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas bajo con un valor de 0 y alto con un valor de 1.

  La variable de entrada nombres carnet (NombresCart) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas bajo con un valor de 0 y alto con un valor de 1.

  La variable de entrada huella carnet (HuellaCart) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas, bajo con un valor de 0 y alto con un valor de 1.

  La variable de entrada foto carnet (FotoCart) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas, bajo con un valor de 0 y alto con un valor de 1.

  La variable de salida información carnet (InformacionCart) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas, bajo con un valor de 0 y alto con un valor de 1.

- InfoSistema: Este módulo consta de de cuatro variables de entrada (identificación sistema, nombres sistema, código sistema, foto sistema) y una salida (información sistema).

  La variable de entrada identificación sistema (IdentificacionSis) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas, bajo con un valor de 0 y alto con un valor de 1.

  La variable de entrada nombres sistema (NombresSis) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas, bajo con un valor de 0 y alto con un valor de 1.

La variable de entrada código sistema (CodigoSis) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas, bajo con un valor de 0 y alto con un valor de 1.

La variable de entrada foto sistema (FotoSis) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas, bajo con un valor de 0 y alto con un valor de 1.

La variable de salida información sistema (InformacionSis) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas, bajo con un valor de 0 y alto con un valor de 1.

- NivelPer: Este módulo consta de dos variables de entrada (criticidad del proceso y rango de permisividad) y una salida (nivel de permisividad).

  La variable de entrada criticidad del proceso (CriticidadPro) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas, bajo con un valor de 0 y alto con un valor de 1.

  La variable de entrada rango de permisividad (RangoPer) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -1.25, 0.0, 2.5, 3.75), medio (x: 2.5, 3.75, 6.25, 7.5) y alto (x: 6.25, 7.5, 10.0, 11.25).

  La variable de salida nivel de permisividad (NivelPer) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: 0.4, 1.0, 2.2, 2.8) y alto (x: 2.2, 2.8, 4.0, 4.6).

- PorcentajeValInfo: Este módulo consta de dos variables de entrada (información carnet y información sistema) y una salida (porcentaje de validez).

  La variable de entrada información carnet (InformacionCart) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas bajo con un valor de 0 y alto con un valor de 1.

  La variable de entrada información sistema (InformacionSis) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas bajo con un valor de 0 y alto con un valor de 1.

  La variable de salida porcentaje de validez (PorcentajeVal) esta expresada mediante una función de tipo trapezoidal y tiene como

variables lingüísticas bajo (x: -0.75, 0.0, 1.5, 2.25), medio (x: 1.5, 2.25, 3.75, 4.5) y alto (x: 3.75, 2 4.5, 6.0, 6.75).

- NivelValidez: Este módulo consta de dos variables de entrada (nivel de permisividad y porcentaje validez de información) y una salida (nivel de validez).

  La variable de entrada nivel de permisividad (NivelPer) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: 0.4, 1.0, 2.2, 2.8) y alto (x: 2.2, 2.8, 4.0, 4.6).

  La variable de entrada porcentaje de validez (PorValInfo) esta expresada mediante una función de tipo trapezoidal y tiene como variables lingüísticas bajo (x: -0.75, 0.0, 1.5, 2.25), medio (x: 1.5, 2.25, 3.75, 4.5) y alto (x: 3.75, 2 4.5, 6.0, 6.75).

  La variable de salida nivel de validez (NivelVal) esta expresada mediante una función de tipo singleton y tiene como variables lingüísticas, bajo con un valor de 0 y alto con un valor de 1.

Este diagrama usa los operadores por defecto es decir que utiliza el operador T-Norma, además para el proceso de defusificación se utilizó el método de FuzzyMean, cabe resaltar este ajuste del sistema fue realizado mediante pruebas no formales con cada uno de los métodos hasta encontrar uno que se ajustara al comportamiento esperado. Finalmente se procedió a exportar el código del modelo a java y crear el prototipo funcional del mismo.

5.2.3.3 Iteración 3

Adecuación de los prototipos producto de las iteraciones 1 y 2 correspondientes a las historias de usuario Nro. 002 y Nro. 003 a la tecnología de WebServices, iteración en la cual fue necesario definir las tarjetas correspondientes a las clases de gestión y cuyo prototipo funcional son los Web Services en Java

Nombre de la clase: gestionSeguridadContrasena	

Responsabilidades
analizarContrasena();
registrarSalida();
controlActivo();
analizarSalida();
medirControl();
	Colaboradores

Tabla 13 CRC gestionSeguridadContrasena

Nombre de la clase: gestionValidezCarnet	

Responsabilidades
validarCarnet();
registrarSalida();
controlActivo();
medirControl();
analizarSalida();
	Colaboradores

Tabla 14 CRC gestionValidezCarnet

Esta historia de usuario surge a partir de la reunión de entrega de los productos de las iteraciones 1 y 2, debido a que analizando que el entorno de implementación de los mismos podía ser muy amplio, así como el hecho de que cada control puede ser usado en diversos procedimientos se decidió basar el desarrollo de los controles haciendo uso de la tecnología de WebServices, logrando de esta manera unos controles más flexibles, con una buena interoperabilidad y con la ventaja de que los cambios que se realicen posteriormente no tuviesen que replicarse en los procedimientos que los utilicen; adicional a esto el procesamiento está del lado del servidor con lo cual se evita las exigencias en cuanto al rendimiento de los dispositivos que hagan uso de los mismos. En la siguiente ilustración se puede apreciar la arquitectura de los controles basados en WebServices.

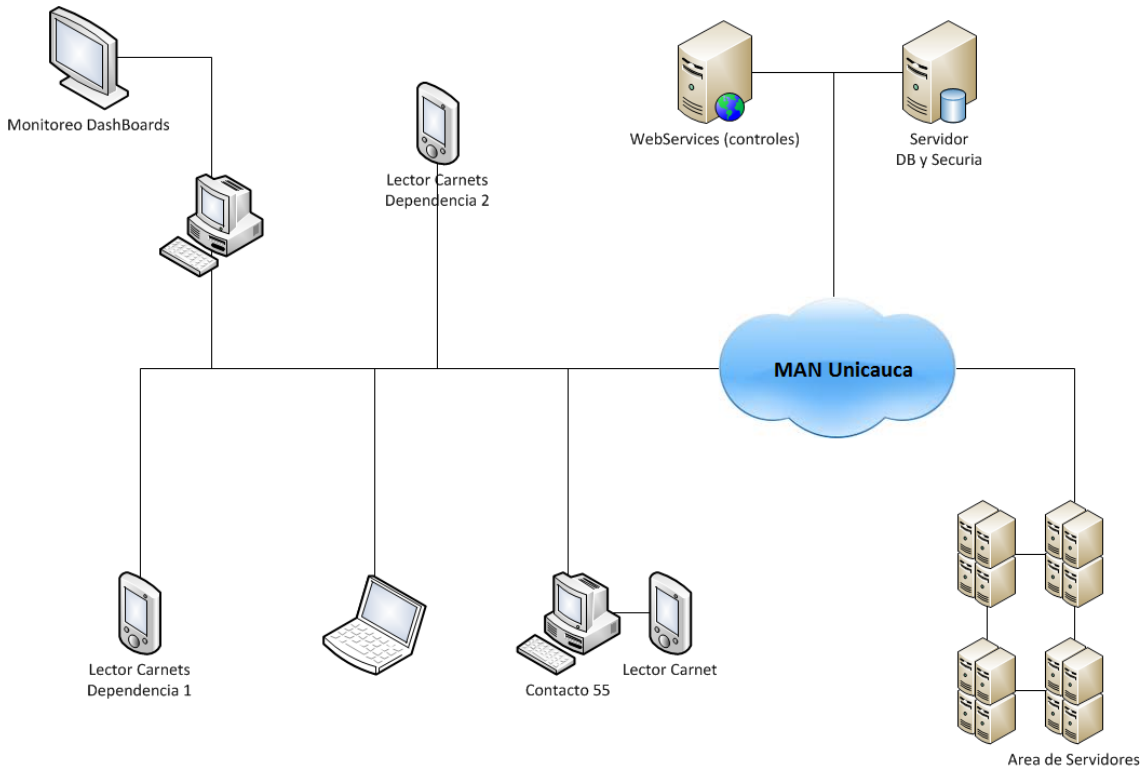

Ilustración 14 Arquitectura basada en Web Services

Los WebServices producto de esta iteración, hacen parte de los entregables del presente proyecto.

5.2.3.4 Iteración 4

Análisis y desarrollo de la historia de usuario Nro. 001, tarjeta de ingeniería 3 y el prototipo funcional de esta (aplicación web sobre php).

5.2.4 Fase evaluación

En esta fase se contemplan las diferentes pruebas que se realizan al desarrollo, el cual es el producto de las anteriores fases teniendo en cuenta las tareas necesarias para el reajuste de los mismos.

5.2.4.1 Evaluación del control de nivel de seguridad de la contraseña

En esta etapa del desarrollo se realizaron una serie de evaluaciones para tratar de verificar que tan acertado o alejado es el control de seguridad de contraseña, para este ejercicio se escogió un conjunto de contraseñas para que fueran evaluadas por tres diferentes expertos y luego estas mismas

contraseñas fueran evaluadas el control con el fin de comparar y concluir acerca de este.

A continuación la lista de contraseña junto con los resultados obtenidos:

Contraseña	Evaluación Experto	Evaluación Control
abcd123	Bajo	Bajo
Qwerty	Bajo	Bajo
12345	Bajo	Bajo
m1m4m1t4m3!!	Bajo	Alto
P4s.w0R!d	Alto	Bajo
MyP4ss	Bajo	Bajo
Monkey	Bajo	Bajo
B4r.c3l0n@	Alto	Alto
r3.4!M@dr1D	Alto	Alto
Leahcim12	Aceptable	Bajo
LuisC1980	Aceptable	Aceptable
Ju4n.C@r!0s	Alto	Alto
Peluchin	Bajo	Bajo
M0t4s	Bajo	Bajo
Hacker	Bajo	Bajo
881207	Bajo	Bajo
pinky82	Bajo	Bajo
Valent1na	Bajo	Bajo
Popayan	Bajo	Bajo
juvaro110	Bajo	Aceptable

Tabla 15 Lista de Contraseñas a Evaluar Experto uno

En la tabla 15 se encuentra una lista con diferentes contraseñas las cuales poseen un nivel de seguridad que va a ser analizado por el experto uno con los rangos de bajo, aceptable y alto. En este caso comparando los resultados obtenidos con el control y los brindados por el experto uno encontramos que coinciden 16 respuestas de un total de 20, y difieren en 4 resultados para los cuales se tiene que en 2 de ellos el sistema es aparentemente más riguroso o exigente para dar su evaluación con respecto a la seguridad de la contraseña.

Lo que nos indica que el control de contraseña segura tiene un porcentaje de acierto del 80% con respecto a los resultados brindados por el experto uno.

Contraseña	Evaluación Experto	Evaluación Control
abcd123	Bajo	Bajo
Qwerty	Bajo	Bajo
12345	Bajo	Bajo
m1m4m1t4m3!!	Aceptable	Alto
P4s.w0R!d	Bajo	Bajo
MyP4ss	Bajo	Bajo
Monkey	Bajo	Bajo
B4r.c3l0n@	Aceptable	Alto
r3.4!M@dr1D	Aceptable	Alto
Leahcim12	Bajo	Bajo
LuisC1980	Bajo	Aceptable
Ju4n.C@r!0s	Bajo	Alto
Peluchin	Bajo	Bajo
M0t4s	Bajo	Bajo
Hacker	Bajo	Bajo
881207	Bajo	Bajo
pinky82	Bajo	Bajo
Valent1na	Bajo	Bajo
Popayan	Bajo	Bajo
juvaro110	Bajo	Aceptable

Tabla 16 Lista de Contraseñas a Evaluar Experto dos

En la tabla 16 se encuentra una lista con diferentes contraseñas las cuales poseen un nivel de seguridad que va a ser analizado por el experto dos con los rangos de bajo, aceptable y alto. En este caso comparando los resultados obtenidos con el control y los brindados por el experto dos encontramos que coinciden 14 respuestas de un total de 20.

Lo que nos indica que el control de contraseña segura tiene un porcentaje de acierto del 70% con respecto a los resultados brindados por el experto dos.

Contraseña	Evaluación Experto	Evaluación Control
abcd123	Bajo	Bajo
Qwerty	Bajo	Bajo
12345	Bajo	Bajo
m1m4m1t4m3!!	Aceptable	Alto
P4s.w0R!d	Alto	Bajo
MyP4ss	Bajo	Bajo
Monkey	Bajo	Bajo
B4r.c3l0n@	Aceptable	Alto
r3.4!M@dr1D	Aceptable	Alto
Leahcim12	Aceptable	Bajo
LuisC1980	Aceptable	Aceptable

Ju4n.C@r!0s	Bajo	Alto
Peluchin	Bajo	Bajo
M0t4s	Bajo	Bajo
Hacker	Bajo	Bajo
881207	Bajo	Bajo
pinky82	Bajo	Bajo
Valent1na	Bajo	Bajo
Popayan	Bajo	Bajo
juvaro110	Aceptable	Aceptable

Tabla 17 Lista de Contraseñas a Evaluar Experto tres

En la tabla 17 se encuentra una lista con diferentes contraseñas las cuales poseen un nivel de seguridad que va a ser analizado por el experto tres con los rangos de bajo, aceptable y alto. En este caso comparando los resultados obtenidos con el control y los brindados por el experto tres encontramos que coinciden 14 respuestas de un total de 20, y difieren en 6 resultados para los cuales se tiene que en dos de estas el control fue aparentemente más riguroso o exigente para la evaluación de la seguridad de las contraseñas. Lo que nos indica que el control de contraseña segura tiene un porcentaje de acierto del 70% con respecto a los resultados brindados por el experto tres.

A partir de los porcentajes de acierto en cada uno de los casos frente a los expertos, se tienen que el porcentaje de acierto promedio del control es del 73.3%.

Con el fin de realizar un análisis general de las evaluaciones hechas por el control frente las evaluaciones de los expertos, se unificaron las tablas anteriores de la siguiente manera:

Contraseña	Experto 1	Experto 2	Experto 3	Control
abcd123	Bajo	Bajo	Bajo	Bajo
Qwerty	Bajo	Bajo	Bajo	Bajo
12345	Bajo	Bajo	Bajo	Bajo
m1m4m1t4m3!!	Bajo	Aceptable	Aceptable	Alto
P4s.w0R!d	Alto	Bajo	Alto	Bajo
MyP4ss	Bajo	Bajo	Bajo	Bajo
Monkey	Bajo	Bajo	Bajo	Bajo
B4r.c3l0n@	Alto	Aceptable	Aceptable	Alto
r3.4!M@dr1D	Alto	Aceptable	Aceptable	Alto
Leahcim12	Aceptable	Bajo	Aceptable	Bajo

LuisC1980	Aceptable	Bajo	Aceptable	Aceptable
Ju4n.C@r!0s	Alto	Bajo	Bajo	Alto
Peluchin	Bajo	Bajo	Bajo	Bajo
M0t4s	Bajo	Bajo	Bajo	Bajo
Hacker	Bajo	Bajo	Bajo	Bajo
881207	Bajo	Bajo	Bajo	Bajo
pinky82	Bajo	Bajo	Bajo	Bajo
Valent1na	Bajo	Bajo	Bajo	Bajo
Popayan	Bajo	Bajo	Bajo	Bajo
juvaro110	Bajo	Bajo	Aceptable	Aceptable

Tabla 18 Evaluación expertos VS Evaluación Control

En la tabla anterior se puede apreciar que las evaluaciones de los expertos no llegan a un acuerdo específico sobre si una contraseña tiene nivel de seguridad bajo, aceptable o alto, lo anterior se debe a que cada experto tiene sus propios criterios de evaluación, pese a lo anterior es evidente que existe un nivel de correlación en sus evaluaciones, en el caso del control cuyo desarrollo se centra en los documentos de buenas prácticas se puede apreciar que existe un alto margen de compatibilidad con los expertos a la hora de identificar niveles bajos de seguridad en las contraseñas; de la misma manera el control solo definió como aceptable o alto (filas sombreadas) las contraseñas que bajo los criterios de evaluación de los expertos estos habían definido en estos dos grupos, siendo los expertos más rigurosos solo en uno de los casos.

Buscando realizar un análisis cuantitativo se definieron los siguientes valores numéricos para cada una de las variables cualitativas:

Valor Cualitativo	Valor Numérico
Bajo	1
Aceptable	2
Alto	3

Tabla 19 Conversión de valores cualitativos a cuantitativos

Valores que con base en la tabla 18 permitieron la definición de la siguiente tabla:

Contraseña	Experto 1	Experto 2	Experto 3	Promedio Expertos	Control	Error
abcd123	1	1	1	1	1	0
Qwerty	1	1	1	1	1	0
12345	1	1	1	1	1	0
m1m4m1t4m3!!	1	2	2	1.66	3	1.34
P4s.w0R!d	3	1	3	2.3	1	1.3
MyP4ss	1	1	1	1	1	0
Monkey	1	1	1	1	1	0
B4r.c3l0n@	3	2	2	2.3	3	0.7
r3.4!M@dr1D	3	2	2	2.3	3	0.7
Leahcim12	2	1	2	1.66	1	0.66
LuisC1980	2	1	2	1.66	2	0.34
Ju4n.C@r!0s	3	1	1	1.66	3	1.4
Peluchin	1	1	1	1	1	0
M0t4s	1	1	1	1	1	0
Hacker	1	1	1	1	1	0
881207	1	1	1	1	1	0
pinky82	1	1	1	1	1	0
Valent1na	1	1	1	1	1	0
Popayan	1	1	1	1	1	0
juvaro110	1	1	2	1.33	2	0.67

Tabla 20 Evaluación cuantitativa resultados control contraseña segura

Con base en los errores calculados se obtuvo el error promedio para esta muestra de 20 elementos el cual alcanzó un valor de 0.35.

Con los resultados obtenidos en la evaluación del control de nivel de seguridad de la contraseña y el análisis hecho en cada uno de los escenarios, se puede concluir que el control de nivel de seguridad de la contraseña, tiene un comportamiento adecuado para las necesidades del presente proyecto.

5.2.4.2 Evaluación del control de nivel de seguridad de la contraseña

Partiendo de las pruebas de evaluación realizadas para el control de nivel de seguridad de la contraseña, en las cuales los resultados fueron evaluados con base en la opinión de varios expertos, se tiene que en el caso del control de validez del carnet, al ser un control propio producto del desarrollo de este proyecto (basándose en las condiciones de la Universidad del Cauca y la información brindada acerca del sistema de carnets institucionales), las pruebas se realizaran con base a una serie de posibles situaciones las cuales

tienen asociada una salida esperada, con base en la cual se evaluaran las salidas del control.

Escenarios planteados	Salida Esperada	Salida del Control
Acceso en las entradas principales con carnet institucional con información completa e información en el sistema completa: Criticidad Dependencia baja, Manejo de información critica en procedimiento baja , nivel de riesgo medio, rango de permisividad anterior medio	Válido	Válido
Acceso en las entradas principales con carnet institucional con información parcial e información en el sistema parcial: Criticidad Dependencia baja, Manejo de información critica en procedimiento baja , nivel de riesgo medio, rango de permisividad anterior medio	Válido	Válido
Acceso en las entradas principales con carnet institucional con información completa e información en el sistema completa (caso especial ejemplo rectoría): Criticidad Dependencia alta, Manejo de información critica en procedimiento baja , nivel de riesgo medio, rango de permisividad anterior medio	Válido	Válido
Acceso en las entradas principales con carnet institucional con información parcial e información en el sistema parcial (caso especial ejemplo rectoría): Criticidad Dependencia alta, Manejo de información critica en procedimiento baja , nivel de riesgo medio, rango de permisividad anterior medio	Inválido	Inválido
Creación de cuenta de correo electrónico con carnet institucional con información completa e información en el sistema completa: Criticidad Dependencia media, Manejo de información critica en procedimiento alta , nivel de riesgo medio, rango de permisividad anterior medio	Válido	Válido
Creación de cuenta de correo electrónico con carnet institucional con información completa y sin información en el sistema (carnet falso): Criticidad Dependencia media, Manejo de información critica en procedimiento alta , nivel de riesgo medio, rango de permisividad anterior medio	Inválido	Inválido
Creación de cuenta de correo electrónico con carnet institucional con información parcial e información en el sistema parcial: Criticidad Dependencia media, Manejo de información	Válido	Inválido

critica en procedimiento alta , nivel de riesgo medio, rango de permisividad anterior medio		
Creación de cuenta de correo electrónico con carnet institucional con información parcial e información en el sistema parcial: Criticidad Dependencia media, Manejo de información critica en procedimiento alta , nivel de riesgo bajo, rango de permisividad anterior medio	Válido	Válido

Tabla 21 Escenarios de prueba control validez de carnet

En la tabla 21 se puede apreciar que las salidas del control tienen un acierto en 7 de los 8 escenarios planteados, lo cual permite establecer un porcentaje de acierto del 87,5%, a partir de lo cual se puede establecer que el control presenta un comportamiento adecuado.

5.2.4.3 Evaluación de los dashboard

Para la evaluación de los dashboard al ser una aplicación de carga y presentación de información, la evaluación se centró en pruebas funcionales, en las cuales se verificó si la información era accedida y presentada de la manera adecuada.

Ilustración 15 Pruebas funcionales dashboard 1

Ilustración 16 Pruebas funcionales dashboard 2

Finalmente a partir de las pruebas de funcionalidad los dashboard, se encontró que la aplicación de monitoreo a parte de cumplir con las especificaciones, también presenta un comportamiento adecuado.

Finalmente con diseño, desarrollo y evaluación haciendo uso del “Modelo para la construcción de soluciones” en conjunto de la metodología de desarrollo “XP Extreme Programming”, se logró la definición y desarrollo de los modelos de lógica difusa necesarios, los cuales una vez integrados a los controles, permitió finalmente la obtención de los dos controles basados en técnicas de inteligencia artificial.

Capítulo VI

Análisis de desempeño eficiencia y tiempo de respuesta

6.1 Pruebas de eficiencia y eficacia

Para el desarrollo de las pruebas de eficiencia y eficacia en tiempo real, se construyeron una serie de pruebas a partir del proceso manual de creación de cuenta, que se desarrolla actualmente en la división de TIC (última visita a la división de TIC 21 de enero de 2013), el proceso mencionado anteriormente tal y como lo entregó el funcionario de la división de TIC es el siguiente:

1. Se solicita de carnet institucional o el recibo de pago.
2. Si es un docente se solicita la resolución.
3. Se llenan los datos de apellidos y nombres.
4. Se selecciona el login que se genera generalmente haciendo uso de los nombres y los apellidos del solicitante.
5. Se solicita un código, el cual en caso de no ser conocido se coloca el número del documento de identidad.
6. Se solicita el documento de identidad y el tipo de este.
7. Se solicita la fecha de nacimiento.
8. Se solicita el país, departamento y el municipio.
9. La contraseña para la cuenta se genera a partir de la página www.password.es y en el caso de que se estén generando cuentas basadas en un listado dado, se utiliza el número de identificación de cada miembro como la contraseña de la cuenta.
10. Se selecciona el tipo de estudiante (pregrado, postgrado, docente, pensionado, contratista, etc.)

En el anterior proceso se encontró que los controles inteligentes diseñados y desarrollados en este proyecto actúan directamente sobre los pasos 1 y 9 del proceso para la creación de cuentas utilizado en la división de TIC; para probar dichos controles se plantearon tres escenarios para cada uno de ellos de la siguiente forma:

Para el control de validez del carnet se planteó un primer escenario en donde el carnet institucional fuera válido, el segundo donde el carnet institucional fuera inválido y como último escenario donde no se presente el carnet institucional sino un recibo de pago.

Para el control de seguridad de la contraseña se planteó un primer escenario en donde se ingresa al control una contraseña generada a través de la página www.password.es, el segundo escenario cuando se introduce como contraseña el número de identificación del solicitante y como último escenario cuando la contraseña es digitada por el solicitante.

Los resultados para estos escenarios plateados fueron los siguientes:

El control de validez del carnet obtuvo los siguientes resultados:

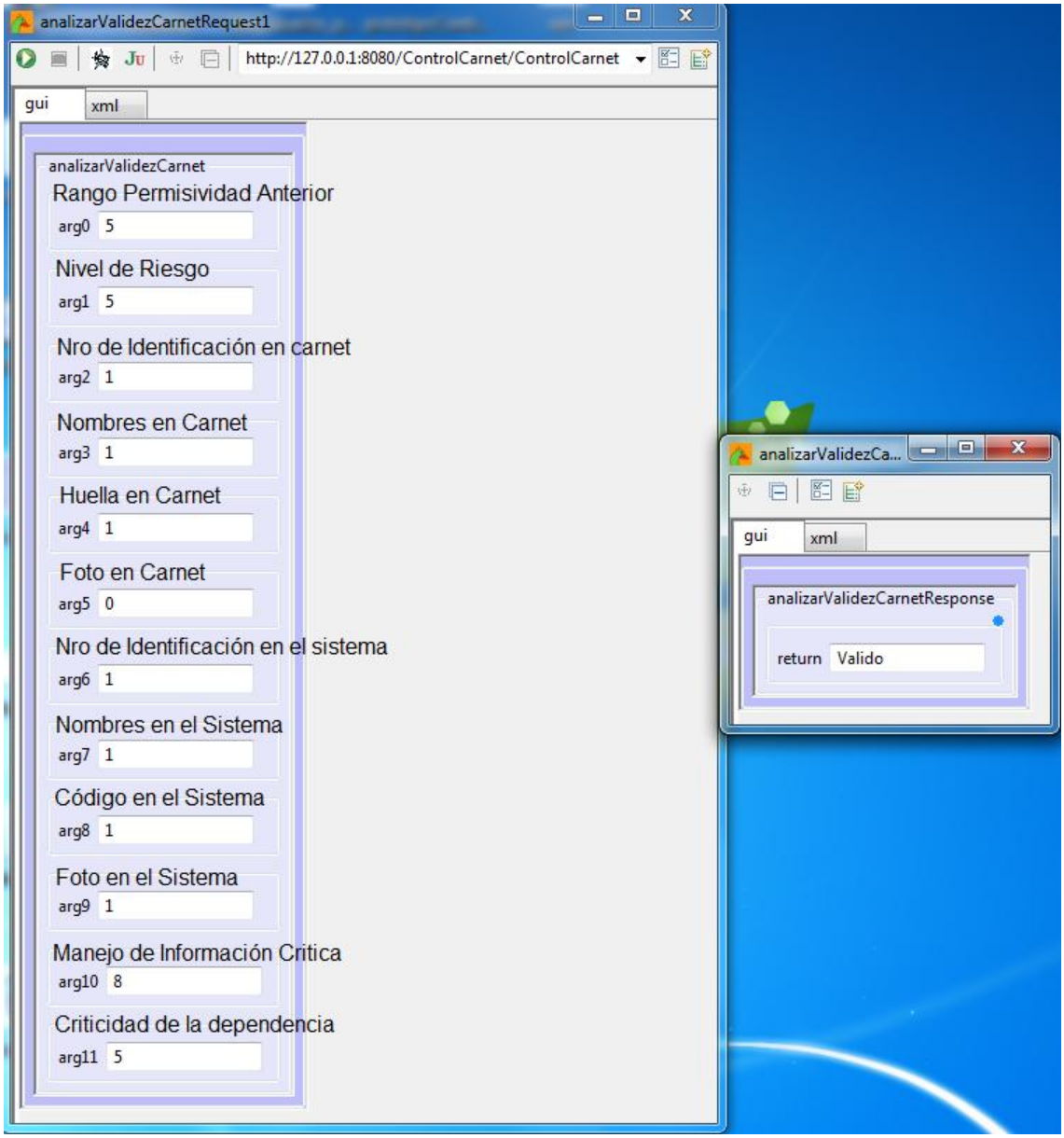

Ilustración 17 Escenario de prueba 1 control validez del carnet

En la ilustración 17 se encuentra el primer escenario de prueba en donde se tiene un carnet institucional válido. Este escenario cuenta con un nivel de riesgo medio, un rango de permisividad anterior medio, con toda la información del solicitante dentro del carnet (número de identificación, nombres y la huella), con toda la información del solicitante en el sistema (número de identificación, nombres, código y foto), un manejo de información crítica alta y una criticidad de la dependencia con un nivel medio. Con todos estos parámetros

establecidos nos encontramos con que la respuesta por parte del control para este escenario es el de un carnet válido.

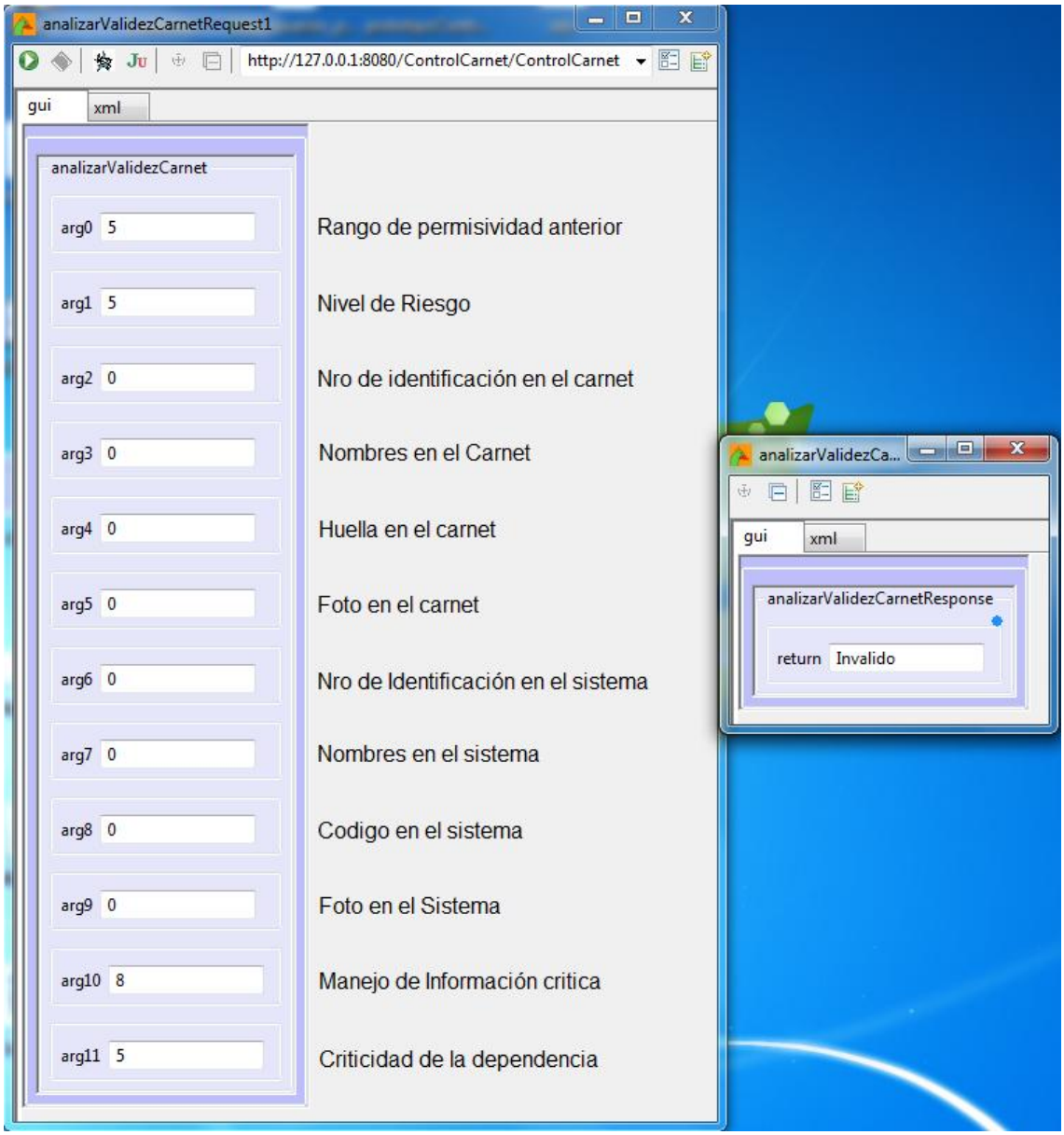

Ilustración 18 Escenario de prueba 2 control validez del carnet

En la ilustración 18 se encuentra el segundo escenario de prueba en donde se tiene un carnet institucional inválido. Este escenario cuenta con un nivel de riesgo medio, un rango de permisividad anterior medio, con la ausencia de toda la información del solicitante dentro del carnet (número de identificación, nombres y la huella), con la ausencia toda la información del solicitante en el sistema (número de identificación, nombres, código y foto), un manejo de

información crítica alta y una criticidad de la dependencia con un nivel medio. Con todos estos parámetros establecidos nos encontramos con que la respuesta por parte del control para este escenario es el de un carnet inválido.
Para el tercer escenario de prueba se tiene que el control de validez del carnet nunca es llamado ya que como no se cuenta con un carnet institucional este no entrara en ejecución, debido a que según los procedimientos definidos en función de las políticas de seguridad (en proceso de aprobación) es requerido el carnet institucional para cualquier tipo de procedimiento.

El control de seguridad de la contraseña obtuvo los siguientes resultados:
Para el primer escenario en donde la contraseña se generó a través de la pagina usada http://password.es/ sin configuraciones adicionales.

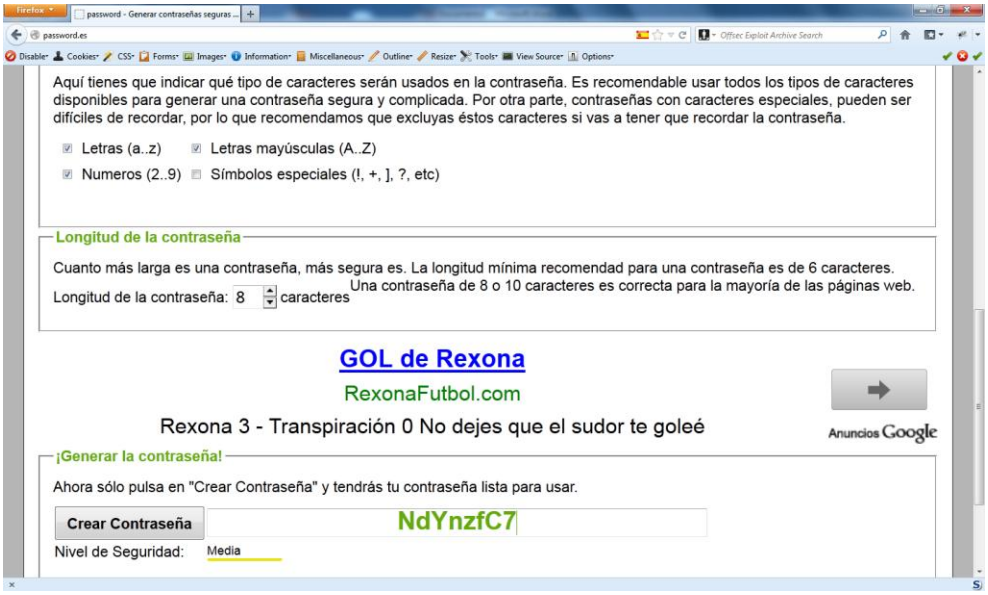

Ilustración 19 Contraseña generada escenario 1 de prueba 1

En la ilustración 19 se muestra que se generó la contraseña “NdYnzfC7”, para la cual el nivel de seguridad frente a la evaluación realizada por el control Inteligente, fue Bajo ilustración 20.

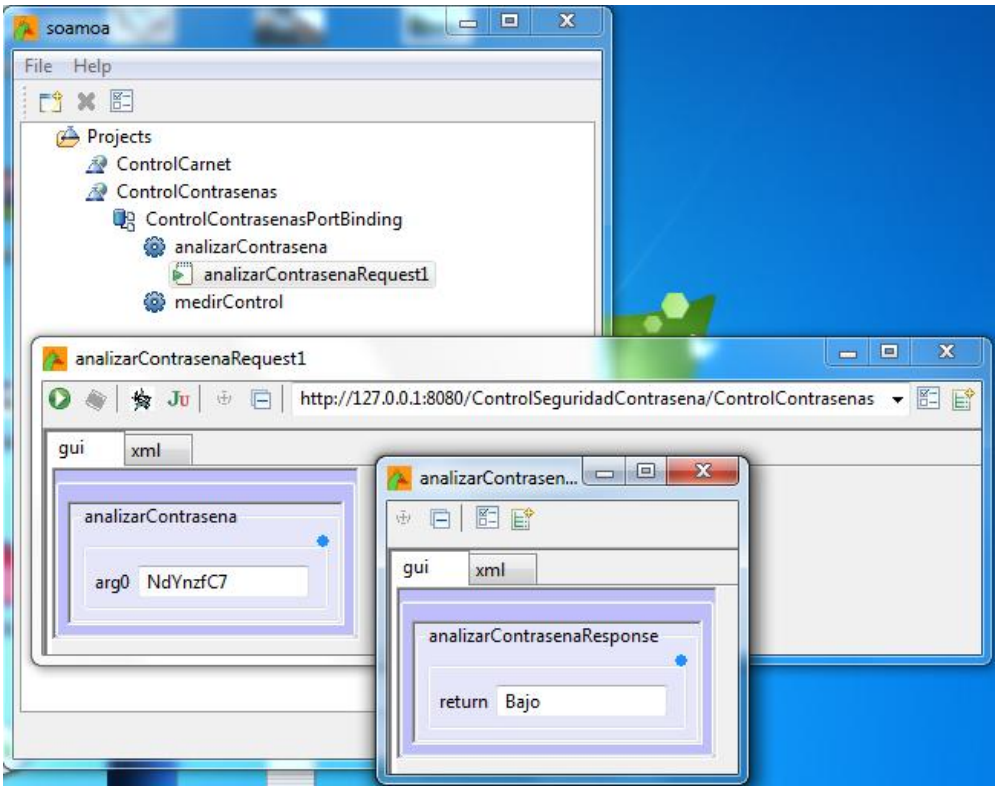

Ilustración 20 Escenario 1, prueba 1 control seguridad de contraseña

De la misma manera se generó una nueva contraseña en el mismo sitio, en este caso con 9 caracteres y todas las opciones disponibles, en este caso se generó la contraseña “hM}g*>OT2” ilustración 21.

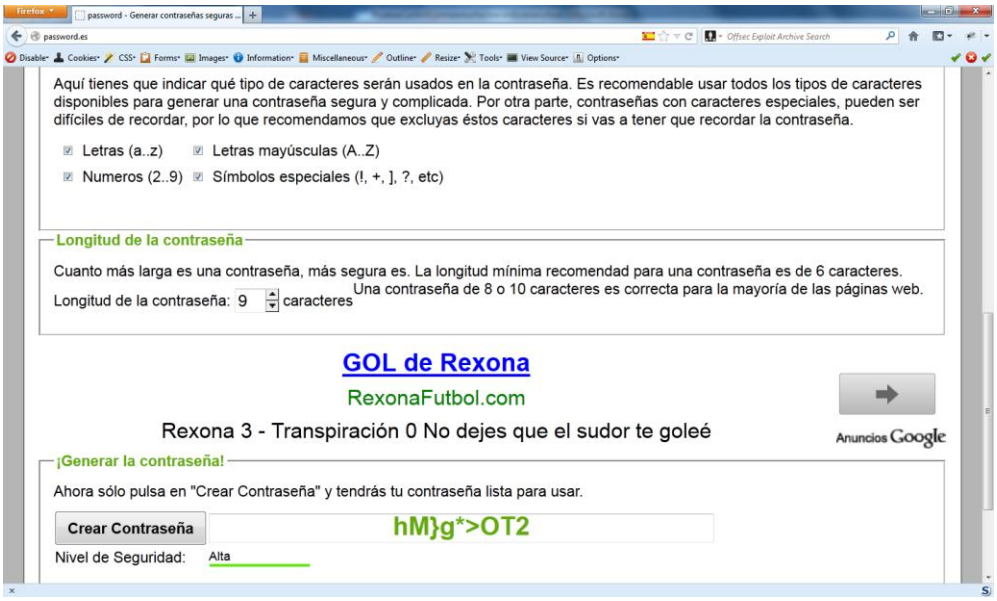

Ilustración 21 Contraseña generada escenario 2 de prueba 1

Una vez generada la contraseña, se analizó haciendo uso del control Inteligente, donde alcanzó un nivel de seguridad Aceptable ilustración 22

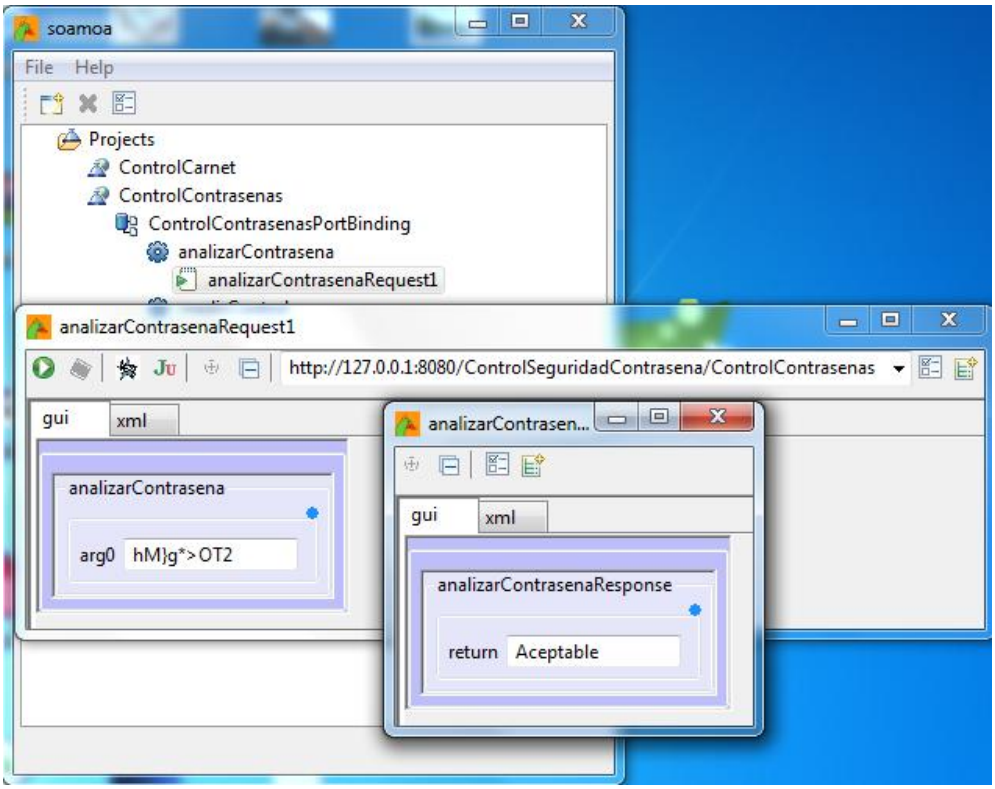

Ilustración 22 Escenario 2, prueba 1 control seguridad de contraseña

Recreando el segundo escenario en el que la contraseña sea para un conjunto de usuarios (listado) sugerido por alguna dependencia, cuya contraseña es el número de identificación se plantearon como muestras 2 números de identificación, las cuales se evaluaron de la siguiente manera.

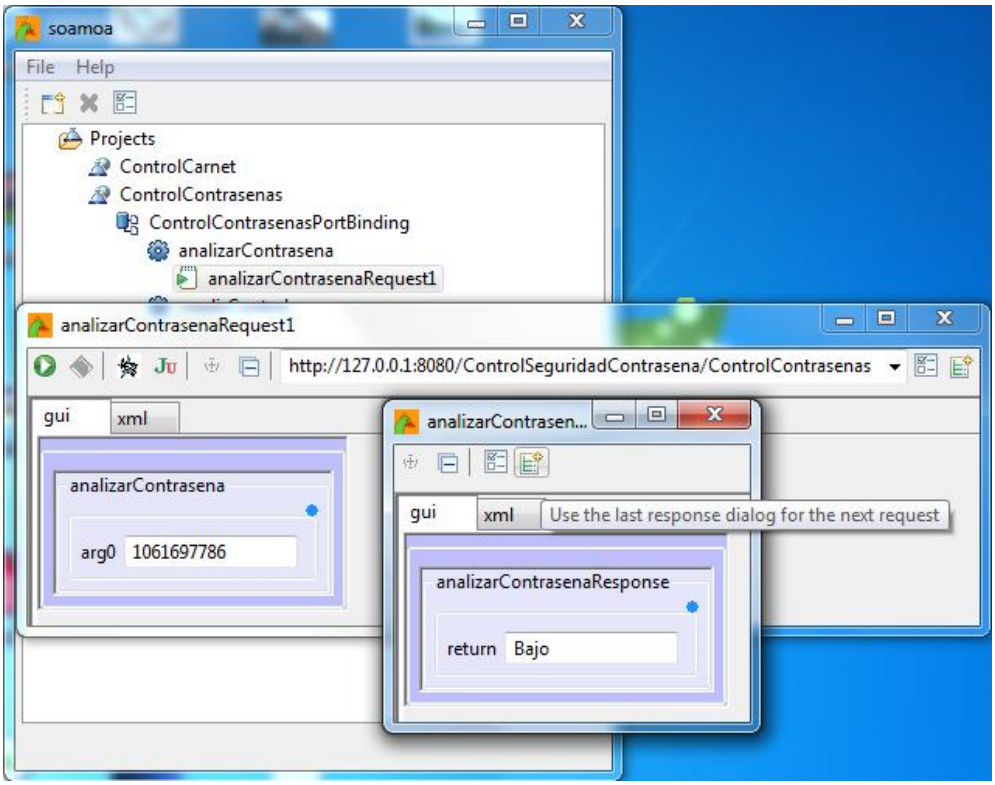

Ilustración 23 Escenario 1, prueba 2 control de seguridad de contraseña

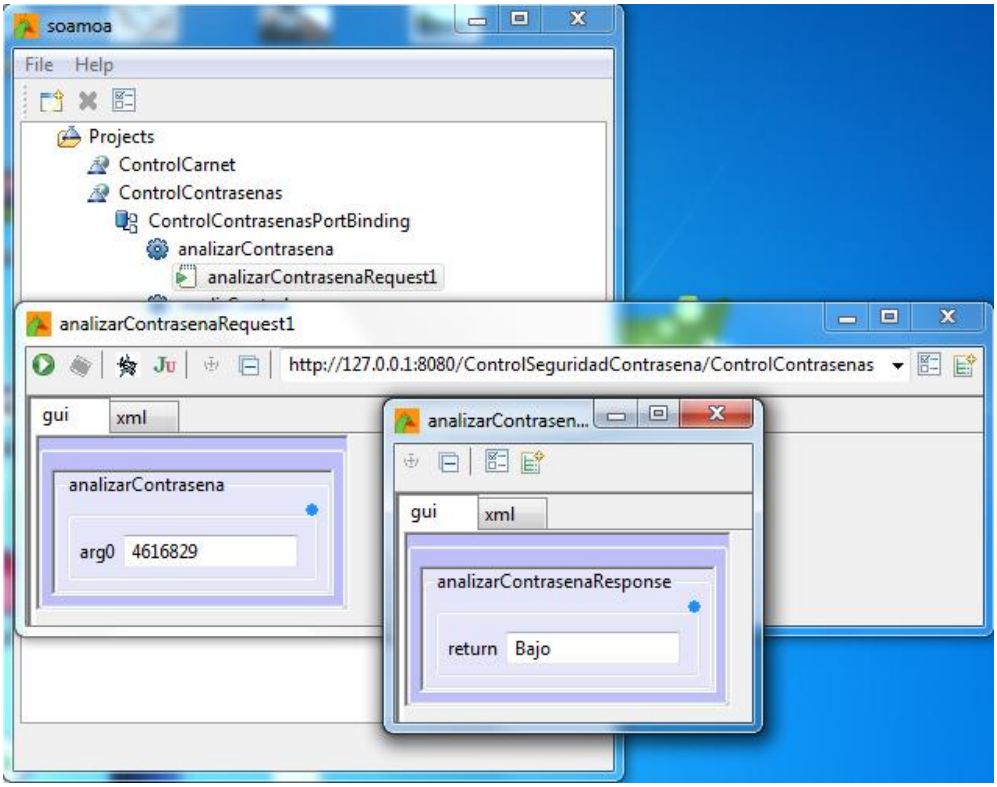

Ilustración 24 Escenario 2, prueba 2 control de seguridad de contraseña

Las ilustraciones 23 y 24 muestran que para los dos casos de prueba utilizados para el segundo escenario las contraseñas fueron evaluadas como bajas por el control inteligente.

Para realizar el tercer escenario se solicitó la colaboración de dos aspirantes a la Universidad del Cauca, en donde se le pidió a cada uno de ellos que brindará una posible contraseña que usarían en el momento de crear su cuenta institucional. Las contraseñas con la evaluación de las mismas fueron:

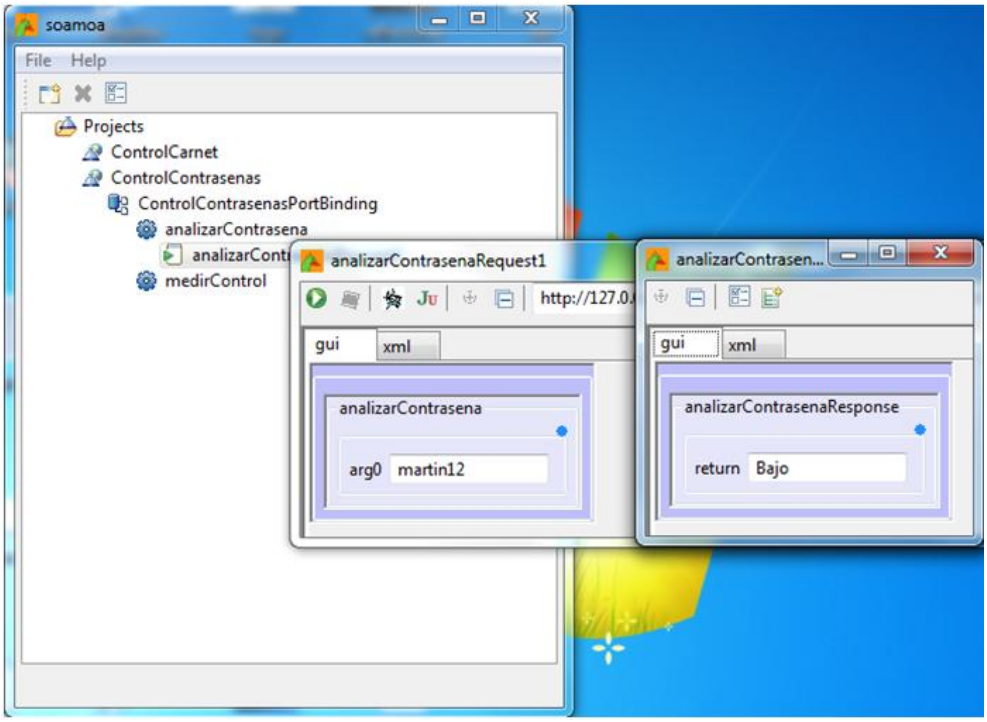

Ilustración 25 Escenario 1, prueba 3 control de seguridad de contraseña

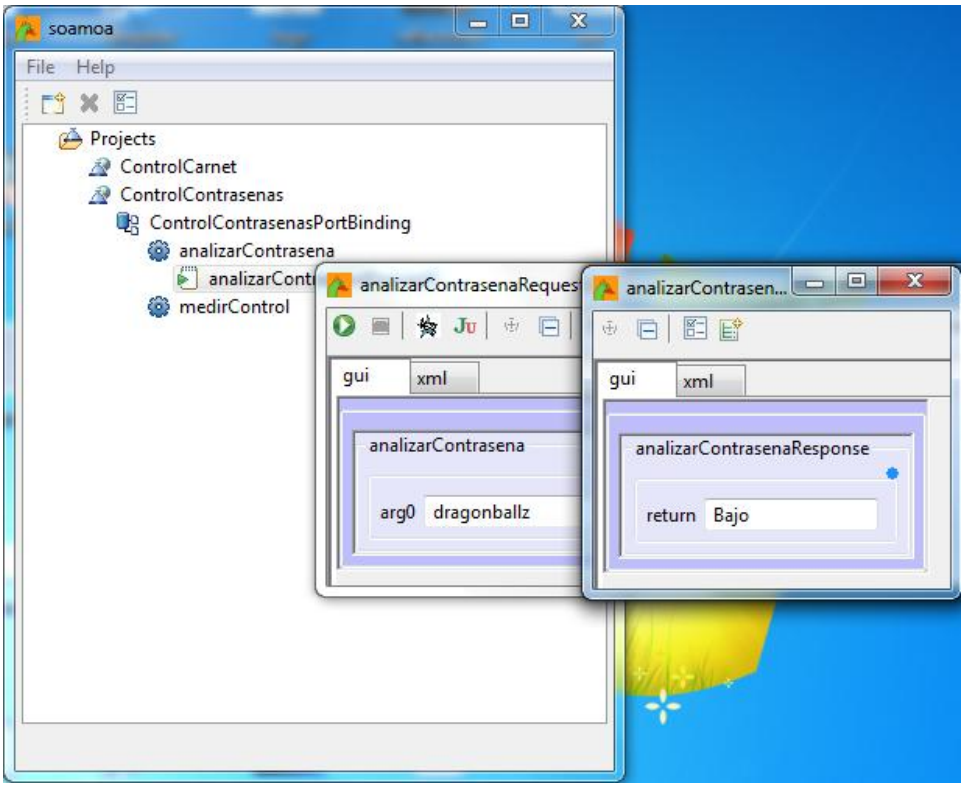

Ilustración 26 Escenario 2, prueba 3 control de seguridad de contraseña

Las ilustraciones 25 y 26 muestran que para los dos casos de prueba usados para recrear el tercer escenario encontramos que la respuesta por parte de estos controles para los dos casos es de un bajo nivel de seguridad.

Capítulo VII

Conclusiones, Recomendaciones y Trabajos futuros

7.1 Conclusiones

Durante la ejecución y el desarrollo del proyecto se obtuvieron diferentes conclusiones las cuales se plantean a continuación:

- En la selección de la técnica de inteligencia artificial a usar, fue muy influyente la necesidad de la definición de reglas basadas en documentos de buenas prácticas, motivo por el cual nos inclinamos en la posible aplicación de una técnica basada en conocimientos.
- A partir de las actividades que permitieron seleccionar las técnicas de inteligencia artificial, las condiciones mencionadas anteriormente, la estructura interna de los controles y la posterior reunión con un grupo expertos, se eligió la lógica difusa como la técnica de inteligencia a usar en el desarrollo de los dos controles inteligentes.
- Para el funcionamiento óptimo de los controles la división de TIC de la Universidad del Cauca debería formalizar y en lo posible automatizar los procesos que son supervisados por dichos controles, esto debido a que en algunos casos los procedimientos pueden ser considerados como críticos o a su vez manejar información crítica para la institución.
- Durante el diseño y el desarrollo de controles inteligentes es fundamental tener siempre de la mano la opinión de expertos, así como desarrollar todo con base en los manuales de procedimientos institucionales y la documentación existente de buenas prácticas.
- El uso de controles inteligentes cuyo desarrollo se realiza basado en documentos de buenas prácticas, en algunas ocasiones puede comportarse de manera similar a la evaluación o la toma de decisiones de parte de un grupo de expertos.
- El uso de controles inteligentes sobre procedimientos institucionales en algunos casos resulta más efectivo y eficiente que el uso de controles convencionales.

7.2 Recomendaciones

Durante la ejecución y el desarrollo del proyecto se obtuvieron diferentes recomendaciones las cuales se plantean a continuación:

- En la selección de las técnicas de inteligencia artificial a aplicar, se recomienda a parte de los criterios de evaluación definidos, tener o buscar siempre las opiniones de un grupo expertos.
- La Universidad del Cauca debe dar prioridad a la búsqueda de una certificación legal por parte de organismos competentes en el estándar ISO/IEC 27001:2005, que permita contar con soporte eficaz y eficiente para brindar seguridad a los activos de información.
- Con el fin de seguir la recomendación anterior la división de TIC de la Universidad del Cauca debería retomar y apoyar de una manera más activa el proyecto SGSI UNICAUCA.
- La Universidad del Cauca en todas sus divisiones pero en especial en la división de TIC debe contar con una mejor documentación de los procesos realizados en la misma, esto en busca de una formalización de los mismos debido a que actualmente muchos de estos no están documentados o no se tiene claro el procedimiento a seguir.
- Las diversas dependencias de la Universidad del Cauca, deberían buscar una centralización de la información, debido a que se detecto que muchas de las dependencias de la Universidad del Cauca manejan su información de manera autónoma lo cual da espacio a inconsistencias así como información duplicada.

7.3 Trabajos Futuros

Durante la ejecución y el desarrollo del proyecto surgieron diversas necesidades o posibles puntos a profundizar, a partir de lo cual se proponen los siguientes trabajos futuros:

- Con los dos controles producto del presente proyecto, se abordaron 4 de los 133 controles que sugiere la norma, a partir de lo cual se plantea como trabajo futuro la implementación de los controles necesarios para abordar los 129 controles restantes que se definen en la norma ISO/IEC 27002:2005.
- En el desarrollo del presente proyecto se aplicó la lógica difusa como técnica de inteligencia artificial, se plantea como trabajos futuros el uso de técnicas que permitan el auto aprendizaje de los controles a partir de su interacción con el entorno.
- Se propone adicionalmente realizar un análisis de los diferentes componentes de los SGSI, con el fin de identificar en cuales de estos es posible y adecuada la aplicación de técnicas de inteligencia artificial.

Bibliografía

[1] ICONTEC, “Estándar Internacional ISO/IEC 27001:2005 Information Technology -- Security techniques --Specification for an Information Security Management System”. Disponible en: http://www.iso27001standard.com/es/iso-27001/blog [Revisado octubre 8, 2010].

[2] ICONTEC, “Estándar Internacional ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management”. Disponible en: http://www.iso27001security.com/html/27002.html [Revisado octubre 8, 2010].

[3] ICONTEC, “Estándar Internacional ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management”. Disponible en: http://www.iso27001security.com/html/27005.html [Revisado octubre 8, 2010].

[4] Ramírez Ramos Osvaldo, “Simulación en simmechanics de un sistema de control difuso para el robot udlap”, Tesis, Universidad de las Américas Puebla, Cholula, Puebla, Mexico, Colombia, 2008.

[5] Olmo Castillo Maria Ángela. (2008). Tutorial de Introducción de Lógica Borrosa. Disponible: http://www.dma.fi.upm.es/java/fuzzy/tutfuzzy/contenido3.html

[6] Arredondo Vidal Tomas. (2012, Junio 27). Introducción a la Lógica Difusa. Disponible: http://profesores.elo.utfsm.cl/~tarredondo/info/soft-comp/Introduccion%20a%20la%20Logica%20Difusa.pdf

[7] IMSE-CNM. (2012, Diciembre 8). Xfuzzy Home Page [En Linea]. Disponible: http://www2.imse-cnm.csic.es/Xfuzzy/index.html

[8] Institute for Information Technology National Research Council Canada (1998, Octubre). FuzzyCLIPS Version 6.04. [En Linea]. Disponible: http://awesom.eu/~cygal/FuzzyCLIPS/fzdocs.pdf

[9] INFORM GmbH and Inform Software Corporation. (2012, Diciembre 20). FuzzyTECH Home Page [En Linea]. Disponible: http://www.fuzzytech.com.

[10] Díaz Toledano Moisés Daniel, “Web Services Introducción y Escenarios para su Uso”. Disponible en: http://www.moisesdaniel.com/es/wri/wsepsu.pdf.

[11] ISOTools. Disponible en: http://www.isotools.org/que-es-isotools.cfm. [Revisado Agosto 8 de 2012].

[12] e-PULPO. Disponible en: http://www.gesconsultor.com/ [Revisado Agosto 8 de 2012].

[13] GesConsultor. Disponible en: http://www.gesconsultor.com [Revisado Agosto 8 de 2012].

[14] Escijas| SGSI. Disponible en: https://sgsi.ecija.com/sgsi/ [Revisado Agosto 8 2012].

[15] AGGIL. Disponible en: http://www.aggil.es/ [Revisado Agosto 8 de 2012].

[16] S2GSI. Disponible en: http://www.sia.es/noticias/sgsi.pdf [Revisado Agosto 8 de 2012].

[17] SECURIA SGSI. Disponible en: http://www.securia.es/ [Revisado Agosto 8 de 2012].

[18] GLOBALSGSI. Disponible en: http://audisec.es/ [Revisado Agosto 8 de 2012].

[19] CALLIOSECURA 17799. Disponible en: http://www.infodom.hr/calliosecura/materijali/Callio_Secura17799_Brochure_2007.pdf [Revisado Agosto 8 de 2012].

[20] Amador Donado Siler, Mera Arcos Andrés Felipe y Mondragón Maca Oscar , “Sistema de alertas de seguridad informática para los servicios críticos de la división de tecnologías de la información y la comunicación de la Universidad del Cauca (Fase I del proyecto SGSI - UNICAUCA),” Tesis, Universidad del Cauca, Popayán, Colombia, 2012.

[21] Bustos M Jose Ricardo “Inteligencia Artificial en el Sector Agropecuario“. Disponible en: http://www.docentes.unal.edu.co/jrbustosm/docs/estado2.pdf [Revisado agosto 15 2012].

[22] López Secundino, García Marco, Hernandez Pedro, Hernandez Alejandro “Control Inteligente de Redes Urbanas de Tráfico“. Disponible en: http://www.docentes.unal.edu.co/jrbustosm/docs/estado2.pdf [Revisado agosto 15 2012].

[23] Duque Mendez Nestor Dario, Chavarro Porras Julio Cesar, Moreno Laverde Ricardo “Seguridad Inteligente”, Universidad Tecnológica de Pereira 2007. Disponible en: http://redalyc.uaemex.mx/redalyc/pdf/849/84903567.pdf [Revisado 15 de Agosto de 2012].

[24] Tsai C., Hsu Y., Lin C., Lin W. (2009). “Intrusion detection by machine learning” [En Linea], Disponible en: http://www.sciencedirect.com/science/article/pii/S0957417409004801.

[25] Hentea Mariana “Intelligent System for Information Security Management: Architecture and Design Issues”, Albany USA, 2007. Disponible en: http://proceedings.informingscience.org/InSITE2007/IISITv4p029-043Hent387.pdf

[26] Jurado Guillermo, Amador Siler, “InForceTechnology” Universidad del Cauca Disponible en: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VII_JornadaSeguridad/InForceTechnologyPaperVIIJNSI.pdf

[27] Serrano Carlos E., “Modelo Integral para el Profesional en Ingeniería”. Colombia: Editorial Universidad del Cauca, 2005. Disponible en: ftp://jano.ucauca.edu.co/proc_acred/Busqueda%20de%20la%20Excelencia/

[28] Stevens, L. “Artificial Intelligence. The Search for the Perfect Machine”, Hayden Book Company, New Jersey: Hasbrouck Heights, 1984, pp 40.

[29] Durkin, J. “Expert Systems: Design and Development”, Maxwell Macmillan, New York, 1994.

[30] Zadeh Lotfi A. (1965) “Fuzzy Sets”. Disponible en: http://www-bisc.cs.berkeley.edu/Zadeh-1965.pdf

[31] McCulloch Warren S., Pitts Walter (1943) “A Logical Calculus Of The Ideas Immanent In Nervous Activity”. Disponible en: http://www.cse.chalmers.se/~coquand/AUTOMATA/mcp.pdf

[32] Pearl, Judea, “Bayes Decision Methods”, Encyclopedia of AI, Wiley Interscience, New York, 1987.

[33] Peña Ayala Alejandro.”Sistemas Basdos en Conocimiento: Una base para su Concepción y Desarrollo”. MEX: Distrito Federal 2006

[34] Joskowicz José, “Reglas y Prácticas en eXtremeProgramming”. Disponible en: http://iie.fing.edu.uy/~josej/docs/XP%20-%20Jose%20Joskowicz.pdf

[35] Fernández Escribano Gerardo “Introducción a Extreme Programming”, Ingeniería de Software II 2002. Disponible en: http://www.info-ab.uclm.es/asignaturas/42551/trabajosAnteriores/Presentacion-XP.pdf