FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE CAJEROS AUTOMÁTICOS QUE PERTENECE A LA RED TRANSACCIONAL COOPERATIVA S.A., UTILIZANDO EL PROTOCOLO SIMPLE NETWORK MANAGMENT PROTOCOL (SNMP) VERSIÓN 3

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Electrónica y Redes de Información

Profesor Guía

Ing. Richard Efraín Góngora Grados

Autor

Alejandro David Vargas Aldás

Año

2015

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

_____

Richard Efraín Góngora Grados
Ingeniero en Sistemas y Redes de Comunicaciones
C.I.: 1708322258

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Alejandro David Vargas Aldás

C.I.: 1719953588

AGRADECIMIENTOS

A DIOS ser maravilloso por darme la vida y el haberme permitido llegar hasta este gran momento de mi formación profesional.

A mis padres y hermano por su gran sustento y por estar a mi lado en cada momento de mi vida.

Al Ingeniero Richard Góngora por haberme brindado la oportunidad de recurrir a su capacidad y conocimiento científico.

Al Gerente de Sistemas de la Empresa Red Transaccional Cooperativa S.A., el Ingeniero Luis Felipe Carrera por la oportunidad que me brindó para desarrollar el proyecto de tesis.

A mis amigos por sus valiosas aportaciones durante la elaboración del proyecto.

DEDICATORIA

A DIOS ser maravilloso por guiarme por el buen camino.

A mis padres por su valioso apoyo, esfuerzo, amor, ayuda y por brindarme lo necesario para culminar mis estudios.

A mi hermano que siempre ha estado junto a mí brindándome su apoyo.

A toda mi familia que es lo mejor y lo más valioso que DIOS me ha dado.

RESUMEN

La detección oportuna de fallos y el monitoreo a los cajeros automáticos son actividades muy importantes para brindar un buen servicio hacia los usuarios, de esto se deriva la necesidad de contar con un software que sea capaz de notificar, detectar y prevenir fallos que puedan presentarse en los cajeros automáticos.

En el caso de la Red Transaccional Cooperativa S.A., (RTC), se evidenció la necesidad de implementar una herramienta que cumpla con los requisitos mencionados anteriormente. Esta deberá monitorear a profundidad los servicios tales como: cajeros automáticos, enlaces entre los cajeros automáticos hacia la Red Coonecta y los dispositivos que poseen los cajeros automáticos.

Para el desarrollo del presente proyecto con base al esquema actual de la Red Coonecta, se implementará un ambiente de pruebas y se probará las diferentes funciones que brinda el protocolo SNMPv3, para luego ser ampliado al resto de cajeros automáticos de las cooperativas de ahorro y crédito, con el fin de mejorar la seguridad, prevenir fallos, tomar las correcciones oportunas y garantizar un nivel de calidad mediante el monitoreo.

ABSTRACT

The early detection of failures and the monitoring to the automatic teller machines are very important activities to provide a good service to the users, from this comes the need of having a software able to notify, detect and prevent failures that may occur in the automatic teller machines.

In the case of Red Transaccional Cooperativa S.A. (RTC), it evidenced the need to implement a tool that comply with the requirements mentioned previously.
This should monitor depth services such as: automatic teller machines, connections between the automatic teller machines to Red Coonecta and the devices that possess the automatic teller machines.

For the development of this project based on the current structure of Red Coonecta, a test environment will be implemented and the different functions provided by the SNMPv3 protocol will be tested, before being extended to other automatic teller machines of credit unions, in order to improve safety, prevent failures, make the appropriate adjustments and ensure a level of quality through monitoring.

ÍNDICE

INTRODUCCIÓN

Red Transaccional Cooperativa S.A., (RTC), es una empresa que contribuye a la integración operativa y el crecimiento del sistema cooperativo de ahorro y crédito mediante la prestación de servicios transaccionales y la ejecución de procesos de consultoría bajo una estrategia de innovación, calidad, competitividad y sostenibilidad de los servicios. (Red Transaccional Cooperativa S.A., s.f.)

En la actualidad, la empresa no cuenta con una herramienta capaz de monitorear a profundidad los servicios brindados a las cooperativas de ahorro y crédito, tales como: cajeros automáticos, enlaces entre los cajeros automáticos hacia la Red Coonecta y los dispositivos que poseen los cajeros automáticos.

El servicio de los cajeros automáticos debe ofrecer seguridad y disponibilidad, tanto para el personal que lo administra como el cliente que lo utiliza. Un cajero automático puede presentar caídas de su enlace, daños en sus dispositivos, robo de información, etc., esto debido a las intermitencias en la red, fallas de dispositivos, caídas de energía, etc., ocasionando malestar y la pérdida de clientes que usan este servicio. De tal manera que, se evidenció la necesidad de implementar una herramienta que monitoree a profundidad los servicios mencionados anteriormente, garantizando un servicio de excelencia y de calidad hacia los clientes.

OBJETIVOS

Objetivo General

Implementar una herramienta de software basado en la utilización del protocolo SNMPv3, con el fin de monitorear y detectar los fallos que puedan presentarse en el enlace de comunicación entre Coonecta Red Cooperativa y los cajeros automáticos que conforman varias cooperativas.

Objetivos Específicos

- Analizar el esquema actual de monitoreo de la Red Coonecta.

- Analizar las características, arquitectura, procesamientos de mensajes, seguridad y control de acceso a la información respecto al protocolo SNMPv3.

- Diseñar una aplicación amigable y de fácil manejo a través del lenguaje de programación *"JAVA"*.

- Implementar un prototipo de la aplicación en un escenario de pruebas.

- Realizar pruebas de cada funcionalidad que ofrece la aplicación y verificar los resultados del cumplimiento de los requerimientos funcionales del usuario.

ANTECEDENTES

La detección oportuna de fallos y el monitoreo a los cajeros automáticos son funciones muy importantes para otorgar un buen servicio hacia los usuarios, de esto proviene la necesidad de contar con un software que sea capaz de notificar, detectar y prevenir fallos que puedan presentarse en los cajeros automáticos; con la finalidad de mejorar la seguridad, tomar las correcciones oportunas y garantizar un nivel de calidad mediante el monitoreo.

ALCANCE

El presente proyecto será desarrollado a través del lenguaje de programación *"JAVA"* y será basado en el protocolo SNMPv3, todo esto con el objetivo de implementar una herramienta capaz de: notificar, detectar y prevenir fallos que puedan presentarse en los cajeros automáticos y sus dispositivos.

JUSTIFICACIÓN

El presente proyecto inicia debido a la necesidad de monitorear a profundidad los servicios brindados por la Red Coonecta hacia las cooperativas de ahorro y crédito, tales como: cajeros automáticos, enlaces entre los cajeros automáticos hacia la Red Coonecta y los dispositivos que poseen los cajeros automáticos.

El servicio de los cajeros automáticos debe ofrecer seguridad y disponibilidad, tanto para el personal que lo administra como el cliente que lo utiliza. Actualmente se requieren conocimientos técnicos tales como: funcionamiento de protocolos de comunicación TCPI/IP, manejo de llaves de encriptación y seguridad física de los cajeros automáticos, esto para romper la seguridad de los cajeros automáticos y así obtener información del cliente, ya sea clonando la tarjeta u obteniendo sus datos personales.

La herramienta a implementar permitirá monitorear a profundidad los servicios brindados hacia las cooperativas de ahorro y crédito; y será basado en el protocolo SNMPv3 para ofrecer seguridad en el envío y recepción de datos.

1. PLANTEAMIENTO DEL PROBLEMA

El Capítulo I contiene una breve descripción de la empresa, sus servicios fundamentales, su crecimiento a nivel nacional y sus necesidades identificadas sobre la cual se fundamenta el desarrollo de la aplicación.

1.1 RED TRANSACCIONAL COOPERATIVA S.A., (RTC)

La Red Transaccional Cooperativa S.A., (RTC), es una institución de servicios auxiliares del sistema financiero, cuya constitución fue aprobada por la Superintendencia de Compañías con Resolución No. 06.Q.IJ.004284, el 06 de noviembre del 2006 y calificada por la Superintendencia de Bancos y Seguros (SBS) mediante la Resolución No. SBS-2007-172, el 28 de febrero del 2007.

Se forma por la decisión de las cooperativas del Ecuador para integrarse mediante servicios transaccionales, estas cooperativas de la red están interconectadas en forma permanente. Su objetivo es actuar como facilitadora de las transacciones entre cooperativas de ahorro y crédito, contribuir a la integración operativa y el crecimiento del sistema cooperativo de ahorro y crédito mediante la prestación de servicios transaccionales y la ejecución de procesos de consultoría bajo una estrategia de innovación, calidad, competitividad y sostenibilidad de los servicios. (Red Transaccional Cooperativa S.A., s.f.)

1.2 CAJEROS AUTOMÁTICOS Y TARJETAS DE DÉBITO

Uno de los servicios principales que brinda la Red Coonecta, es el monitoreo a los cajeros automáticos y la emisión de tarjetas de débito, en el cual participan 62 entidades que operan más de 200 cajeros automáticos y han emitido más de 500 mil tarjetas de débito bajo la marca *"De Una"* que identifica a los tarjetahabientes de la Red Coonecta.

Un factor importante para el éxito alcanzado con estos servicios ha sido la interacción de la Red Coonecta con la red de cajeros automáticos y tarjetas de débito operada y administrada por BANRED.

Figura 1. Integración COONECTA - BANRED (Febrero 03, 2015)
Tomado de: (Red Transaccional Cooperativa S.A., s.f.)

El modelo ha sido beneficioso tanto para la Red Coonecta como para la entidad BANRED, con la cual se ha mantenido este convenio y para las instituciones miembros de la Red Coonecta que participan en el servicio.

Desde que la Red Transaccional Cooperativa S.A., (RTC), inició con el servicio de cajeros automáticos para las cooperativas afiliadas a la Red, se ha tenido una tasa de crecimiento del 24%. (Red Transaccional Cooperativa S.A., s.f.)

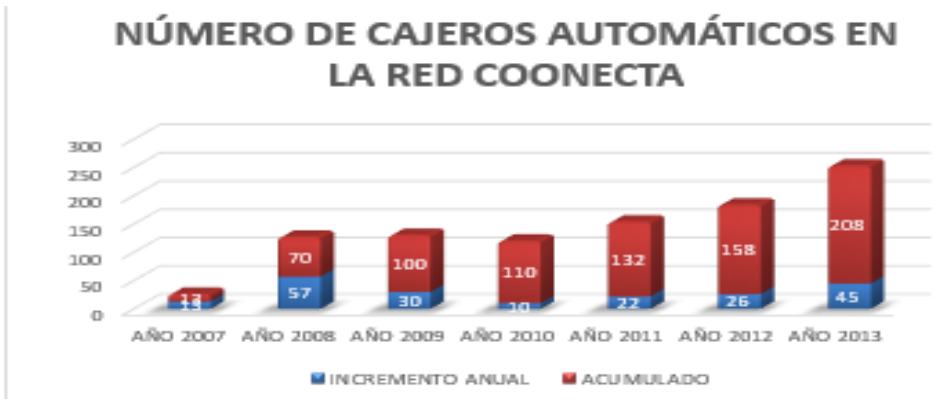


Figura 2. Evolución de ventas de Cajeros Automáticos 2007 – 2013
Tomado de: (Red Transaccional Cooperativa S.A., s.f.)

Desde el 2007 hasta el 2013 la emisión de tarjetas de débito se ha incrementado con un promedio de 38%.

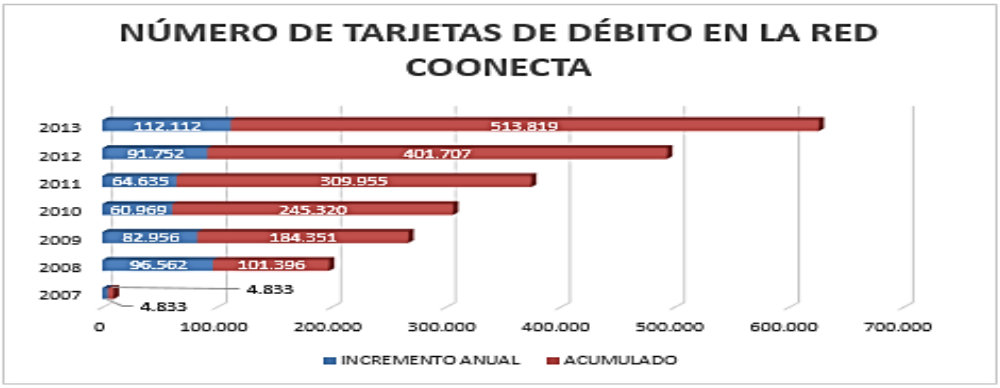


Figura 3. Evolución de tarjetas 2007 – 2013
Tomado de: (Red Transaccional Cooperativa S.A., s.f.)

1.2.1 Transacciones en los Cajeros Automáticos

Desde el 2009 el número de transacciones en los cajeros automáticos ha ido creciendo a lo largo del tiempo en un promedio del 57%.

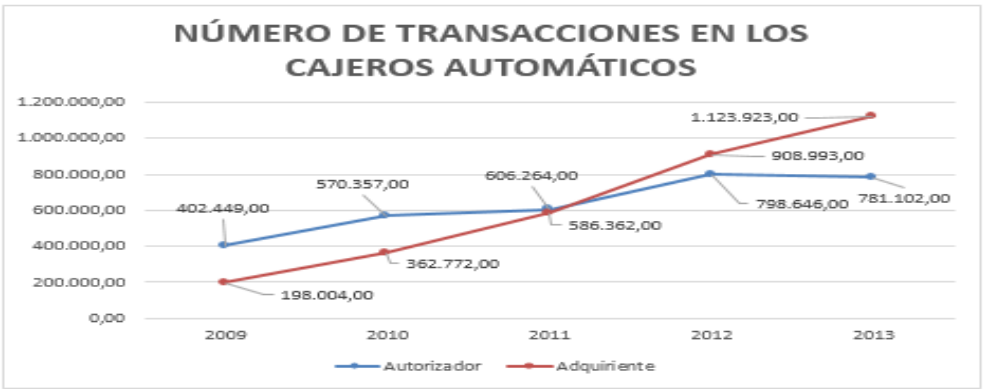


Figura 4. Evolución de transacciones 2007 – 2013
Tomado de: (Red Transaccional Cooperativa S.A., s.f.)

1.3 NECESIDADES DE LA INSTITUCIÓN

En reuniones en conjunto con el gerente y el equipo de sistemas, se conversó y se evidenció la necesidad de implementar una herramienta que monitoree a profundidad los servicios brindados hacia las cooperativas de ahorro y crédito, esto con el objetivo principal en generar mejoras en el servicio.

El siguiente diagrama muestra la propuesta a la integración del protocolo SNMPv3 al modelo de operación actual, tanto en las modalidades (Back-End y Front-End) que mantienen el servicio con la Red Coonecta.

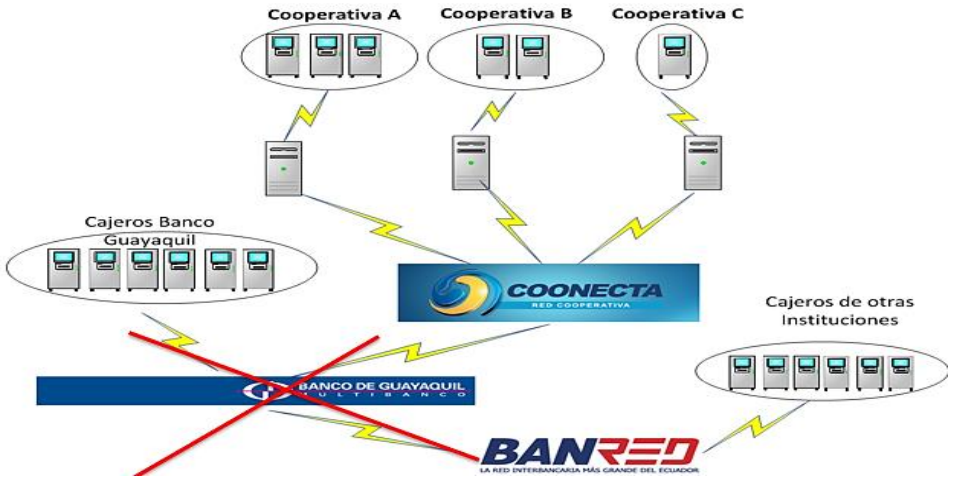


Figura 5. Modelo Back-End
Tomado de: (Red Transaccional Cooperativa S.A., s.f.)

En esta modalidad, la entidad mantiene una infraestructura tecnológica suficiente para soportar la administración de la base de datos y la transaccionalidad local. Coonecta provee el servicio y Switch Transaccional, el mismo que se alojará en los servidores de la Entidad, garantizando la transaccionalidad mediante un *"Acuerdo de Nivel de Servicio"*.

Además permite a la entidad independencia tecnológica, ya que no dependerá de un Switch Central para resolver y ejecutar las transacciones locales que se

presenten dentro de los cajeros automáticos que pertenecen a la entidad, pero evidentemente requiere una inversión mayor en infraestructura propia.

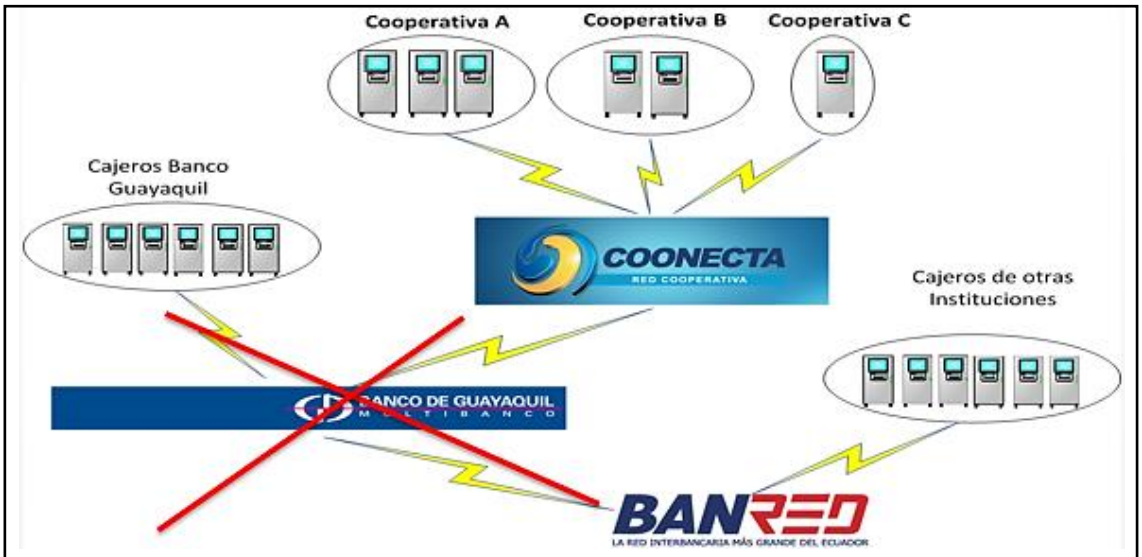


Figura 6. Modelo Front-End
Tomado de: (Red Transaccional Cooperativa S.A., s.f.)

En esta modalidad, la transaccionalidad se da a través del Switch Centralizado que opera en Coonecta, quien mantiene la administración de la base de datos y la cada una de las transacciones locales que se presenten en la entidad. La inversión que debería realizar la entidad en infraestructura tecnológica no es significativa, dado que Coonecta asume parte de esta inversión poniendo a disposición de las entidades usuarias una infraestructura centralizada.

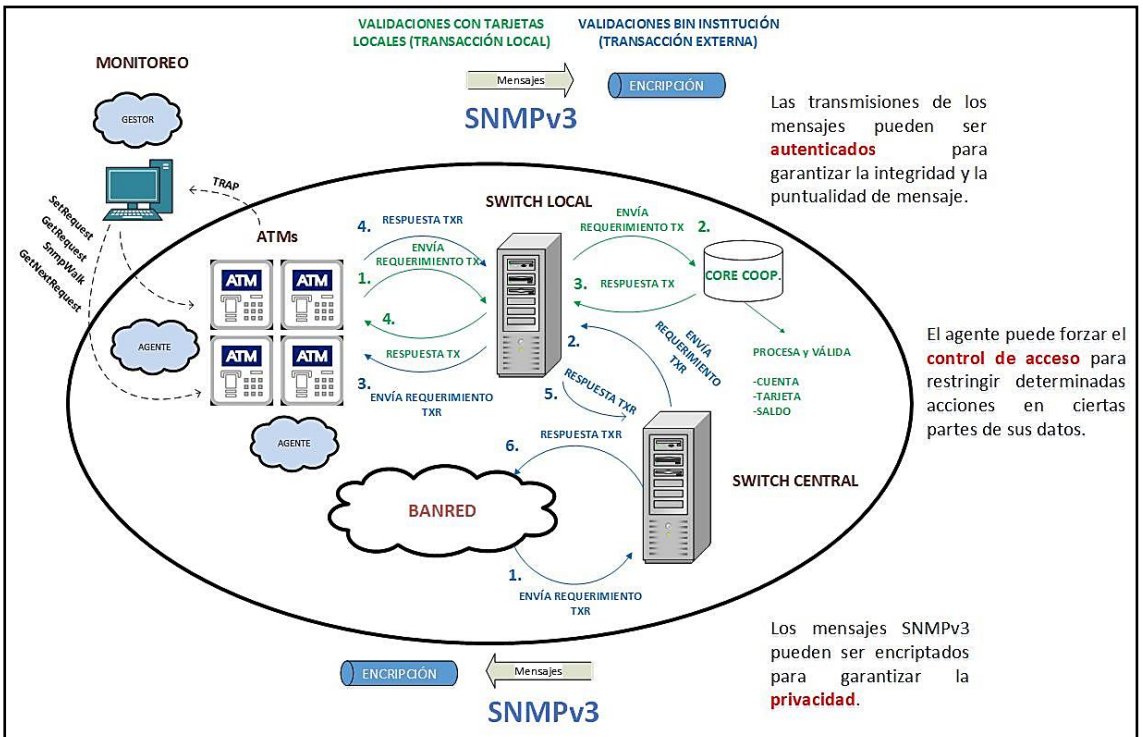


Figura 7. Propuesta a la integración del protocolo SNMPv3 para el monitoreo a los Cajeros Automáticos de las cooperativas de Ahorro y Crédito afiliadas a la Red Coonecta, tanto para el servicio Front-End y Back-End

- **Transacción Local (TX):** Se considera como *"Transacción Local"*, cuando un cliente que pertenece a una cooperativa A, realiza una transacción en un cajero A. Es decir de su propia institución.

- **Transacción Externa (TXR):** Se considera como *"Transacción Externa",* cuando un cliente que pertenece a otra institución, realiza una transacción en un cajero de la cooperativa.

La herramienta a implementar para el monitoreo permitirá recopilar información de los cajeros automáticos y será basada en el protocolo SNMPv3, que a través de este, sea capaz de: notificar, detectar, prevenir fallos que puedan presentarse en los cajeros automáticos.

Los resultados esperados son:

- Mejorar el servicio
- Mejorar la imagen institucional
- Mejorar la seguridad e integridad de los datos
- Mayor agilidad en el resultado de la transacción
- Obtener información útil acerca del funcionamiento de los cajeros automáticos
- Reducir problemas del funcionamiento de la red
- Obtener diagnósticos preventivos que permitan tener arreglos antes de que el usuario final vea el mensaje de error en el cajero automático

2. SUSTENTACIÓN TEÓRICA

El Capítulo II describe los fundamentos teóricos y definiciones acerca de los temas que se encuentran relacionados con el proyecto. Se empieza con una introducción teórica sobre las redes informáticas, modelos de red, administración de redes y posteriormente se realiza un estudio basado al protocolo SNMPv1, SNMPv2 y SNMPv3.

2.1 REDES INFORMÁTICAS DE COMPUTADORAS

La importancia que hoy en día tiene la información es indiscutible, esta puede ser manipulada, alternada y formateada; utilizando computadoras interconectadas entre si formando una red. Las redes informáticas son un conjunto de equipos que están interconectados por un medio físico o inalámbrico y son capaces de comunicarse entre sí mediante dispositivos electrónicos.

2.2 MODELOS DE RED

2.2.1 Modelo de Referencia OSI

Este modelo es fundamental para la comunicación de equipos vía red, es considerada la mejor herramienta de enseñanza hacia el usuario para la comprensión del intercambio de datos a mediante la red.

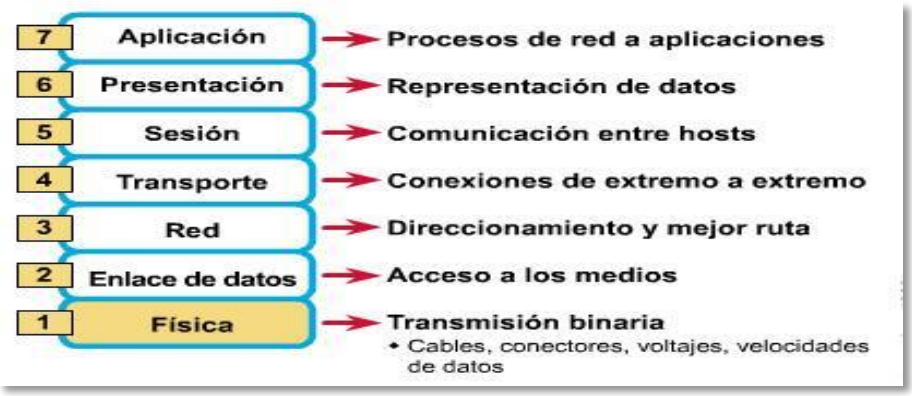


Figura 8. Modelo de Referencia OSI
Tomado de: (García, s.f.)

2.2.2 Modelo de referencia TCP/IP

Este es un modelo que puede ser implementado en cualquier tipo de red y facilita el intercambio de información sin depender del tipo de tecnología.

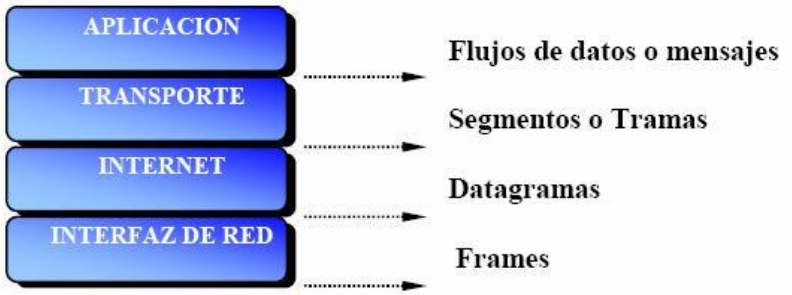


Figura 9. Modelo de Referencia TCP/IP
Tomado de: (Redes y Comunicaciones, s.f.)

2.3 INTRODUCCIÓN A LA ADMINISTRACIÓN DE RED

La administración de red es un factor esencial en el éxito de funcionamiento de la misma, ya que las empresas cada vez son más dependientes de estos servicios de red. Realizar correctamente la administración de las redes asegura que los servicios prestados a través de ella estén en buen funcionamiento.

Para los proveedores de servicios, el correcto funcionamiento de los servicios de la red es de gran importancia, por lo que la gestión ineficaz puede llevar al deterioro de los servicios de red y por lo tanto la pérdida de negocio.

2.3.1 Gestión de Red

La gestión de red garantiza un nivel de servicio en una organización al máximo tiempo posible minimizando la pérdida que ocasionaría una caída o funcionamiento incorrecto del sistema.

Los elementos que son objetos de control por un sistema de gestión de red son fundamentalmente los equipos conectados: servidores, ordenadores personales, estaciones de trabajo, así como elementos y equipos de interconexión tales como: cables, puentes, routers, etc.

2.4 PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED – SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

SNMP es un protocolo que apareció en 1988 y administra las redes. Su principal objetivo es mantener en funcionamiento dispositivos tales como: routers, switches, servidores, etc.

SNMP funciona sobre el protocolo de transporte TCP/IP, pero se utiliza con mayor frecuencia sobre UDP que es un protocolo sin conexión y vulnerable a la suplantación de ataques IP.

Existen versiones del protocolo, tales como: SNMPv1, SNMPv2 y SNMPv3. Las versiones SNMPv1 y SNMPv2 tienen características en común, pero SNMPv2 desde su aparición en 1993 ofreció mejorías para reducir la carga de tráfico adicional y solución a los problemas de monitorización remota. La versión SNMPv3 apareció en 1997, añadiendo mejoras sobre los aspectos en relación a la seguridad, brindando autentificación, privacidad y control de acceso.

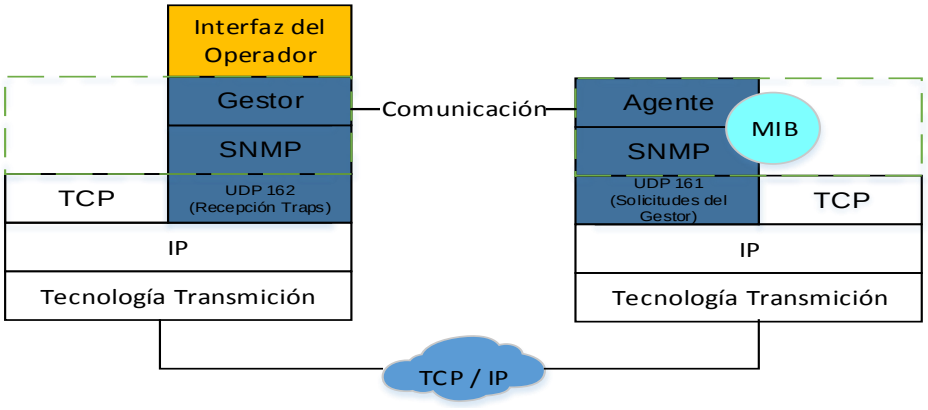


Figura 10. Estructura del funcionamiento SNMP

Tomado de: (SNMP, 2004)

2.4.1 Componentes SNMP

- **Dispositivos**: Son los elementos de la red, la cual pueden constan: routers, impresoras, servidores, switches, computadoras, etc.

- **Agentes:** Mantienen a los dispositivos gestionando información sobre su estado y configuración. Reciben órdenes e informan eventos o notificaciones críticas al gestor.

- **Gestores**: Se ejecutan en las estaciones encargadas de monitorizar la red, su objetivo consiste en obtener información específica y peticiones de los agentes SNMP.

2.4.2 Comandos Básicos

- **Lectura**: El gestor supervisa los dispositivos de red.
- **Escritura**: El gestor controla elementos de la red.
- **Notificación**: El agente reportar eventos que ocurren al gestor.

2.4.3 Autenticación y Privacidad

Los mecanismos de autenticación y privacidad han sido la mayor debilidad en los protocolos SNMPv1 y SNMPv2. Estas son basadas en categorías llamadas *“communities”*, en la cual cada *“community”* tiene asociado un nombre y una contraseña.

En SNMPv3 se añaden mecanismos adicionales que permiten realizar el proceso de una forma segura, brindando una mejoría en la autenticación y cifrado de datos para la privacidad.

2.4.4 Base de Información de Administración – Management Information Base (MIB)

La MIB es una base de datos, el cual contiene información estructurada en forma de árbol de todos los dispositivos SNMP que se pueden gestionar en una red de comunicaciones, esto permite poder revisar y controlar los componentes de las redes.

El formato de cada uno de los objetos de una MIB está definido mediante la notación ASN.1 (Abstract Syntax Notation 1), que es una notación estándar definida en ITU-T X.208 y en ISO 882. Esta notación permite describir de forma entendible y flexible cada objeto de la plataforma y permite la comunicación entre dos computadoras sin algún inconveniente.

El subconjunto de ASN.1 utilizado en SNMP está definida en la *“RFC1155”* y se la conoce como SMI (Structure of Management Information).

2.4.4.1 Estructura de Información de Gestión - Structure of Managment Information (SMI)

La SMI identifica y especifica el tipo de dato a ser usado en una MIB, estas se declaran empleando un lenguaje llamado ASN.1, el cual definen los atributos de un objeto y hace que los contenidos de las variables sean funcionales.

El objetivo principal de la SMI es mantener simplicidad y extensibilidad para poder introducir nuevos objetos en la MIB.

2.4.4.2 Estructura de la MIB

La MIB describe la totalidad de los objetos SNMP que se encuentran en la red. Los OID (Object Indentifier), son objetos que describen la dirección del objeto MIB, cada objeto tiene un identificador único que sirve para nombrarlo.

Las variables son expresadas en el código ASCII, con números enteros separados por puntos.

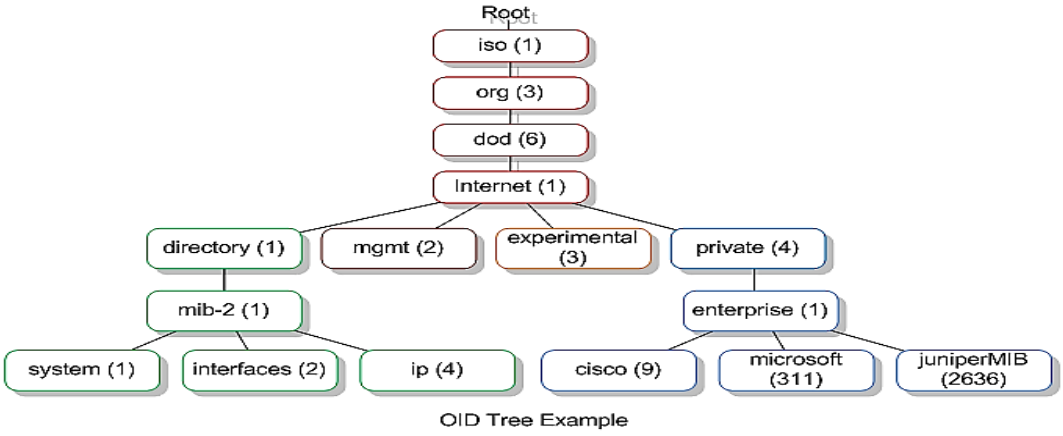


Figura 11. Estructura de la MIB

T**omado de:** (Network Management, s.f.)

2.4.4.3 Codificación

La codificación es el método que permite convertir la información en un símbolo de otro sistema para ser transmitida en una red de comunicaciones. Los objetos pertenecientes a la MIB son codificados mediante las BER (Basic Encoding Rules), el cual define como debe codificarse y decodificarse los valores de cada objeto pertenecientes al estándar ASN.1, y de esta manera pueda ser transmitida a través de la red de comunicaciones.

2.4.5 MIB II

La MIB II definida en *"RFC 1213",* es una base de datos muy amplia para gestionar los equipos conectados a internet.

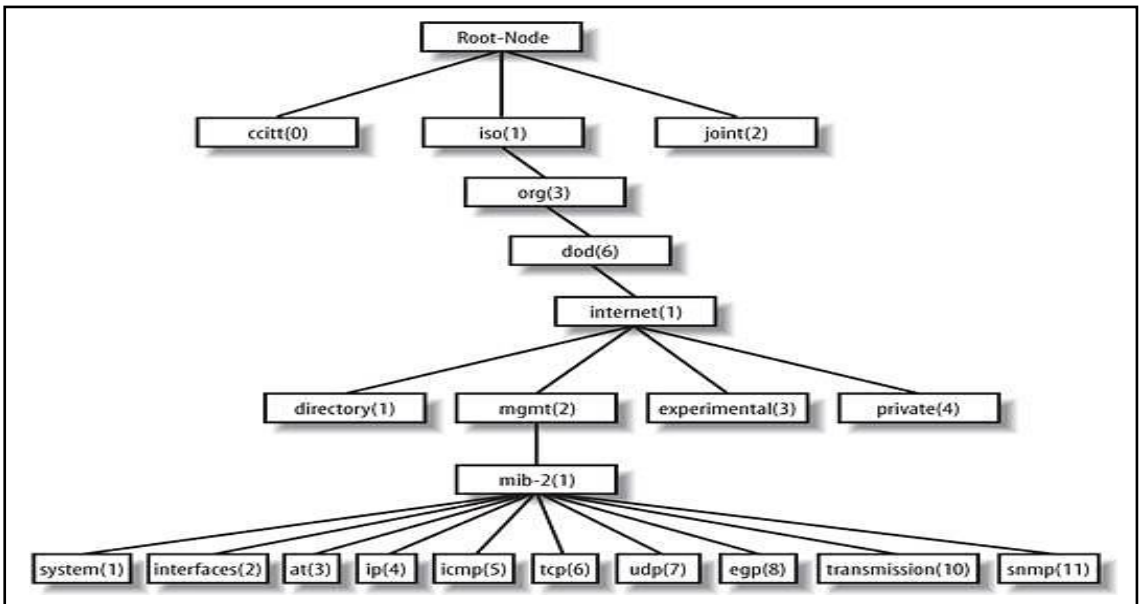


Figura 12. Estructura de la MIB II

Tomado de: (Network Management, s.f.)

La MIB II está compuesta por los siguientes elementos:

- **System:** Brinda información general del sistema.
- **Interfaces:** Se guarda información de interfaces de redes que se encuentran en el sistema.
- **Address Translation (at):** Se guardan las direcciones de enlace.
- **Ip:** Se guarda información sobre el protocolo IP.
- **Icmp:** Se guarda contadores de paquetes ICMP.
- **Tcp:** Se guarda información referente a las configuraciones del protocolo tcp.
- **Udp:** Se guarda información referente a las configuraciones del protocolo udp.
- **Egp:** Se guarda información referente a las configuraciones del protocolo egp.
- **Transmission:** Se guarda información sobre los protocolos de acceso.
- **Snmp:** Enlaza la estación de gestión y los agentes.

2.4.6 Formato del mensaje SNMP

SNMP utiliza la conexión UDP para el envío de mensajes PDU's, entre los gestores y los agentes. Cada mensaje para SNMPv1 y SNMPv2 contiene el siguiente formato.

- **Versión**: Versión de protocolo que se utiliza como: SNMPv1 o SNMPv2.
- **Comunidad:** Usado para el procedimiento de autenticación.
- **Pdu:** Es el contenido de información del protocolo, el que depende de la operación que se ejecute.

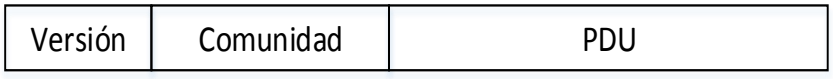


Figura 13. Formato del mensaje SNMP
Tomado de: (3Cu Electrónica, s.f.)

2.4.6.1 Operaciones SNMP

SNMP es un protocolo de solicitud y respuesta, mediante el NMS (Network Management System) se emite una solicitud y los dispositivos administrados retornan una respuesta. Este comportamiento se implementa mediante el uso de una de las cinco operaciones del protocolo: GetRequest, GetNextRequest, SetRequest, SnmpWalk y Trap.

1. **GetRequest (Entidad Gestora > Agente)**

Es utilizada por el gestor, este solicita el valor de una o algunas instancias de un elemento que está dentro del agente.

2. **GetNextRequest (Entidad Gestora > Agente)**

Es utilizada por el gestor para descubrir dinámicamente la estructura de una MIB y el contenido de sus tablas. Esta operación recorre el valor del objeto en una tabla o una lista dentro de un agente.

3. **SetRequest (Entidad Gestora > Agente)**

Es utilizada por el gestor para colocar valores de los objetos dentro de un agente.

4. **SnmpWalk (Entidad Gestora > Agente)**

Es utilizada por el gestor para recorrer todas las instancias de objetos a partir de un identificador dado dentro de un agente.

5. Trap (Agente > Entidad Gestora)

Es utilizada por el agente hacia el gestor para reportar eventos de estado de un elemento de red.

2.5 SNMPV3

La versión SNMPv3 define un nuevo modelo de seguridad y mejoras en la configuración remota. Esta versión intenta solucionar los problemas de seguridad existentes en las versiones anteriores del protocolo.

La seguridad ha sido la mayor debilidad de SNMP desde sus inicios, la autenticación en las versiones SNMPv1 y SNMPv2 son compuestas por una contraseña enviado en texto claro entre un gestor y agente. Cada mensaje en SNMPv3 contiene parámetros de seguridad que están codificados.

SNMPv3 brinda las siguientes características:

- **Integridad:** Garantiza al mensaje que no sea alterado al recorrer la red.
- **Autentificación:** Determina que el mensaje provenga de una origen válido y asegura que fue recibido.
- **Encriptación:** Cifra el contenido del mensaje, con el fin de impedir ser leído por un origen no autorizado.

2.5.1 Arquitectura SNMPv3

La arquitectura SNMPv3 está basada en el USM (User-Based Security Model) para la seguridad de mensajes y en el VACM (View-Based Access Control) para el control de acceso.

2.5.2 Entidad SNMP

2.5.2.1 Motor SNMP

Es la parte esencial de cualquier entidad SNMP y se encarga de implementar los siguientes procesos:

- ✓ Envío de mensajes
- ✓ Recepción de mensajes
- ✓ Autenticación
- ✓ Cifrado y descifrado de mensajes
- ✓ Control de acceso

El motor SNMP consta de las siguientes componentes:

- **Dispatcher (Despachador):** Permite el envío y recibo de mensajes SNMP. Determina si la versión del mensaje recibido es (SNMPv1, SNMPv2, o SNMPv3) y si soporta la versión, entrega los mensajes al *"Subsistema de Procesamiento de Mensajes"*.

- **Message Processing Subsystem (Subsistema de Procesamiento de Mensaje):** Prepara los mensajes a ser enviados y extrae los datos de aquellos mensajes recibidos.

- **Security Subsystem (Subsistema de Seguridad)**: Autentifica, cifra y descifra los mensajes. La autenticación puede usar *"communitys"* para las versiones SNMPv1 y SNMPv2, y *"USM"* para la versión SNMPv3.

- **Access Control Subsystem (Subsistema de Control de Acceso):** Establece que usuarios y que operaciones se les autoriza el acceso hacia los objetos de la MIB.

2.5.2.2 Aplicaciones SNMP

Son subsistemas que los servicios de un motor SNMP usan para cumplir con los trabajos relacionados al procesamiento de la información de gestión.

- **Command Generator (Generador de Comandos):** Genera las PDU GetRequest, GetNextRequest, SnmpWalk y SetRequest. Procesa su respectiva respuesta a los pedidos que se han generado.

- **Response Generator (Generador de Respuestas):** Recibe las PDU GetRequest, GetNextRequest, SnmpWalk y SetRequest. Genera la respuesta GetResponse adecuada, esto para ser enviado al gestor.

- **Notification Originator** (**Originador de Notificaciones):** Monitoriza eventos y genera Traps para ser enviadas al gestor.

- **Receptor de Notificaciones (Notification Receiver):** Espera una notificación Trap y genera la respuesta para el mensaje.

- **Emisor Proxy (Proxy Forwarder):** Facilita el paso de mensajes entre entidades SNMP, soporta todos los comandos SNMP.

2.5.3 Entidad Gestor

Consta de los siguientes subsistemas:

- **Motor:**
  - Despachador
  - Subsistema de procesamiento de mensajes
  - Subsistema de seguridad

- **Aplicaciones:**
  - Aplicación generadora de comandos
  - Aplicación originadora de notificaciones
  - Aplicación receptora de notificaciones

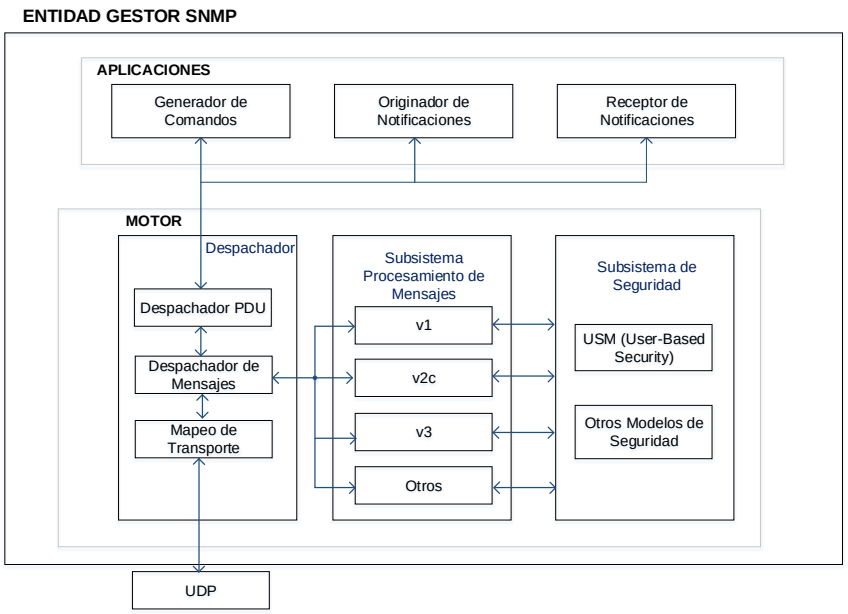


Figura 14. Entidad Gestor SNMPv3

Tomado de: (Millán, 2015)

2.5.4 Entidad Agente

Contiene los siguientes subsistemas:

- **Motor:**
  - Despachador
  - Subsistema de procesamiento de mensajes
  - Subsistema de seguridad
  - Subsistema de control de acceso

- **Aplicaciones:**
  - Aplicación contestadora de comandos
  - Aplicación originadora de notificaciones
  - Emisor proxy

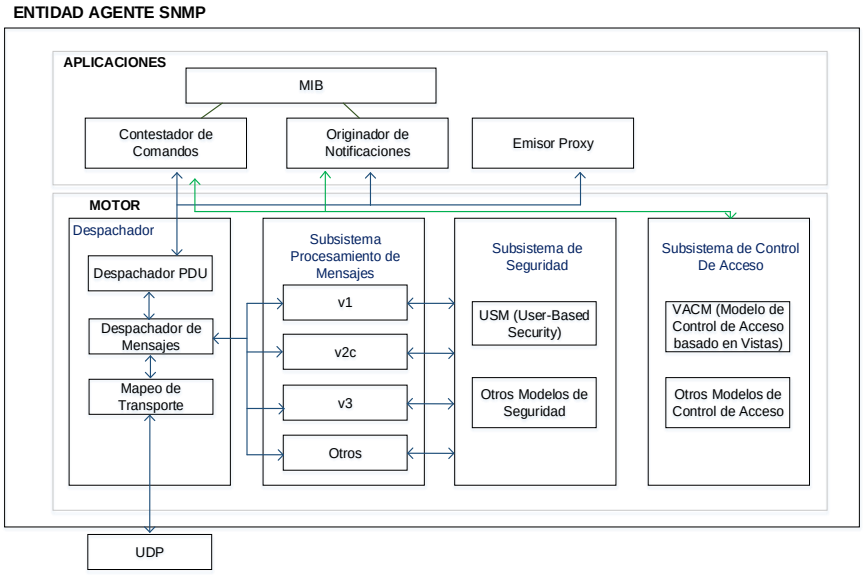


Figura 15. Entidad Agente SNMPv3
Tomado de: (Millán, 2015)

2.6 MODELO DE SEGURIDAD BASADO EN USUARIO – USER BASED SECURITY MODEL (USM)

El USM utiliza el concepto de usuario para que los parámetros de seguridad, tales como: protocolos de autentificación, privacidad y claves, se configuren en el agente y el gestor. En los intercambios de mensajes entre el gestor y el agente, hay una comprobación de integridad de datos y autentificación de origen de datos.

Este modelo consiste en tres módulos con diferentes especificaciones.

- **Módulo de autenticación:** Se asegura de que el mensaje provenga de la fuente de donde dice ser generado y que en el transcurso del envío no haya sido alterado.

- **Módulo timeliness:** Proporciona la protección contra el retraso o retransmisión maliciosa de los mensajes.

- **Módulo de privacidad**: Proporciona el cifrado y descifrado del contenido de datos de un mensaje.

Actualmente los protocolos de autenticación MD5 y SHA; y los protocolos de privacidad DES y AES se integran en la USM.

2.6.1 Autenticación

2.6.1.1 Algoritmo de Resumen de Mensaje - Message Digest Algorithm (MD5)

El algoritmo MD5 es el hash más seguro y de mayor uso en el mundo. Este algoritmo MD5 procesa mensajes de cualquier longitud.

2.6.1.2 Algoritmo de Hash Seguro – Secure Hash Algorithm (SHA)

Usa la función hash SHA-1 y se emplea en varias aplicaciones de seguridad de uso común y protocolos.

Existen notables diferencias entre MD5 y SHA-1. MD5 realiza una ejecución más rápida de algoritmo que SHA-1; sin embargo, a pesar de que SHA-1 es más lento, genera un “resumen” de mensaje de mayor longitud lo cual hace que el algoritmo sea más robusto contra ataques de fuerza bruta. En ambos casos, los dos algoritmos son no reversibles; es decir, no es posible revertir al mensaje original a partir del *“resumen”* y llave secreta.

2.6.2 Privacidad

2.6.2.1 Cifrado Estándar de Datos – Data Encryption Estandar (DES)

Es un algoritmo de cifrado de información simétrico, esto quiere decir que utiliza una llave similar tanto para encriptar como para desencriptar. Utiliza una clave muy corta, por lo que se considera inseguro para muchas aplicaciones, ocasionando que las claves sean rotas en menos de 24 horas.

2.6.2.2 Cifrado Estándar Avanzado – Advanced Encryption Standard (AES)

Es uno de los algoritmos más seguros y más utilizados hoy en día, puede ser descrito como un mensaje cifrado iterativo y simétrico.

2.7 MODELO DE CONTROL DE ACCESO BASADO EN VISTA - VIEW-BASED ACCESS CONTROL MODEL (VACM)

Este modelo implica al control de grupos de usuarios y sentencias de acceso que definen qué vistas puede utilizar un grupo de usuarios determinado para leer, escribir o recibir un mensaje en una MIB local accedida por una entidad remota.

Los cinco elementos que conforma el VACM son los siguientes:

2.7.1 Grupos

Un grupo es identificado por un “*groupName*” y es un conjunto de secuencias a quienes se les asigna derechos de acceso a determinados objetos de la MIB.

2.7.2 Nivel de Seguridad

Es el grado de seguridad con el cual un mensaje SNMP es enviado.

2.7.3 Contexto

Un contexto es un subconjunto, al cual se le asigna un nombre de las instancias de objetos que tienen asignado diferentes derechos de accesos en la MIB local.

2.7.4 Vista

Es una familia de subárboles de objetos, que define un conjunto específico de objetos gestionados. Un subárbol puede o no estar incluido o excluido de la vista.

2.7.5 Derechos de Acceso

Son las normas de acceso que se asignan a un contexto SNMP.

3. DESARROLLO DEL SOFTWARE

El Capítulo III permitirá conocer los conceptos fundamentales para el desarrollo de la aplicación, por lo cual se parte definiendo el lenguaje de programación Java y sus principales componentes. También se describe el agente a ser usado para el procesamiento de mensajes SNMPv3 y se plantea un análisis de requerimiento con el fin de identificar lo que va hacer la aplicación.

3.1 TECNOLOGÍAS UTILIZADAS

3.1.1 Java

*"Java es un lenguaje de programación orientado a objetos que fue desarrollado por Sun Microsystems en 1995. Se destaca por ser un lenguaje de propósito general y multiplataforma**,** además de todo ello mantiene las características que todo lenguaje debe tener: seguridad, robustez**,** multihilo y en general con un gran desempeño".* (Java, s.f.)

3.1.2 Glassfish

Es un servidor de aplicaciones que brinda tecnologías en la plataforma de Java EE, este soporta tecnologías tales como: JSP, JSF, Servlets, etc.

3.1.3 NetBeans

NetBeans es un entorno de desarrollo completo y profesional, contiene muchas funcionalidades para distintos tipos de aplicaciones en la cual se puede escribir, compilar, depurar y ejecutar aplicaciones.

3.1.4 NuDesign SNMPv3 Master Agent (Agente)

Es un agente que corre bajo la versión de 32/64 bit en: Windows XP, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Vista, Windows 7 y Windows 8. Es compatible solo para Windows y de fácil uso que permite realizar todos los requisitos de configuración necesarios para que corra en modo SNMPv1, SNMPv2 o SNMPv3.

3.1.5 Wireshark

Es una herramienta que permite capturar y monitorizar los paquetes de red que pasan por el equipo.

3.2 ANÁLISIS DE REQUERIMIENTO

Se especificará las funciones necesarias de la aplicación, para resolver y satisfacer las necesidades del usuario. Para lo cual se hará una recopilación de requerimientos y luego se implementará el modelo de caso de uso.

3.3 RECOPILACIÓN DE REQUERIMIENTOS

Se identificarán los usuarios que van a interactuar con la aplicación y los requisitos que éstos demandan de la misma.

3.3.1 Usuarios

Todas las actividades que se realiza en el sistema tiene como fin mantener un desempeño óptimo en todos sus procesos, estas actividades están a cargo del administrador general del mismo sistema, que en este caso viene a ser el personal encargado de monitorear la operación y desempeño de servicios de los cajeros automáticos.

3.3.2 Requisitos funcionales

Los requisitos funcionales especifican los servicios que debe proporcionar el sistema y así satisfacer los requerimientos de los usuarios.

- **Inicio de Sesión:** La aplicación debe solicitar el nombre del usuario y la respectiva contraseña para el acceso a la misma. Si el nombre del usuario y la contraseña son válidas, entonces el sistema debe presentar la página principal donde se halla el menú para acceder a las demás funciones de la aplicación.

- **Administrar Cuentas de Usuarios:** Es la manera en la cual se identifica y se autentifica a un usuario con la aplicación. La aplicación debe permitir crear y eliminar cuentas de usuarios para el ingreso y accesos a las funciones proporcionadas por la misma.

- **Configurar Parámetros:** La configuración debe mostrar al usuario valores de los parámetros para el envío de mensajes SNMPv3.

  La siguiente tabla muestra la descripción, valores permitidos y valor recomendado para el envío de mensajes SNMPv3.

Tabla 1. Parámetros del mensaje SNMPv3

Nombre	Detalles
Nivel de seguridad	**Descripción:** Es el nivel de seguridad del mesnaje enviado. **Valores permitidos:** Sin autenticación ni privacidad, con autenticación pero sin privacidad y con autenticación y privacidad. **Valor por defecto (recomendado):** Usuario con autenticación y privacidad.
Puerto de comandos	**Descripción:** Es el puerto destino al cual se enviarán los comandos de solicitud. **Valor por defecto (recomendado):** 161

- **Visualizar notificaciones recibidas:** La captura de notificaciones deberá visualizarse según el error ocurrido.

  Para visualizar las notificaciones recibidas por el cajero automático, se debe llenar el siguiente parámetro, descritos en la siguiente tabla.

Tabla 2. Notificación SNMPv3

Parámetro	Descripción
Dirección IP	Es la dirección IP del cajero automático que será monitoreado.
Nombre	Es el nombre asignado al cajero automático.

- **Navegar en un grupo MIB:** La aplicación debe permitir que el usuario navegue en una o varias bases MIB y a través de ellas ejecutar operaciones SNMPv3.

- **Ejecutar operaciones SNMPv3:** La aplicación debe permitir la emisión de un tipo mensaje SNMPv3 hacia el cajero automático. El mensaje puede ser de tipo Get, GetNext, SnmpWalk o Set.

  Para ejecutar una operación SNMP, se debe llenar los parámetros descritos en la siguiente tabla.

Tabla 3. Operación SNMPv3

Parámetro	Descripción
Dirección IP	Es la dirección IP del cajero automático, al cual va dirigido el mensaje.
OID	Es el objeto identificador del objeto MIB destino. El valor de este campo es establecido automáticamente cuando se selecciona un nodo del árbol MIB.
Sintaxis	Sintaxis del objeto MIB. El valor es establecido automáticamente cuando se selecciona un nodo del árbol MIB.

- **Gestión de MIBs:** La aplicación debe permitir agregar y la eliminar bases MIB según requiera el usuario.

- **Gestión de Cuentas de Usuarios SNMPv3 (Agente):** El agente debe permitir crear y eliminar cuentas de usuarios para aprobar o denegar el acceso a las funcionabilidades SNMPv3.

  La descripción de cada campo del formulario se detalla a continuación.

Tabla 4. Gestión de cuentas de usuario

Parámetro	Descripción
usmUserName	Es el nombre de seguridad del usuario.
AuthProtocol Password	Es el password de autenticación del usuario.
PrivProtocol Password	Es el password de privacidad del usuario.
Grupo VACM	Es el grupo VACM al cual pertenece el usuario.

3.3.3 Requisitos no funcionales

Definen las propiedades y restricciones de la aplicación referidas a las tecnologías utilizadas para su implementación.

- **Utilización del protocolo SNMPv3 para el monitoreo de los cajeros automáticos:** Únicamente SNMPv3 será el protocolo implementado en la aplicación y deberá cumplir con los requisitos funcionales mencionados anteriormente.

- **Utilización del lenguaje de programación Java:** La aplicación deberá ser implementada mediante el lenguaje de programación Java, para que ésta a futuro pueda ser instalada en cualquier plataforma que soporte JVM.

- **Manejo de la aplicación a través de un entorno web:** La aplicación deberá ser de tipo web, de manera que a futuro pueda ser utilizada desde cualquier sitio.

3.4 MODELO DE CASO DE USO

Representa los distintos requerimientos que hacen los usuarios al sistema, especificando funcionalidades y comportamiento del sistema al interactuar con los usuarios, mientras los que provocan su ejecución se denominan *"Actores"*.

3.4.1 Actor

Un actor es un usuario el cual interactúa con el sistema.

3.4.2 Caso de uso

Es un trabajo específico que se lo realiza bajo una orden de un usuario o un sistema externo.

La definición del caso de uso se realiza utilizando el siguiente formato:

Tabla 5. Definición de caso de uso

Requisito: Requisito funcional.
Caso de uso: Nombre del caso de uso.
Actor: Actor que interactúa en el caso de uso.
Descripción: Definición del caso de uso.

Las definiciones de los casos de uso de la aplicación son las siguientes:

Tabla 6. Caso de uso – Inicio de Sesión

Requisito: Inicio de Sesión.
Caso de uso: Iniciar Sesión.
Actor: Administrador General.
Descripción: Los actores usarán este caso de uso para el acceso a la aplicación. La aplicación verificará el nombre de usuario y la contraseña de autenticación.

Tabla 7. Caso de uso – Cuentas de Usuarios

Requisito: Administrar Cuentas de Usuarios.
Caso de uso: Cuentas de Usuarios.
Actor: Administrador General.
Descripción: Los actores usarán este caso de uso para crear y eliminar cuentas de usuarios.

Tabla 8. Caso de uso - Configurar Parámetros

Requisito: Configurar Parámetros.
Caso de uso: Configurar Parámetros.
Actor: Administrador General.
Descripción: Los actores usarán este caso de uso para configurar valores de parámetros de mensajes SNMPv3.

Tabla 9. Caso de uso - Navegar en grupo MIB

Requisito: Navegar en un grupo MIB.
Caso de uso: Navegar en grupo MIB.
Actor: Administrador General.
Descripción: Los actores usarán este caso de uso para navegar a través de la estructura en forma de árbol de una determinada MIB.

Tabla 10. Caso de uso - Ejecutar operaciones SNMPv3

Requisito: Ejecutar operaciones SNMPv3.
Caso de uso: Ejecutar operaciones SNMPv3.
Actor: Administrador General.
Descripción: Los actores usarán este caso de uso para emitir un tipo de mensaje SNMPv3 hacia el cajero automático.

Tabla 11. Caso de uso - Visualizar notificaciones recibidas

Requisito: Visualizar notificaciones recibidas.
Caso de uso: Visualizar notificaciones.
Actor: Administrador General
Descripción: Los actores usarán este caso de uso para ver las notificaciones recibidas del cajero automático.

Tabla 12. Caso de uso – Gestión de MIBs

Requisito: Gestión de MIBs.
Caso de uso: Gestión de MIBs.
Actor: Administrador General.
Descripción: Los actores usarán este caso de uso para agregar y/o eliminar archivos MIBs.

Tabla 13. Caso de uso - Gestión de Cuentas de Usuarios SNMPv3 (Agente)

Requisito: Gestión de Cuentas de Usuarios SNMPv3 (Agente).
Caso de uso: Gestión de Cuentas de Usuarios SNMPv3 (Agente).
Actor: Administrador General.
Descripción: Los actores usarán este caso de uso a través de un agente para crear y eliminar cuentas de usuarios snmpv3.

3.4.3 Diagrama de casos de uso

Representan a los actores, a los casos de uso y las diferentes relaciones entre ambos. Este se obtiene a partir de la descripción de los requisitos funcionales y de la definición de los casos de uso.

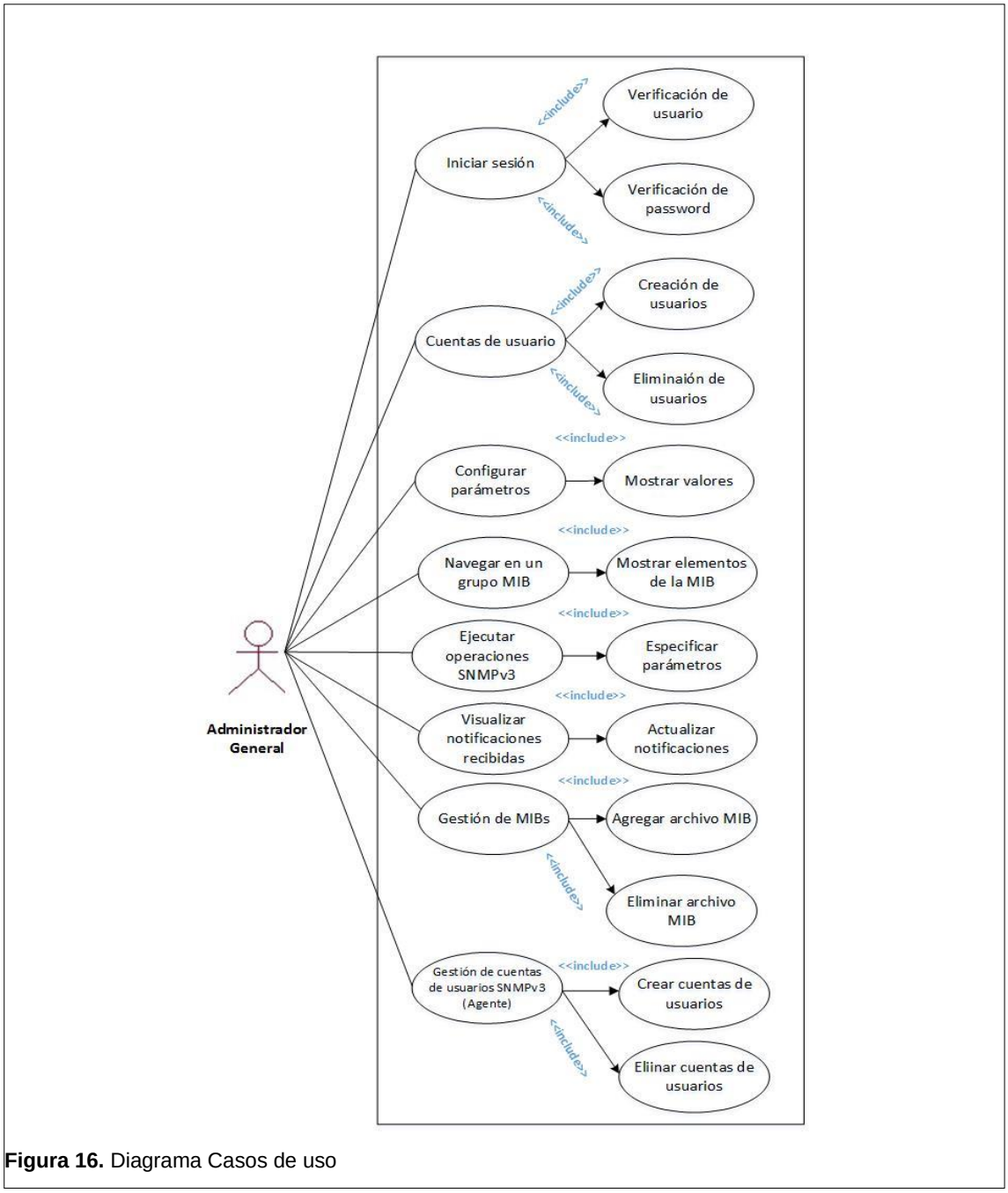


Figura 16. Diagrama Casos de uso

4. PRUEBAS Y RESULTADOS

El Capítulo IV trata acerca de las pruebas de funcionabilidad con la aplicación para verificar si se cumplen los requisitos funcionales y no funcionales tratados en el capítulo anterior; y además se obtiene un análisis de los resultados conseguidos. Previo a esto se describe la definición, características principales, funcionalidades principales que presta la aplicación y una descripción general de su interfaz gráfica.

4.1 CARACTERÍSTICAS DE LA APLICACIÓN

4.1.1 Definición

El nombre asignado de la aplicación desarrollada es AppSNMPV3, que son siglas que significan: *"Aplicación SNMPv3"*. Esta es una aplicación que permite ejecutar operaciones y recibir notificaciones automáticas de monitorización y está basada en el protocolo SNMPv3.

4.1.2 Características Principales

- Usa el protocolo SNMPv3
- Ha sido desarrollada en Java
- Es una aplicación tipo Web
- Trabaja con un agente, el cual envía información al servidor relativo al monitoreo del cajero automático

4.1.2.1 Funcionalidades Principales

- Monitorea y diagnostica el cajero automático
- Detecta eventos ocurridos en el cajero automático mediante las notificaciones automáticas
- Brinda seguridad al sistema mediante la funcionabilidad *"USM"*

- Controla el ingreso a la aplicación
- Maneja elementos del subsistema *“VACM”*

4.1.2.2 Descripcion de la Interfaz Gráfica

Las figuras a continuación muestran las interfaces gráficas más representativas de la aplicación y sus componentes.

Figura 17. Página Inicio de sesión

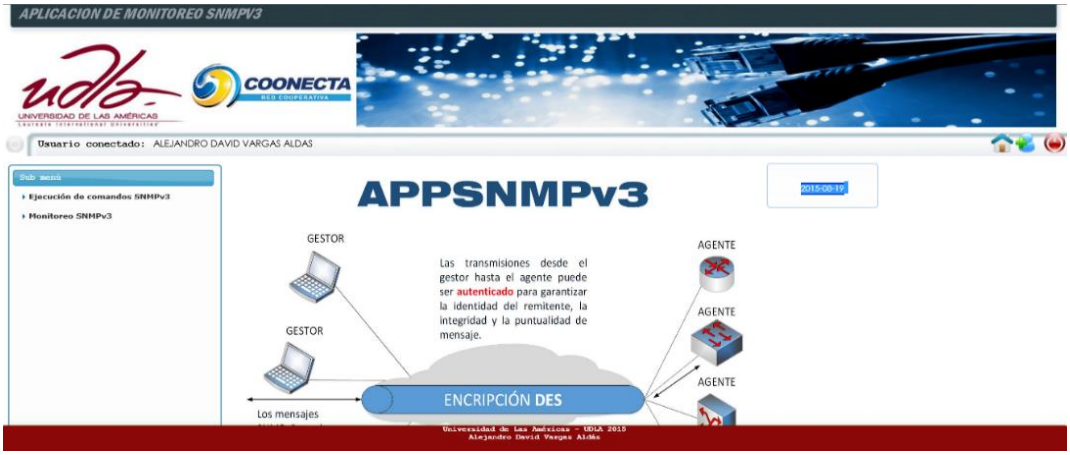


Figura 18. Página Bienvenida

Figura 19. Menú para agregar cuentas de usuarios

Figura 20. Menú para agregar cajeros automáticos

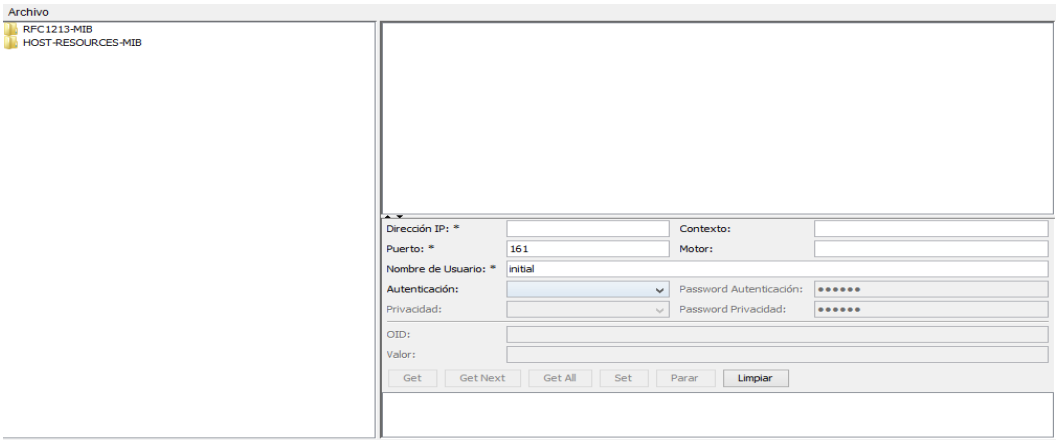


Figura 21. Menú para ejecutar operaciones SNMPv3 hacia el cajero automático

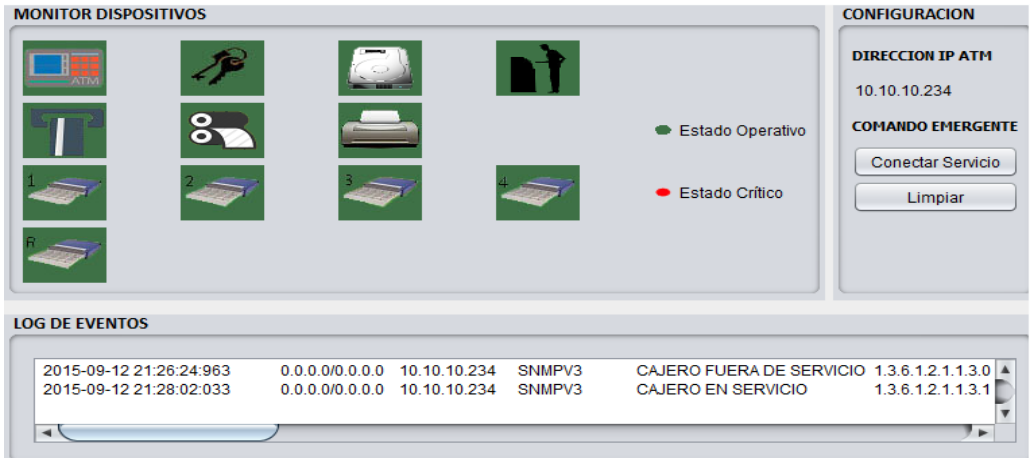


Figura 22. Página para visualizar las notificaciones automáticas enviadas por el cajero automático

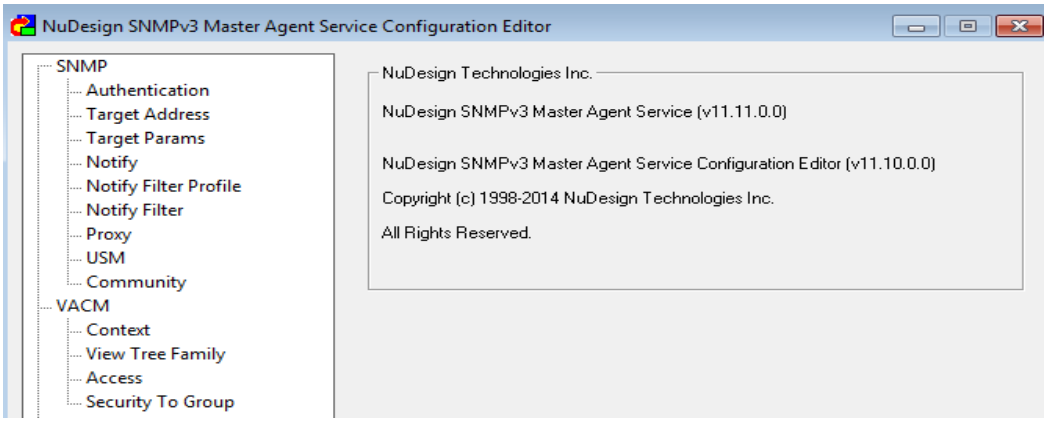


Figura 23. Menú para configurar mensajes SNMPv3 (Agente localizado en el Cajero Automático)

Figura 24. Pantalla del cajero automático (Propiedad Red Coonecta)

4.2 PRUEBAS

A continuación se describirá cómo se ha probado las diferentes funciones de la aplicación en un ambiente de pruebas determinado.

4.3 CONFIGURACIÓN DEL AGENTE NUDESIGN SNMPV3 MASTER AGENT

Mediante el agente *"NuDesign SNMPv3 Master Agent"* que ha sido descargo he instalado en el cajero automático, se le ha realizado la configuración necesaria para el funcionamiento de los mensajes SNMPv3.

4.3.1 Página SNMPv3 – SNMPv3 Page

- **Version:** Para iniciar el agente en modo SNMPv3, se debe seleccionar "*SNMPv3"* en la página SNMP. Este corresponde a la versión de SNMP.

- **Port Number:** El puerto por defecto es el 161 y se usará para escuchar los mensajes SNMP.

- **NumWorkerThreads:** Define la cantidad de mensajes que podrán ser procesados simultáneamente.
  - Para este caso se ha ingresado el número ***"3"*** que es suficiente.

- **Engine**: Es el identificador del motor autorizado a la cual va dirigido el mensaje de solicitud.

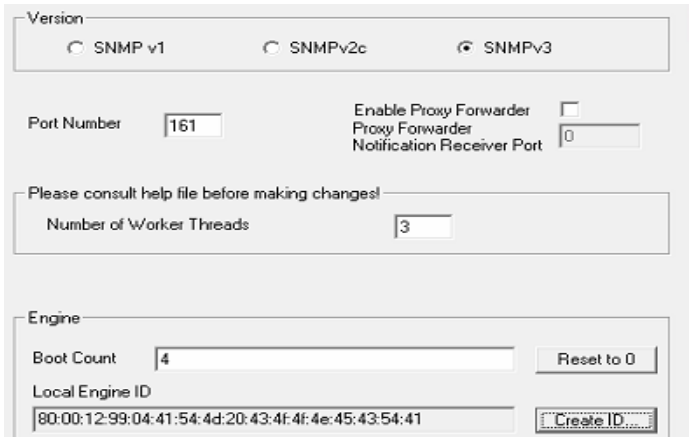


Figura 25. Menú para seleccionar la versión SNMP

4.3.2 Crear ID del Motor – Create Engine ID

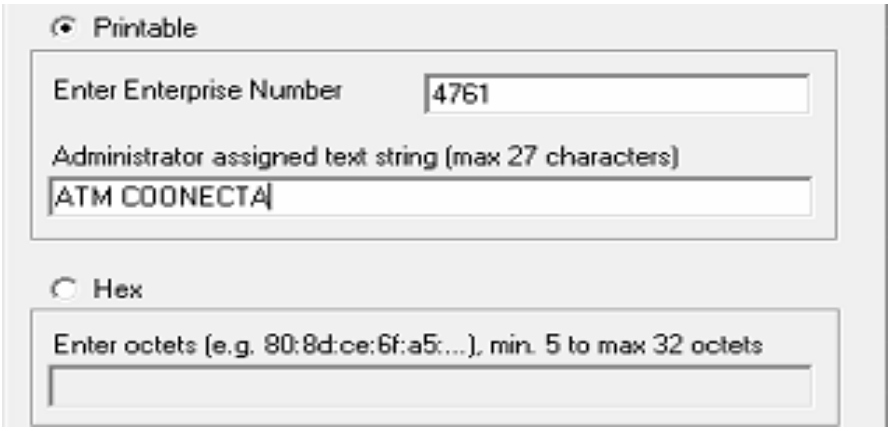


Figura 26. Menú para crear un ID del Motor

- **Printable:** Al seleccionar *"Printable"*, se debe ingresar el *"Enterprise Number"* y una *"cadena de texto"*.

- **Enterprise Number**: Se otorga a la empresa un ID único.
  - Para este caso se ha definido el número ***"4761"***.

- **Administrator assigned text string:** Es una cadena de texto de hasta 27 caracteres que describe de forma exclusiva el ID del motor SNMP.
  - Para este caso se ha definido el nombre de ***"ATM COONECTA"*.**

4.3.3 Seguridad SNMPv3 – SNMPv3 Security

4.3.3.1 Autenticación - Authentication

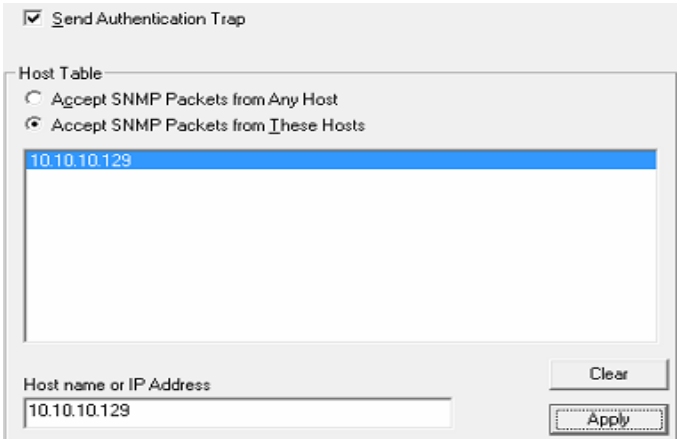


Figura 27. Menú para configurar la Autenticación de los mensajes

- **Send Authentication Trap:** El agente podrá o no enviar un *"trap"* a uno o varios destinos.
  - Para este caso se habilitado la casilla ***"trap"***.

- **Host Table:** Permite aceptar paquetes SNMP de una lista de hosts o desde todos los hosts.
  - Para este caso se aceptará paquetes solamente provenientes de la máquina servidor, cuya dirección IP es ***"10.10.10.129"***.

4.3.3.2 USM

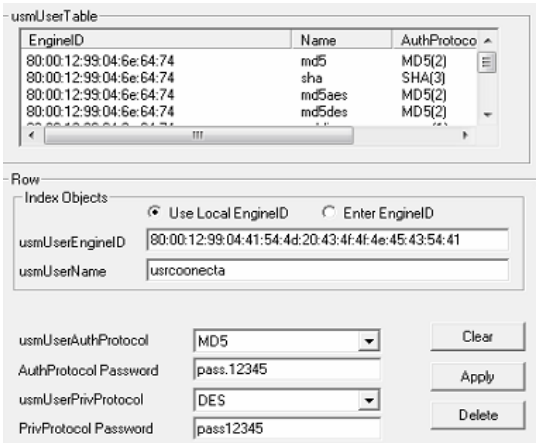


Figura 28. Menú para configurar la seguridad USM del usuario

- **usmUserEngineID**: Es un identificador único y propio del motor SNMP.

- **usmUserName:** Es el nombre de seguridad del usuario.
  - Para este caso se ha definido el nombre de usuario ***"usrcoonecta"***.

- **usmUserAuthProtocol:** Indica si los mensajes a ser enviados podrán ser autenticados.
  - Para este caso se ha definido el protocolo de autenticación ***"MD5"***.

- **AuthProtocolPassword:** Es la contraseña para generar la clave de seguridad.
  - Para este caso se ha definido la contraseña ***"pass.12345"***.

- **usmUserPrivProtocol**: Indica si los mensajes a ser enviados podrán ser privados.
  - Para este caso se ha definido el protocolo de privacidad ***"DES"***.

- **PrivProtocolPassword**: Es la contraseña para generar la clave de seguridad.
  - Para este caso se ha definido la contraseña ***"pass12345"***.

4.3.4 Tablas de Direcciones de Destino – Target Address Tables

4.3.4.1 Parámetros de Destino – Target Parameters

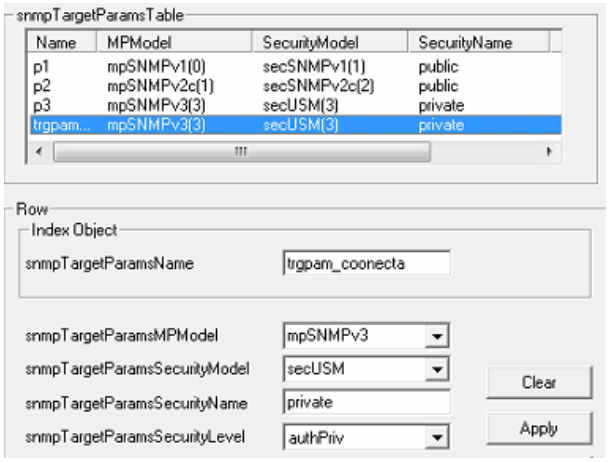


Figura 29. Menú para configurar los Parámetros de Destino del mensaje

- **snmpTargetParamsName:** Es un identificador único para indexar la tabla.
  - Para este caso se ha definido el nombre ***"trgpam_coonecta"***. Este se relaciona con *"snmpTargetAddrParams"*.

- **snmpTargetParamsMPModel:** Es el modelo del procesamiento del mensaje.
  - Para este caso se ha seleccionado el protocolo ***"mpSNMPv3"***.

- **snmpTargetParamsSecurityModel:** Es el modelo de seguridad.
  - Para este caso se ha seleccionado el modelo ***"secUSM"***.

- **snmpTargetParamsSecurityName:** Es la seguridad que identifica al identificador.
  - Para este caso se ha definido el nombre ***"private"***.

- **snmpTargetParamsSecurityLevel:** Es el nivel de seguridad.
  - Para este caso se ha seleccionado la seguridad ***"authPriv"***.

4.3.4.2 Dirección de Destino – Target Address

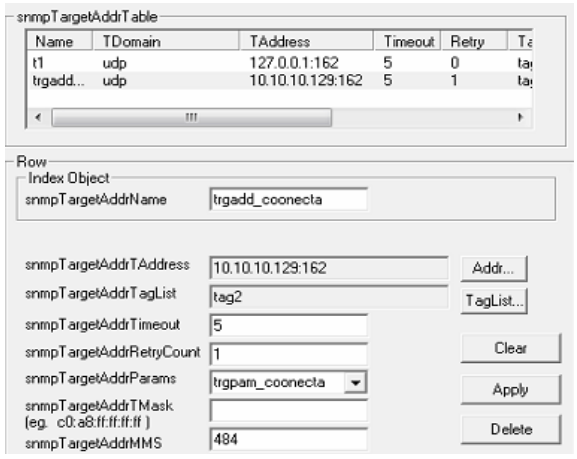


Figura 30. Menú para configurar la Dirección de Destino del mensaje

- **snmpTargetAddrName:** Es un identificador único para indexar la tabla.
  - Para este caso se ha definido el nombre ***"trgadd_coonecta".***

- **snmpTargetAddrTAddress:** Es una dirección y el puerto de destino.
  - Para este caso se ha definido la dirección IP del servidor y su puerto ***"10.10.10.129:162"***.

- **snmpTargetAddrTagList:** Es usado para las notificaciones.
  - Para este caso se ha importado la configuración de la etiqueta ***"tag2"***, desde la página *"Notification".*

- **snmpTargetAddrTimeout:** Refleja el tiempo de espera para la comunicación con la dirección de transporte de destino.
  - Para este caso se ha definido un timeout de ***"5"*** segundos.

- **snmpTargetAddrRetryCount**: Es el número de reintentos a intentarse cuando no se recibe una respuesta para un mensaje generado.
  - Para este caso se ha definido el número de reintentos a ***"1".***

- **snmpTargetAddrParams**: Es un identificador que contiene parámetros para ser usados al generar mensajes a esta dirección de transporte.
  - Para este caso se ha importado la configuración de ***"trgpam_coonecta",*** desde la página *"Target Parameters"***.**

- **snmpTargetAddrMMS:** Es el valor máximo del tamaño de un mensaje.
  - Para este caso se ha definido el tamaño ***"484"***.

4.3.5 Tablas de Notificación – Notification Tables

4.3.5.1 Notificación – Notification

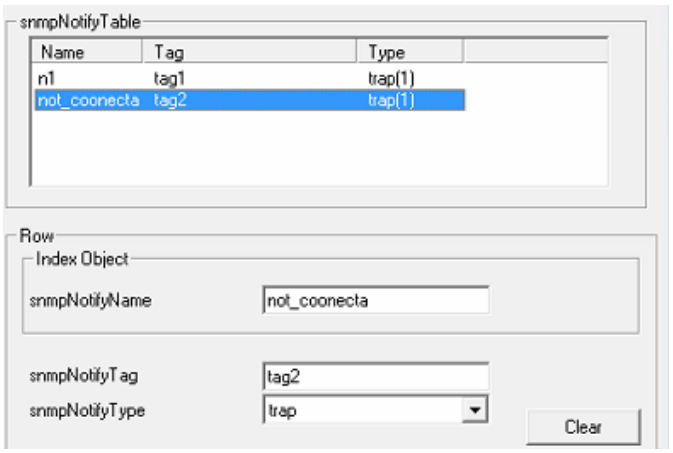


Figura 31. Menú para configurar la Notificación de algún evento

- **snmpNotifyName:** Es un identificador único para indexar la tabla.
  - Para este caso se ha definido el nombre ***"not_coonecta"***.

- **snmpNotifyTag:** Es un valor de la etiqueta para las notificaciones.
  - Para este caso se ha definido la etiqueta ***"tag2"***. Este se relaciona con *"snmpTargetAddrTagList"*.

- **snmpNotifyType:** Puede ser de tipo *"trap"* o *"inform"*.
  - Para este caso se ha seleccionado el tipo ***"trap"***.

4.3.5.2 Notificación al Perfil Filtrado – Notification Filter Profile

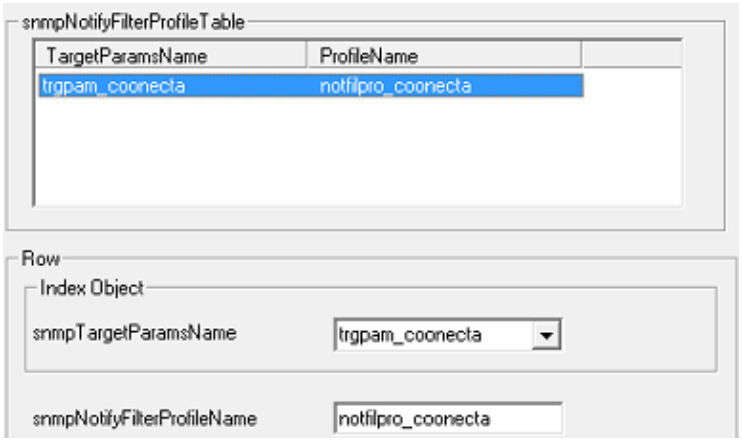


Figura 32. Menú para configurar la Notificación a un Perfil determinado

- **snmpTargetParamsName:** Este es un objeto externo de *"snmpTargetParamsTable"*.
  - Para este caso se ha importado la configuración de ***"trgpam_coonecta"*,** desde la página *"Target Parameters"*.

- **snmpNotifyFilterProfileName:** Es un nombre único asignado al *"snmpNotifyFilterProfileName"*.
  - Para este caso se ha definido el nombre ***"notfilpro_coonecta"***.

4.3.5.3 Filtro de Notificación – Notification Filter

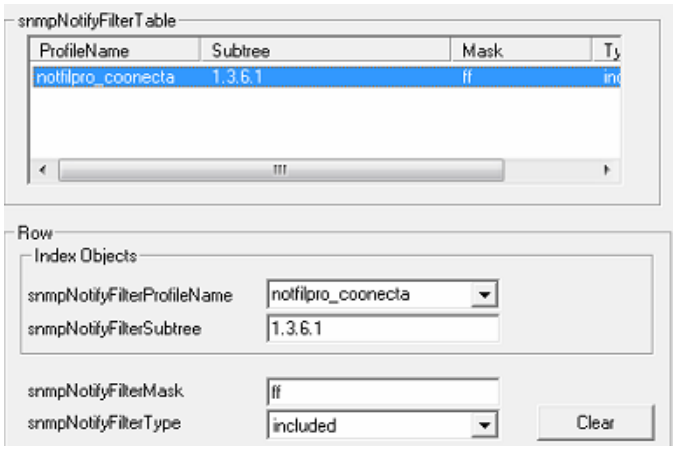


Figura 33. Menú para configurar el Filtro de un objeto externo para la Notificación

- **snmpNotifyFilterProfileName:** Es un objeto externo de *"snmpNotifyFilterProfileTable".*
  - Para este caso se ha importado la configuración de ***"notfilpro_coonecta"*** desde la página *"Notification Filter Profile"***.**

- **snmpNotifyFilterSubtree:** Define una familia de subárboles.
  - Para este caso se ha especificado el subárbol ***"1.3.6.1"***.

- **SnmpNotifyFilterMask**: Define la máscara.
  - Para este caso se ha especificado la máscara ***"ff"*.**

- **SnmpNotifyFilterType:** Indica si el subárbol correspondiente y la máscara está incluido o excluido de esta configuración.
  - Para este caso se ha seleccionado ***"INCLUDED"***.

4.3.6 VACM

4.3.6.1 Contexto – Context

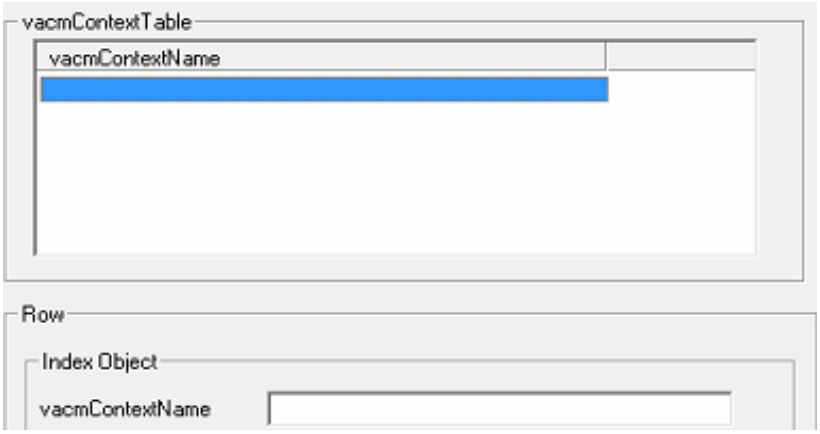


Figura 34. Menú para configurar un Contexto para el menaje

- **vacmContextName:** Es un nombre de identificación única de un contexto. El contextName *"vacío",* representa el contexto predeterminado.

4.3.6.2 Seguridad al Grupo – Security to Group

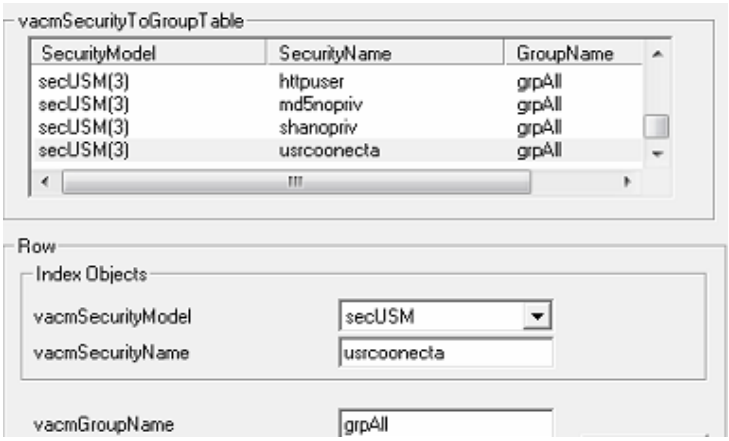


Figura 35. Menú para Referenciar la Seguridad al Grupo

- **vacmSecurityModel:** Es el modelo de seguridad que se referencia.
  - Para este caso se ha definido el modelo de seguridad ***"secUSM".***
- **vacmSecurityName:** Es el nombre para la seguridad.
  - Para este caso se ha definido el nombre ***"usrcoonecta".***

- **vacmGroupName:** Es el nombre del grupo al que la fila pertenece.
  - Para este caso se ha definido el grupo ***"grpAll".*** Este se relaciona con *"snmpTargetAddrParas".*

4.3.6.3 Acceso – Access

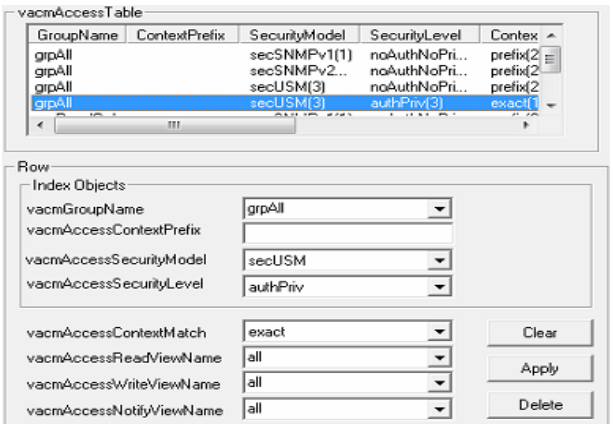


Figura 36. Menú para configurar los Accesos de Políticas al Grupo

- **vacmGroupName:** Se define una política para el control de acceso de un grupo.
  - Para este caso se ha importado la configuración de ***"grpAll",*** desde la página *"Security to Group".*

- **vacmAccessContextPrefix:** Es un nombre de contexto completo o el prefijo de un nombre de contexto.

- **vacmAccessSecurityModel:** Define un modelo de seguridad en particular.
  - Para este caso se ha seleccionado el modelo de seguridad ***"secUSM"*.**

- **vacmAccessSecurityLevel:** Es el nivel de seguridad requerido.
  - Para este caso se ha seleccionado el nivel de seguridad ***"authPriv"*.**

- **vacmAccessContextMatch:** Define si el valor del contexto es exacta o es prefijo.
  - Para este caso se ha dado el acceso ***"all"*.**

- **vacmAccessReadViewName:** Autoriza acceso de lectura.
  - Para este caso se ha dado el acceso ***"all"*.**

- **vacmAccessWriteViewName:** Autoriza el acceso de escritura.
  - Para este caso se ha dado el acceso ***"all"*.**

- **vacmAccessNotifyViewName:** Autoriza el acceso para la notificación.
  - Para este caso se ha dado el acceso ***"all"*.**

4.3.6.4 Vista MIB – MIB View

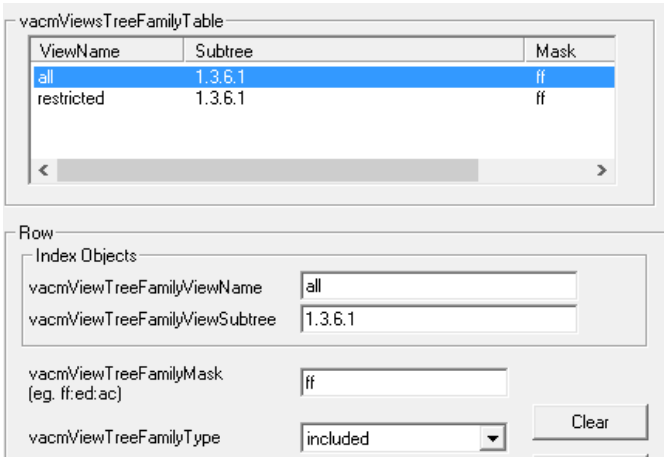


Figura 37. Menú para configurar Permisos para acceder a una Vista MIB

- **vacmViewTreeFamilyViewName:** Es el nombre asignado al subárbol.
  - Para este caso se ha definido el nombre ***"all"***.
- **vacmViewTreeFamilyViewSubtree:** Define una familia de subárboles.
  - Para este caso se ha definido la familia ***"1.3.6.1"***.

- **vacmViewTreeFamilyMask:** Es la máscara de una familia de subárboles.
  - Para este caso se ha definido la máscara ***"ff"*.**

- **vacmViewTreeFamilyType**: Indica si la familia correspondiente y la máscara está incluido o excluido de la configuración.
  - Para este caso se ha seleccionado el valor ***"included"*.**

4.4 ADMINISTRACIÓN DE CUENTAS DE USUARIO

4.4.1 Iniciar Sesión

Figura 38. Menú para el ingreso de credenciales del usuario

- Para este caso se ingresa con el usuario ***"0123456789"*** y la contraseña ***"1234"***

4.4.2 Creación de un usuario

Figura 39. Menú para Crear a un usuario

- Para este caso se ha creado un usuario con los siguientes datos: cédula ***"1212345678",*** apellidos ***"VARGAS",*** nombres ***"DAVID",*** clave ***"5556",*** teléfono ***"0995060777"*** y dirección ***"Av. Republica e ignasio san maria".***

4.5 MANEJO DE MIBS

4.5.1 Selección de MIB

Previamente a la ejecución de comandos SNMPv3, se ha cargado la base *"MIB-RFC1213"*. Esta base muestra su estructura en forma de árbol y está conformada por una lista desplegable de propiedades a nivel de gestión de red.

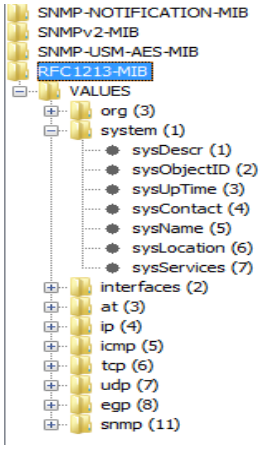


Figura 40. MIB Seleccionada RFC1213

4.6 MONITOREO AL CAJERO AUTOMÁTICO

Para verificar los mensajes que se envían desde la aplicación (Servidor) con el cajero automático (Cliente) y viceversa. Se ha hecho uso de la herramienta de captura y análisis de paquetes de red *"Wireshark"* versión 1.12.6, la cual ha sido instalada en el sistema operativo del cajero automático.

4.6.1 Ejecución de Operaciones SNMPv3

Al ejecutar cualquier mensaje SNMPv3 a excepción del comando "*Trap*", estos se ejecutan en cuatro pasos fundamentales en la cual participan:

- **Cliente:** En este caso viene a ser el cajero automático.

- **Servidor:** En este caso viene a ser el navegador web en donde se maneja la aplicación.
- **Cajero Automático:** En este caso es el elemento que se va a gestionar.

Los pasos para ejecutar operaciones SNMPv3 son los siguientes:

1. El servidor envía al cliente la petición de información del cajero automático.
2. El cliente mediante el agente recibe los mensajes, los procesa e interpreta su contenido.
3. El agente forma el tipo de mensaje SNMPv3 de respuesta requerido y lo envía hacia el servidor.
4. El servidor recibe el mensaje de respuesta, procesa su contenido y genera una respuesta que sea legible para el usuario.

4.6.1.1 Mensaje GetRequest

Se han capturado cuatro mensajes SNMPv3 al ejecutar la operación GetRequest. De estos paquetes, los dos primeros se han configurado de manera correcta y los dos restantes se han configurado de manera incorrecta. Esto para ver los tipos de respuesta que envía el cliente al servidor.

1. Mensaje GetRequest solicitando la descripción del cajero automático

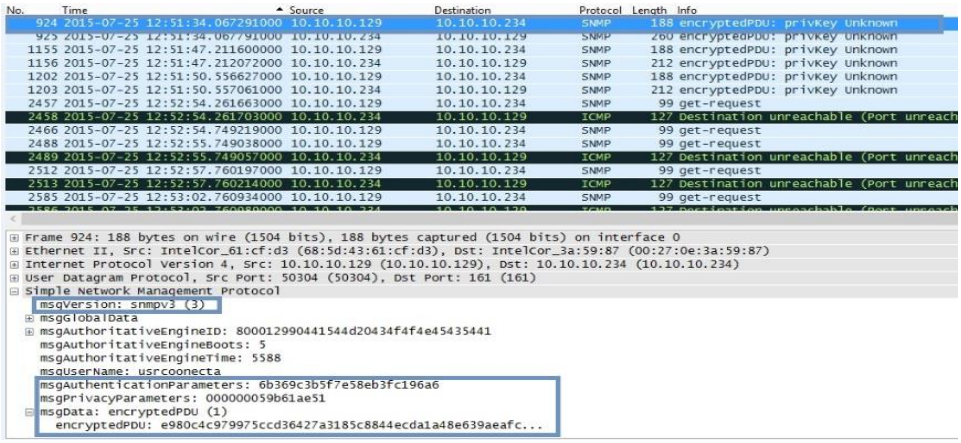


Figura 41. Mensaje GetRequest enviado hacia el Cajero Automático

Como se puede apreciar en la figura, el mensaje fue enviado desde el servidor hacia el cliente y viceversa. Este cumple con los parámetros de seguridad que brinda el protocolo SNMPv3, ya que en la parte seleccionada se puede verificar que el mensaje enviado usa la versión 3 de SNMP y además cuenta con protección privada y encriptada, por lo cual no permitirá que estos valores sean descifrados por cualquier usuario. El mismo caso sucede con la siguiente figura capturada a continuación.

2. Mensaje GetRequest solicitando la localización del cajero automático

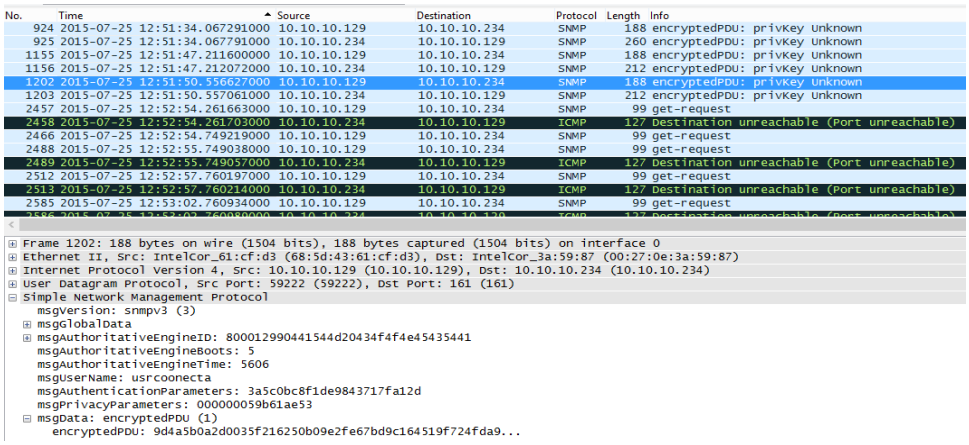


Figura 42. Mensaje GetRequest enviado al Cajero Automático

3. Mensaje GetRequest con fallo en la autenticación del usuario

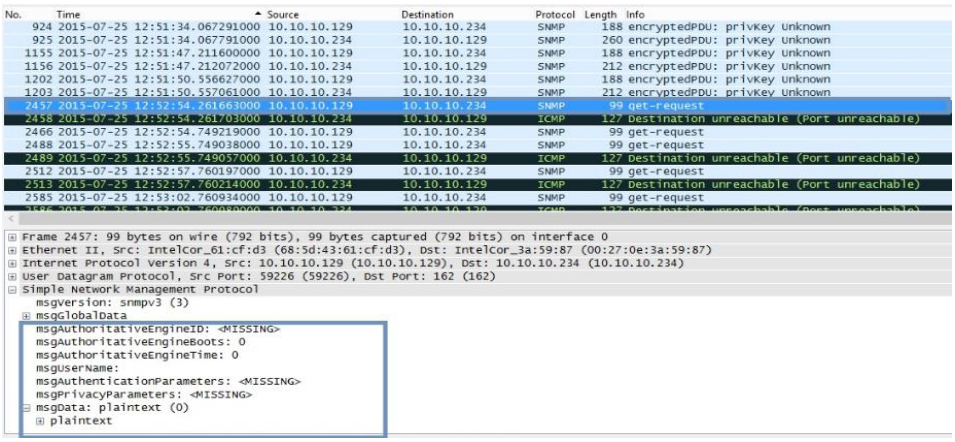


Figura 43. Mensaje GetRequest enviado al Cajero Automático

En esta figura, el mensaje enviado desde el servidor hacia el cliente no ha podido ser procesado, esto debido a que el password de autenticación de usuario no es el correcto.

4. Mensaje GetRequest con timeout

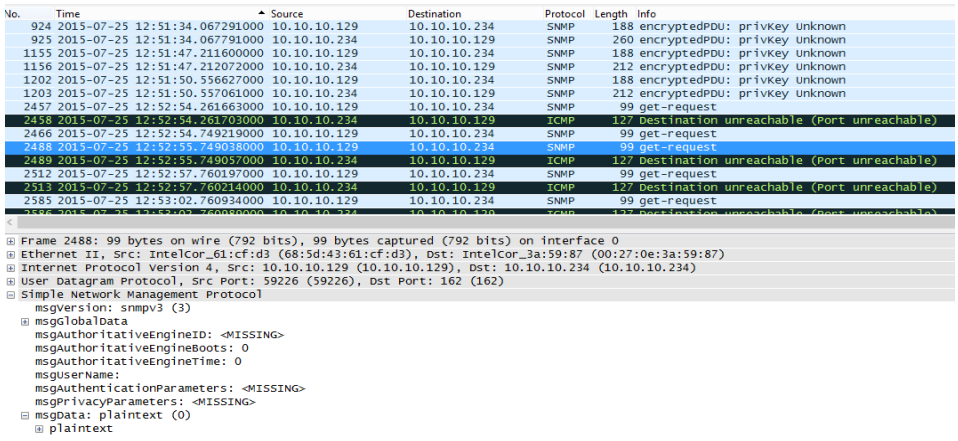


Figura 44. Mensaje GetRequest enviado al Cajero Automático

En esta figura, el mensaje enviado desde el servidor hacia el cliente tampoco pudo ser procesado, esto debido a que el puerto del SNMP ha sido cambiado, provocando que se genere un timeout en la transmisión del mensaje.

5. Visualización de los mensajes GetRequest que se enviaron desde el servidor

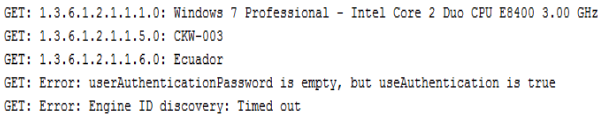


Figura 45. Datos GetRequest que se enviaron al Cajero Automático visualizados desde la aplicación

4.6.1.2 Mensaje GetNextRequest

En las siguientes figuras, se detallan los resultados al enviarse el mensaje *“GetNextRequest”.*

1. **Mensaje GetNextRequest solicitando la dirección IP del cajero automático**

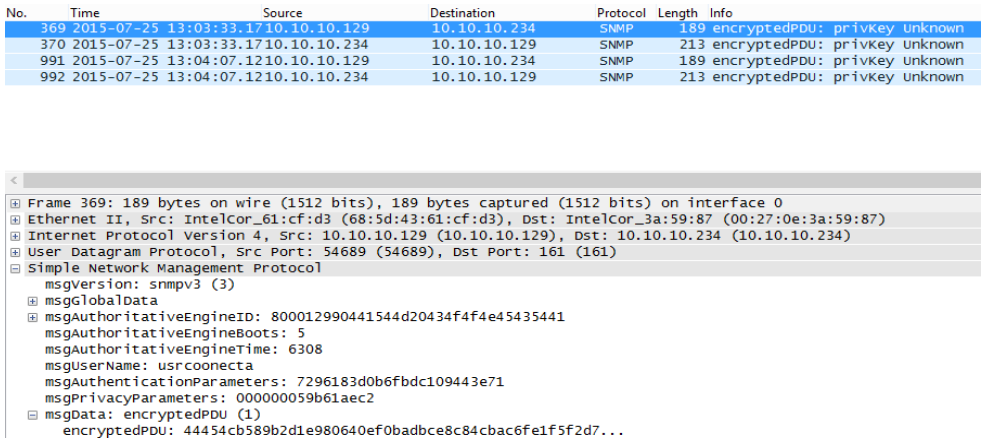


Figura 46. Mensaje GetNextRequest enviado al Cajero Automático

2. **Mensaje GetNextRequest solicitando la máscara del cajero automático**

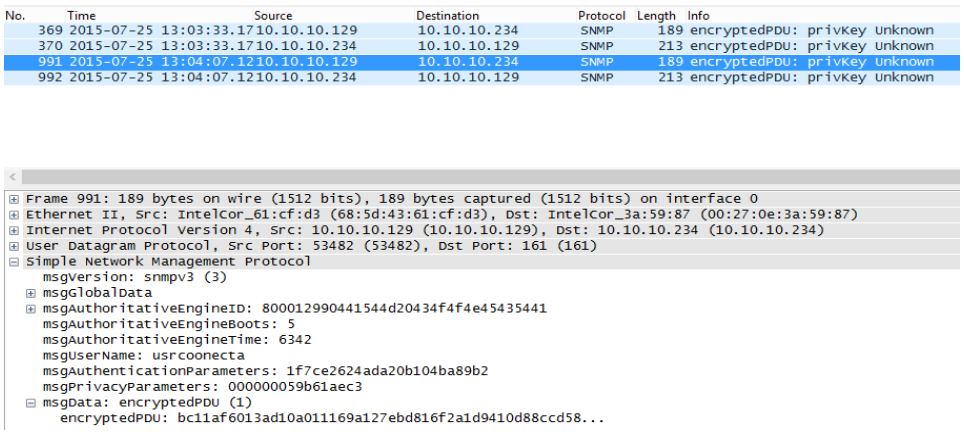


Figura 47. Mensaje GetNextRequest enviado al Cajero Automático

3. **Visualización de los mensajes GetNextRequest que se enviaron desde el servidor**

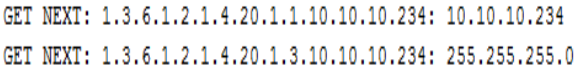


Figura 48. Datos GetNextRequest que se enviaron al Cajero Automático visualizados desde la aplicación

4.6.1.3 Mensaje SnmpWalk

En la siguiente figura, se muestra los resultados al enviarse el mensaje *"SnmpWalk".*

1. **Mensaje SnmpWalk solicitando información completa del cajero automático**

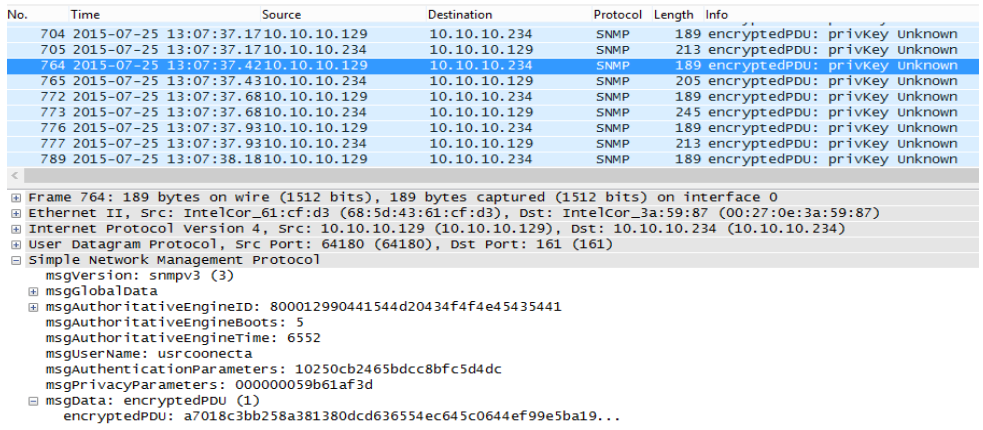


Figura 49. Mensaje SnmpWalk enviado al Cajero Automático

2. **Visualización de los mensajes SnmpWalk que se enviaron desde el servidor**

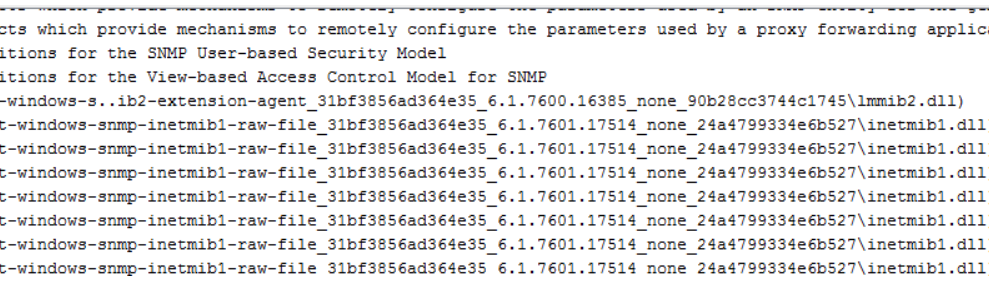


Figura 50. Datos SnmpWalk que se envió al Cajero Automático visualizado desde la aplicación

4.6.1.4 Mensaje SetRequest

En la siguiente figura, se muestra los resultados al enviarse un mensaje *"SetRequest".*

1. **Mensaje SetRequest colocando un valor dentro del cajero automático**

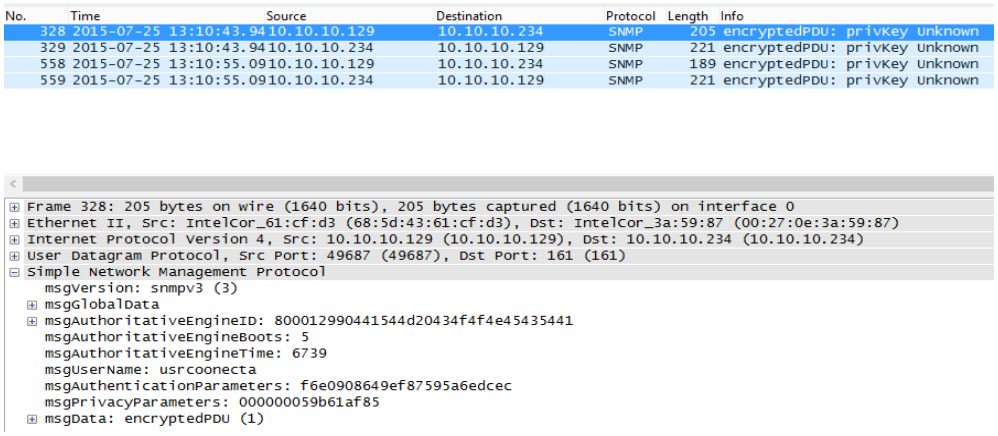


Figura 51. Mensaje SetRequest enviado al Cajero Automático

2. **Visualización del mensaje SetRequest que se enviaron desde el servidor**

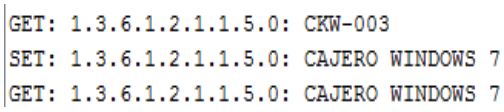


Figura 52. Datos SetRequest que se envió al Cajero Automático visualizado desde la aplicación

4.6.2 Notificaciones Automáticas

En las siguientes figuras, se muestran las capturas de las notificaciones automáticas *"Trap" más comunes*.

1. Desconexión del cajero automático

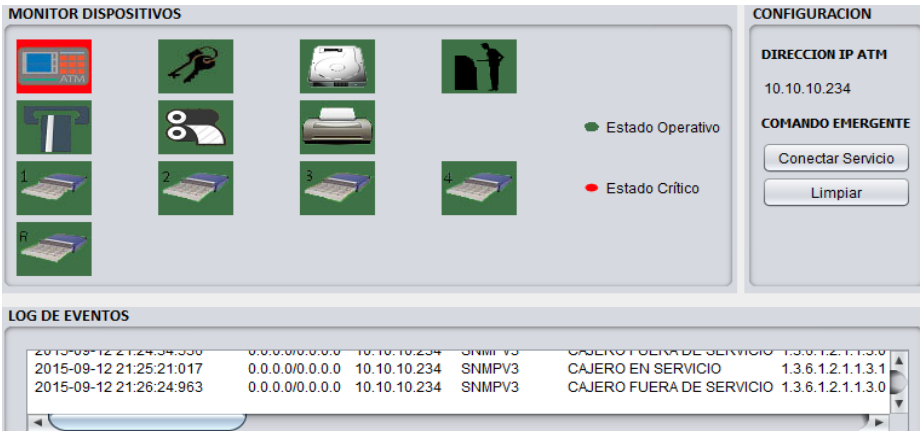


Figura 53. Visualización de la notificación Desconexión del cajero automático desde la Pantalla de Monitoreo

Figura 54. Visualización de la notificación Desconexión del cajero automático desde la Pantalla del Cajero Automático

2. Fallo del lector de tarjetas

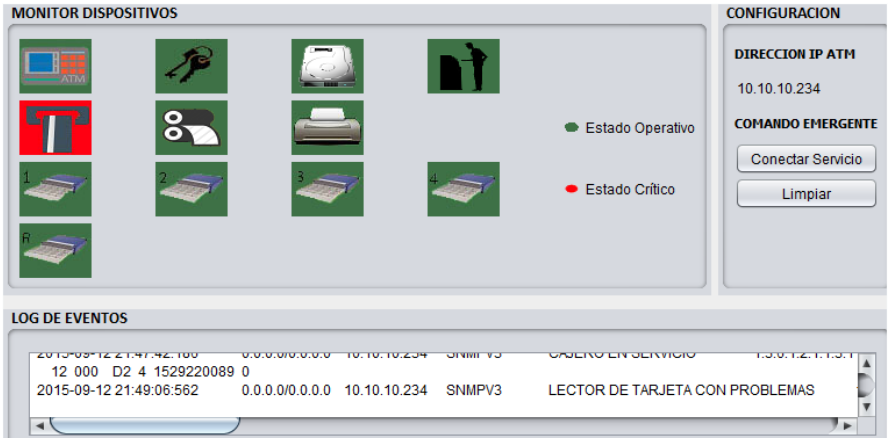


Figura 55. Visualización de la notificación Fallo del lector de tarjetas desde la Pantalla Monitoreo

Figura 56. Visualización de la notificación Fallo del lector de tarjetas desde la Pantalla del Cajero Automático

3. Fallo de la impresora y del rollo de papel

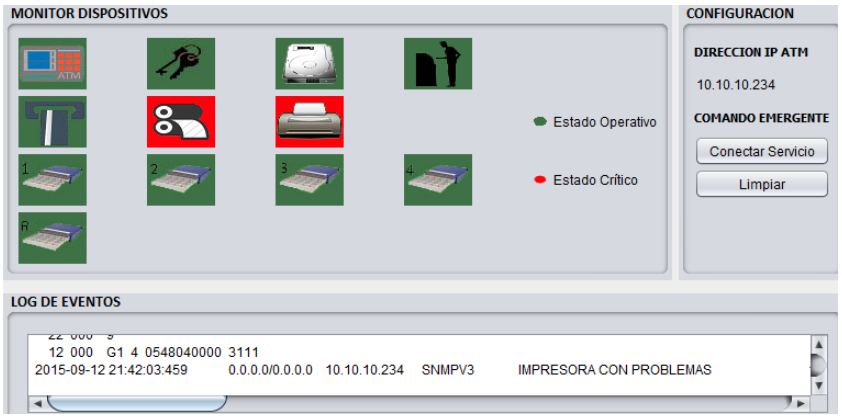


Figura 57. Visualización de la notificación Fallo de la impresora desde la Pantalla Monitoreo

Figura 58. Visualización de la notificación Fallo de la impresora desde la Pantalla Cajero Automático

4. Fallo de los cajetines

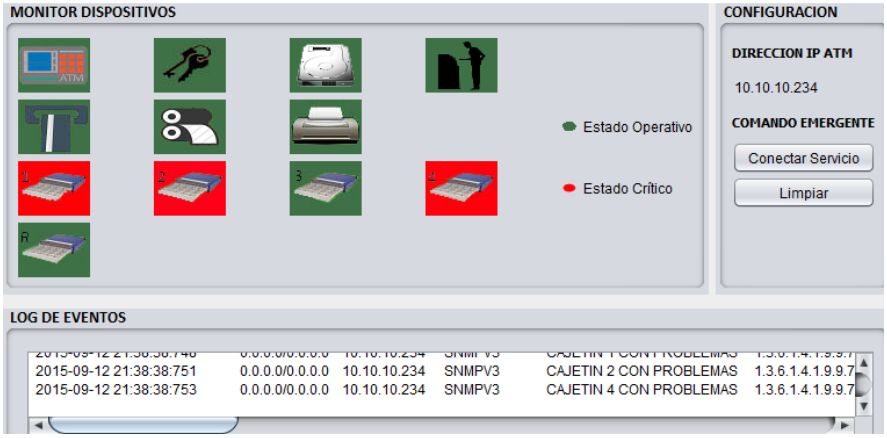


Figura 59. Visualización de la notificación Fallo de los cajetines desde la Pantalla Monitoreo

Figura 60. Visualización de la notificación Fallo de los cajetines desde la Pantalla Cajero Automático

"Estas operaciones fueron realizadas en un ambiente solo para pruebas y con la respectiva autorización otorgada por la empresa Red Transaccional Cooperativa S.A., (RTC)".

4.7 ANÁLISIS DE RESULTADOS

Según estas pruebas realizadas, se han cumplido los objetivos, debido a que la aplicación utiliza el protocolo SNMPv3 para el envío de mensajes al cajero automático, es de tipo web y la seguridad ha sido implementada en base al modelo USM y VACM.

En cuanto a los requisitos funcionales y no funcionales, todos éstos fueron cumplidos satisfactoriamente, ya que la aplicación dispone de un control de ingreso a la misma mediante el inicio de sesión, permite la configuración de parámetros en el servidor y en el cliente para el envío y control a los mensajes SNMPv3, permite ver la estructura en forma de árbol de una base MIB y permite conocer fallas en el cajero automático mediante la recepción de notificaciones automáticas.

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- El nivel de seguridad proporcionado por las versiones del protocolo SNMPv1 y SNMPv2 en comparación con el protocolo SNMPv3, no es el adecuado debido a que es muy bajo y sus funciones suelen ser muy limitadas. Además no brindan un buen soporte en la cuestión de autenticación y privacidad.

- SNMPv3 es el protocolo de gestión de red que brinda mayor soporte al manejo de seguridad, ya que incluye autenticación, privacidad, autorización y control de acceso en los datos que pasan por la red, evitando que los menajes sean expuestos y se generen pérdidas.

- La aplicación es de tipo web y puede instalase en varios sistemas operativos, gracias a esto el acceso puede realizarse a través de un navegador web. Además brinda un monitoreo en tiempo real a los cajeros automáticos y dispone de las seguridades necesarias para transmitir información sensible, dado que utiliza el protocolo SNMPv3, protegiendo a la información transmitida desde la aplicación hacia el cajero automático y viceversa contra varias amenazas que atentan a la integridad de los datos.

- El agente dispone de los mecanismos de seguridad y control necesarios. Como resultado de esto, el administrador general podrá crear y eliminar de manera remota, adecuada y rápida a usuarios USM, vistas MIB, derechos de acceso y grupos VACM.

- En base a las pruebas realizadas se verificó el cumplimiento de los requerimientos funcionales, ya que cada prueba realizada fue exitosamente alcanzada.

- Cada prueba realizada previamente fue hecha en un escenario ideal, con todas las precauciones de no cometer errores para que la aplicación funcione adecuadamente.

- El esquema actual de monitoreo de la Red Coonecta no brinda las seguridades necesarias para el monitoreo a los a los cajeros automáticos, es por esta razón que se propuso y se integró el protocolo SNMPv3, para monitorear a profundidad los servicios brindados hacia las cooperativas de ahorro y crédito; ofreciendo seguridad en el envío y en la recepción de mensajes.

5.2 RECOMENDACIONES

- El nivel de seguridad brindado por las versiones SNMPv1 y SNMPv2 no es el adecuado para la gestión de red, esto debido a que no ofrecen las seguridades necesarias para el manejo de la información a través de la red. Existen varios softwares que gracias a su desarrollo y tecnología, permiten analizar y capturar los datos que pasan en la red y debido a esto se puede obtener y robar información sensible. Por esta razón se recomienda utilizar solamente el protocolo SNMPv3, que brinda seguridad a los elementos mediante la autenticación y encriptación de paquetes que se transmiten a través de la red.

- Para mejorar la aplicación, se podría incluir a futuro nuevas funcionalidades relacionadas con la administración de la red, como el traceroute, escaneo de puertos abiertos para los dispositivos de la red y un análisis del tráfico de la red.

- Para poder monitorear los cajeros automáticos, es necesariamente que cada uno de estos tenga instalado un agente para el envío de mensajes y las notificaciones automáticas SNMPv3, tal manera que mediante la aplicación se pueda interactuar en tiempo real con el cajero automático.

- Implementar un plan de capacitación al personal involucrado del Departamentos de Sistemas sobre la configuración, uso de la aplicación y del agente.

- Antes de realizar cualquier operación, se debe tomar muy en cuenta todas las medidas de seguridad y conocer muy bien el uso de la herramienta, puesto a que su función es solamente para monitorear cajeros automáticos y es un factor muy importante para la empresa.

- Mejorar el módulo de monitoreo de la empresa para llevar estadísticas de cajeros automáticos monitoreados diariamente.

- Para optimizar el funcionamiento del programa, se aconseja utilizar siempre tecnología de última generación.

GLOSARIO DE TÉRMINOS

AT: Significa (Address Translation), en esta se guardan direcciones a nivel de enlace que corresponden a una dirección IP.

AES: Significa (Advanced Encryption Standard), es el algoritmo más seguro de cifrado de clave simétrica y el más utilizado hoy en día. Proporciona una clave de encriptación de 128-, 192-, o 256- bits. Cada tamaño de la clave de cifrado hace que el algoritmo se comporte ligeramente diferente. (BitZipper, s.f.)

ASCII: Significa (American Standard Code for Information Interchange**),** es un código numérico que representa los caracteres, usando una escala decimal del 0 al 127. Esos números decimales son convertidos por la computadora en números binarios para ser posteriormente procesados. (InformáticaHoy, s.f.)

ASN.1: Significa (Abstract Syntax Notation 1), describe de forma independiente y flexible cada objeto de la plataforma y permite la comunicación entre dos computadoras sin algún inconveniente. El protocolo SNMP usa el ASN.1 para representar sus objetos gestionables. (Protocolo ASN.1 Protocolo SNMP, s.f.)

BER: Significa (Basic Encoding Rules), estas son las reglas definidas originalmente en el estándar ASN.1 para codificar información, esto para que pueda ser interpretado en cualquier máquina de la misma manera.

DES: Significa (Data Encryption Standard), es un esquema de encriptación simétrico. Está basado en las teorías criptográficas existentes hasta el momento. (Herramientas Web, s.f.)

EGP: Significa (Exterior Gateway Protocol), es un protocolo usado para enviar y recibir información de enrutamiento entre sistemas autónomos.

HASH: Conocido como “resumen”, es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una

longitud fija que representa un resumen de toda la información que se le ha dado.

ICMP: Significa (Internet Control Message Protocol), es un protocolo que permite administrar información relacionada con errores de los equipos en red, es de características similares a UDP, pero con un formato mucho más simple, y su utilidad no está en el transporte de datos de usuario, sino en controlar si un paquete no puede alcanzar su destino. (CCM, s.f.)

IP: Significa (Internet Protocol), es un número único que no se puede repetir con el cual se identifica a una computadora conectada a una red que corre el protocolo IP.

ITU-T X.208: Es una especificación de ASN.1.

ISO 882: Es una especificación de ASN.1.

JAVA EE: Significa (Java Enterprise Edition), facilitan el desarrollo y despliegue de aplicaciones empresariales multi-capa, brindando técnicas que proporcionan soluciones completas, seguras y estables para el desarrollo. (Jatun, 2012)

JSP: Significa (JavaServer Pages), es una tecnología que crea páginas web dinámicas basadas en HTML, XML, entre otros tipos de documentos.

JSF: Significa (JavaServer Faces), es una tecnología para aplicaciones Java, basadas en web para el desarrollo de interfaces en aplicaciones Java EE.

SERVLET: Es una clase en el lenguaje de programación Java utilizada para ampliar las capacidades de un servidor. Son utilizados comúnmente para extender aplicaciones alojadas por servidores web, de tal manera que puedan

ser vistos como applets de Java que se ejecutan en servidores en vez de navegadores web.

JVM: Significa (Java Virtual Machine), es una máquina virtual ejecutable en una plataforma específica, capaz de interpretar y ejecutar instrucciones expresadas en un código binario especial, el cual es generado por el compilador del lenguaje Java.

MD5: Significa (Message-Digest Algorithm 5), es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

MIB: Significa (Management Information Base), describe la totalidad de los objetos SNMP que se encuentran en la red.

MIB II: Significa (Management Information Base II), es la base de datos común para la gestión de equipos en internet.

NMS: Significa (Network Management System), ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados.

PDU: Significa (Protocol Data Unit), se utiliza para el intercambio de datos entre unidades disparejas, dentro de una capa del modelo OSI.

RFC 1213: Define la de base de información para la gestión de redes de TCP/IP basado en internet, corresponde a la MIB-II.

RFC 1155: El subconjunto de ASN.1 utilizado en SNMP está definida en RFC 1155 y se la conoce como SMI.

SHA: Significa (Secure Hash Algorithm), es un sistema de funciones hash criptográficas.

SMI: Significa (Structure of Managment Information), identifica y especifica los tipos de datos que se pueden utilizar en la MIB.

SNMP: Significa (Simple Network Management Protocol), es un protocolo de la capa de aplicación que proporciona el intercambio de información entre dispositivos de red.

TCP: Significa (Transmission Control Protocol), es un protocolo que se ocupa en verificar la correcta entrega de paquetes y que en los datos no hayan errores. (jojooa, s.f.)

UDP: Significa (User Datagram Protocol), es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP. Este protocolo es muy sencillo, debido a que no brinda detección de errores.

USM: Significa (User-Based Security Model), pertenece a la arquitectura de SNMPv3 para la seguridad de los mensajes.

VACM: Significa (View-Based Access Control), pertenece a la arquitectura de SNMPv3 para el control de acceso.

REFERENCIAS

3Cu Electrónica. (s.f.). SNMP. Recuperado el 01 de Mayo de 2015 de https://sites.google.com/site/3cuelectronica/home/ethernet/snmp

BitZipper. (s.f.). Encriptación AES. Recuperado el 21 de Febrero de 2015 de http://www.bitzipper.com/es/aes-encryption.html

CCM. (s.f.). El protocolo ICMP. Recuperado el 23 de Julio de 2015 de http://es.ccm.net/contents/265-el-protocolo-icmp

Desarrolloweb. (s.f.). Qué es MVC. Recuperado el 03 de Enero de 2015 de http://www.desarrolloweb.com/articulos/que-es-mvc.html

García, S. (2015). Examinar el Modelo OSI. Recuperado el 01 de Enero de 2015 de https://sites.google.com/site/ivangarciasanchez90/objetivos/desarrollo-tema-1/6º

Herramientas Web. (s.f.). DES. Recuperado el 12 de Mayo de 2015 de http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html

InformáticaHoy. (s.f.). ¿Qué es el código ASCll?. Recuperado el 25 de Enero de 2015 de http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-el-codigo-ASCII.php

Jatun. (2012). Java Enterprise Edition. Recuperado el 23 de Abril de 2015 de http://www.jatun.com/web/company/training/javaee5

Java. (s.f.). ¿Qué es la tecnología Java y para qué la necesito?. Recuperado el 21 de Junio de 2015 de https://www.java.com/es/download/faq/whatis_java.xml

jojooa. (s.f.). Definicion de TCP - ¿qué es TCP?. Recuperado el 03 de Enero de 2015 de https://sites.google.com/site/jojooa/informatica-tecnologia/definicion-de-tcp-que-es-tcp

joomla. (s.f.). ¿Que son los EJB?. Recuperado el 25 de Diciembre de 2014 de http://javagratis.net63.net/programacion-java/ejb/61-ique-son-los-ejb.html

Libros Web. (s.f.). La arquitectura MVC. Recuperado el 12 de Noviembre de 2015 de http://librosweb.es/libro/jobeet_1_4/capitulo_4/la_arquitectura_mvc.html

Millán, R. (2015). SNMPv3. Recuperado el 13 de Julio de 2015 de http://www.ramonmillan.com/tutoriales/snmpv3.php

Network Management. (s.f.). SNMP Tutorial Part 2: Rounding Out the Basics. Recuperado el 14 de Febrero de 2015 de http://www.networkmanagementsoftware.com/snmp-tutorial-part-2-rounding-out-the-basics

Protocolo ASN.1 Protocolo SNMP. (s.f.). Protocolo ASN1 y Protocolo SNMP. Recuperado el 12 de Octubre de 2014 de http://everpec.blogspot.com/

Red Transaccional Cooperativa S.A., (s.f.). Coonecta. Recuperado el 12 de Enero de 2015 de http://www.coonecta.com.ec/

Redes y Comunicaciones. (s.f.). MODELO TCP/IP. Recuperado el 12 de Marzo de 2015 de http://confiredeco.blogspot.com/2013/04/modelo-tcpip.html

Saydam, T., & Magedanz, T. (1996). Networks and Network Management into Service and Service Management (4 ed.). Journal of Networks and Systems Management.

SNMP. (2004). PROTOCOLO SNMP. Recuperado el 23 de Julio de 2015 de http://publicaciones.urbe.edu/index.php/telematique/article/viewArticle/782/1886

ANEXOS

ANEXO 1

DESCRIPCIÓN GENERAL
DE LA EMPRESA RED TRANSACCIONAL COOPERATIVA S.A., (RTC)

Reseña Histórica

La Red Transaccional Cooperativa S.A., (RTC), nace por la iniciativa de WOCCU (World Council of Credit Unions, Inc) y por la decisión de las cooperativas de ahorro y crédito del Ecuador, para integrarse mediante servicios transaccionales y con esto facilitar las transacciones entre cooperativas de ahorro y crédito del país.

La Red Coonecta inicialmente se formó con 9 cooperativas de ahorro y crédito, actualmente mantiene una participación que forman parte de la Red con más de 90 instituciones financieras (Cooperativas, Bancos y Mutualistas), a través de las cuales la Red Coonecta tiene una cobertura nacional con presencia en las 24 provincias del país con más de 400 puntos de servicio y alrededor de 3,5 millones de clientes de las diferentes entidades que conforman la Red, brindando servicios transaccionales en funcionamiento a nivel nacional.

La experiencia de la Red Coonecta constituye un referente en la región y posiblemente a nivel mundial sobre un caso éxito de generación de Redes en beneficio de sus entidades miembros y sobre todo fomentando la inclusión financiera mediante la oferta de productos y servicios innovadores y acordes a las particularidades del segmento población con el cual trabajan las entidades miembros de la Red. (Coonecta, s.f.)

Planeación Estratégica

MISIÓN

Contribuir a la integración operativa y el crecimiento del sistema cooperativo de ahorro y crédito mediante la prestación de servicios transaccionales y la ejecución de procesos de consultoría bajo una estrategia de innovación, calidad, competitividad y sostenibilidad de los servicios.

VISIÓN

Ser la red de negocios transaccionales del sector cooperativo y de microfinanzas con una cobertura al 100% de cantones del Ecuador, integrada internacionalmente y referente de éxito en las redes a nivel mundial.

VALORES

COOPERACIÓN/INTEGRACIÓN

Manteniendo una actitud de cooperación con las otras personas que integran el equipo de trabajo, compartiendo responsabilidades. A nivel de las instituciones, disponiendo de apertura a generar alianzas que permitan implementar procesos que impliquen economías de escala entre los integrantes de RTC.

INNOVACIÓN

Ser pioneros y ejercer un liderazgo a través de ideas novedosas y creativas, con el fin de producir cambios en la institución, las instituciones integradas a la Red Coonecta y los sistemas sociales.

COMPROMISO

Estar orgulloso de pertenecer y trabajar como parte integrante de la institución.

COMPETITIVIDAD

Tener un permanente afán de superarse y de dar lo mejor de uno mismo en las responsabilidades asignadas. A nivel institucional mantener una actitud constante de mejoramiento y de brindar los mejores servicios a las instituciones. (Coonecta, s.f.)

Estructura Orgánica

Del organigrama presentado, se observa una organización de tipo vertical, donde la delegación de autoridad va de arriba hacia abajo.

ANEXO 2

SERVICIOS
DE LA EMPRESA RED TRANSACCIONAL COOPERATIVA S.A., (RTC)

La Red Transaccional Cooperativa S.A., (RTC), está enfocada en el mercado del sistema financiero y cooperativo del Ecuador, teniendo como base a más de 90 instituciones financieras (Cooperativas, Bancos y Mutualistas) a las cuales se les oferta los siguientes servicios y productos: (Coonecta, s.f.)

Monitoreo a los Cajeros Automáticos 24/7

Consiste en el monitoreo a la operación, desempeño de servicios y cajeros automáticos que permiten realizar diferentes tipos de transacciones de manera rápida y sencilla través de uso de una tarjeta de débito o crédito.

Agencias Compartidas

Es el producto que integra a las cooperativas de la red, permitiendo a sus socios realizar varias transacciones.

Remesas

Las remesas enviadas por los migrantes son canalizadas por la Red Transaccional Cooperativa S.A., (RTC), a través de 9 empresas remesadoras.

Bono de Desarrollo Humano (BDH)

Es un beneficio estatal mensual de USD $35.00 que está condicionado al cumplimiento de requisitos establecidos por el programa de Protección Social.

Tarjetas de Débito

Es una tarjeta plástica con una banda magnética o integrada con chip, usada para extraer dinero de un cajero automático.

Ventanilla Móvil

Es un sistema que mediante el uso de un celular y una mini impresora se puede efectuar recaudación de créditos y ahorros de manera remota en tiempo real, visitando a los socios en su trabajo o domicilio. La Red Coonecta proporciona las licencias de uso del software para este producto.

Recaudación Rise

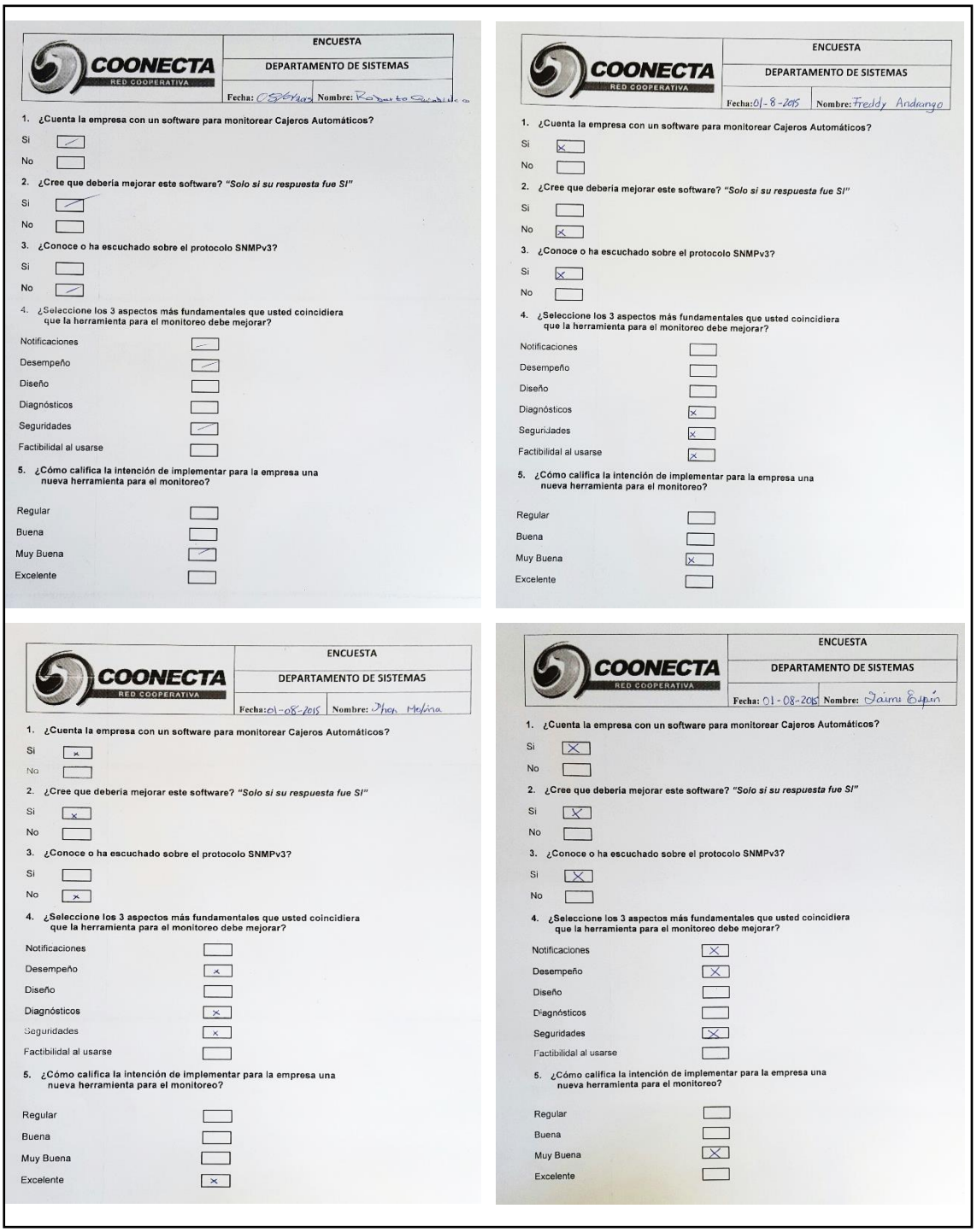
Es la recaudación de impuestos a través de las cooperativas. El Rise por medio del pago de cuotas mensuales, reemplaza el pago del IVA y del impuesto de la renta y tiene por objeto mejorar la cultura tributaria en el país.

Pago de Matriculación Vehicular

Es la implementación de un sistema que permite realizar la recaudación de la matriculación vehicular en las agencias de las cooperativas afiliadas a la Red Coonecta.

ANEXO 3

ENCUESTA REALIZADA AL PERSONAL
DE LA EMPRESA RED TRANSACCIONAL COOPERATIVA S.A., (RTC)



COONECTA
RED COOPERATIVA

ENCUESTA
DEPARTAMENTO DE SISTEMAS

Fecha: 05/08/2015 Nombre: Roberto Saavedra

1. ¿Cuenta la empresa con un software para monitorear Cajeros Automáticos?
   Si [/]
   No [ ]
2. ¿Cree que debería mejorar este software? *"Solo si su respuesta fue SI"*
   Si [/]
   No [ ]
3. ¿Conoce o ha escuchado sobre el protocolo SNMPv3?
   Si [ ]
   No [/]
4. ¿Seleccione los 3 aspectos más fundamentales que usted coincidiera que la herramienta para el monitoreo debe mejorar?
   Notificaciones [ ]
   Desempeño [/]
   Diseño [ ]
   Diagnósticos [ ]
   Seguridades [/]
   Factibilidal al usarse [ ]
5. ¿Cómo califica la intención de implementar para la empresa una nueva herramienta para el monitoreo?
   Regular [ ]
   Buena [ ]
   Muy Buena [/]
   Excelente [ ]

COONECTA
RED COOPERATIVA

ENCUESTA
DEPARTAMENTO DE SISTEMAS

Fecha: 01-8-2015 Nombre: Freddy Andango

1. ¿Cuenta la empresa con un software para monitorear Cajeros Automáticos?
   Si [X]
   No [ ]
2. ¿Cree que debería mejorar este software? *"Solo si su respuesta fue SI"*
   Si [ ]
   No [X]
3. ¿Conoce o ha escuchado sobre el protocolo SNMPv3?
   Si [X]
   No [ ]
4. ¿Seleccione los 3 aspectos más fundamentales que usted coincidiera que la herramienta para el monitoreo debe mejorar?
   Notificaciones [ ]
   Desempeño [ ]
   Diseño [ ]
   Diagnósticos [X]
   Seguridades [X]
   Factibilidal al usarse [X]
5. ¿Cómo califica la intención de implementar para la empresa una nueva herramienta para el monitoreo?
   Regular [ ]
   Buena [ ]
   Muy Buena [X]
   Excelente [ ]

COONECTA
RED COOPERATIVA

ENCUESTA
DEPARTAMENTO DE SISTEMAS

Fecha: 01-08-2015 Nombre: Jhon Medina

1. ¿Cuenta la empresa con un software para monitorear Cajeros Automáticos?
   Si [X]
   No [ ]
2. ¿Cree que debería mejorar este software? *"Solo si su respuesta fue SI"*
   Si [X]
   No [ ]
3. ¿Conoce o ha escuchado sobre el protocolo SNMPv3?
   Si [ ]
   No [X]
4. ¿Seleccione los 3 aspectos más fundamentales que usted coincidiera que la herramienta para el monitoreo debe mejorar?
   Notificaciones [ ]
   Desempeño [X]
   Diseño [ ]
   Diagnósticos [X]
   Seguridades [X]
   Factibilidal al usarse [ ]
5. ¿Cómo califica la intención de implementar para la empresa una nueva herramienta para el monitoreo?
   Regular [ ]
   Buena [ ]
   Muy Buena [ ]
   Excelente [X]

COONECTA
RED COOPERATIVA

ENCUESTA
DEPARTAMENTO DE SISTEMAS

Fecha: 01-08-2015 Nombre: Jaime Espín

1. ¿Cuenta la empresa con un software para monitorear Cajeros Automáticos?
   Si [X]
   No [ ]
2. ¿Cree que debería mejorar este software? *"Solo si su respuesta fue SI"*
   Si [X]
   No [ ]
3. ¿Conoce o ha escuchado sobre el protocolo SNMPv3?
   Si [X]
   No [ ]
4. ¿Seleccione los 3 aspectos más fundamentales que usted coincidiera que la herramienta para el monitoreo debe mejorar?
   Notificaciones [X]
   Desempeño [X]
   Diseño [ ]
   Diagnósticos [ ]
   Seguridades [X]
   Factibilidal al usarse [ ]
5. ¿Cómo califica la intención de implementar para la empresa una nueva herramienta para el monitoreo?
   Regular [ ]
   Buena [ ]
   Muy Buena [X]
   Excelente [ ]

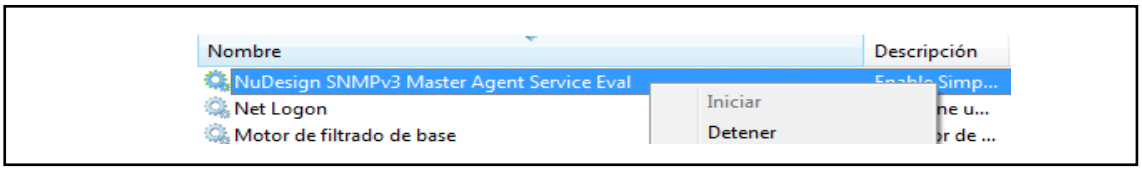
ANEXO 4

MANUAL DE USUARIO PARA EL USO DE LA APLICACIÓN

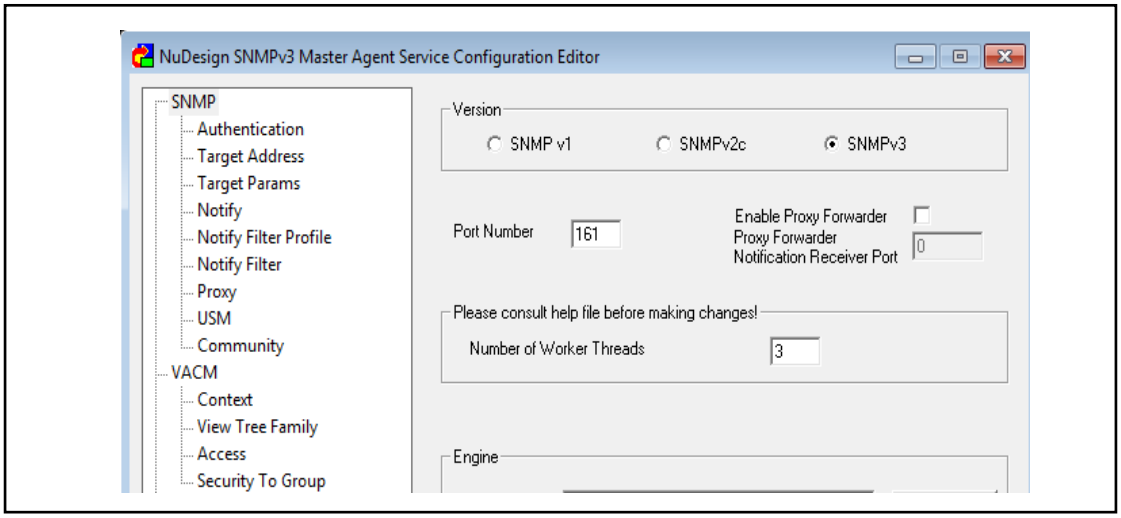
El siguiente manual de usuario ha sido desarrollado en base a las pruebas realizadas localmente entre Servidor – Cliente y viceversa. En este participará el Servidor (Aplicación para el envío de comandos SNMPv3) y Cliente (Agente en el Cajero Automático para la configuración de mensajes y notificaciones automáticas SNMPv3).

1. **Descargar e instalar el agente *"NuDesign SNMPv3 Master Agent"* en el cajero automático**

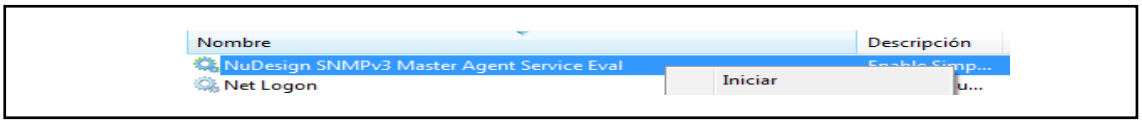
2. **Parar el servicio del agente *"NuDesign SNMPv3 Master Agent"***



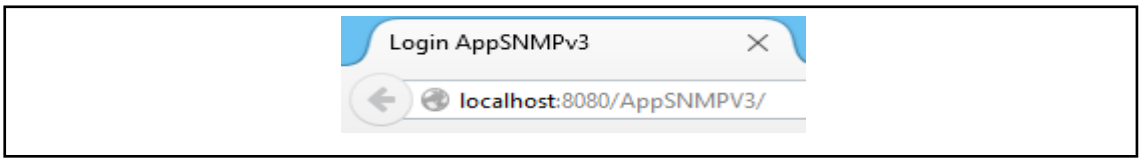
3. **Abrir la aplicación *"NuDesign SNMPv3 Master Agent"* y realizar las configuraciones necesarias para el envío de mensajes SNMPv3**



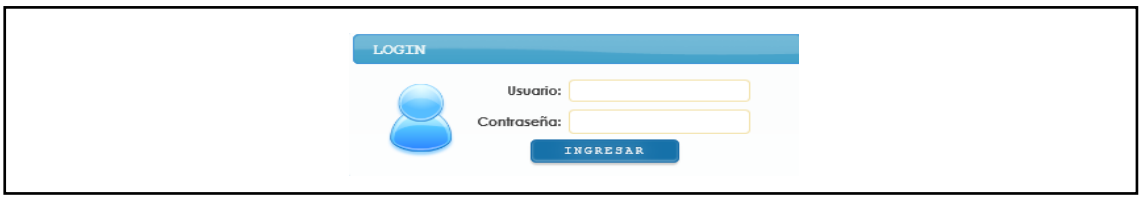
4. Iniciar el servicio del agente *“NuDesign SNMPv3 Master Agent”*



5. Correr la aplicación Web

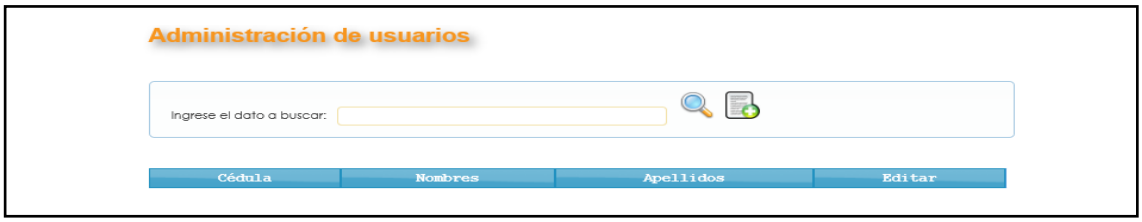


6. Autenticarse para ingresar al sistema



7. Ingresar a la administración de cuentas de usuarios

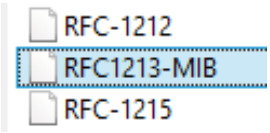
8. Crear o Modificar cuentas de usuarios



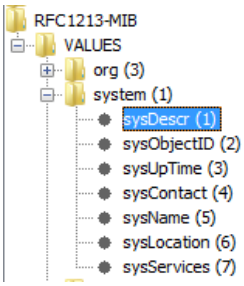
9. Ingresar a la Ejecución de comandos SNMPv3

10. Cargar o Descargar archivos MIBs

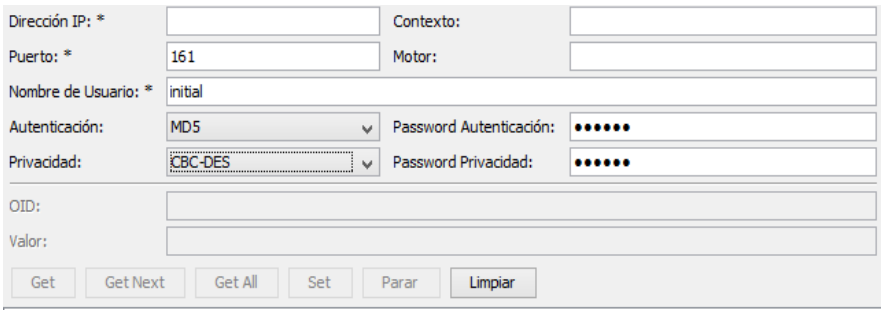
11. Seleccionar la Base MIB a cargar o descargar



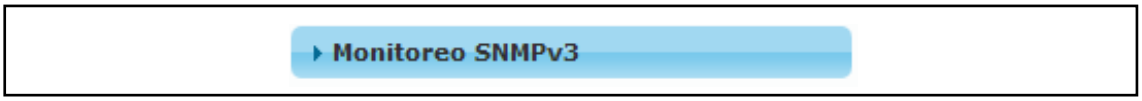
12. Seleccionar un valor a gestionar en la MIB



13. Configurar parámetros para el envío de mensajes SNMPv3



14. **Ingresar a la administración de cajeros automáticos**

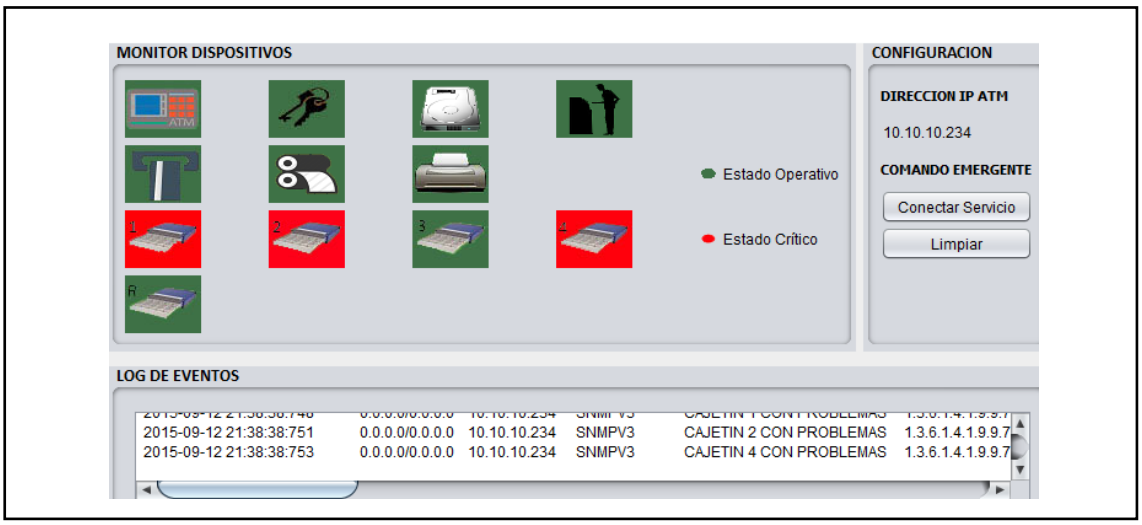


15. **Crear o Modificar lista de cajeros automáticos**

16. **Ingresar al monitoreo de notificaciones automáticas del cajero automático**

Nombre	Dirección IP	Estado	Editar	
atm	0.0.0.0	DESCONECTADO	Edición	Monitorear
coonecta	192.168.7.7	DESCONECTADO	Edición	Monitorear
atm test	127.0.0.1	DESCONECTADO	Edición	Monitorear
atm coonecta	10.10.10.234	OPERATIVO	Edición	Monitorear

17. **Verificar las notificaciones automáticas emitidas por el cajero automático desde la aplicación de monitoreo**



18. Verificar los mensajes emitidos desde el cajero automático

ANEXO 5

ELEMENTOS UTILIZADOS PARA EL DESARROLLO DE LA APLICACIÓN

CAJERO AUTOMÁTICO

Características Principales

Modelo: DIEBOLD

Sistema Operativo: Windows 7

Memoria RAM: 4 GB

Disco Duro: 300 GB

Procesador: Intel Core 2 Duo 32-bit

LAPTOP

Características Principales

Modelo: DELL Inspiron 5520

Sistema Operativo: Windows 8.1

Memoria RAM: 16 GB

Disco Duro: 1 TB

Procesador: Intel Core i7 64-bit