Universidad Siglo 21

Trabajo Final de Graduación

Licenciatura en Informática

Proyecto de Aplicación Profesional (PAP)

Sistema de monitorización de activos de red basado en información de SNMP

ARCURI, Edgardo Antonio

VINF0490

Abril 2017

Tabla de Contenido

Resumen

Actualmente las redes cumplen un rol fundamental en el desenvolvimiento de las tareas cotidianas de cualquier organización. Cada vez son más los servicios corporativos que brindan las organizaciones basados en redes IP, lo que provoca un crecimiento tanto en cantidad como en variedad de dispositivos conectados. Las actividades se tornan funcionalmente dependientes del correcto funcionamiento de la red. Las interrupciones no programadas impactan negativamente la prestación y la calidad de los servicios que se brindan y por ende, afectan el desarrollo normal de las actividades de la organización.

Surge así la necesidad de contar con herramientas que ayuden a los administradores de red a supervisar su funcionamiento y a detectar, de forma temprana, los incidentes que interrumpen la conectividad. Tomar conocimiento en el momento que un incidente se ha producido, favorece la reducción del tiempo total transcurrido hasta la resolución del problema.

Un protocolo de red útil para la supervisión de redes es el SNMP (Protocolo Simple de Administración de Redes) que permite conformar un sistema de gestión compuesto por un gestor, agentes y bases de datos, integrando dispositivos de distintos fabricantes.

En este proyecto se describe el desarrollo de una aplicación web que realiza la función de gestor y utiliza la información generada y transmitida por los agentes SNMP de los dispositivos de red para monitorear el funcionamiento de una red, detectar fallas en la conectividad y determinar el alcance del problema.

Abstract

Currently the networks have a key role in the development of the daily tasks of any organization. Increasingly corporate services provided by organizations based on their IP networks, resulting in growth in both quantity and variety of connected devices. The activities become functionally dependent on the proper functioning of the network. Unscheduled interruptions negatively impact the delivery and quality of the services provided and thus affect the normal development of the organization's activities.

This raises the need for tools to help network administrators to monitor performance and detect early incidents that disrupt connectivity. Take knowledge at the time that an incident has occurred, it favors reducing the total time to resolution of the problem.

A useful network protocol for network monitoring is Simple Network Management Protocol (SNMP) that helps build a management system consisting of a manager, agents and databases, integrating devices from different manufacturers.

In this project the development of a web application that performs the function of manager is described. It use the information generated and transmitted by SNMP agents network devices to monitor the operation of a network , detecting failures in connectivity and determine the extent of the problem.

Sistema de monitorización de activos de red basado en información de SNMP

1. Introducción

1.1 Introducción – Marco de referencia institucional

El siguiente proyecto de aplicación profesional se desarrolla en la Estación Experimental Agropecuaria (EEA) Balcarce dependiente del Instituto Nacional de Tecnología Agropecuaria (INTA), organismo dedicado a la experimentación, investigación y transferencia de tecnología agropecuaria. Su campus está ubicado en el km 73,5 de la ruta nacional 226, en la localidad de Balcarce y posee una Red de gran dimensión, con varios edificios interconectados y numerosos servicios y activos de red. La EEA depende del Centro Regional Buenos Aires Sur (CERBAS) y de la EEA dependen 10 unidades denominadas Agencias de Extensión, de menor dimensión, ubicadas en localidades cercanas a Balcarce. Las redes de estas 12 unidades son administradas por el Grupo de Infraestructura y Servicios de Red del Departamento de Documentación e Informática de la EEA Balcarce, conformado por un administrador de red, un técnico en redes y dos profesionales de sistemas que colaboran trabajando a tiempo parcial con tareas de la red.

La mayoría de las aplicaciones administrativas y contables de la institución funcionan de forma on-line. Las tareas de investigación requieren de acceso a bibliografía e información de la web, las herramientas de comunicación para realizar extensión agropecuaria, utilizan la red y sus servicios y la realización de reuniones virtuales requieren de garantía de conectividad y ancho de banda. Las actividades son cada vez más dependientes del correcto funcionamiento de la red.

Además de los servidores, el equipamiento informático del personal, impresoras de red, equipos de laboratorios y celulares corporativos que se conectan, en los últimos años se han agregado varios servicios como alarmas, controles de acceso, reconocimiento de datos biométricos, cámaras IP y videoconferencias. Como consecuencia de ello, ha crecido en gran número y variedad, los dispositivos conectados a la red, provocando que su administración se vuelva cada vez más compleja y evidenciando la necesidad de contar con herramientas que ayuden a sus administradores a supervisar su funcionamiento. El grupo de Redes no cuenta

con un sistema de monitorización de los activos de red aunque cree que actualmente es necesario.

Las interrupciones no programadas en el funcionamiento de la red impactan negativamente la prestación y la calidad de los servicios que se brindan. Estas pueden deberse a fallas de tipo físico o lógico entre las que podemos mencionar: a) en activos: fallas en el suministro de energía, en los sistemas de provisión de energía ininterrumpida (UPS), componentes quemados o en mal funcionamiento, saturación, falta de actualización del sistema operativo, errores o pérdida total de configuración; b) en medios de transmisión: fallas en la conectividad de cables, fibras ópticas o señal inalámbrica, en la velocidad de transmisión, equipos inalámbricos mal orientados, señal wifi obstaculizada y c) de conexiones: dispositivos conectados en puertos destinados a otro tipos de dispositivos y la conexión no autorizada de equipamiento de red, entre otros.

En las redes abarcadas por el proyecto, este tipo de fallas ocurren frecuentemente, no son detectadas a tiempo y afectan sobremanera el desarrollo normal de las actividades de la organización. ¿Es posible detectar de forma automática y en el momento de su ocurrencia, las fallas que suceden en la red, determinar el alcance de afectación y alertar al personal responsable de solucionarlas?

A continuación se abordará la justificación del problema y se enuncia el objetivo general y los objetivos específicos. Se presenta el marco teórico en busca de una respuesta a la problemática planteada desde la teoría. Luego se expone la metodología con los instrumentos utilizados para recabar, analizar y evaluar la información. Continúa con el diagnóstico donde se presentan los resultados obtenidos luego de haber aplicado los instrumentos mencionados en la metodología y luego se desarrolla la propuesta de solución a la problemática en cuestión. Por último se describe el desarrollo del Proyecto.

1.2 Justificación

Actualmente, los primeros que detectan un incidente o problema en la red, son los usuarios. Recién cuando ellos lo comunican, el grupo de redes comienza manualmente a realizar pruebas con comandos básicos para encontrar el problema verificando interfaces o activos caídos y el funcionamiento de la red en general. Es de gran interés de este grupo cambiar la forma en que se realizan las actividades que conforman la supervisión del

funcionamiento de los activos de la red. Contar con una herramienta de monitorización sería de gran ayuda en las actividades diarias que desarrolla este grupo para prevenir o detectar de forma temprana incidentes en el funcionamiento de la red, con la posibilidad de realizar un diagnóstico rápido y propiciar una solución más eficiente, lo que incrementaría el nivel de prestación de servicios de la red, en beneficio de los usuarios de toda la organización. Stallings (2004) considera que no es posible gestionar sólo con el esfuerzo humano una red fiable y extensa y que, debido a su complejidad, es necesario contar con herramientas automáticas de gestión de la red.

La mayoría de los elementos activos de la red dispone del protocolo SNMP de gestión de redes y se dispone de buena infraestructura de red y capacidad de procesamiento y almacenamiento sobrante en los servidores, lo que a priori, hace factible el proyecto.

2. Objetivo general y objetivos específicos

2.1 Objetivo general del proyecto

Implementar un sistema web que permita la monitorización de activos de red y sirva de herramienta a los administradores de red para la detección de fallas en su funcionamiento y la determinación del alcance de afectación.

2.2 Objetivos específicos del proyecto

- Entender sobre los componentes activos de una red, su conectividad, protocolos que ejecutan y tipos de fallas que presentan.
- Identificar las necesidades y requerimientos de los administradores y técnicos de redes con respecto a la monitorización del funcionamiento de la red y sus activos
- Determinar la infraestructura de la red de la organización. Identificar los elementos activos de red, la dependencia funcional de los mismos y los protocolos que implementan.
- Determinar la forma y la factibilidad de obtener el estado de funcionamiento de los activos y las fallas que producen.

- Elaborar un proyecto que contenga una propuesta de solución que permita, de forma on-line, la visualización del estado de funcionamiento y de la ocurrencia de un incidente en la red.
- Desarrollar un software web que controle de forma frecuente el estado de funcionamiento de los activos, lo muestre de forma gráfica y alerte sobre fallas en el momento de su ocurrencia.
- Poner en servicio el sistema web de monitoreo.

2.3 Objetivo general del sistema

Monitorizar el funcionamiento de los elementos activos de una red, detectar y registrar fallas, generar alertas, declarar incidentes en el sistema de gestión de incidentes de la organización y mostrar de forma gráfica el estado de la red, el lugar de ocurrencia y la zona afectada.

2.4 Límite

La actividad que da comienzo al sistema es cuando un elemento activo de red es conectado y puesto en funcionamiento en la red y la que da fin, es cuando se lo desconecta de forma definitiva de la red.

2.5 Alcance

Proceso de detección de fallas en el funcionamiento de la red y determinación del alcance del incidente.

Proceso de declaración de un nuevo incidente ante el Sistema de Gestión de Incidentes de la organización.

2.6 No Contempla

Proceso de resolución del incidente y su registración.

Proceso de administración y gestión del incidente.

Proceso de detección y registración de la causa del incidente.

3. Marco Teórico

3.1 Protocolos de Control en Internet

Existen varios protocolos de control que se utilizan en la capa de red, ICMP (Protocolo de Mensajes de Control en Internet, del inglés *Internet Control Message Protocol*) y DHCP (Protocolo de Configuración Dinámica de Host, del inglés *Dynamic Host Control Protocol*), entre otros. ICMP emite un mensaje al emisor si algo inesperado ocurre durante el procesamiento de un paquete en un enrutador. Dos de esos mensajes son el ECHO (eco) y el ECHO REPLY (respuesta de eco) que son utilizados por el comando ping para ver si un host o interfaz responde. DHCP recibe la MAC de una Pc en un paquete DHCP Discover y asigna una dirección IP a la Pc enviando un paquete DHCP OFFER (Tanenbaum y Wetherall, 2012).

Debido a que el protocolo de control ICMP es sumamente útil para verificar la conectividad, lo utilizaremos en este proyecto para verificar el estado de conectividad de los dispositivos de red.

3.2 Redes Virtuales de Área Local

Las Redes Virtuales de Área Local (VLAN, del inglés *Virtual Local Area Network*) permiten dividir una gran Red de Área Local (LAN, del inglés *Local Area Network*) física en LAN lógicas más pequeñas. Los administradores de red las utilizan por varias razones: para reflejar la estructura de la organización en vez del diseño físico de edificios; para separar la carga ya que las distintas redes puede tener diferencias de carga muy importantes; para segmentar las redes y disminuir el tráfico de difusión que se produce tanto cuando no se conoce la ubicación de un dispositivo destino como cuando una interfaz de red se avería o desconfigura y también por seguridad para no permitir que dispositivos de una red puedan acceder a los dispositivos de las otras redes. Hay distintas formas de definir VLANs, una de ellas es la de VLANs por puerto, donde se le indica al switch a cuáles VLANs se puede acceder a través de qué puertos (Tanenbaum y Wetherall, 2012).

En una red con VLANs configuradas por puerto, como el caso de la red de nuestro proyecto, si a un dispositivo que pertenece a una VLAN se lo conecta a un puerto al cual no se le han configurado los permisos para que esa VLAN pueda acceder a través de él, presentará una falla en la conectividad.

3.3 El estándar IEEE 802.1Q

El estándar IEEE 802.1Q emitido en 1998 agrega en el encabezado de la trama Ethernet una etiqueta que contiene la VLAN. Los dispositivos agregan la etiqueta VLAN en la trama para que los puertos troncales de los dispositivos que la reciben sepan a qué VLAN pertenece esa trama (Tanenbaum y Wetherall, 2012).

En la red de nuestro proyecto, los enlaces troncales de los switchs de los edificios utilizan el estándar 802.1Q para transportar las vlans hasta el switch de capa 3 de la sala de servidores, encargado de direccionar el tráfico entre las redes virtuales o hacia Internet. A través de este protocolo, el switch conoce a qué VLAN pertenece la trama recibida.

3.4 Tecnología MPLS

La tecnología MPLS (Conmutación Multiprotocolo mediante Etiquetas, del inglés, *MultiProtocol Layer Switching*) es utilizada principalmente por los Proveedores de Servicios de Internet (ISP, del inglés *Internet Services Provider*). El último enrutador antes de ingresar a la MPLS agrega al paquete una etiqueta delante del encabezado de IP. El reenvío está basado en esa etiqueta y no en la dirección de destino (Tanenbaum y Wetherall, 2012).

Las redes de cada una de las unidades abarcadas por este proyecto se interconectan a través de una red que utiliza tecnología MPLS. Los activos que se encuentran en la red de la aplicación son accesibles a través de la misma red, mientras que los activos que se encuentran en otras unidades, son accesibles a través de la MPLS.

3.5 Protocolo de Datagrama de Usuario

El Protocolo de Datagrama de Usuario (UDP, del inglés *User Datagram Protocol*) es un protocolo de la capa de transporte no orientado a la conexión, permitiendo que las aplicaciones envíen sus datagramas sin establecer una conexión. Utiliza dos puertos, el origen, abierto por la aplicación que envía el paquete y el destino, que sirve para entregar los datos a la aplicación que está escuchando en ese puerto. Cuando se produce una respuesta, se invierten los puertos (Tanenbaum y Wetherall, 2012).

En el proyecto utilizaremos el protocolo SNMP para conocer el estado de funcionamiento de los dispositivos de la red. Éste utiliza el protocolo UDP con los puertos destino 161 y 162.

3.6 T.I.C. (Tecnología de la Información y Comunicación)

3.6.1 Protocolo Simple de Administración de Red

Internet Engineering Task Force (IETF) es una gran comunidad internacional abierta de diseñadores de red, operadores, proveedores e investigadores interesados en la evolución de la arquitectura y el buen funcionamiento de Internet (Internet Engineering Task Force [IETF], 2015). La IETF es quien regula y publica las *Request for Comments* (RFC) que son propuestas con el propósito de lograr definir estándares. En la RFC 1157, la IETF define la primera versión del *Simple Network Management Protocol* (SNMP), denominada SNMPv1. Con el propósito de mejorar la funcionalidad, IETF define a través de las RFCs 3416–3418, la segunda versión, SNMPv2. La última, es la SNMPv3, que agrega mejoras en la seguridad. En 2002 queda definido el estándar en las RFCs 3410-3418 y 2756 (Mauro y Schmidt, 2005).

SNMP es un protocolo para la gestión de dispositivos de redes IP que permite tanto la obtención de datos y de estados como la configuración de parámetros de los dispositivos activos de una red, suministrando al administrador de red, de información online para la detección de fallas y la medición del desempeño, y de una herramienta útil para la configuración remota de parámetros.

En nuestro proyecto, para supervisar el funcionamiento de los dispositivos de la red, nos basaremos en información suministrada por el protocolo SNMP.

3.6.2 Arquitectura de SNMP

Según la RFC 1157 (IETF, 2015) la arquitectura de SNMP consta de los siguientes componentes:

- Uno o varios NMS (Estaciones de Gestión, del inglés *Network Management Station*): encargados de monitorear y controlar los elementos de red.

- Agentes: son los responsables de ejecutar en el dispositivo de red la función solicitada por el NMS.
- Protocolo de gestión de redes SNMP: es quien comunica la información de gestión entre los agentes y las estaciones.

En nuestro proyecto implementaremos un NMS en una máquina virtual de un servidor con virtualizaciones, configuraremos los agentes en los dispositivos y el SNMP será el encargado de realizar la comunicación entre ellos.

3.6.3 Funcionamiento de SNMP

SNMP es un protocolo de la capa de aplicación que utiliza UDP en la capa de transporte y como es un protocolo no orientado a la conexión, el impacto sobre el rendimiento de la red es bajo. Los NMS envían consultas a los agentes utilizando UDP en puerto 161 y esperan la respuesta. Si un NMS envía una consulta y no obtiene respuesta del agente luego de un tiempo determinado, asume que se ha perdido, por lo que vuelve a enviarla una cantidad configurable de veces. Los agentes reciben las peticiones y envían las respuestas al NMS utilizando UDP también en el puerto 161. Los agentes son también los encargados de enviar los traps. Cuando un agente envía un trap no sabe si el NMS lo ha recibido, éste último nunca se entera que un dispositivo quiso enviarle un trap y el agente no sabe que debe volver a enviarlo. Para los traps se utiliza UDP en el puerto 162 (Mauro y Schmidt, 2005).

3.6.4 Comunidades SNMP

"SNMPv1 y SNMPv2 utilizan el concepto de comunidades para establecer la confianza entre estaciones y agentes. Un agente se configura con 3 nombres de comunidad: *read-only* (sólo lectura), *read-write* (lectura y escritura) y *trap*." (Mauro y Schmidt, 2005, p. 21-22).

Es muy común encontrar en la configuración default de distintos tipos de dispositivos y de distintos fabricantes, la comunidad *public* para sólo lectura y *private* para lectura-escritura.

En el proyecto configuraremos la comunidad “SnmpEEAB”, de sólo lectura, en los agentes que se encuentran en los dispositivos de las redes que se administran.

3.6.5 Estructura de la Información de Gestión y MIBs

La Estructura de la Información de Gestión (SMI, del inglés *Structure Management Information*) en su versión 1, SMIv1, definida en la RFC 1155 define cómo deben ser nombrados los objetos administrados y especifica sus datos asociados. La SMIv2 definida en la RFC 2578 ofrece mejoras, extiende el árbol de objetos agregando la rama “snmpv2” al subárbol “internet” (ver Figura 1) y define más tipos de datos. Los objetos administrados se organizan en forma de árbol. OID es el nombre o identificador que define de forma única a un objeto y está conformado por una serie de enteros basados en los nodos del árbol y separados por puntos. También puede utilizarse la secuencia de nombres de los nodos (Mauro y Schmidt, 2005).

“El estándar SMI especifica que todas las variables MIB deben definirse y ser referidas por medio de la *Abstract Sintax Notation One* (ASN.1) de ISO.” (Comer, 1996, p. 461).

A modo de ejemplo, el árbol MIB que se muestra en la Figura 1, contiene algunos de los nodos que utilizaremos en el proyecto para recuperar información desde los dispositivos activos de la red.

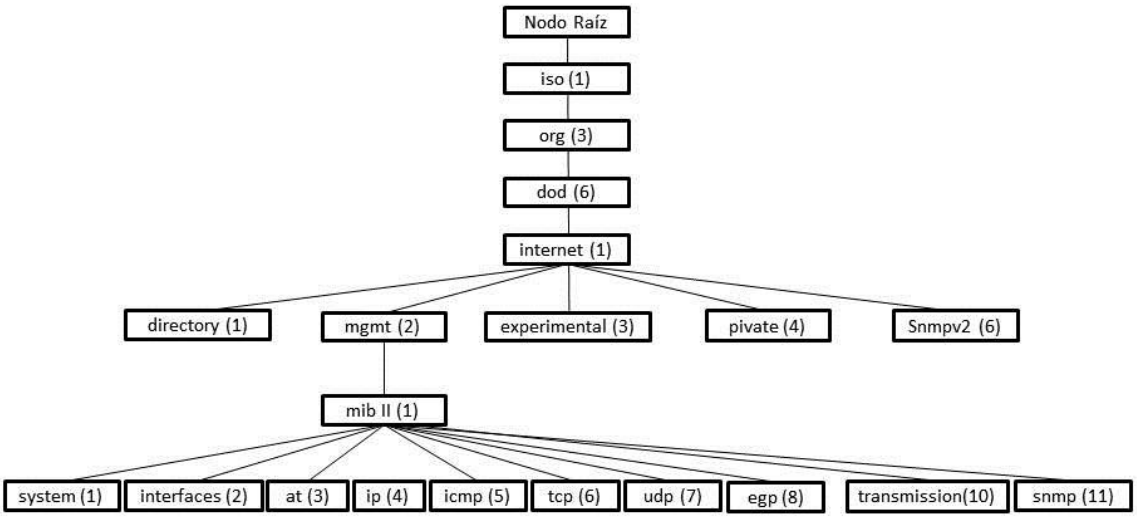


Figura 1: Subárbol MIB II
Fuente: Mauro y Schmidt (2005)

Continuando con Mauro y Schmidt (2005), la OID 1.3.6.1.2.1, o bien, iso.org.dod.internet.mgmt.mibii identifica al subárbol MIB II, que contiene, entre otros, lo siguiente:

- system (.1): lista de objetos del sistema operativo del agente (tiempo desde el último arranque, nombre de host, nombre del contacto, entre otros).
- interfaces (.2): estatus de cada interface de red administradas (cantidad de interfaces, status up o down, octetos enviados y recibidos, errores, etc.).
- ip (.4): aspectos del protocolo de internet que incluye aspectos del ruteo IP.
- icmp (5): aspectos del protocolo de mensajes de control de internet (número de solicitudes eco recibidas, errores, etc.).
- tcp (6): datos de conexiones del protocolo de transporte de internet, entre otros.
- udp (7): estadísticas del protocolo de datagrama de usuario (número de datagramas enviados y recibidos).

La rama private definida en la SMI es para que usuarios, instituciones, vendedores de hardware y/o software definan sus propios objetos.

3.6.6 SNMPv3

SNMPv3 no agrega nuevas operaciones pero realiza un aporte importante sobre la seguridad ya que en las versiones anteriores SNMPv1 y SNMPv2 la autenticación es mediante contraseña que es igual al nombre de la comunidad enviada en texto plano. SNMPv3 provee autenticación basada en usuario mediante algoritmos de cifrado conocidos (Mauro y Schmidt, 2005).

3.6.7 Operaciones SNMP

3.6.7.1 Operación GET y GETRESPONSE (de lectura y a partir de SNMPv1)

Para traer valores desde la MIB de un dispositivo, el NMS envía al agente la operación get con una lista de objetos MIB que desea conocer. El agente recibe el pedido y luego de ser procesado, responde con una operación getresponse (Mauro y Schmidt, 2005).

3.6.7.2 Operación GETNEXT (de lectura y a partir de SNMPv1)

Para traer valores desde la MIB de un dispositivo, el NMS envía al agente una operación getnext que realiza una secuencia de comandos. Por cada objeto que trae, una consulta getnext y un getresponse son generados hasta que el agente retorna un error, dando señal que no hay más objetos para traer (Mauro y Schmidt, 2005).

3.6.7.3 Operación GETBULK (de lectura y desde SNMPv2)

La operación getbulk soluciona el problema de la cantidad de objetos que get puede responder, ya que le indica al agente que traiga tantos objetos como pueda.

Dos campos deben ser definidos: nonrepeaters y max-repetitions. Nonrepeaters N indica que los primeros N objetos pueden ser traídos con un simple getnext operation. Max-repetitions M le dice que intente hasta M getnext operations para traer el remanente de objetos (Mauro y Schmidt, 2005).

3.6.7.4 Errores de operaciones

En las respuestas a las distintas operaciones realizadas GETRESPONSE nos devuelve un código que indica si fue procesado correctamente por el agente o si hubo algún error. Según la RFC 1157 los códigos son:

noError(0): el pedido fue procesado correctamente
tooBig(1): la respuesta es demasiado grande para entrar dentro de una respuesta
noSuchName(2): el OID no existe
badValue(3): valor inconsistente con el tipo de dato
readOnly(4): es de sólo lectura
genErr(5): ocurrió un error al recuperar el valor y no es ninguno de los anteriores

3.6.8 Traps (desde SNMPv1)

Según la RFC 1157 el trap es originado por el agente y enviado al NMS cuando detecta que algo ha sucedido. El tipo de trap puede ser identificado por su número que varía de 0 a 6, que indican:

- El coldStart(0), que el agente se ha reiniciado a sí mismo y que la configuración puede ser alterada.
- El warmStart(1), que el agente se ha reiniciado a sí mismo y la configuración NO es alterada.
- El linkDown(2), que falla una interfaz y se ha puesto en estado “down”
- El linkUp(3), que un interfaz ha vuelto al estado “up”.
- El authenticationFailure(4), que falló la autenticación
- El egpNeighborLoss(5), que un vecino EGP ha fallado.
- El enterpriseSpecific(6), que es un trap definido por el fabricante

3.6.9 Inform (desde SNMPv2)

Cuando un inform es enviado, el receptor envía una respuesta de recepción del evento al enviador. Si un agente utiliza un inform para enviar un trap se soluciona el problema de no conocer si el trap ha sido recibido por el NMS (Mauro y Schmidt, 2005).

En el proyecto utilizaremos algunas de las operaciones descriptas de SNMP para solicitar información del estado de funcionamiento de los dispositivos, a aquellos que implementen agentes de este protocolo. A través de la información obtenida y analizando los traps recibidos desde los agentes, se puede conocer el dato que más nos interesa del activo en este proyecto, es el estado de las interfaces de las cuales depende funcionalmente otro activo de red.

3.7 La API SNMP4J

SNMP4J es una API orientada a objetos SNMP para java, de código abierto, bajo licencia Apache 2.0. Soporta comandos tanto para gestores como para agentes (SNMP4J, 2016).

El proyecto utiliza esta API para la creación, envío y recepción de comandos SNMP entre el gestor y los agentes.

3.8 Configuración de agentes SNMP en los activos de red

El procedimiento para la configuración de los agentes SNMP en los activos de red puede realizarse de distintas maneras, dependiendo de las prestaciones que el activo posea. Si el activo posee Web Management y ofrece la posibilidad de configurar el agente SNMP, se lo configura en una interfaz web. Por el contrario, el activo puede no poseer la funcionalidad de Web Management o bien poseerla, pero no ofrecer la posibilidad de configuración web del agente SNMP a través de ella, en dicho caso, es necesario configurarlo ejecutando una secuencia de comandos de configuración a través de la Interface de Línea de Comandos (CLI, del inglés *Command Line Interface*). A esta interface se puede acceder remotamente mediante el comando telnet direccionado a la IP del activo, o bien, conectándose de forma directa a la interface "Consola" del activo, que puede ser un puerto Serie o un puerto Ethernet.

3.9 Proceso Unificado de Desarrollo de Software

Según Jacobson, Booch y Rumbaugh (2000) el Proceso Unificado es un marco de trabajo que sirve de guía en las tareas y actividades necesarias para el desarrollo de software, desde los requerimientos del usuario hasta el producto finalizado. Dentro de sus características podemos mencionar:

- Está basado en componentes: se forma por componentes de software interconectados por interfaces.
- Está dirigido por Casos de Uso: el producto se debe ajustar a las necesidades del cliente. Un caso de uso son funcionalidades del sistema que proporciona al usuario un resultado importante que necesita o desea.
- Está centrado en la Arquitectura: a través de la arquitectura se puede tener una clara perspectiva del sistema completo desde diferentes vistas y resaltando las características más importantes, lo que resulta útil para comprender el sistema y organizar su desarrollo.
- Es iterativo e incremental: para lograr el objetivo general del proyecto se lo divide en pequeñas partes más manejables, cada una de ellas es una iteración, que una vez finalizada, produce un incremento en el producto.

3.9.1 Flujos de Trabajo

Cada iteración tiene 5 flujos de trabajo:

- Requisitos
- Análisis
- Diseño
- Implementación
- Pruebas

3.9.2 Fases

El ciclo de vida del proyecto se divide en cuatro fases, cada una de las cuales termina con un hito:

- Inicio: objetivos del proyecto
- Elaboración: arquitectura del sistema
- Construcción: capacidad operativa inicial
- Transición: entrega del producto

Como marco de trabajo para que guíe las actividades del proyecto relacionadas al desarrollo de software nos basaremos en el Proceso Unificado de Desarrollo de Software.

3.10 Lenguaje de Modelado Unificado

Según Booch, Rumbaugh y Jacobson (2006) el Lenguaje de Modelado Unificado (UML, del inglés *Unified Modeled Language*) es un lenguaje gráfico de modelado orientado a objetos. Permite comunicar la estructura deseada y el comportamiento del sistema, visualizar y controlar la arquitectura, comprender mejor el sistema y controlar el riesgo. Además, es apropiado para modelar cualquier tipo y tamaño de sistemas, desde grandes sistemas empresariales hasta aplicaciones distribuidas basadas en Web, como es el caso de nuestro proyecto.

Consta de 3 elementos principales: los bloques básicos de construcción de UML, las reglas que permiten combinarlos y mecanismos comunes.

3.10.1 Bloques de Construcción de UML

Siguiendo a Booch, Rumbaugh y Jacobson (2006) los bloques de construcción orientados a objetos son de 3 clases:

1. Elementos
    a. Estructurales: son las partes estáticas de un modelo y representan conceptos o cosas materiales (ej. clases, interfaces)
    b. De Comportamiento: son las partes dinámicas de un modelo, son los verbos de un modelo y representan comportamiento y tiempo en el espacio. Hay 3 tipos de elementos de comportamiento:
        i. Interacción: conjunto de mensajes intercambiados entre un conjunto de objetos en un contexto particular con un propósito específico
        ii. Máquinas de estados: secuencia de estados por los que pasa un objeto
        iii. Actividad: secuencia de pasos que ejecuta un proceso
    c. De Agrupación: son las partes organizativas de un modelo, son partes que incluye muchos elementos agrupados (ej. 1 paquete)
    d. De Anotación: son las partes explicativas de un modelo (ej. comentarios, notas)
2. Relaciones
    a. De Dependencia: un cambio en un elemento afecta a otro elemento
    b. De Asociación: relación de conexión entre objetos. La agregación es un tipo especial de asociación que representa una relación de todo y sus partes.
    c. De Generalización: relación de especialización o generalización
    d. De Realización: un clasificador especifica un contrato que otro clasificador garantiza que cumplirá
3. Diagramas: representación gráfica de un conjunto de elementos
    a. Clases: diagrama de vista estática que muestra las clases del sistema con sus atributos y operaciones y sus relaciones.
    b. Objetos: diagrama de vista estática que muestra los objetos, sus datos y sus relaciones en un instante dado.

c. Casos de Uso: diagrama de vista dinámica donde se representa un caso de uso, sus actores (o roles) y sus relaciones. Muestran el comportamiento del sistema ante un estímulo de los actores.
d. Secuencia: diagrama de vista dinámica que muestra la interacción entre los objetos intervinientes en un caso de uso resaltando el orden temporal de los mensajes entre objetos.
e. Colaboración: diagrama de vista dinámica que muestra la interacción entre los objetos intervinientes en un caso de uso resaltando la organización estructural de los objetos que envían y reciben mensajes.
f. Estados: diagrama de vista dinámica que muestra estados, transiciones, eventos y actividades.
g. Actividades: diagrama de vista dinámica que muestra el flujo de las actividades modelando el funcionamiento del sistema
h. Componentes: diagrama de vista estática que describe la organización y las dependencias entre componentes
i. Despliegue: diagrama de vista estática que muestra la configuración de nodos de procesamiento y los componentes que residen en ellos

3.10.2 Reglas de UML

Continuando con Booch, Rumbaugh y Jacobson (2006), UML es un lenguaje, tiene reglas sintácticas y semánticas para establecer nombres a los elementos, relaciones y diagramas, para el alcance, la visibilidad del elemento para ser vistos y usados por otro elemento, la integridad de las relaciones entre elementos y la ejecución de un modelo dinámico.

3.10.3 Mecanismos comunes

De acuerdo a Booch, Rumbaugh y Jacobson (2006), son los mecanismos comunes que se aplican de forma consistente a través de todo el lenguaje. Son:

1. Especificaciones: proporcionan la explicación textual que está detrás de la notación gráfica

2. Adornos: son la representación visual de los aspectos más importantes del elemento.
3. Divisiones comunes:
4. Mecanismos de extensibilidad: UML permite a través de estos mecanismos extender su lenguaje de forma controlada. Ofrece mecanismos de:
    a. Estereotipos: permite crear nuevos tipos de bloques de construcción. Ej.: modelado de excepciones.
    b. Valores etiquetados: permite añadir nueva información en las especificaciones
    c. Restricciones: permite añadir nuevas reglas

En nuestro proyecto nos basaremos en UML como el lenguaje gráfico orientado a objetos que utilizaremos para construir todos los modelos.

3.11 Herramienta de modelado UML

Una herramienta de modelado UML es una aplicación de software que dispone de los elementos principales del Lenguaje Unificado de Modelado y facilita la realización de diagramas.

3.11.1 ArgoUML

"ArgoUML es una herramienta de modelado UML de código abierto que incluye soporte para todos los diagramas estándar UML 1.4. Se ejecuta en cualquier plataforma Java y está disponible en 10 idiomas. ArgoUML se distribuye bajo la Licencia Pública Eclipse (EPL) 1.0" (Tigris.org, 2015).

3.12 Ambiente de Desarrollo Integrado

Un ambiente de desarrollo integrado (IDE, del inglés *Integrated Development Environment*), es una aplicación de software que a través de un gran conjunto de herramientas facilitan el desarrollo de software.

3.12.1 Netbeans IDE

El ambiente de desarrollo integrado NetBeans, gratuito y de código abierto, permite desarrollar rápidamente aplicaciones Java de escritorio, móviles y web, así como también aplicaciones HTML5, JavaScript, PHP y C/C++ (NetBeans, 2015).

3.13 ProjectLibre

Es una herramienta de código libre y abierto para la Gestión de Proyectos, que permite realizar, entre otras funciones, Diagramas de Gantt, Diagramas de Red, WBS, Cálculo del Valor Ganado, Histogramas de Recursos, etc. (ProjectLibre, 2016).

3.14 Bizagi Modeler

Es una herramienta freeware que permite modelar y documentar procesos de negocios basados en BPMN, del inglés *Business Process Model and Notation* (Bizagi, 2016).

3.15 Bases de Datos

Tabla 1.
Comparación de algunas características de las Bases de Datos que se utilizan en el Organismo

Características	PostgreSQL	MySQL Server	SQL Server
Licencias gratuitas	PostgreSQL License, Open Source License, similar a BSD o MIT Licenses	Community Server - GNU General Public License, version 2	Express
Licencias comerciales	-	Standard, Enterprise y Cluster CGE	Standard, Enterprise y Business Inteligence
Open Source	SI	SI	NO
Conectores (licencias gratuitas)	C/C++, .Net, ODBC, JDBC, Python, PHP, Perl, entre otros.	.Net, ODBC, JDBC, Python, C/C++, PHP, Perl, entre otros.	JDBC, ODBC, PHP,.Net, entre otros
Plataforma (licencias gratuitas)	Linux y Windows, entre otros.	Linux y Windows, entre otros.	Windows
Tamaño máximo DB (licencias gratuitas)	Sin límite (de tabla 32 TB)	Sin Límite	10 GB
Características (licencias gratuitas)	Transacciones, Vistas, Triggers y Subconsultas.	Transacciones, Vistas, Triggers y Subconsultas.	Transacciones, Vistas, Reports, Triggers y Subconsultas.
Otras características (licencias gratuitas)	Soporte para objetos geográficos (PostGis).		Hasta 4 núcleos Memoria máxima por instancia: 1 GB.

Fuente: datos obtenidos de los Sitios Web de PostgreSQL, MySql y Microsoft.

En el proyecto se utilizará la base de datos PostgreSQL ya que es de código abierto y es una Base de Datos utilizada por el grupo de Sistemas de Información de la organización para algunas aplicaciones.

3.16 Lenguajes de Programación

Tabla 2.
Comparación de algunas características de los Lenguajes de Programación que se utilizan en el organismo

Características	**Java**	**ASP.Net**
Licencia gratuitas	Standard Edition - GNU General Public License, v.2	Free
Empresa	Oracle (Open Source)	Microsoft
Paradigma	Orientado a Objetos Imperativo	Multiparadigma
Plataforma	Multiplataforma	Multiplataforma
Web Server Scripting	Java Server Pages (JSP) Java Server Faces (JSF)	Active Server Page (ASP) ASP.Net
Acceso a Datos	JDBC	ADO.Net
Http Engine	Apache Tomcat Glassfish	IIS
Ambiente de Desarrollo	Netbeans Eclipse Aplicaciones open source	Visual Studio Aplicaciones open source
Otras características	Existen APIs Open Source para SNMP	Existen librerías Open Source para SNMP

Fuente: datos obtenidos de los Sitios Web de Java y ASP.Net.

3.17 jQuery

jQuery es una biblioteca de Javascript que simplifica la forma de interactuar con documentos hmtl y funciona con muchos navegadores. Es software libre y de código abierto bajo Licencia MIT y la Licencia Pública General de GNU v2 (jQuery, 2016).

En el proyecto utilizaremos jQuery en algunas partes del desarrollo de la aplicación web.

3.18 Apache Tomcat

Apache Tomcat es una implementación de código abierto de Java Servlets y Java Server Pages, liberado bajo la Licencia Apache Versión 2 (Apache Tomcat, 2016).

En el proyecto utilizaremos Apache Tomcat como servidor web.

3.19 Productos de mercado con características similares

Existen varios productos para la supervisión del funcionamiento de redes utilizando SNMP, muy completos y disponibles desde hace varios años. Algunos ejemplos son: PRTG, NAGIOS, MUNIN, GANGLIA y ZENOSS, entre otros. La siguiente tabla muestra la comparación de algunas características de dos de los productos mencionados.

Tabla 3.
Comparación de algunas características de productos disponibles en el mercado

	PRTG Network Monitor	**Nagios**
Licenciamiento	Freeware hasta 100 sensores. Cada aspecto que se monitorea en un dispositivo equivale a un sensor. Pago: por cantidad de sensores en varios rangos, desde u$s 1600 con un límite de 500 sensores, hasta u$s 9500 (límite de 5000 sensores). Sin límite: u$s 13500	GNU GPL sólo módulo Core. Pago: por módulos Nagios XI Standard: por cantidad de nodos: u$s 1995 hasta 100 nodos, u$s 2995 por 200 nodos y u$s 4995 sin límite. Nagios XI Enterprise u$s 1500 adicionales
Costo del soporte y actualizaciones	Por un año u$s 13500, por 2 años: u$s 16537 y por 3 años u$s 19237	Por año: desde u$s 995 a u$s 1495 según cantidad de llamados
S.O. Estación	Windows	Linux y Unix
Uso de Agentes	SI	SI
S.O. de Agentes	Linux, Unix y Windows	Linux, Unix y Windows
WebApp	SI	SI
Protocolos	SNMP, Packet Sniffing y NetFlow	SNMP
Autodetección de Red	SI	SI
Alertas por email o SMS	SI	SI
Inventario de Red	SI	SI
Programación de Plugins	SI	SI
Idioma	Inglés y Español, entre otros	Inglés y Español, otros
Otras funcionalidades	Monitorización de ancho de banda	Analizador de tráfico y Log Server, entre otros

Fuente: datos obtenidos desde los Sitios Web de Nagios y Paessler.

Estos productos tienen versiones de libre uso y comerciales. Los de libre uso son limitados a cantidad de módulos, sensores o dispositivos. Munin, Nagios, Zenoss y Ganglia corren bajo Linux y algunos también bajo Unix. PRTG corre bajo Sistema Operativo Windows.

El sistema a desarrollar pretende brindar una interfaz simple, clara e integral de todos los dispositivos de la red administrados con una mirada distinta, más orientada a visualizar a simple vista los cambios de estado de la conectividad, la dependencia funcional de los activos y el alcance de un incidente, sin limitaciones en la cantidad de dispositivos a monitorear.

4. Diseño Metodológico

4.1 Recolección de datos

- Análisis de la información institucional publicada en el Sitio Web de la EEA Balcarce (www.inta.gob.ar/balcarce).
- Entrevista a personal de Recursos Humanos y al Asistente Operativo de Dirección para el relevamiento funcional y funciones de cada área. El instrumento utilizado fue la guía de entrevista que figura en el Apéndice A.
- Técnica de Observación para comprender la estructura y funcionalidad de los grupos Comunicaciones e Informática.
- Entrevista al personal del Grupo de Soporte Técnico de Informática para comprender sus actividades. El instrumento utilizado fue la guía de entrevista que figura en el Apéndice B.
- Entrevista al personal del Grupo de Sistemas de Información para comprender sus actividades. El instrumento utilizado fue la guía de entrevista que figura en el Apéndice C.
- Entrevista al personal del Grupo de Redes y Servicios para conocer sus necesidades y capturar los requerimientos del sistema. Técnica de observación directa para comprender las actividades comparando la prestación de servicios en situaciones de funcionamiento normal y ante incidentes de red. El instrumento utilizado para la entrevista fue la guía de entrevista que figura en el Apéndice D.
- Técnica de observación directa y análisis de información de la documentación de la red, para relevar la información de la infraestructura de red, el diseño físico y lógico, los activos que la conforman, la conectividad troncal y de los servidores y servicios de la sala de servidores. El instrumento utilizado para la observación directa fue la guía de observación que figura en el Apéndice E.

Población: elementos activos de las redes de las siguientes unidades del INTA: CERBAS, EEA Balcarce, AER Balcarce, AER Mar del Plata, AER Tandil, AER Olavarría, AER Necochea, AER Cte. N. Otamendi, AER Lobería, AER Benito Juárez, AER Gral. La Madrid y AER Laprida. Como elementos activos de la red se consideran: firewalls, switchs de capa 2 y capa 3, impresoras de red, equipos troncales wifi, puntos de acceso wifi, routers wifi,

equipos de videoconferencia, equipos IP de laboratorios, cámaras IP, controles de acceso a puertas, equipos de reconocimiento de datos biométricos, servidores, consolas de virtualización de servidores, servidores de almacenamiento y estación permanente de gps.

Muestra: 153 elementos activos de red

4.2 Desarrollo del Proyecto

- Para la construcción del software se utilizará la metodología del Proceso Unificado de Desarrollo de Software.
- Para el modelado del sistema se utilizará el Lenguaje de Modelado Unificado (UML).
- La herramienta de modelado será ArgoUML versión 0.34.
- El Ambiente de Desarrollo Integrado (IDE) a utilizar será Netbeans versión 8.0.2
- El lenguaje de programación será Java.
- La Base de Datos a utilizar será PostGreSQL 9.4
- Para la Gestión del Proyecto se utilizará ProjectLibre versión 1.6.2
- Para los Diagramas BPM se utilizará bizagi Modeler versión 2.7.0.2

5. Relevamiento

5.1 Relevamiento Estructural

El campus de la EEA está ubicado en la localidad de Balcarce, provincia de Buenos Aires, en la Ruta Nacional 226 km. 73,5. En la siguiente imagen satelital se agregó en color negro un edificio construido posteriormente a la toma de las imágenes, el nuevo edificio del Área de Agronomía.

El área de influencia de la EEA comprende diez partidos del sudeste y centro de la provincia de Buenos Aires (zona marcada en el mapa de la Figura 2), abarcando una superficie de 4,2 millones de hectáreas.

Figura 2. Imagen satelital del campus de la EEA Balcarce
Google Earth [software]

El campus posee cerca de 30 edificios de distintas dimensiones y distantes entre sí. La red LAN del campus tiene una topología de red extendida e interconecta 22 de estos edificios ya sea a través de fibra óptica, cable UTP o enlaces inalámbricos. Los enlaces que provienen de los gabinetes de telecomunicaciones principales de los edificios rematan en la Sala de Servidores del edificio de Informática.

En los edificios la conexión se realiza a través de cableado estructurado con cables UTP de Categoría 6, y los puestos de trabajo rematan en los diferentes gabinetes de telecomunicaciones que poseen switchs de capa 2, algunos de 1000 mbps y otros de 100 mbps. Las conexiones cableadas rematan en Patch Panels y a través de Patch Cord se conectan al switch. Los puertos de estos switch asignan la VLAN que le corresponde según el edificio o tipo de dispositivo conectado, ya que existen VLAN que son para segmentar la red, otras para seguridad y otras para diferenciar el tipo de dispositivos que se conecta o servicio que brinda. Los puntos de acceso wifi emiten dos señales: Privado y Público, asociadas a dos VLANs diferentes. Los enlaces troncales de los switchs transportan las vlans hasta el switch de capa 3 de la sala de servidores. Es allí donde el tráfico es direccionado, a través de los switchs y firewalls, a las subredes de otras vlans o bien ruteado a Internet (a través de una red MPLS).

En esta sala también están los servidores que alojan los servicios. Algunos servidores, los más potentes, están virtualizados. Entre los servidores y servicios se encuentran:

- Active Directory
- DHCP (*Dynamic Host Configuration Protocol*)
- Antivirus Corporativo
- WSUS (*Windows Server Update Services*)
- File Server
- Aplicaciones y Bases de Datos
- Web de Intranet

Entre los activos que conforman la red se encuentran:

- Firewalls
- Switchs de Capa 3
- Switchs de Capa 2
- Access Point wifi
- Routers wifi
- Equipos troncales Wifi
- Módulos MiniGBic FO
- Media Converter FO/UTP
- Impresoras de Red
- Equipos de Videoconferencias
- Estación permanente GPS
- Controles de acceso de puertas
- Cámaras IP
- Equipos de reconocimiento de datos biométricos (huellas digitales)
- Sistemas de Energía ininterrumpida (UPS)
- Equipos de Laboratorios con acceso IP

Las 11 unidades restantes (Centro Regional y 10 Agencias de Extensión), que también son administradas por el grupo de Redes de la EEA Balcarce, poseen un único edificio y un único gabinete de telecomunicaciones cada una, donde se aloja el firewall que comunica la red interna con la red MPLS. Estos firewalls ofrecen también servicios de DHCP y punto de

acceso wifi. Las Pcs de las agencias tienen agentes que apuntan a los servidores de actualizaciones y antivirus corporativo de la EEA, mientras que la autenticación de usuario la realizan en cualquiera de los servidores de dominio disponible en la MPLS.

En todas las unidades, el tráfico saliente hacia la MPLS es procesado según tres órdenes de prioridad: alto, medio y bajo, y utilizando un ancho de banda determinado, dependiendo de la aplicación destino, protocolo que utilice o la conexión que origina el tráfico.

La Red MPLS del INTA a nivel país, la conforman aproximadamente 300 redes LAN, correspondientes a las unidades del INTA ubicadas en distintas localidades. Doce de estas redes son las descriptas en este relevamiento. Al estar todas las unidades interconectadas a través de la MPLS, los dispositivos conectados en las redes pueden accederse desde cualquier unidad.

5.2 Relevamiento Funcional

5.2.1 Organigrama

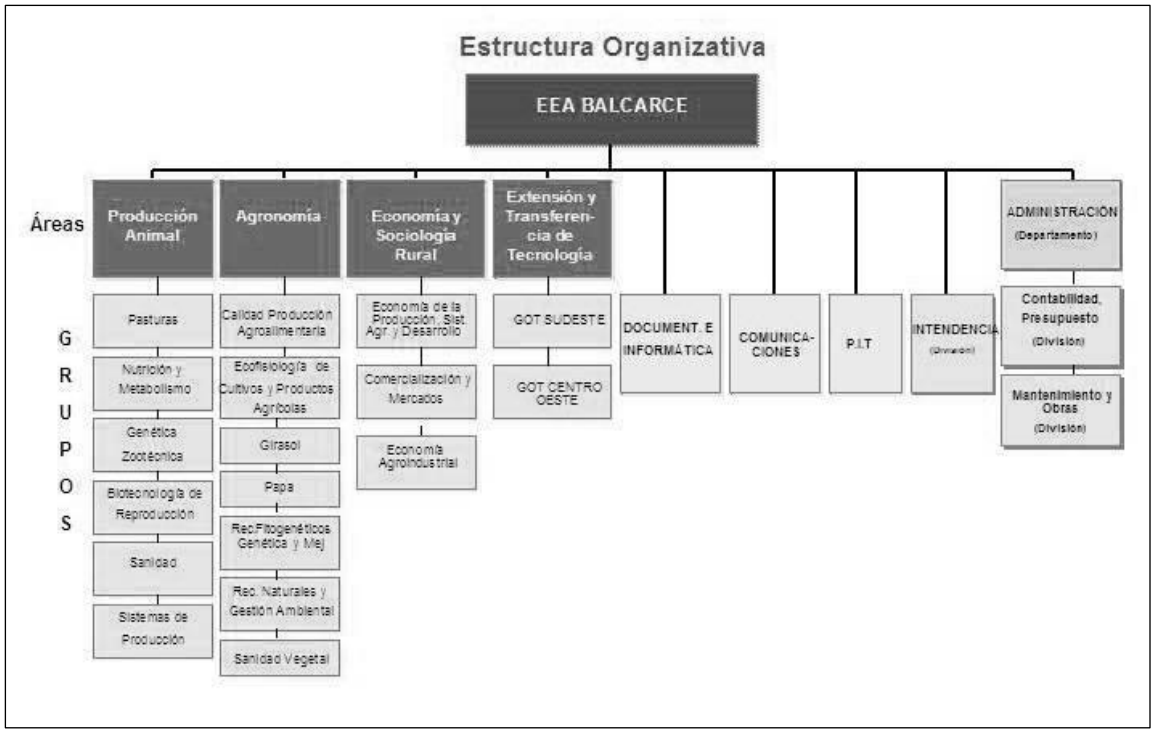


Figura 3. Estructura Organizativa de la EEA Balcarce
Fuente: Resolución 395/04 del Consejo Directivo del INTA

Es una organización del tipo mixta, una parte mantiene una estructura jerárquica y otra parte es matricial donde los Programas Nacionales, Proyectos de Investigación y Proyectos Regionales con enfoque territorial cruzan a la organización, permitiendo la interacción entre investigadores y extensionistas.

5.2.2 Funciones de las Áreas

Las Áreas de Producción Animal, Agronomía y Economía y Sociología Rural realizan, a través de sus grupos, las actividades de investigación y experimentación agropecuaria. Poseen laboratorios que ofrecen servicios de análisis a externos como productores agropecuarios, profesionales, particulares, organismos, empresas privadas y otros laboratorios públicos y privados. También se realizan análisis de uso interno para investigación y formación académica, como tesis de grado y posgrado.

El Área de Extensión y Transferencia de Tecnología tiene como función la difusión y transferencia de los resultados de la investigación tecnológica y las acciones de capacitación.

El Grupo de Comunicaciones se encarga de comunicar tanto interna como externamente las actividades de la UIB en diferentes formatos a través de sus subgrupos: Diseño Gráfico, Sitio Web, Publicaciones, y Prensa y Difusión.

La División Intendencia es la encargada del mantenimiento del Campus, vehículos y maquinaria agrícola institucional.

El Departamento de Administración está compuesto por 2 divisiones: a) Contabilidad y Presupuesto: encargada de la parte administrativa, contabilidad, compras, suministros y tesorería y b) Mantenimiento y Obras: responsable de los servicios básicos (electricidad, agua, telefonía analógica y gas), obras y el mantenimiento de los edificios.

El Grupo de Documentación e Informática abarca los sectores de Biblioteca e Informática. Funcionalmente, Informática está dividida en 3 subgrupos: Soporte Técnico, Sistemas de Información e Infraestructura y Servicios de Red.

a) Soporte Técnico

Está compuesto por 3 técnicos, y su actividad principal es la de soporte técnico en hardware y software, asistencia y capacitación de usuarios en el uso de software, licenciamiento de software y la pertenencia patrimonial de la Pc. También interviene en el

proceso de compras de Pcs y en el proceso de reparación de equipamiento informático por parte de terceros, entre otras funciones.

b) Sistemas de Información

Integrado por 2 profesionales de sistemas, su actividad principal es el desarrollo de software y de intermediario en los desarrollos de aplicaciones de escritorio o web que se contratan a terceros. También se encarga de los celulares corporativos, copias de seguridad de la información contenida en las bases de datos, administra el servidor que aloja aplicaciones y bases de datos, brinda ayuda al grupo de redes en servidores y servicios, entre otras funciones.

c) Infraestructura y Servicios de Red

Este grupo es el usuario del sistema, compuesto por 2 técnicos, es el grupo que debe garantizar el acceso a la Red, a los servicios y a Internet, y la calidad del servicio.

Dentro de sus principales actividades se encuentran:

- Administración de servidores y servicios.
- Administración y mantenimiento de la infraestructura de red.
- Administración y configuración de los activos de red.
- Administración de políticas de firewall, uso de ancho de banda y enlaces de telecomunicaciones.
- Administración de usuarios y contraseñas de la unidad organizativa de la EEA.
- Gestión ante Gerencia de Informática de INTA Central de solicitud de creación de emails y listas de distribución masiva de emails.
- Administración de permisos de envío, moderación y miembros de las listas.
- Servicio de videoconferencias y reuniones virtuales.

Los grupos informáticos, cada uno en su temática, dan servicio a 12 unidades del INTA (1 Centro Regional, 1 EEA y 10 Agencias de Extensión).

5.3 Sistema de Gestión de Incidentes

El Sistema de Gestión de Incidentes que utilizan los informáticos para atender los problemas e incidentes de sus usuarios es un software que sirve de herramienta de Mesa de Ayuda, compatible con ITIL (Biblioteca de Infraestructura de Tecnologías de Información, del inglés *Information Technology Infrastructure Library*).

Los usuarios, con su dirección de mail corporativa, envían un email describiendo el incidente a una dirección específica. Al recibirlo, el sistema abre un nuevo ticket y se lo asigna automáticamente al equipo de soporte que atiende la unidad donde se encuentra dicho usuario. Para esta asignación utiliza atributos del usuario definidos en el AD (Directorio Activo, del inglés *Active Directory*) del dominio corporativo.

Existen grupos de técnicos de soporte conformados según la unidad donde desempeña su tarea o la temática de su actividad. Los técnicos de soporte son definidos en un nivel determinado, siendo el nivel 1 el más bajo. El ticket puede derivarse entre grupos de técnicos de un mismo nivel o entre grupos de distintos niveles. De esta manera los técnicos pueden realizar consultas al resto, opinar, hacer comentarios, pueden resolver parcialmente el problema y/o derivarse los tickets hasta su resolución. El usuario, a través del número de ticket puede ver todo el trabajo que se está realizando, el estado en que se encuentra el problema, quién tiene asignado actualmente su ticket, en pocas palabras, puede realizar el seguimiento de resolución de su incidente.

Una vez resuelto el incidente el técnico informa al usuario de su resolución con un email que puede enviar desde el mismo sistema y registra, entre otros datos, el impacto, el activo afectado, los detalles de su resolución, lo categoriza y cierra. El usuario recibe esta información y la notificación que el ticket ha sido cerrado.

5.4 Procesos de Negocio

Proceso: Detección de fallas en el funcionamiento de la red y determinación del alcance del incidente

Áreas: Área/Unidad del usuario que reporta la falla
Grupo Infraestructura de Redes y Servicios
Gerencia de Informática

Paso:

- **Usuario**:
  Solicita asistencia mediante el Sistema de Gestión de Tickets, llamada telefónica o concurre al edificio del Grupo de Informática porque tiene un problema
  - Si la solicitud fue realizada mediante el Sistema de Gestión de Incidentes:
    - **Sistema de Gestión de Incidentes de Gerencia de Informática**:
      Recibe solicitud de asistencia, crea un nuevo ticket y lo deriva a los informáticos de la unidad que concuerde con el dato de unidad del usuario solicitante registrado en Active Directory. Notifica mediante email a los informáticos involucrados.
    - **Informático de Redes y Servicios**:
      Recibe notificación y abre ticket
      Evalúa la descripción del incidente detallada en el ticket
      - Si la descripción es insuficiente contacta al Solicitante
        - **Usuario**: amplía detalles del incidente
      - Si la descripción es suficiente continúa
  - Si la solicitud fue realizada telefónica o personalmente:
    - **Informático de Redes y Servicios**: indaga durante la conversación detalles del incidente
  - **Informático de Redes y Servicios**: evalúa correspondencia
    - Si el tema del incidente corresponde a Soporte Técnico, no modifica el ticket y Fin del Proceso
    - Si el tema del incidente corresponde a Sistemas de Información, no modifica el ticket y Fin del Proceso
    - Si el tema del incidente corresponde a Redes y Servicios, evalúa el tema:
      - Si el incidente es de temas distintos a conectividad, pasa al subproceso de resolución de incidentes de otros temas y Fin del Proceso
      - Si el incidente es de conectividad:
        Consulta la documentación de red
        Realiza pruebas básicas de red para ver el funcionamiento
        Determina el Alcance del Incidente
        - Si el alcance afecta a un solo usuario: pasa al subproceso de resolución de incidentes de red que afectan a un usuario
        - Si el alcance afecta a un grupo de usuarios: pasa al subproceso de resolución de incidentes de red que afectan a un grupo de usuarios
        - Si el alcance afecta a toda la red: pasa al subproceso de resolución de incidentes de red que afecta a toda la red

  Una vez solucionado el problema, completa el ticket agregando los siguientes datos: tipo de incidente, nivel de afectación de usuarios, técnico interviniente, resolución, activos afectados, entre otros datos y cierra el ticket.

- **Sistema de Gestión de Incidentes de Gerencia de Informática**:
  Almacena Ticket y envía respuesta al usuario con la resolución del incidente.
- **Usuario**: recibe respuesta del incidente
- **Sistema de Gestión de Incidentes de Gerencia de Informática**:
  - En caso de que el ticket se haya resuelto en períodos de encuesta de satisfacción, envía encuesta de satisfacción al usuario
    - **Usuario**: Recibe encuesta de Satisfacción
      - Si responde encuesta:
        - **Sistema de Gestión de Incidentes:** recibe y almacena formulario para su posterior análisis, Fin del Proceso
      - Si no responde encuesta, Fin del Proceso
  - Si no es período de encuestas, Fin del Proceso

Diagrama BPM:

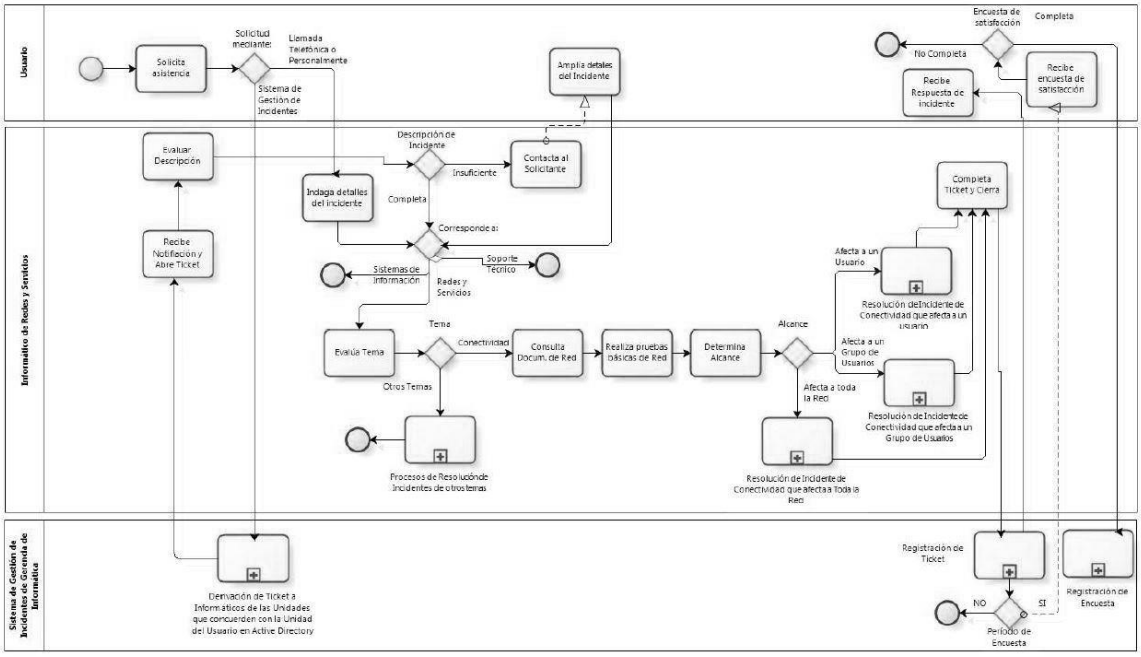


Figura 4. Modelo del Proceso de Detección de fallas en el funcionamiento de la Red y determinación del alcance del incidente
bizagi Modeler (versión 2.7.0.2) [software]

Proceso: Declaración de incidentes en el Sistema de Gestión de Incidentes de la organización.

Áreas: Usuario o Sistema que pretende declarar un nuevo incidente
Sistema de Gestión de Incidentes de la Organización
Informáticos de unidades

Paso:

- **Usuario/Sistema**:
  Envía un email a la dirección de email específica de pedidos de asistencia del Sistema de Gestión de Incidentes desde una dirección de email corporativa
- **Sistema de Gestión de Incidentes de Gerencia de Informática**:
  - Recibe solicitud de asistencia y crea un nuevo ticket
  - Busca en el Active Directory a qué unidad pertenece el usuario que envía el email
  - Busca qué Informáticos atienden en esa unidad
  - Deriva el ticket a los informáticos de la unidad y lo notifica mediante un email. También notifica al usuario por email que el ticket ha sido creado, a qué informático fue asignado y le brinda un link para que el usuario pueda realizar el seguimiento de la solución a su problema.
- **Informático de Unidades**:
  - Recibe la notificación de que el ticket ha sido creado
  - Subproceso de Resolución de Incidente
  - Una vez resuelto, carga la resolución, categoriza el ticket y lo cierra
- **Sistema de Gestión de Incidentes**:
  - Notifica la resolución y el cierre del ticket
  - Registra Ticket
  - Fin del Proceso
- **Usuario/Sistema**: recibe la notificación de la resolución y que el ticket ha sido cerrado

Diagrama BPM:

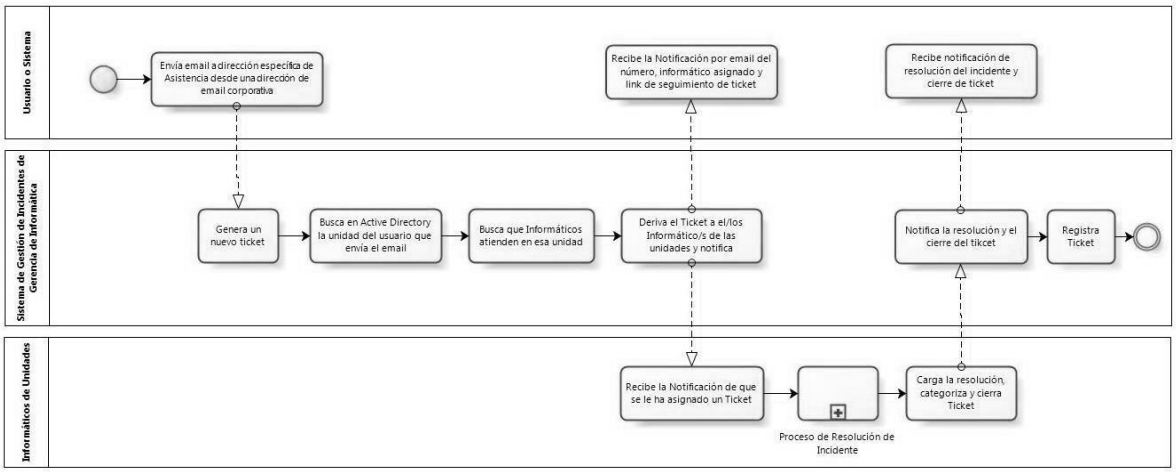


Figura 5. Modelo del Proceso de Declaración de Incidentes en el Sistema de Gestión de Incidentes de la organización
bizagi Modeler (versión 2.7.0.2) [software]

6. Diagnóstico

El modelo de proceso de detección de fallas en el funcionamiento de la red y determinación del alcance del incidente (Figura 4) muestra claramente que recién se reacciona ante una falla en la red cuando el usuario, ya sea mediante un llamado telefónico, un ticket en el sistema de gestión de incidentes (Mesa de ayuda) o concurriendo personalmente hasta el edificio de informática, avisa que un problema ha ocurrido y solicita asistencia para su solución.

Si la solicitud se realizó mediante el sistema de gestión de incidentes puede no estar bien expresada o ser insuficiente en detalles para detectar cuál es el problema que el usuario realmente tiene, en dicho caso se lo contacta para solicitarle más detalle y así comprender el problema. Recién allí los técnicos de redes comienzan a realizar pruebas básicas de red para ver cuál es el alcance del problema, que puede ser: afecta a un único usuario, afecta a varios usuarios o a toda la red. Una vez determinado el alcance se continúa, en distintos subprocesos, con actividades técnicas propias de redes que incluyen: control del funcionamiento, configuración y consistencia de datos del Servicio DHCP; control del estado del cableado estructurado y señal inalámbrica; control del funcionamiento de los activos, estados de sus puertos, configuración de VLAN y la revisión de la configuración de 802.1Q en los puertos troncales de los activos. También puede deberse a que sea un problema a derivar al grupo de soporte técnico, como fallas en las placas de red Ethernet, inalámbrica o sus drivers, pero esto se encuentra fuera de nuestro alcance.

Queda evidenciado que no se conoce de forma online ni con anterioridad al momento del incidente, el estado del funcionamiento de la red, activos y servicios, y que transcurre mucho tiempo desde que ocurre un incidente hasta que el técnico de redes toma conocimiento y comienza a intentar solucionarlo. Tengamos en cuenta que si el incidente que afectó a un usuario o a un grupo implica la pérdida de conectividad, no puede acceder al sistema de gestión de incidentes para abrir un ticket ni tampoco enviar un email a la dirección de mail que abre un ticket automáticamente. Debe conseguir que otro usuario que disponga de servicio, lo envíe por él o bien comunicarse con informática, encontrar a un técnico disponible o concurrir hasta el edificio de informática. Todo esto repercute negativamente en los tiempos transcurridos desde la ocurrencia del incidente hasta su solución y por ende, en la calidad del servicio brindado.

7. Propuesta de Solución

Del análisis de datos se obtuvo que un gran número de dispositivos de las redes administradas implementan agentes SNMP en algunas de sus versiones (ver Apéndice F). Considerando esta información, la propuesta de solución es desarrollar una herramienta web de monitorización de equipos y dispositivos de red, de distintos sistemas y fabricantes, que a través de una interfaz visual simple y clara, muestre información online obtenida regularmente desde los activos de red utilizando el protocolo SNMP y comandos básicos de red, permitiendo al administrador y a los técnicos de redes, supervisar el funcionamiento de la red, prevenir fallas y detectar de forma temprana los incidentes. Además permite, tanto al grupo de redes como a los afectados, conocer el alcance del problema. El sistema deberá mostrar el punto de falla y los activos que dependen funcionalmente del que ha fallado.

Esto implica un cambio en el proceso de detección de fallas y supervisión del funcionamiento de la red, pasando a ser automático y proactivo, en contraposición con la forma manual y reactiva con que se realiza actualmente. Favorece a una solución más rápida y eficiente de incidentes, en beneficio del grupo de redes y servicios y de toda la organización en general.

8. Proyecto de Desarrollo

8.1 Participantes del Proyecto

Tabla 4.
Participantes del proyecto, roles y responsabilidades

Rol en el Proy.	**Rol en la Organización**	**Responsabilidades**
Líder del Proyecto Análisis del Sistema Diseño del Sistema Desarrollador	Alumno = Administrador de Red	Planificar y controlar el proyecto Dirigir y asignar recursos Coordinar actividades Capturar, especificar y validar requerimientos Interactuar con el Cliente Modelar el Sistema Definir la arquitectura que guiará el desarrollo Codificar componentes en lenguaje de programación
Pruebas	Técnico de Red Alumno = Administrador de Red	Diseñar casos de prueba Ejecutar los casos de prueba y sugerir mejoras
Implantación	Responsable de Sistemas de Información Alumno = Administrador de Red	Implantar en ambiente operacional Breve capacitación de usuarios Evaluación del sistema e informe final

8.2 Fases e Iteraciones

Tabla 5.
Fases e iteraciones

Fase	Iteraciones	Duración	Hito de Fin de Fase
Inicio	1	2 semanas	Requerimientos y Casos de Uso identificados. Aceptación del Cliente
Elaboración	2	4 semanas	Casos de Uso analizados y diseñados
Construcción	3	9 semanas	Capacidad operativa parcial del producto y pruebas realizadas
Transición	2	2 semanas	Producto y documentación entregada. Puesta en Servicio. Capacitación realizada

8.3 Estimaciones de Recursos

8.3.1 Tiempo

El proyecto tendrá una duración total de 17 semanas y media, con una variación de 10 a 14 horas laborales cada una, distribuidas en cada participante de acuerdo a la siguiente tabla:

Tabla 6.
Estimación de Tiempo

Participante	Día	Horario	Lugar	Total hs. Semanales
Técnico de Red	Viernes	14 a 16	Organización	2
Responsable de Sistemas de Información	Viernes	14 a 16	Organización	2
Administrador de Red	Viernes	14 a 17	Organización	10
	Sábado	9 a 12	Org. u Hogar	
		16 a 20	Hogar	

8.3.2 Recursos Humanos:

Administrador de Red - Alumno: 176 hs
Técnico de Red: 28 hs
Responsable de Sistemas de Información: 12 hs

8.3.3 Infraestructura edilicia, de red, hardware y software disponible a utilizar

Sala de Servidores con control de acceso por tarjetas de proximidad, alarma, doble aire acondicionado, vigilancia por cámaras de circuito cerrado, con grabación en DVR, equipo electrógeno propio con buen mantenimiento, luz de emergencia, dos matafuegos HCFC-123.

Un Servidor HP Proliant DL380 G6 Quad Core Xeon 3 GHz – 2U Montable en rack server – 8 Bahías para Discos HotSwap 2.5'' - 2 Discos SATA 350 GB en Raid 0+1 – 16 GB RAM – 2 puertos Gigabit Ethernet.

Una partición VMWare ESXi de 4 GB RAM y 140 GB Disco (100 GB disponibles)

Switchs de Capa 3 y Capa 2 con puertos Giga Ethernet disponibles.

Vlan exclusiva para Servidores con host disponibles para asignar.

Cableado Estructurado de Cat 6 con jacks de Cat 6, certificado.

Switch KVM de 8 puertos para compartir monitor, mouse y teclado entre servidores.

Un Sistema Operativo Windows 2008 Server Standard R2 con el servicio Web Server activo, atendiendo en puertos 80 y 443.

Gestores de Base de Datos PostgreSQL, MySQLServer y SQL Server Express.

Protección Antivirus Kaspersky V. 10 (Licencia Corporativa).

Descarga de actualizaciones desde el Servidor Windows Server Update Services (WSUS) Local.

8.3.4 Costos

Recursos Humanos: $ 26227

Requerimientos: $ 3625

Análisis y Diseño: $ 4875

Implementación: $ 7062.50

Pruebas: $ 6321.50

Despliegue: $ 4344

Infraestructura: $ 0

Licencias de software: $ 0

Sobre costos de RRHH: no es costo adicional, es lo que costaría a la Organización en horas sueldos del Administrador de Red, el Técnico de Red y el Responsable de Sistemas de Información, si el proyecto se desarrollara íntegramente en horario laboral.

8.4 Cronograma de Actividades

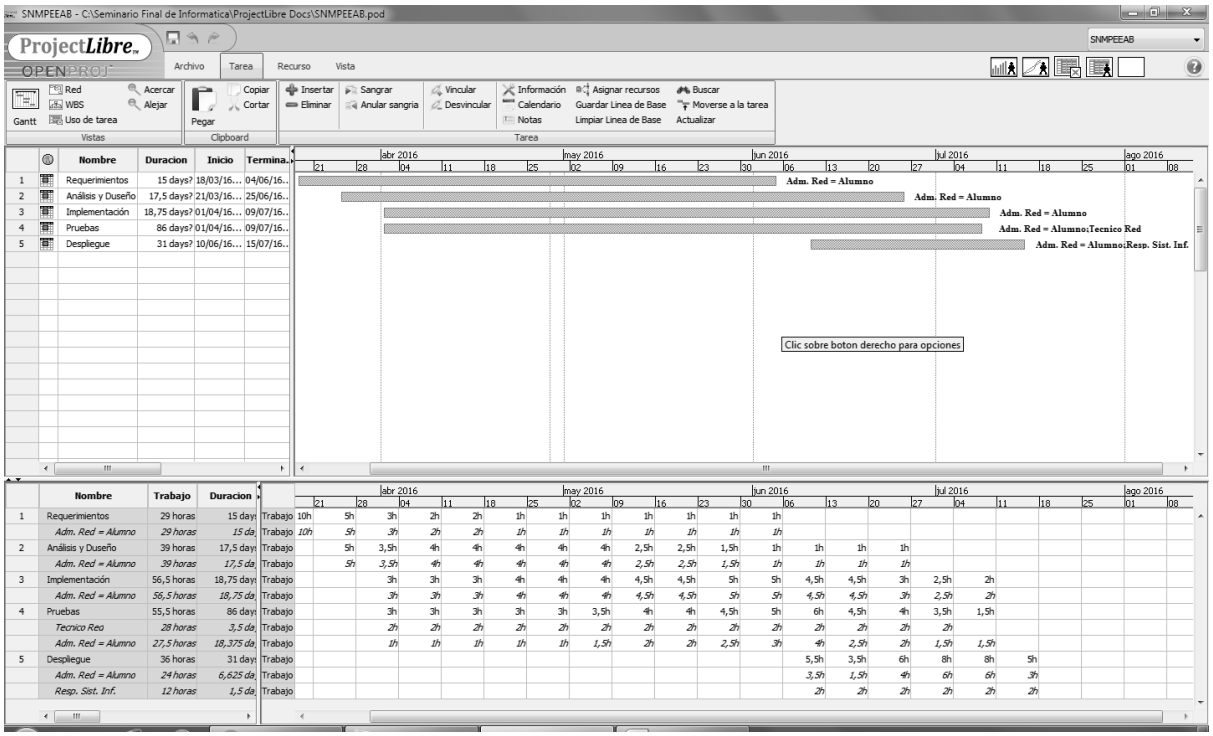


Figura 6. Cronograma de Actividades del Proyecto
ProjectLibre (versión 1.6.2) [software]

9. Desarrollo del Proyecto

9.1 Requerimientos Funcionales

1) Iniciar Sesión autenticando en Active Directory

   Descripción: el sistema debe permitir el inicio de sesión validando credenciales de usuario y contraseña del Active Directory del dominio corporativo del cliente. En caso que el servicio de AD no responda y el usuario que intenta ingresar sea un administrador de red registrado en el sistema, deberá permitir el ingreso validando una clave de la propia aplicación.

   Prioridad: crítico

2) Asignar un perfil al usuario que inició sesión

   Descripción: el sistema debe asignarle un perfil al usuario que ha iniciado sesión, pudiendo ser de tres tipos: Administrador de Red, Técnico de Red o Usuario. El perfil de usuario dispondrá únicamente de la funcionalidad de ver la falla y el alcance del incidente, el Administrador y el Técnico de Redes dispondrán de la funcionalidad

completa del sistema (se registran con perfiles distintos sólo para posibles requerimientos futuros).

Prioridad: crítico

3) Administración de datos

Descripción: el sistema debe permitir el agregado, la consulta, la modificación, el marcado como eliminado (eliminación lógica) y el listado de datos de:

   a. Usuarios
   b. Activos de red
   c. Dependencia funcional de los activos.
   d. Tipos de activos
   e. Tipos de troncales
   f. Lugar (ubicación de activos)
   g. Edificios
   h. Áreas
   i. Unidades
   j. VLANs
   k. Redes

Prioridad: crítico

4) Configurar opciones para el monitoreo y para la aplicación

Descripción: el sistema debe permitir la configuración de opciones de monitoreo tales como tiempos entre ejecución, comunidades SNMP, protocolos y puertos; y de la aplicación tales como datos del dominio corporativo de la empresa, dirección de email específica de apertura de tickets, envío de emails a administradores de red o declaración automática de incidentes en el Sistema de Gestión.

Prioridad: crítico

5) Obtener y mostrar de forma gráfica el estado de funcionamiento de los activos de red

Descripción: el sistema debe obtener y mostrar de forma gráfica el estado de funcionamiento y de conectividad de los activos de red. El sistema deberá actualizar el estado a intervalos regulares de tiempo. La interfaz debe tener en cuenta la dependencia funcional de los activos. Ante la detección de un incidente, deberá realizar la acción configurada para comunicar incidentes: sólo visualización gráfica, enviar emails a los administradores de red o declarar automáticamente un incidente en

el sistema de gestión de incidentes de la organización (las últimas dos opciones incluyen la primera).

Prioridad: crítico

6) Recibir traps de los Agentes SNMP

   Descripción: el sistema deberá recibir los traps enviados desde los agentes SNMP, procesarlos y resaltar el activo que lo ha generado. El sistema deberá facilitar la lectura del trap recibido y resaltar los traps que informen sobre problemas de funcionamiento que impliquen la pérdida de conectividad de un activo.

7) Habilitar y deshabilitar modo monitoreo

   Descripción: el sistema debe permitir a los usuarios con perfil de administradores/técnicos de red, que habiliten o deshabiliten el modo monitoreo de la red.

   Prioridad: importante

8) Habilitar y deshabilitar el modo "en seguimiento" de un activo

   Descripción: el sistema deberá permitir habilitar o deshabilitar el modo "en seguimiento" de un activo, a los usuarios con perfil de administrador/técnico de red. Este modo permite que si durante el monitoreo o en la recepción de un trap, se informa de un incidente que se produjo en un activo declarado en seguimiento, se forzará el envío de un email a los administradores de red independientemente de cualquier otro valor de configuración.

   Prioridad: importante

9) Declarar un incidente manualmente (enviar email al Sistema de Gestión de Incidentes)

   Descripción: el sistema deberá permitir a un usuario que posea perfil de administrador o técnico de red, seleccionar un activo que presente fallas y declarar de forma manual un Incidente enviando un email al Sistema de Gestión de Incidente con el objetivo de abrir un nuevo ticket de asistencia.

   Prioridad: importante

10) Reportes de estado de funcionamiento de activos y traps recibidos

    Descripción: el sistema deberá listar, según distintos criterios de selección, los estados de funcionamiento de los activos de red almacenados durante los monitoreos y los traps recibidos.

    Prioridad: secundario

9.2 Requerimientos No Funcionales

a) Del Producto

1. Confiabilidad

   Descripción: debe ser tolerante a fallos y de fácil recuperación. No debe haber pérdida de información.

   Importancia: alta
2. Disponibilidad

   Descripción**:** debe estar disponible en todo momento, las 24 hs del día y los 7 días de la semana.

   Importancia**:** alta
3. Usabilidad

   Descripción: debe tener interfaces sencillas, de fácil lectura, comprensión y navegabilidad. No más de dos clicks para obtener la información del funcionamiento y no más de tres para ver detalles del activo.

   Importancia: alta
4. Performance

   Descripción: el tiempo de respuesta de la aplicación será insignificante ya que dependerá muchísimo de la performance de la red en el momento de su utilización. Será de baja utilización de recursos, tanto de procesamiento, como de disco y memoria.

   Importancia: media
5. Portabilidad

   Descripción**:** debe poder ser utilizado desde cualquier navegador Web convencional

   Importancia**:** media

b) Organizacionales

1. De Políticas y Procedimientos existentes

   Descripción**:** debe respetar los lineamientos sobre el desarrollo de sitios web que define la Gerencia de Comunicaciones, la identidad visual y las Políticas de TI de la Organización.

   Importancia**:** alta

c) De Implementación

1. Software de bases de datos

   Descripción: el software de base de datos a utilizar debe ser PostGreSQL, MySQL o SQL Server Express, ya que son los gestores de bases de datos implementados por el grupo “Sistemas de Información” y disponibles en los servidores de la organización.

   Importancia: alta

2. Lenguaje de Programación

   Descripción: el lenguaje de programación a utilizar debe ser JAVA o ASP.NET, ya que son los lenguajes utilizados por el grupo “Sistemas de Información” para desarrollo de aplicaciones.

   Importancia: alta

9.3 Diagrama de Caso de Uso

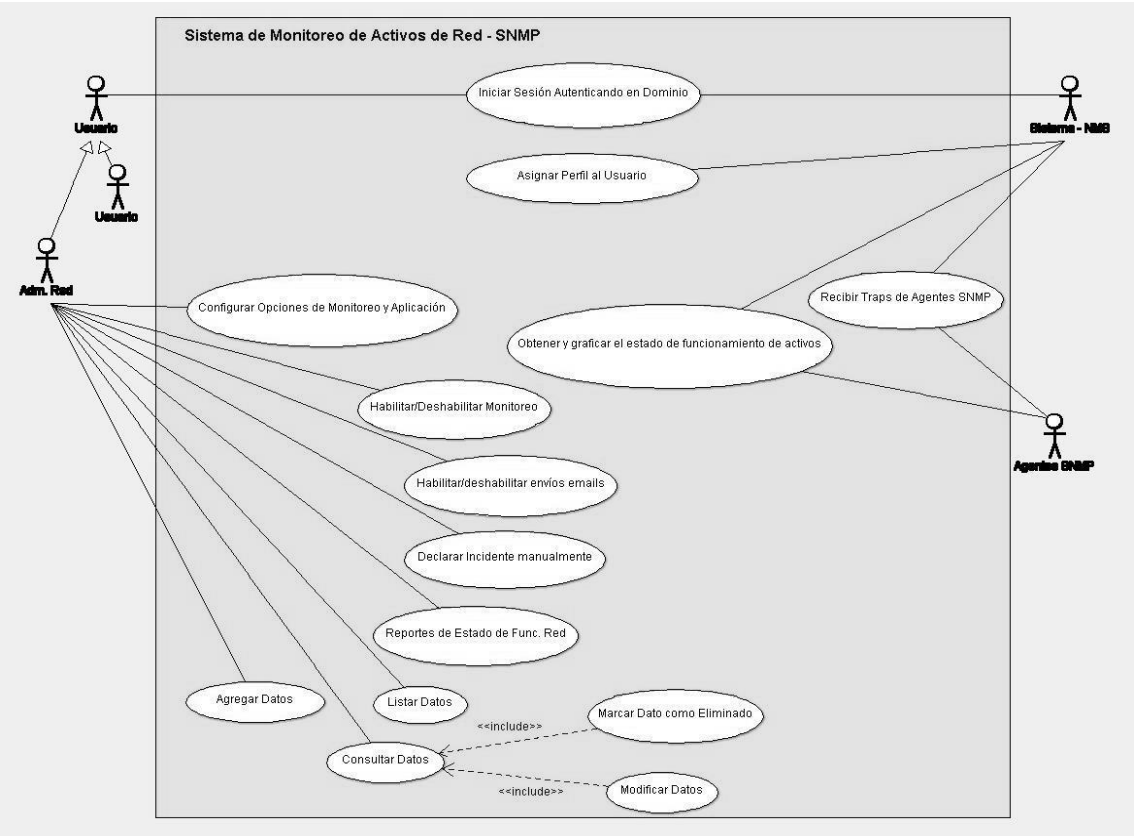


Figura 7. Diagrama de Casos de Uso

9.4 Listado de Actores

Usuario

Nombre: Usuario
Descripción: es el usuario antes de que se le asigne un perfil, es quien intenta abrir una sesión para utilizar la aplicación.
Rol: depende del perfil que el sistema le asigne.

Administradores y/o Técnicos de Redes

Nombre: Adm. Red
Descripción: usuario con perfil de Administrador de Red o Técnicos de Redes, ambos se unifican bajo el nombre "Adm. Red" ya que tendrán los mismos accesos y privilegios dentro de la aplicación.
Rol: Pueden realizar todas las funciones disponibles de la aplicación.

Usuario de Red

Nombre: Usuario de Red
Descripción: usuario con perfil de Usuario de la Red, es un usuario sin privilegios que utiliza los recursos de la red
Rol: sólo podrán ver dónde se produjo la falla y su alcance.

Sistema

Nombre: Sistema
Descripción: es la aplicación.

Network Management System

Nombre: NMS
Descripción: también es la aplicación pero cuando está cumpliendo funciones de NMS del protocolo SNMP.
Rol: es quien realiza todos los procesos de envío de solicitudes a los agentes SNMP y escucha sus respuestas, como así también sus traps.

Agentes SNMP

Nombre: Agentes SNMP
Descripción: son las porciones de software instalados en los dispositivos con funciones del protocolo SNMP
Rol: se comunican con los NMS, procesan sus solicitudes y envían respuestas y también envían traps por cuenta propia ante la ocurrencia de un suceso fuera de lo normal.

9.5 Casos de Uso

9.5.1 Caso de Uso 1: Iniciar Sesión en Active Directory

Tabla 7.
Caso de Uso 1

Identificación	01 - CU_SesionInAD
Nombre	Iniciar Sesión Autenticando en AD
Descripción:	
Permite ingresar a la aplicación validando las credenciales de usuario (nombre de usuario y contraseña) en el Active Directory del dominio corporativo. En caso que el servicio de AD no responda y el usuario que intenta ingresar sea un administrador de red registrado en el sistema, debe permitir el ingreso validando una clave de la propia aplicación.	
Actores:	
Usuario Sistema	
Pre-condición:	
El usuario que ingresa a la aplicación debe poseer un usuario de AD del dominio corporativo o debe estar registrado como un administrador/técnico de red y conocer la clave de su usuario en la aplicación	
Post-condición:	
Credenciales validadas Sesión iniciada	
Flujo Normal:	
1. Usuario: ingresa al sistema mediante un explorador web. 2. Sistema: presenta la pantalla de inicio de sesión que requiere el ingreso por teclado de un nombre de usuario de AD y su contraseña. 3. Usuario: ingresa ambos datos y presiona “Iniciar Sesión”. 4. Sistema: recupera datos del dominio y del servidor controlador de dominio almacenados en la Tabla Opciones de la Base de Datos. 5. Sistema: envía a validar las credenciales al servicio de AD, está disponible y las credenciales ingresadas son válidas. 6. Sistema: crea una sesión web y se la asigna al usuario. 7. CU_AsignarPerfil	
Flujo Alternativo:	
5.1 Sistema: El servicio de AD está disponible pero las credenciales NO son válidas. Ya sea que el usuario no existe o la contraseña sea incorrecta, el sistema arrojará el error “Usuario y Clave NO son válidos”, blanquea campos de usuario y contraseña. Vuelve a paso 2. 5.2 Sistema: El servicio de AD no responde en tiempo y forma. Independientemente que el servicio no funcione o no sea alcanzable por el sistema por un problema de red: 5.2.1 Sistema: busca en la base de datos de usuarios y lo encuentra, por lo tanto es un usuario con perfil de administrador de red o técnico de red 5.2.1.1 Sistema: solicita una clave propia de la aplicación para ese usuario. 5.2.1.1.1 La clave del usuario en la aplicación es correcta, sigue paso 6. 5.2.1.1.2 La clave del usuario en la aplicación es incorrecta, arroja el error “Clave de Aplicación NO Válida” y vuelve a paso 2. 5.2.2 Sistema: busca en la base de datos de usuarios y NO lo encuentra, por lo tanto es un usuario común. Vuelve a paso 2.	

Diagramas de Secuencia

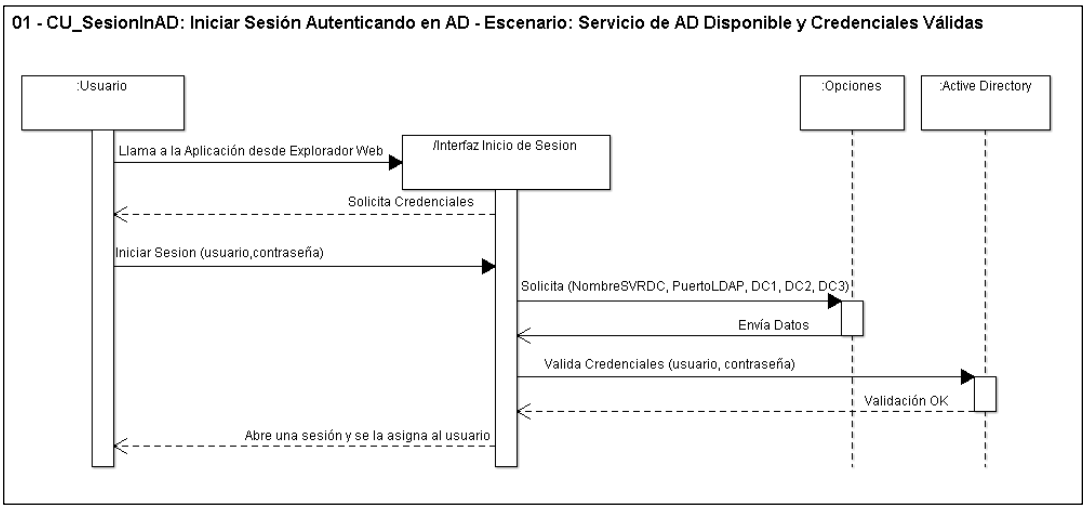


Figura 8. Diagrama de Secuencia Caso de Uso 1 – Escenario 1

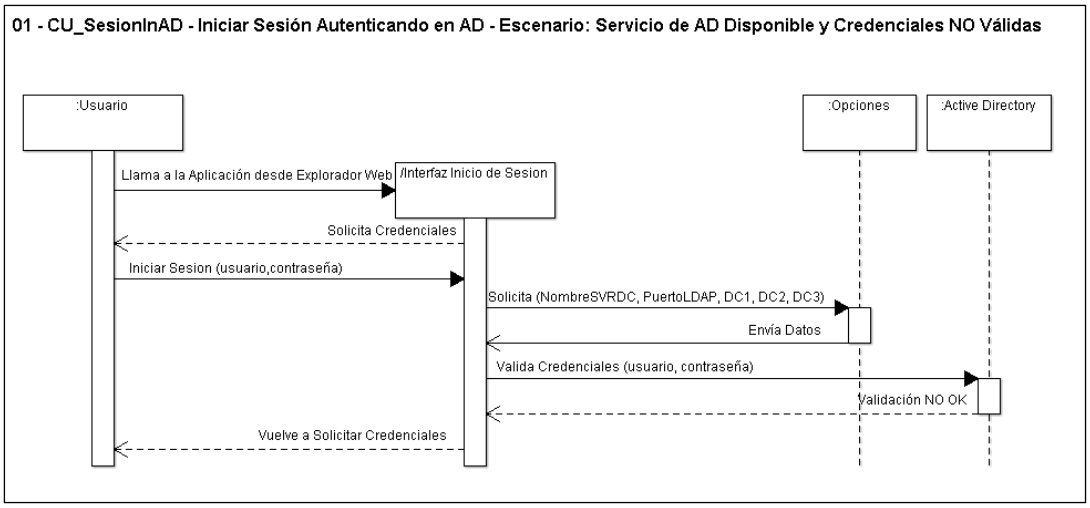


Figura 9. Diagrama de Secuencia Caso de Uso 1 – Escenario 2

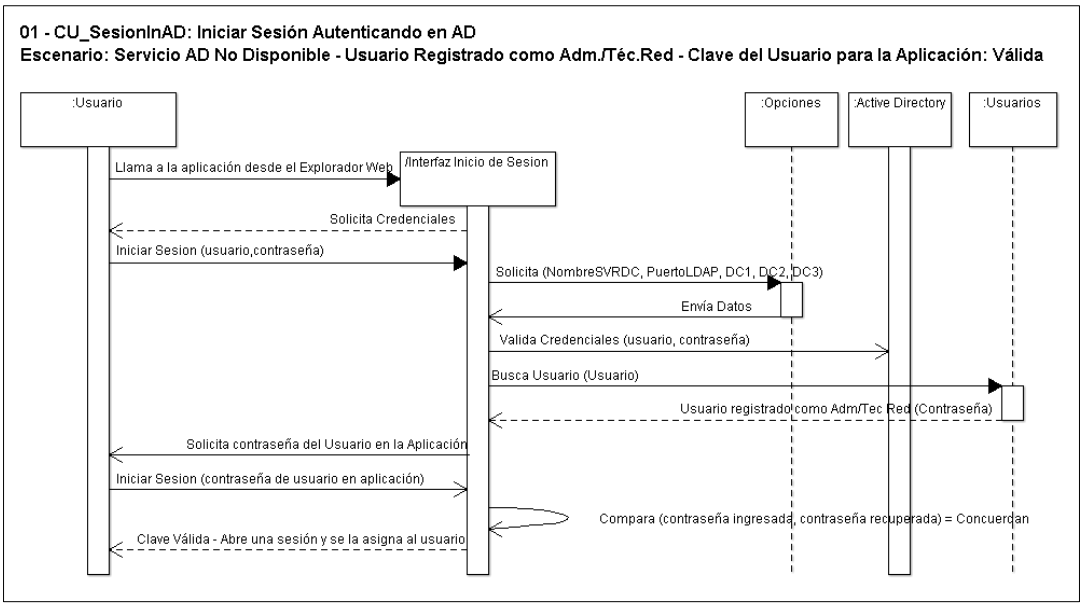


Figura 10. Diagrama de Secuencia Caso de Uso 1 – Escenario 3

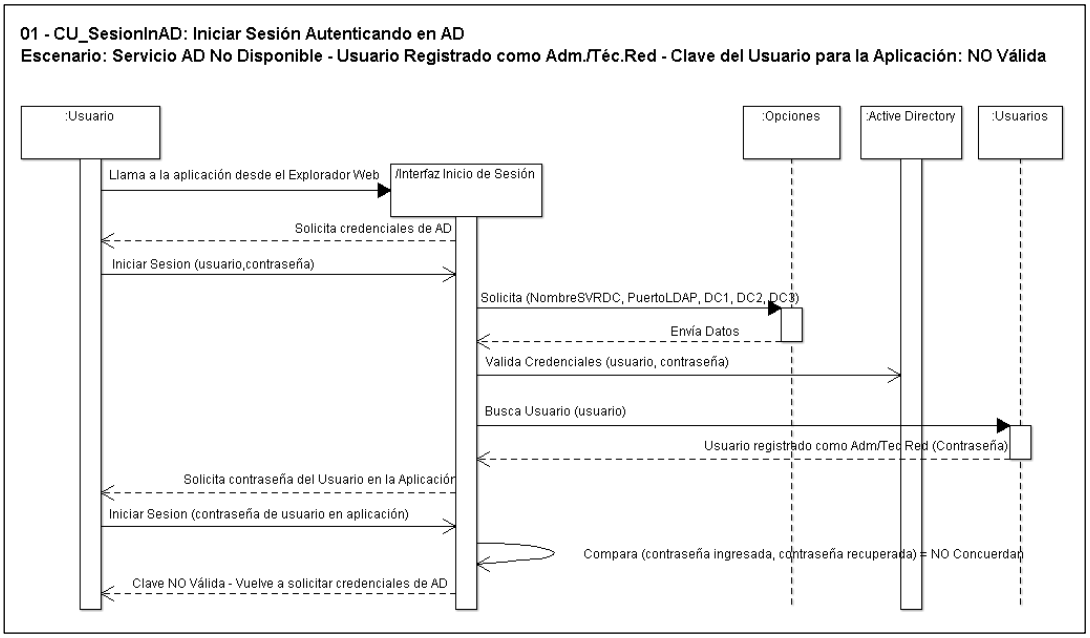


Figura 11. Diagrama de Secuencia Caso de Uso 1 – Escenario 4

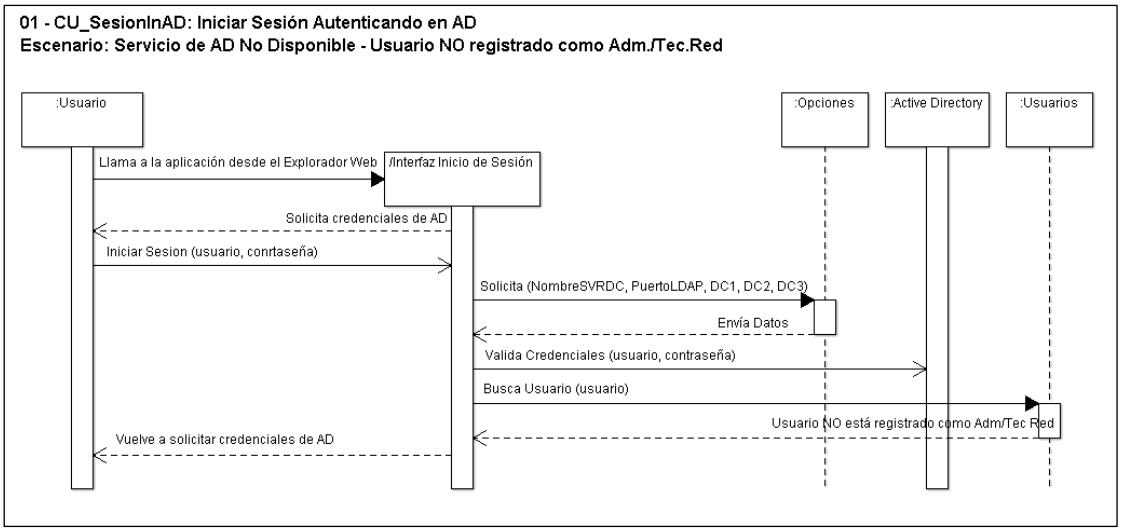


Figura 12. Diagrama de Secuencia Caso de Uso 1 – Escenario 5

Diagrama de Colaboración

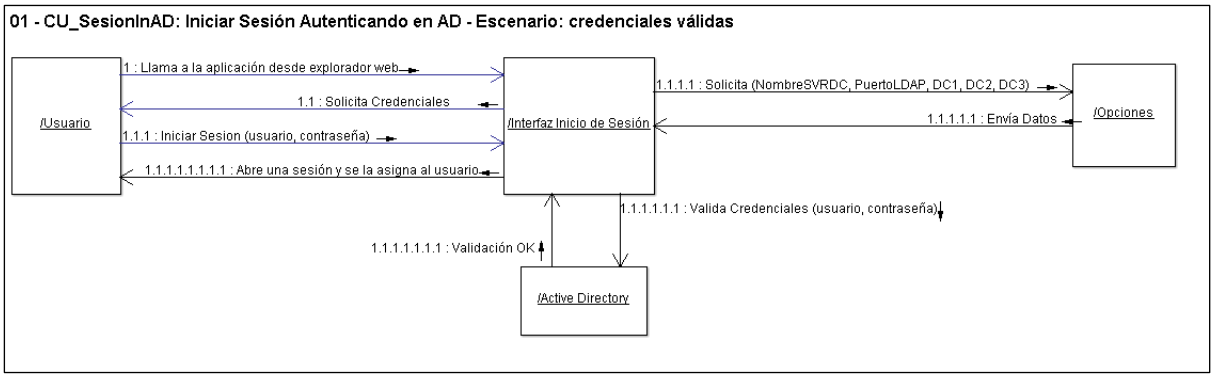


Figura 13. Diagrama de Colaboración Caso de Uso 1 – Escenario 1

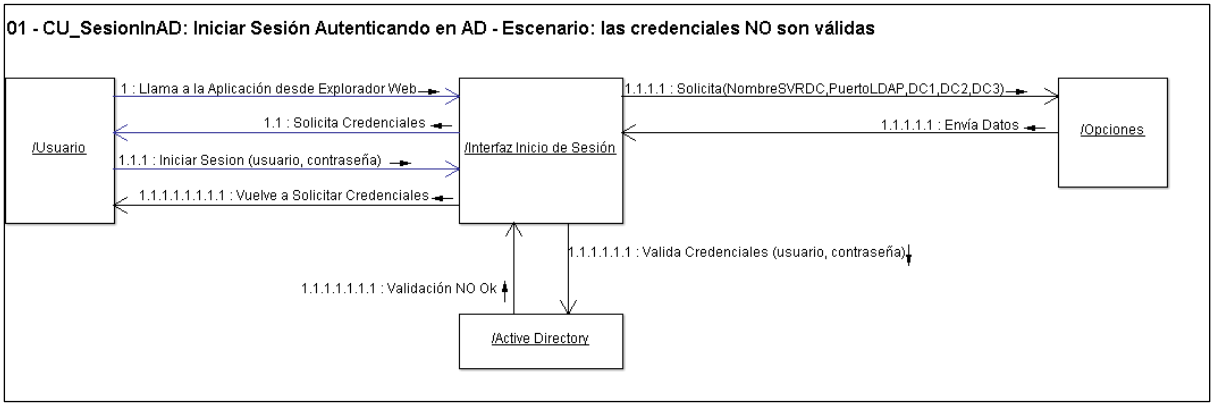


Figura 14. Diagrama de Colaboración Caso de Uso 1 – Escenario 2

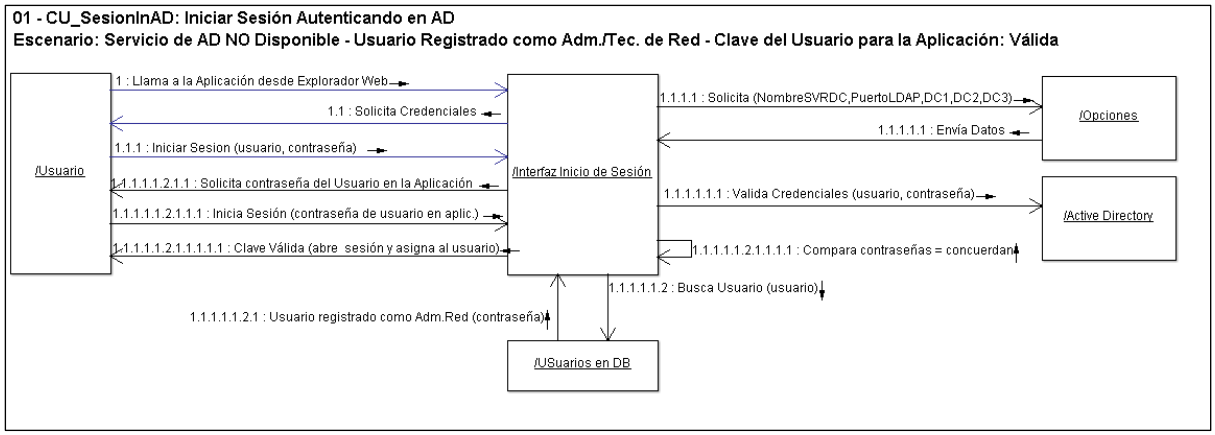


Figura 15. Diagrama de Colaboración Caso de Uso 1 – Escenario 3

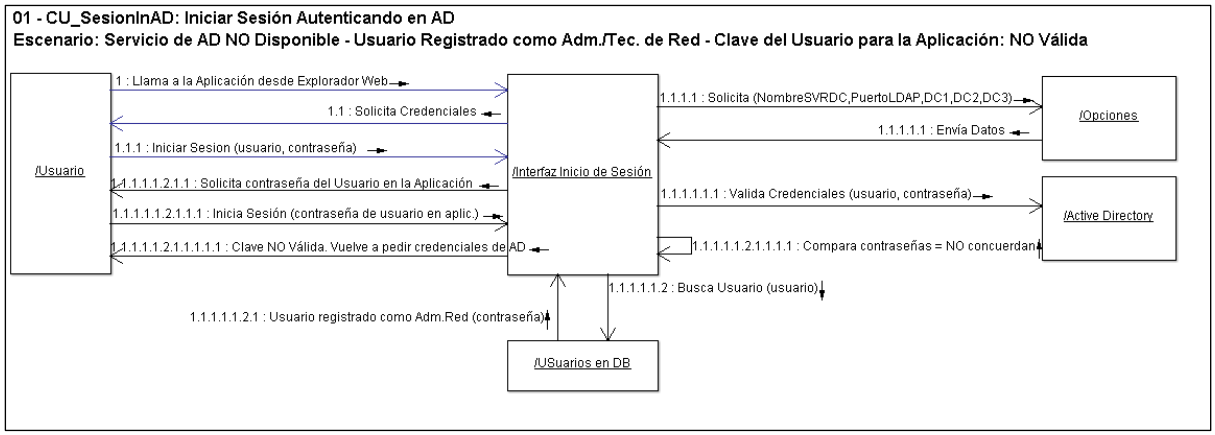


Figura 16. Diagrama de Colaboración Caso de Uso 1 – Escenario 4

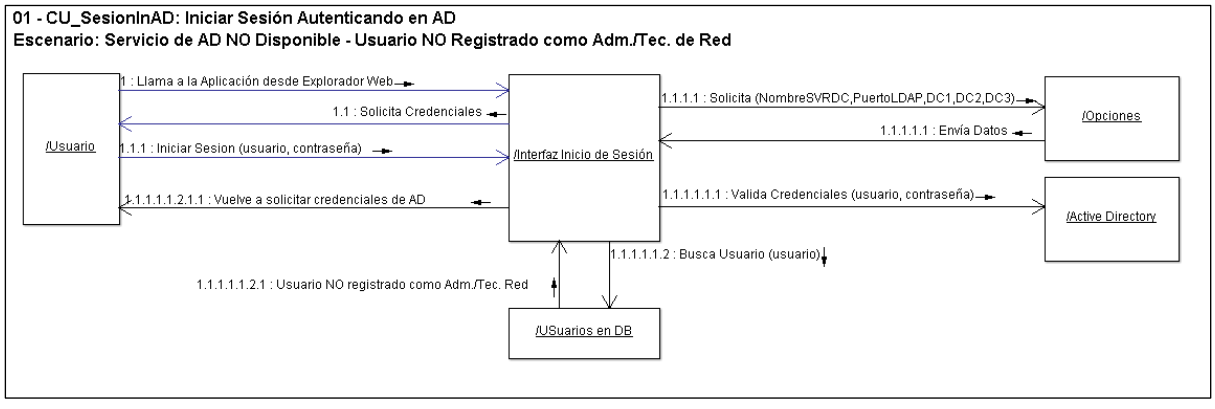


Figura 17. Diagrama de Colaboración Caso de Uso 1 – Escenario 5

Interfaz Inicio de Sesión

Figura 18. Interfaz de inicio de sesión

9.5.2 Caso de Uso 2: Asignar Perfil al Usuario

Tabla 8.
Caso de Uso 2

Identificación	02 - CU_AsignarPerfil
Nombre	Asignar Perfil al Usuario
Descripción:	
De acuerdo al usuario que inicie sesión, se le asigna el perfil de Adm. de Red o Técnico de Red (disponen de la funcionalidad completa del sistema) o de Usuario de Red (sólo dispondrá de la funcionalidad de ver la falla y el alcance del incidente).	
Actores:	
Sistema	
Pre-condición:	
Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD	
Post-condición:	
Perfil de usuario asignado Estructura de almacenamiento creada Interfaz con el menú que corresponda según el perfil asignado al usuario y mostrando el estado de funcionamiento de los activos y su dependencia funcional Modo Monitoreo ACTIVO	
Flujo Normal:	
1. Sistema: busca si el usuario que acaba de iniciar sesión está registrado como Administrador o Técnico de Red 2. Sistema: el usuario está registrado, es un Administrador o Técnico de Red, por lo que le corresponde el menú de Administrador de Red. 3. Sistema: registra el acceso del usuario a la aplicación 4. Sistema: recorre todos los activos y la dependencia funcional de los mismos para armar la estructura de almacenamiento de datos. 5. Sistema: muestra cada activo con su dependencia funcional marcado con Estado “Desconocido”. 6. Sistema: establece y muestra en la interfaz que el modo monitoreo está ACTIVO 7. CU_EstadoRed	
Flujo Alternativo:	
2.1 Sistema: el usuario NO está registrado como Administrador o Técnico de Red, entonces se trata de un usuario común, por lo que le corresponde el menú de Usuario. Continúa en 3.	

Diagramas de Secuencia

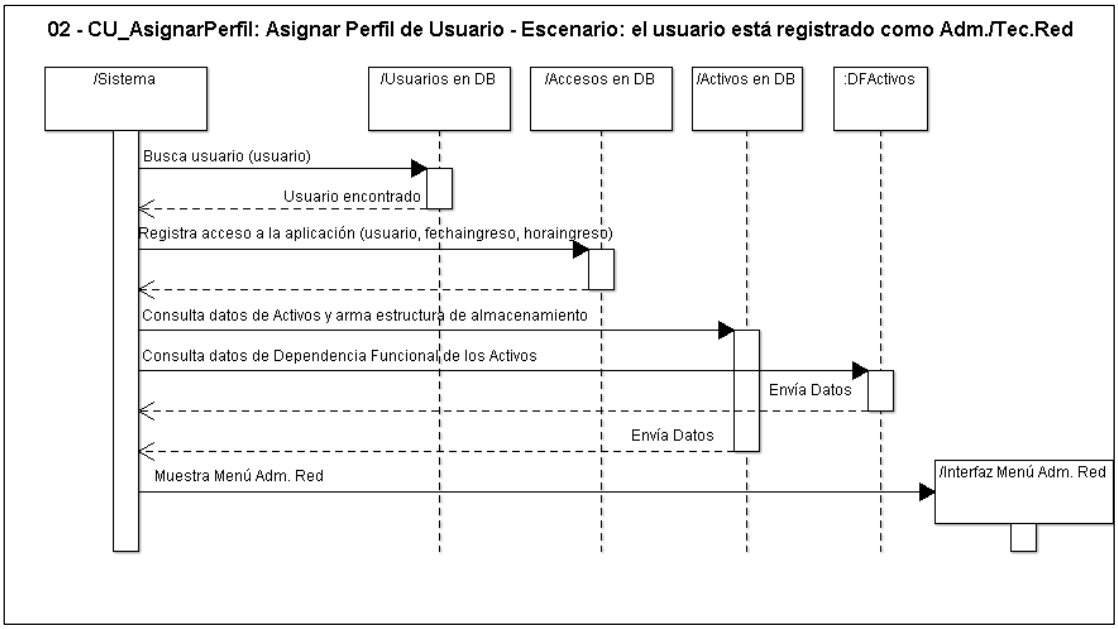


Figura 19. Diagrama de Secuencia de Caso de Uso 2 – Escenario 1

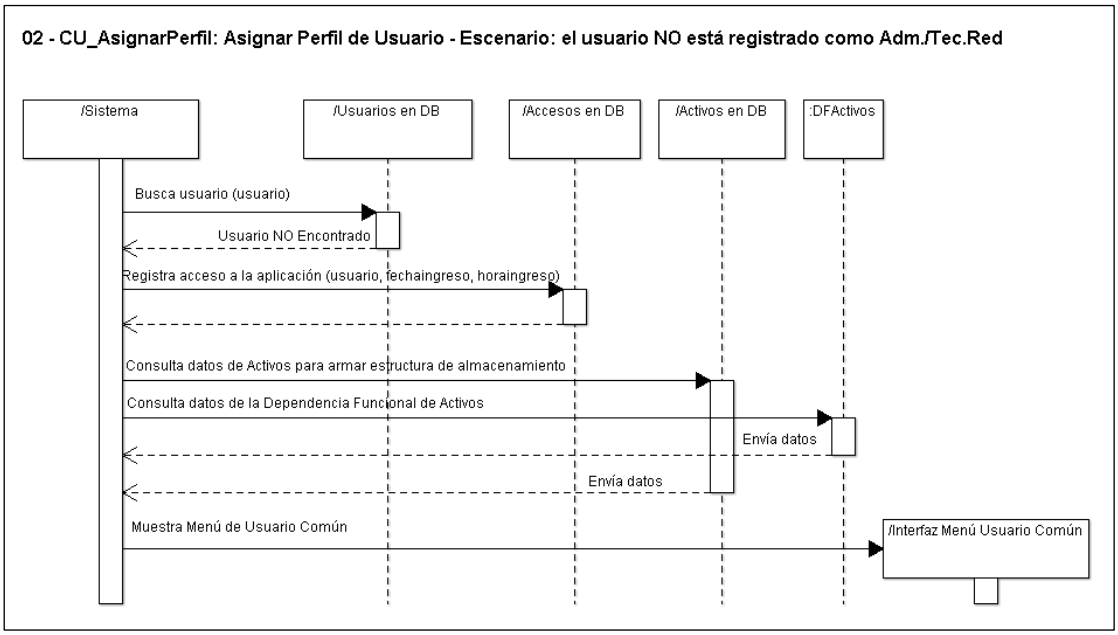


Figura 20. Diagrama de Secuencia de Caso de Uso 2 – Escenario 2

Diagrama de Colaboración

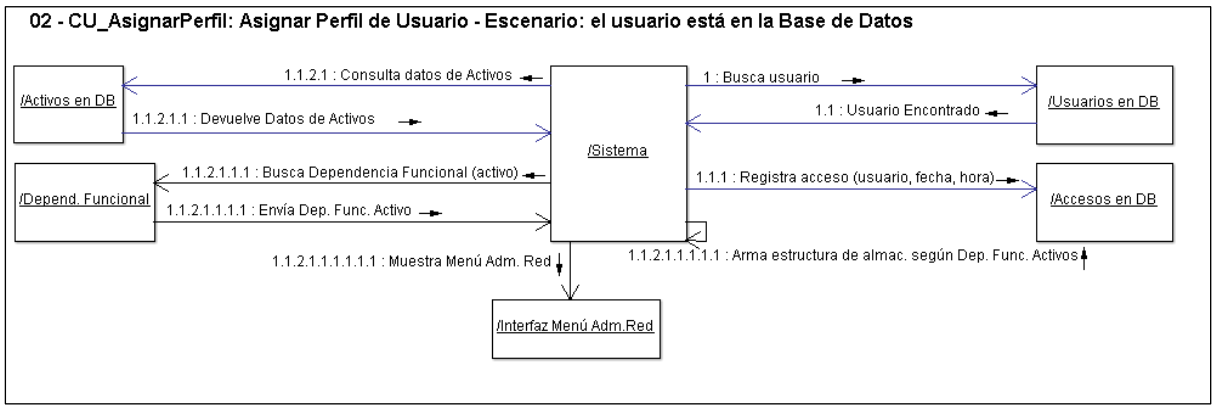


Figura 21. Diagrama de Colaboración de Caso de Uso 2 – Escenario 1

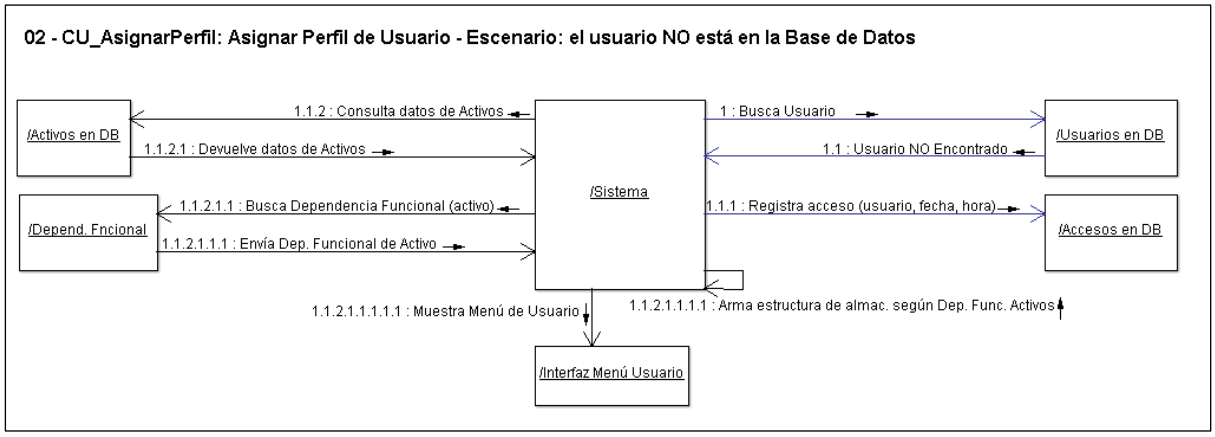


Figura 22. Diagrama de Colabración de Caso de Uso 2 – Escenario 2

Interfaz “Menú Administrador de Red”

Figura 23. Interfaz Menú Administrador de Red

9.5.3 Caso de Uso 3

9.5.3.1 Caso de Uso 3a: Agregar Registros (genérico)

Tabla 9.
Caso de Uso 3a

Identificación	03a - CU_AltaReg
Nombre	Agregar Registros
Descripción:	
Permite agregar un registro en una tabla de una base de datos. Es un modelo genérico que se usa para agregar registros en las tablas de: usuarios, activos de red, dependencia funcional de los activos, tipos de activos, tipos de troncales, tipos de puertos, lugar (ubicación de activos), edificios, áreas, unidades, vlans y redes.	
Actores:	
Adm. Red Sistema	
Pre-condición:	
Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD El usuario de la aplicación debe poseer un perfil de Adm. de Red	
Post-condición:	
Registro agregado	
Flujo Normal:	
1. Adm. Red: solicita la opción "ABM". 2. Sistema: muestra el formulario con los campos y habilita su edición. En ciertos campos, el sistema recupera desde la base de datos los posibles valores que pueden tomar y los ofrece como opción de selección. 3. Adm. Red: completa los datos y presiona "Agregar" 4. Sistema: controla datos requeridos, realiza la validación y consistencia de los datos ingresados 5. Sistema: agrega el registro en la base de datos. Muestra el mensaje "Registro Agregado" 6. Fin	
Flujo Alternativo:	
4.1 Sistema: no se ingresaron todos los datos requeridos, el sistema muestra el aviso "Faltan completar datos requeridos" y devuelve el control al formulario, continúa en paso 3 4.2 Sistema: los valores ingresados no superan la validación, el sistema da aviso y devuelve el control al formulario, continúa en paso 3 4.3 Sistema: los valores ingresados son inconsistentes, el sistema da aviso y devuelve el control al formulario, continúa en paso 3 Nota: En caso que se estén realizando altas en las tablas de Activos y Dependencia Funcional de Activos, y el Estado del Monitoreo sea "ON", el sistema deberá mostrar el mensaje "Monitoreo Detenido", detener el monitoreo y poner el temporizador en cero. Los activos conservarán el último estado obtenido.	

Diagrama de Secuencia

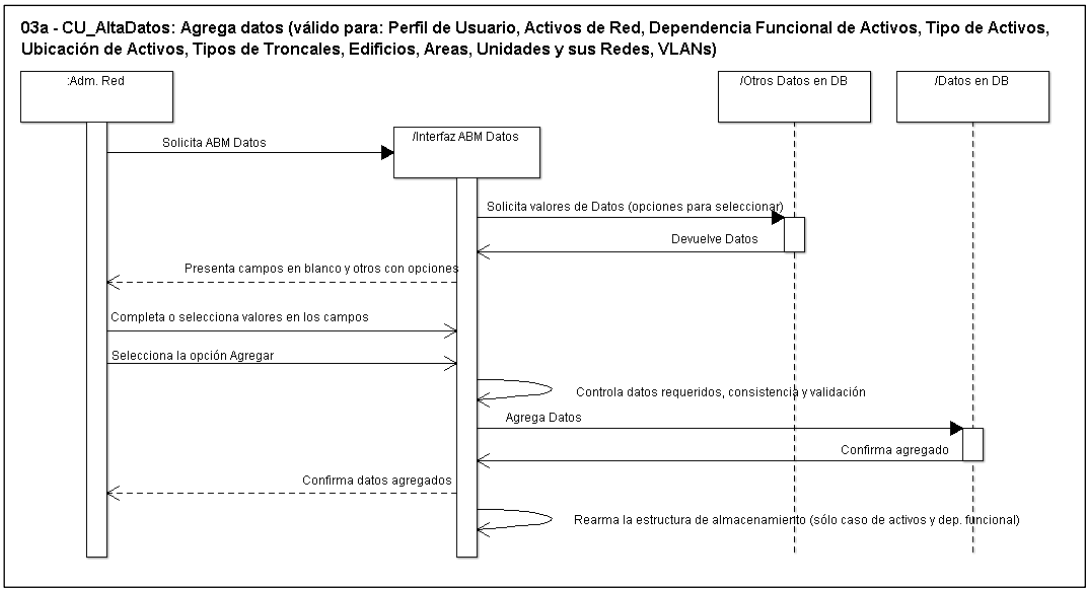


Figura 24. Diagrama de Secuencia de Caso de Uso 3a

9.5.3.2 Caso de Uso 3b: Consulta de Registros (genérico)

Tabla 10.
Caso de Uso 3b

Identificación	03b - CU_ConsultaReg
Nombre	Consultar un Registro
Descripción:	
Permite realizar la consulta de un registro almacenado en una tabla. Es un modelo genérico que se usa para consultar registros de las tablas: usuarios, activos de red, dependencia funcional de los activos, tipos de activos, tipos de troncales, tipos de puertos, lugar (ubicación de activos), edificios, áreas, unidades, vlans y redes.	
Actores:	
Adm. Red Sistema	
Pre-condición:	
Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD El usuario de la aplicación debe poseer un perfil de Adm. de Red	
Post-condición:	
Datos presentados en los campos del formulario con los datos que se han recuperado desde la base de datos	
Flujo Normal:	
1. Adm. Red: solicita la opción “ABM”. 2. Sistema: muestra el formulario con los campos y habilita su edición. En ciertos campos, el sistema recupera desde la base de datos los posibles valores que pueden tomar y los ofrece como opción de selección. 3. Adm. Red: completa el campo de búsqueda 4. Adm. Red: selecciona la opción “Consultar” 5. Sistema: realiza la búsqueda con el valor del campo indicado 6. Sistema: encuentra en la tabla el registro que coincida con el criterio de búsqueda y presenta los datos recuperados en los campos del formulario 7. Fin	
Flujo Alternativo:	
6.1 Sistema: no encuentra en la tabla un registro que coincida con el criterio de búsqueda, muestra el aviso “NO se encontraron registros”. Fin	

Diagrama de Secuencia

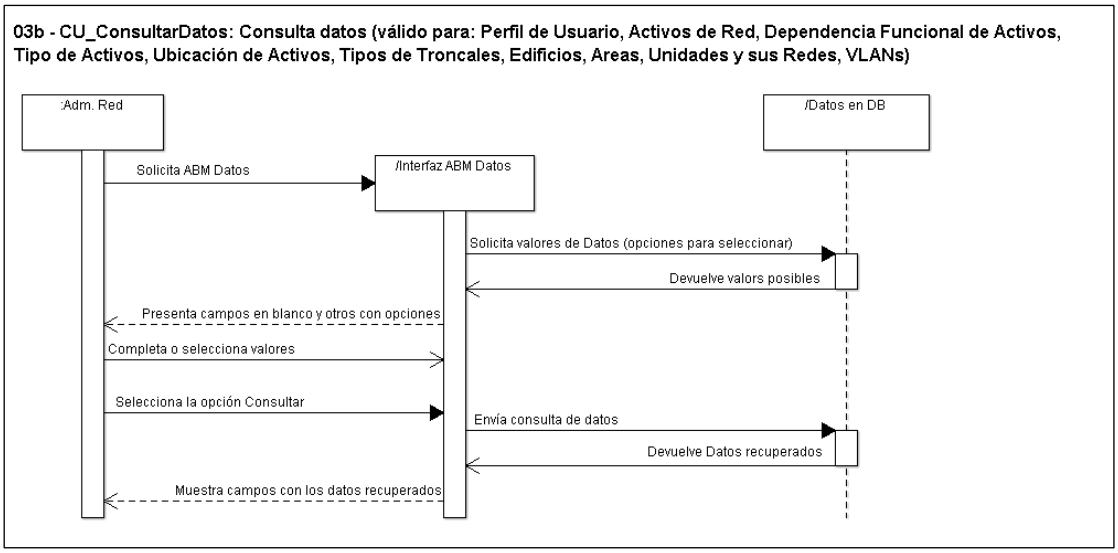


Figura 25. Diagrama de Secuencia de Caso de Uso 3b

9.5.3.3 Caso de Uso 3c: Modificar Registros (genérico)

Tabla 11.
Caso de Uso 3c

Identificación	03c - CU_ModificarReg
Nombre	Modificar Registros
Descripción:	
Permite realizar la modificación de los datos de un registro almacenado en una tabla. Es un modelo genérico que se usa para modificar registros de las tablas: usuarios, activos de red, dependencia funcional de los activos, tipos de activos, tipos de troncales, tipos de puertos, lugar (ubicación de activos), edificios, áreas, unidades, vlans y redes.	
Actores:	
Adm. Red Sistema	
Pre-condición:	
Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD El usuario de la aplicación debe poseer un perfil de Adm. de Red Debe haberse ejecutado exitosamente el Caso de Uso 03b - CU_ConsultaReg	
Post-condición:	
Registro almacenado modificado	
Flujo Normal:	
1. Adm. Red: completa los campos descriptivos y selecciona “Modificar” 2. Sistema: controla que en los campos requeridos se hayan ingresado valores 3. Actualiza el registro en la tabla de la base de datos y muestra el mensaje “Datos Actualizados” 4. Fin	
Flujo Alternativo:	
2.1 Sistema: falta completar el valor de un campo requerido. Muestra el mensaje de error “Dato Requerido Faltante” y vuelve al paso 1. 3.1 Sistema: se produjo un error en la actualización. Muestra mensaje de error y vuelve al paso 1. Nota: En caso que se estén realizando modificaciones en las tablas de Activos y Dependencia Funcional de Activos, y el Estado del Monitoreo sea “ON”, el sistema deberá mostrar el mensaje “Monitoreo Detenido”, detener el monitoreo y poner el temporizador en cero. Los activos conservarán el último estado obtenido.	

Diagrama de Secuencia

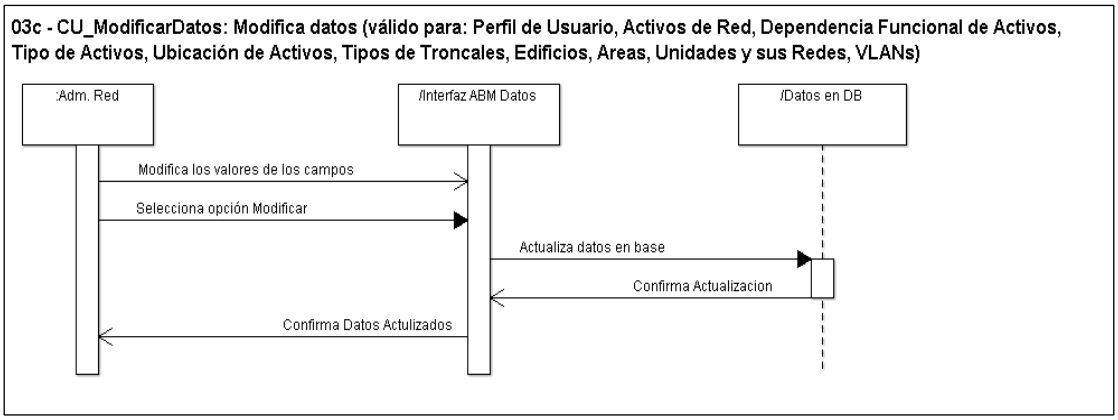


Figura 26. Diagrama de Secuencia de Caso de Uso 3c

9.5.3.4 Caso de Uso 3d: Marcar Registro como Eliminado – Eliminación lógica (genérico)

Tabla 12.
Caso de Uso 3d

Identificación	03d - CU_EliminarReg
Nombre	Marcar Registro como Eliminado (eliminación lógica)
Descripción:	
Permite marcar el registro de una tabla de una base de datos como eliminado. Es un modelo genérico que se usa para marcar registros como eliminados de las tablas: usuarios, activos de red, dependencia funcional de los activos, tipos de activos, tipos de troncales, tipos de puertos, lugar (ubicación de activos), edificios, áreas, unidades, vlans y redes.	
Actores:	
Adm. Red Sistema	
Pre-condición:	
Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD El usuario de la aplicación debe poseer un perfil de Adm. de Red Debe haberse ejecutado exitosamente el Caso de Uso 03b - CU_ConsultaReg	
Post-condición:	
Registro marcado como eliminado	
Flujo Normal:	
1. Adm. Red: selecciona “Marcar registro como eliminado ” 2. Sistema: solicita confirmación para que el registro sea marcado como eliminado 3. Adm. Red: confirma 4. Sistema: muestra el mensaje “Registro marcado como eliminado” y asigna el valor “verdadero” al campo “Eliminado” del registro 5. Fin	
Flujo Alternativo:	
3.1 Adm. Red: No Confirma. Sistema: no realiza acción y continúa en paso 5 Nota: En caso que se esté marcando como eliminado un registro de las tablas de Activos o Dependencia Funcional de Activos, y el Estado del Monitoreo sea “ON”, el sistema deberá mostrar el mensaje “Monitoreo Detenido”, detener el monitoreo y poner el temporizador en cero. Los activos conservarán el último estado obtenido.	

Diagrama de Secuencia

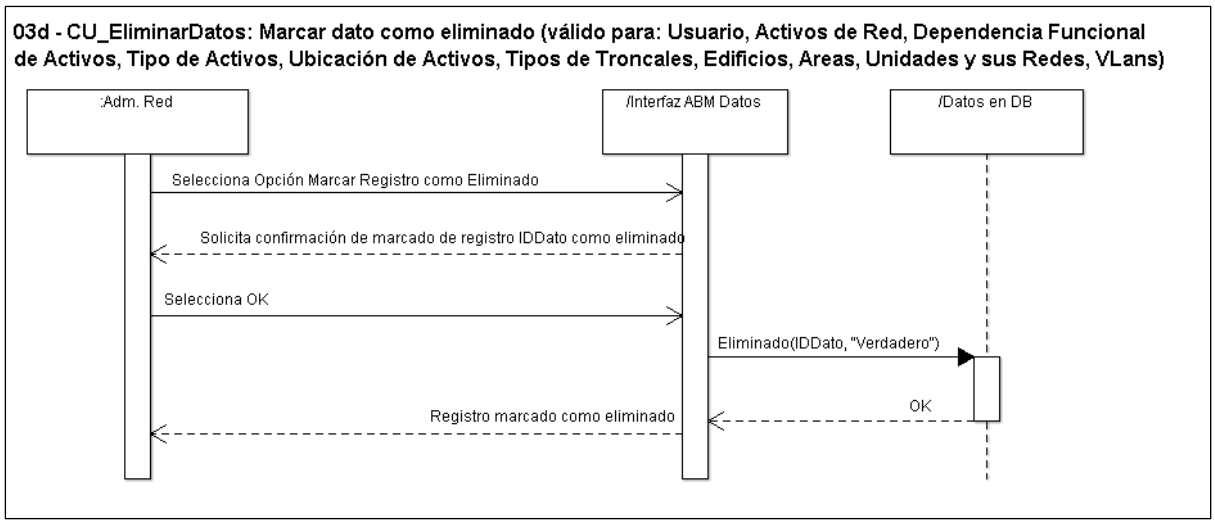


Figura 27. Diagrama de Secuencia de Caso de Uso 3d

9.5.3.5. Caso de Uso 3e: Listar Registros (genérico)

Tabla 13.
Caso de Uso 3e

Identificación	03e - CU_ListarReg
Nombre	Listar Registros
Descripción:	
Permite listar los registros recuperados desde una tabla de una base de datos. Es un modelo genérico que se usa para listar registros de las tablas: usuarios, activos de red, dependencia funcional de los activos, tipos de activos, tipos de troncales, tipos de puertos, lugar (ubicación de activos), edificios, áreas, unidades, vlans y redes.	
Actores:	
Adm. Red Sistema	
Pre-condición:	
Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD El usuario de la aplicación debe poseer un perfil de Adm. de Red	
Post-condición:	
Listado de registros formateados para impresión	
Flujo Normal:	
1. Adm. Red: selecciona “Listar” 2. Sistema: recupera los datos de la base de datos y lista los registros en una página nueva con un formato adecuado para impresión 3. Fin	
Flujo Alternativo:	
2.1 Sistema: no encuentra registros en la tabla para listar, muestra el mensaje “No se encontraron registros.”. Fin	

Diagrama de Secuencia

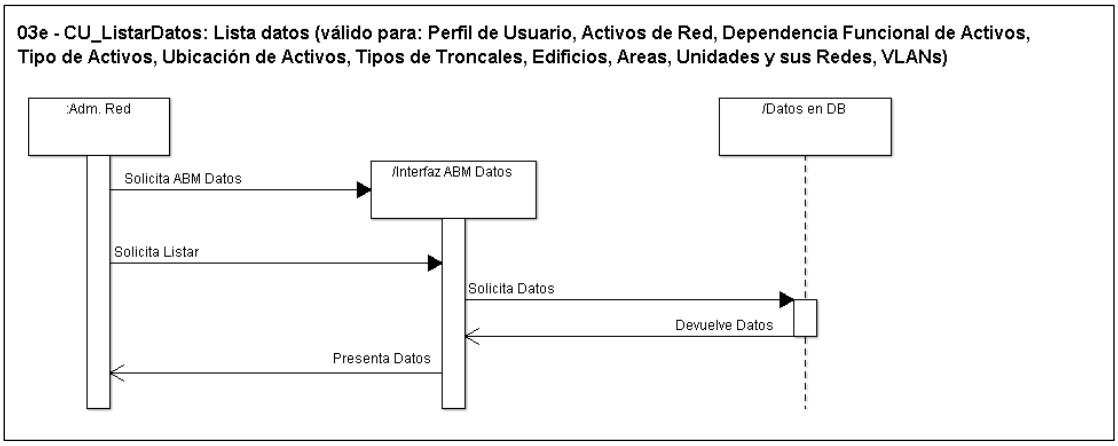


Figura 28. Diagrama de Secuencia de Caso de Uso 3e

Interfaz ABM Registros (algunos ejemplos)

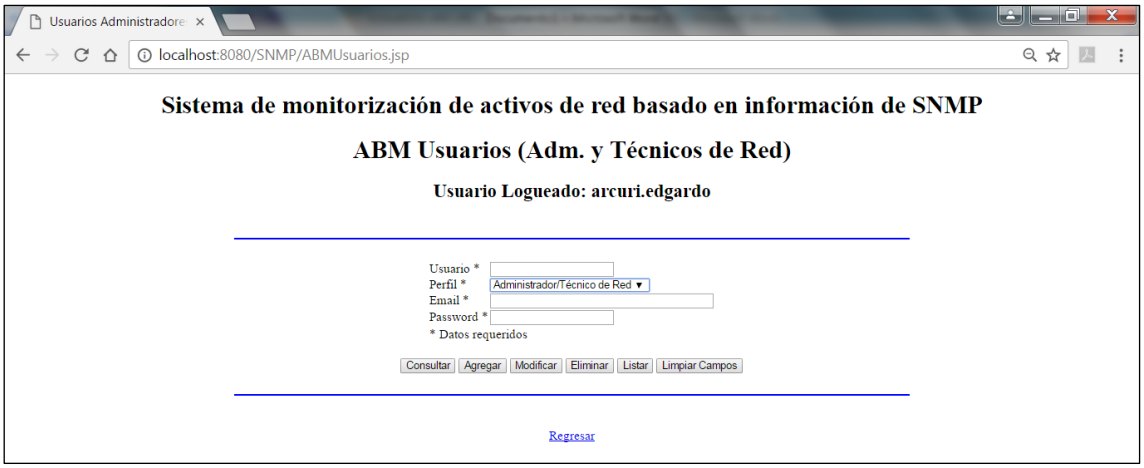


Figura 29. Interfaz Agregar, Consultar, Modificar y Listar Usuarios

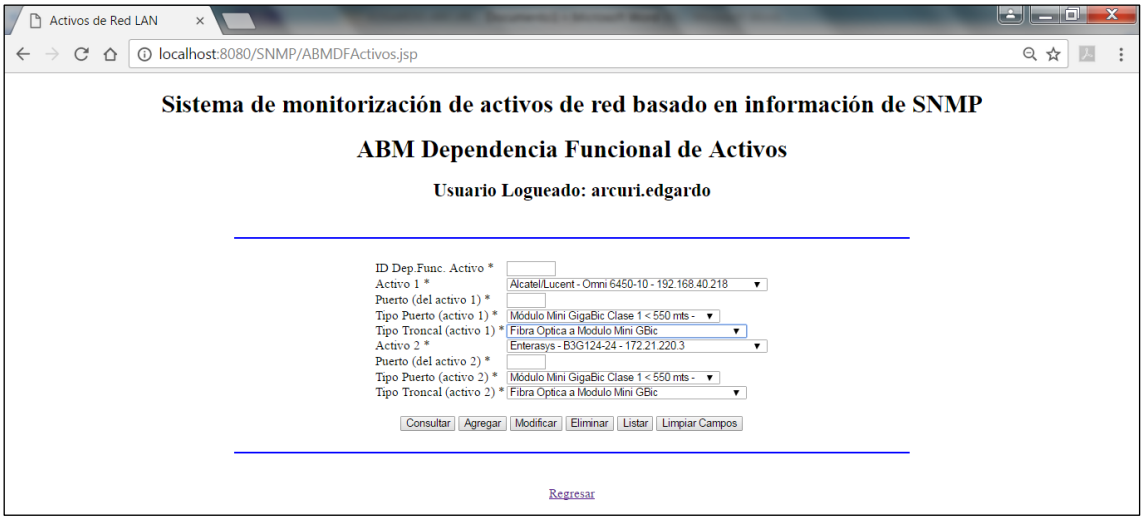


Figura 30. Interfaz Agregar, Consultar, Modificar y Listar Dep. Funcional de Activos

Id Lugar	Lugar	Id Edificio	Eliminado
1	Sala de Servidores	1	f
2	Ante Sala de Servidores	1	f
3	Laboratorio de Redes	1	f
4	Puerta Acceso Sala Servdores	1	f
5	Puerta de Entrada Edificio	1	f
6	Sala de Reuniones Informática	1	f
7	Salón de Actos	3	f
8	Sala de Reuniones Dirección	3	f
9	Rack de Comunicaciones	2	f
10	Pasillo Comunicaciones	2	f
11	Pasillo Contabilidad	3	f
12	Oficina Contabilidad	3	f
13	Oficina de Personal	3	f
14	Oficina de Patrimonio	3	f
15	Mesa de Entradas	3	f
16	Sec. Dirección	3	f
17	Dirección	3	f
18	INTEA S.A.	2	f
19	Oficina Tesoreria	3	f
20	Oficina Diseño Gráfico	2	f
21	Rack Fitotécnico (Galpón RRNN)	4	f
22	Oficina Trigo	4	f
23	Rack Principal - A	5	f
24	Rack B - 2	5	f
25	Rack C - 3	5	f
26	Rack D - 4	5	f
27	Rack E - 1	5	f

Figura 31. Listado de Lugares

Id Activo	Id Lugar	Vlan Id	IP	Id Tipo Activo	Marca	Modelo	Posee SNMP	Versión Agente	Seguimiento	Eliminado
1	1	1	192.168.40.217	1	Fortinet	Fortigate 80C	t	v3	f	f
2	1	1	192.168.40.217	1	Fortinet	Fortigate 80C	t	v3	t	f
3	1	1000	192.168.40.218	2	Alcatel/Lucent	Omni 6450-10	t	v3	f	f
4	1	1000	192.168.40.219	2	Alcatel/Lucent	Omni 6450-10	t	v3	f	f
5	1	1000	172.21.220.22	2	Alcatel/Lucent	Omni 6850-24	t	v3	f	f
6	1	1000	172.21.220.21	3	Enterasys	A2H124-48	t	v2	f	f
7	3	1010	172.21.223.141	4	Alcatel Lucent	Omni Access 103	f		f	f
8	6	1010	172.21.223.142	4	Alcatel Lucent	Omni Access 103	f		f	f
9	97	1000	172.21.220.20	3	Enterasys	A2H124-48	t	v2	f	f
10	102	1010	172.21.223.152	4	Alcatel Lucent	Omni Access 103	f		f	f
11	98	1010	172.21.223.151	4	Alcatel Lucent	Omni Access 68	f		f	f
12	96	1000	172.21.223.9	3	TrendNet	TEG-224WS	t	v1t	f	f
13	53	1000	172.21.224.9	3	TrendNet	TEG-2224WS	t	v1t	f	f
14	103	1000	172.21.224.8	3	TrendNet	TEG-224WS	t	v1t	f	f
15	95	1000	172.21.222.9	3	TrendNet	TE100-S24WS	t	v1	f	f
16	23	1000	172.21.220.3	3	Enterasys	B3G124-24	t	v2	f	f
17	24	1000	172.21.220.4	3	Enterasys	B3G124-48	t	v2	f	f
18	24	1000	172.21.220.4	3	Enterasys	B3G124-24	t	v2	f	f
19	30	1010	172.21.223.167	4	Alcatel Lucent	Omni Access 103	f		f	f
20	30	1010	172.21.220.68	4	Engenius	EAP 9550	t	v2	f	t
21	105	1010	172.21.223.165	4	Alcatel Lucent	Omni Access 103	f		f	f
22	28	1010	172.21.223.174	4	Alcatel Lucent	Omni Access 103	f		f	f
23	29	1010	172.21.223.166	4	Alcatel Lucent	Omni Access 103	f		f	f
24	25	1000	172.21.220.5	3	Enterasys	B3G124-48	t	v2	f	f
25	25	1000	172.21.220.5	3	Enterasys	B3G124-24	t	v2	f	f
26	32	1010	172.21.223.168	4	Alcatel Lucent	Omni Access 103	f		f	f
27	33	1010	172.21.223.169	4	Alcatel Lucent	Omni Access 103	f		f	f

Figura 32. Listado de Activos

9.5.4 Caso de Uso 4: Configurar Opciones de Monitoreo y de Aplicación

Tabla 14.
Caso de Uso 4

Identificación	04 - CU_Opciones
Nombre	Configurar Opciones para el Monitoreo y para la Aplicación
Descripción:	
Permite configurar opciones para el monitoreo y para la aplicación tales como tiempos intermedios entre ejecuciones, comunidades SNMP, protocolos y puertos, datos del dominio corporativo del cliente, envío de emails a administradores de red, apertura automática de tickets ante la ocurrencia de incidentes, entre otros.	
Actores:	
Adm. Red Sistema	
Pre-condición:	
Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD El usuario de la aplicación debe poseer un perfil de Adm. de Red	
Post-condición:	
Flujo Normal:	
4. Adm. Red: solicita la opción “Configurar Opciones”. 5. Sistema: recupera desde la base de datos los datos almacenados de las opciones, los muestra en campos y habilita su edición. Presenta sólo dos opciones: “Actualizar Datos” y “Cancelar” 6. Adm. Red: cambia los datos 7. Adm. Red: presiona “Actualizar Datos” 8. Sistema: actualiza los datos en la base de datos. Muestra el mensaje “Datos Actualizados” 9. Sistema: vuelve a la página que lo solicitó	
Flujo Alternativo:	
4.1 Adm. Red: presiona “Cancelar”. Sistema: muestra el mensaje “Los datos NO han sido actualizados” Sistema: vuelve a la página que lo solicitó	

Diagrama de Secuencia

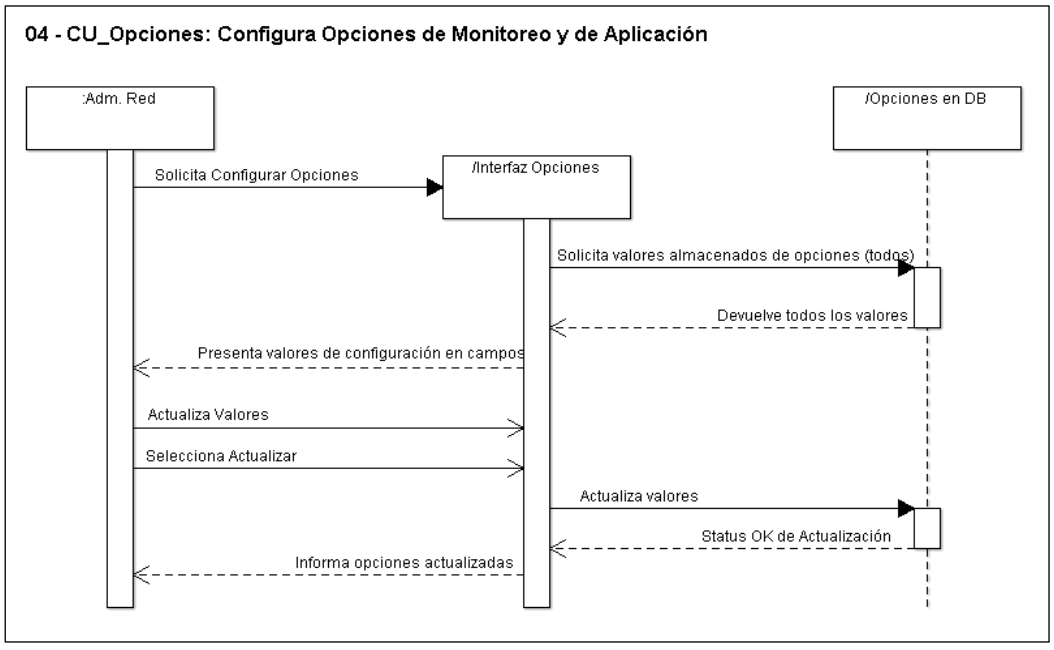


Figura 33. Diagrama de Secuencia Caso de Uso 4

Diagrama de Colaboración

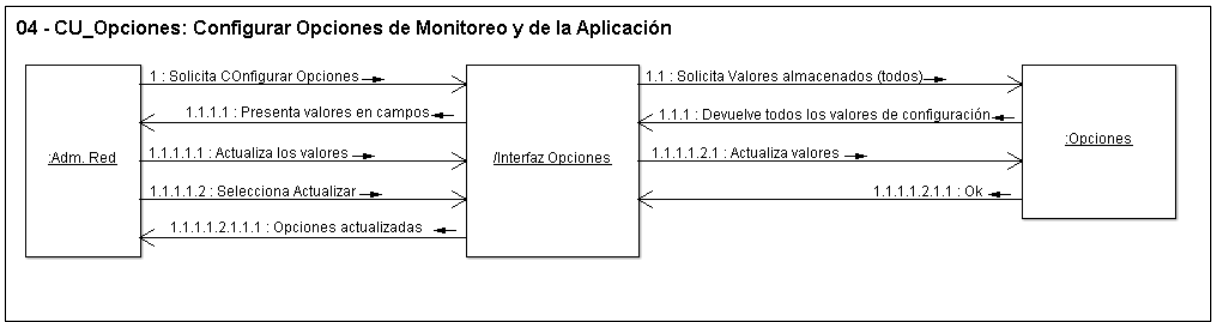


Figura 34. Diagrama de Colaboración Caso de Uso 04

Interfaz "Configurar Opciones"

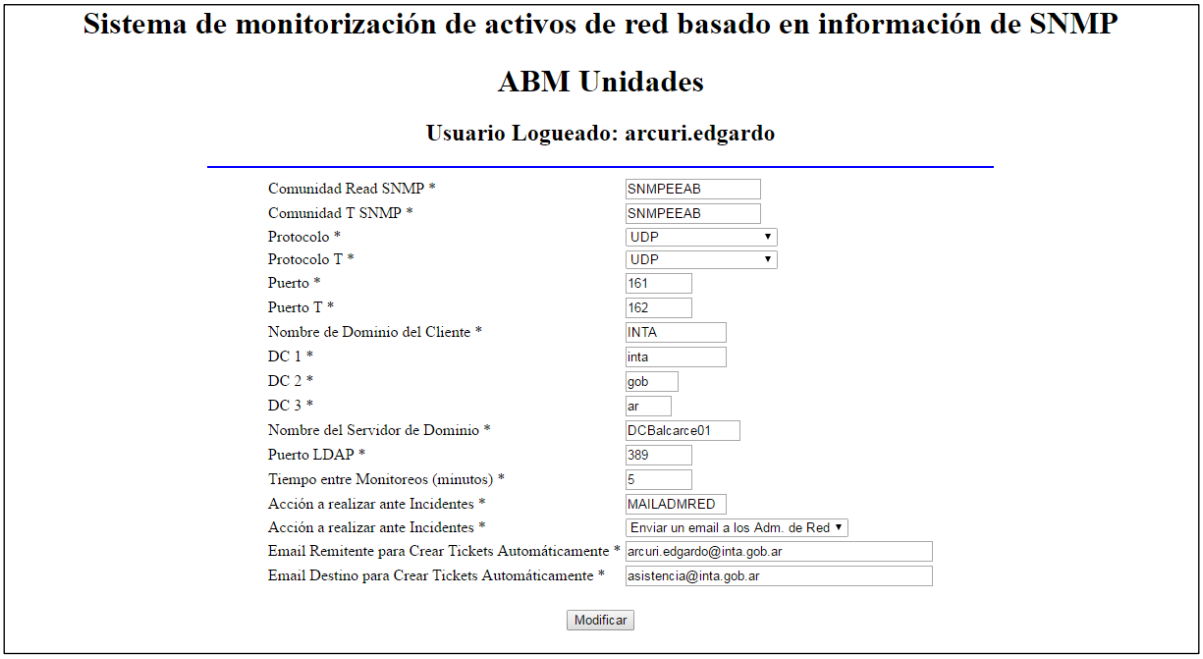


Figura 35. Interfaz Configurar Opciones

9.5.5 Caso de Uso 5: Estado de la Red

Tabla 15.
Caso de Uso 5

Identificación	05 - CU_EstadoRed
Nombre	Obtener y mostrar de forma gráfica el estado de funcionamiento de los activos de red
Descripción:	
El sistema debe obtener y mostrar de forma gráfica el estado de funcionamiento y de conectividad de los activos de red. El sistema deberá actualizar el estado a intervalos regulares de tiempo. La interfaz debe tener en cuenta la dependencia funcional de los activos. Ante la detección de un incidente, deberá realizar la acción configurada para comunicar incidentes: sólo visualización gráfica, enviar emails a los	

administradores de red o declarar automáticamente un incidente en el sistema de gestión de incidentes de la organización (las dos últimas opciones incluyen la primera).

Actores:

Sistema
NMS (Sistema)
Agentes SNMP

Pre-condición:

Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD.
Debe haberse iniciado recientemente una nueva sesión, el temporizador de tiempo entre monitoreo ha llegado a cero o el modo Monitoreo cambió de "Off" a "On".
El modo monitoreo debe estar ACTIVO.
Para las consultas SNMP: el activo a consultar debe poseer un agente SNMP,
debe tener habilitado el servicio y configurado con el mismo nombre de comunidad SNMP que el de la aplicación.

Post-condición:

Monitoreo de los activos.
Gráfica del estado de funcionamiento de la red mostrado en pantalla.

Flujo Normal:

1. Sistema: detecta que el temporizador ha llegado a cero, un usuario ha iniciado una nueva sesión recientemente o el modo Monitoreo cambió de "Off" a "On".
2. Sistema: por cada activo almacenado en la estructura de datos:
   - 2.1. Sistema: resalta el activo de forma gráfica indicando que comienza el monitoreo del mismo (Estado: "En Monitoreo")
   - 2.2. Sistema: envía comandos básicos de red probando la conectividad del activo
   - 2.3. NMS: envía comandos de SNMP a activos para consultar el estado de funcionamiento de interfaces de las cuales depende funcionalmente otro activo cuyo monitoreo es de interés.
   - 2.4. Agente SNMP: recibe consulta del NMS, la procesa recuperando datos desde la MIB y envía la respuesta al NMS
   - 2.5. NMS: recibe respuesta del agente SNMP
   - 2.6. Sistema: muestra gráficamente el estado de funcionamiento del activo de acuerdo a los datos obtenidos que puede ser "No Verificable", "Off" u "On".
   - 2.7 Sistema: el estado del activo es "On", continúa.
   - 2.8 Sistema: registra en la base de datos el estado de funcionamiento del activo.
3. Sistema: recupera de la tabla "Opciones" el valor del intervalo de tiempo entre monitoreo y lanza un nuevo temporizador.

Flujo Alternativo:

2.7.1 Sistema: el valor es "Off" o "No Verificable". Recupera desde la tabla "Opciones" el valor de la acción que debe realizar ante Incidentes y la misma está configurada como "Sólo visualización gráfica".
- 2.7.1.1 Recupera desde la tabla "Activos" el valor de "Activo En Seguimiento". Es Falso, continúa sin realizar acción.
- 2.7.1.2 Recupera desde la tabla "Activos" el valor de "Activo En Seguimiento". Es Verdadero, procede como en punto 2.7.2.

2.7.2 Sistema: el valor es "Off" o "No Verificable". Recupera desde la tabla "Opciones" el valor de la acción que debe realizar ante Incidentes y la misma está configurada como "Envíe email a Administradores de Red". Recupera desde la base de datos los emails de todos los usuarios que sean Adm. de Red y envía un email con todas las direcciones en "Para", detallando el incidente.

2.7.3 Sistema: el valor es "Off" o "No Verificable". Recupera desde la tabla "Opciones" el valor de la acción que debe realizar ante Incidentes y la misma está configurada como "Declarar incidente". Recupera desde la base de datos la dirección específica de email para solicitud de asistencia en el Sistema de Gestión de Incidentes y envía un email para abrir un nuevo ticket.

Diagrama de Secuencia

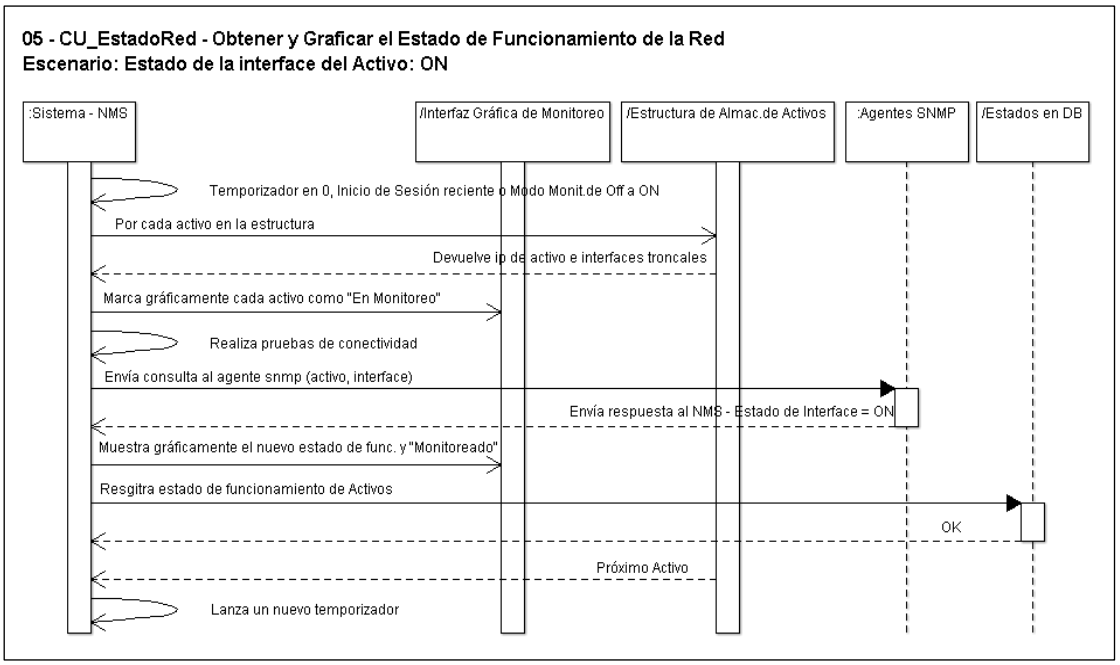


Figura 36. Diagrama de Secuencia Caso de Uso 05 – Escenario 1

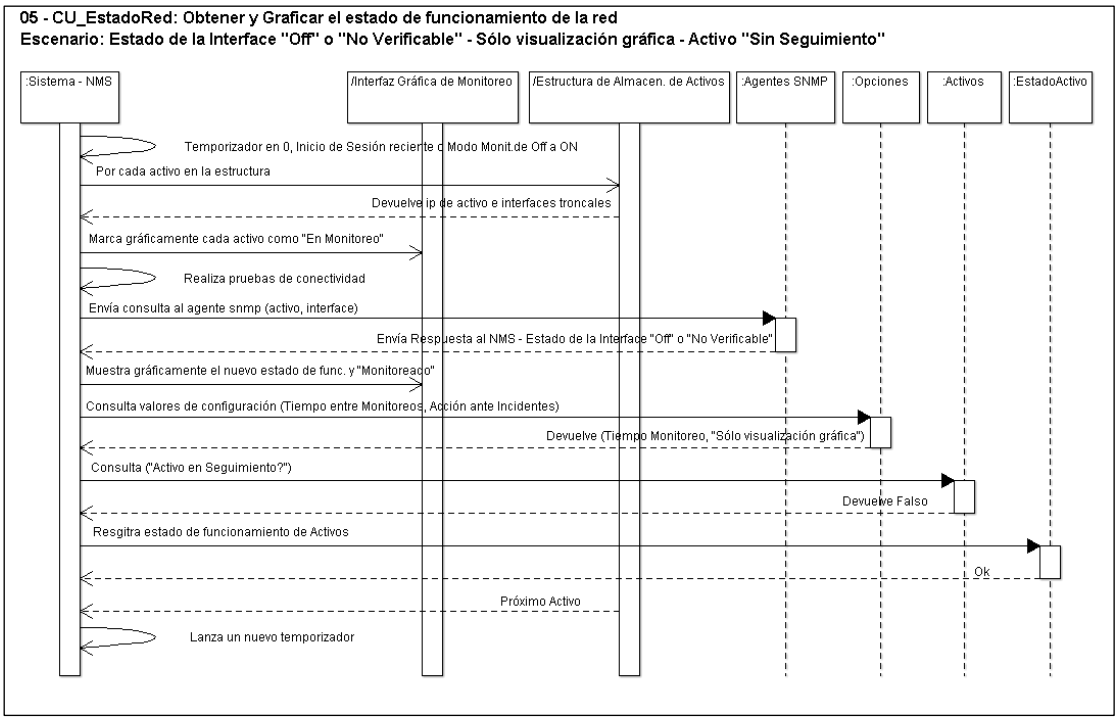


Figura 37. Diagrama de Secuencia Caso de Uso 05 – Escenario 2

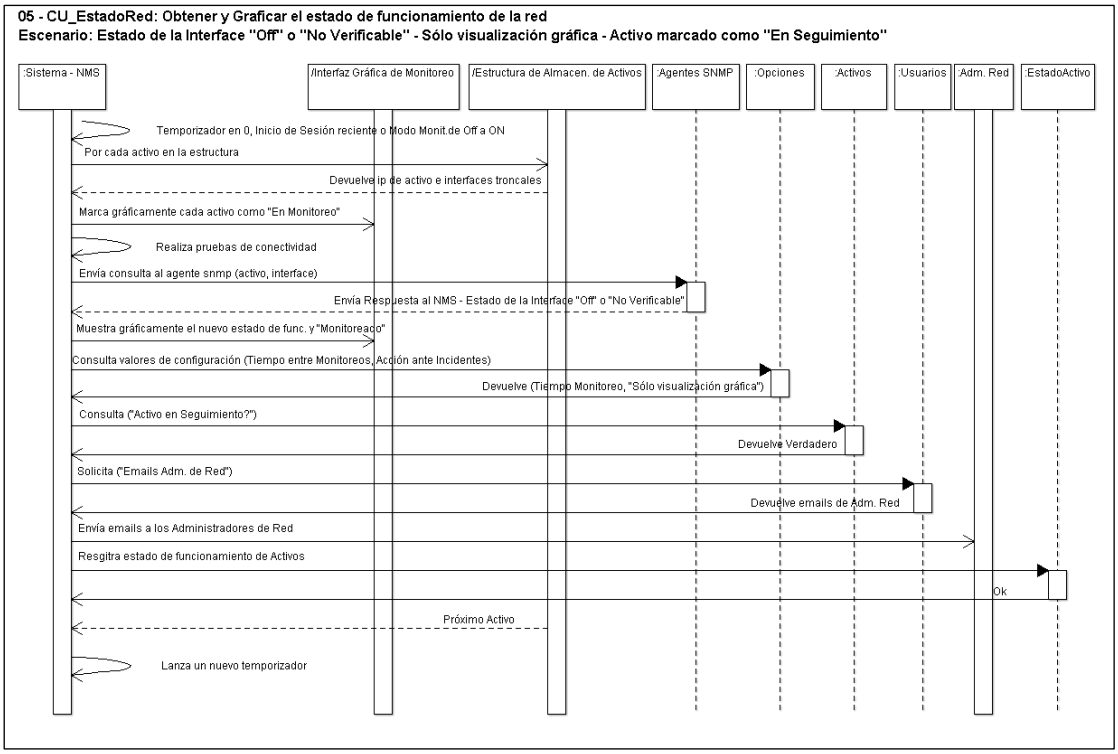


Figura 38. Diagrama de Secuencia Caso de Uso 05 – Escenario 3

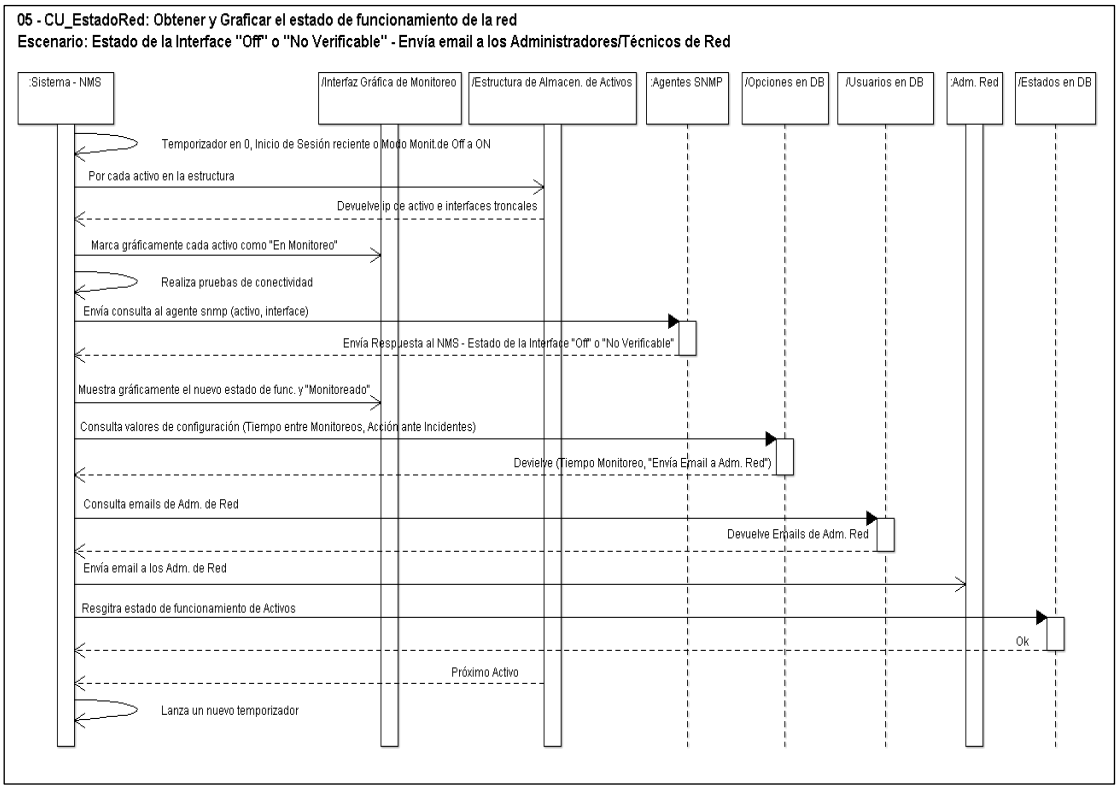


Figura 39. Diagrama de Secuencia Caso de Uso 05 – Escenario 4

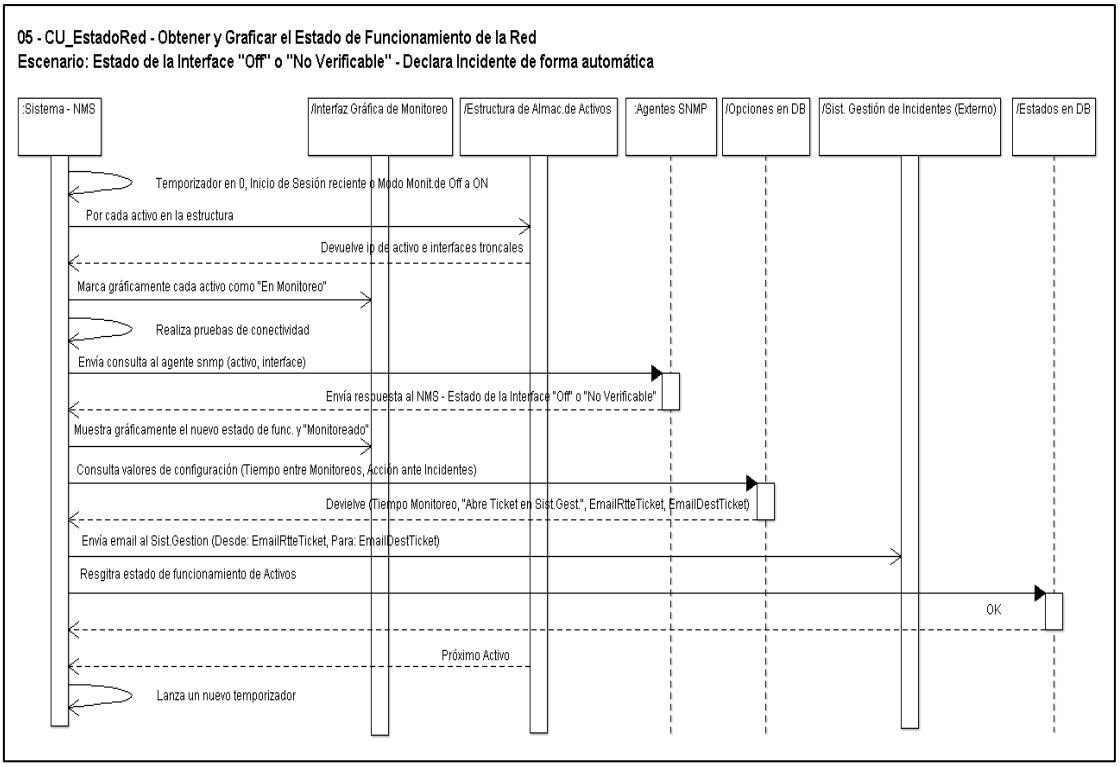


Figura 40. Diagrama de Secuencia Caso de Uso 05 – Escenario 5

9.5.6 Caso de Uso 6: Traps

Tabla 16.
Caso de Uso 6

Identificación	06 - CU_Traps
Nombre	Recibir traps de los agentes SNMP
Descripción:	
El sistema deberá recibir los traps enviados desde los agentes SNMP, procesarlos y resaltar el activo que lo ha generado. El sistema deberá facilitar la lectura del trap recibido y resaltar gráficamente los traps que informen sobre problemas de funcionamiento que impliquen la pérdida de conectividad de un activo.	
Actores:	
Agente SNMP NMS Sistema	
Pre-condición:	
Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD El modo monitoreo debe estar ACTIVO El activo debe poseer Agente SNMP El agente SNMP debe estar habilitado y configurado con el mismo nombre de comunidad SNMP que el de la aplicación	
Post-condición:	
Interfaz de estado de funcionamiento de los activos de red actualizada con los traps recibidos.	
Flujo Normal:	
1. Agente SNMP: envía un trap al NMS. 2. NMS: recibe el trap enviado por el agente. 3. Sistema: resalta el activo con una marca de “Trap Recibido” y pone a disposición el contenido del trap para su lectura. 4. Sistema: procesa el contenido del trap y su código es 2, lo que corresponde a una interfaz caída. 5. Sistema: busca con la ip del activo que informa y la interfaz caída, en la tabla de dependencia	

funcional de activos y el resultado es que existe un activo que depende funcionalmente de esa interfaz y del activo que informa.

6. Sistema: recupera de la tabla “Opciones” el valor de la acción que debe realizar ante Incidentes y la misma está configurada como “Sólo visualización gráfica”.
7. Recupera desde la tabla “Activos” el valor de “Activo En Seguimiento”. Es Falso, continúa.
8. Sistema: registra información del trap en la base de datos.
9. Sistema: registra estado de funcionamiento del activo en la base de datos
10. Sistema: independientemente del estado en que se encuentre el modo de monitoreo, si no existe temporizador en curso lanza uno nuevo con temporizador = 0, y si existe, modifica el tiempo a 0.

Flujo Alternativo:

4.1 Sistema: procesa el contenido del trap y NO trata sobre una interfaz caída. Realiza paso 8 y Fin.

5.1 Sistema: la búsqueda arroja que NO existe un activo que dependa funcionalmente de esa interfaz y del activo que informa. Realiza paso 8 y Fin.

6.1 Sistema: recupera de la tabla “Opciones” el valor de la acción que debe realizar ante Incidentes y la misma está configurada como “Envíe email a Administradores de Red”. Recupera desde la base de datos los emails de todos los usuarios que sean Administrador de Red y envía un email con todas las direcciones en “Para”, detallando el incidente. Continúa en paso 8.

6.2 Sistema: recupera de la tabla “Opciones” el valor de la acción que debe realizar ante Incidentes y la misma está configurada como “Declarar incidente automáticamente”. Recupera desde la base de datos la dirección específica de email para solicitud de asistencia en el Sistema de Gestión de Incidentes y envía un email para abrir un nuevo ticket. Continúa en paso 8.

7.1 Recupera desde la tabla “Activos” el valor de “Activo En Seguimiento”. Es Verdadero, procede como en punto 6.1.

Diagrama de Secuencia

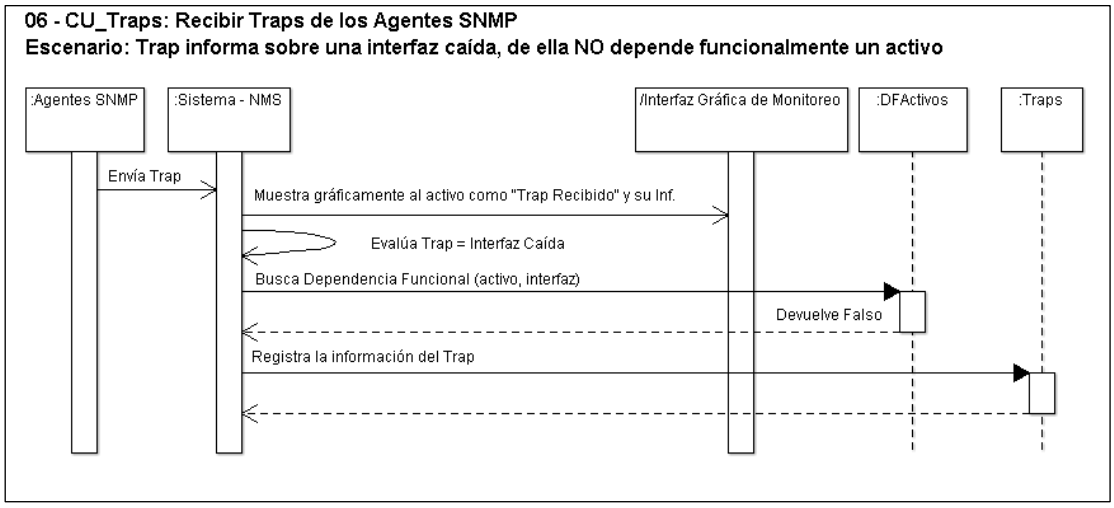


Figura 41. Diagrama de Secuencia Caso de Uso 06 – Escenario 1

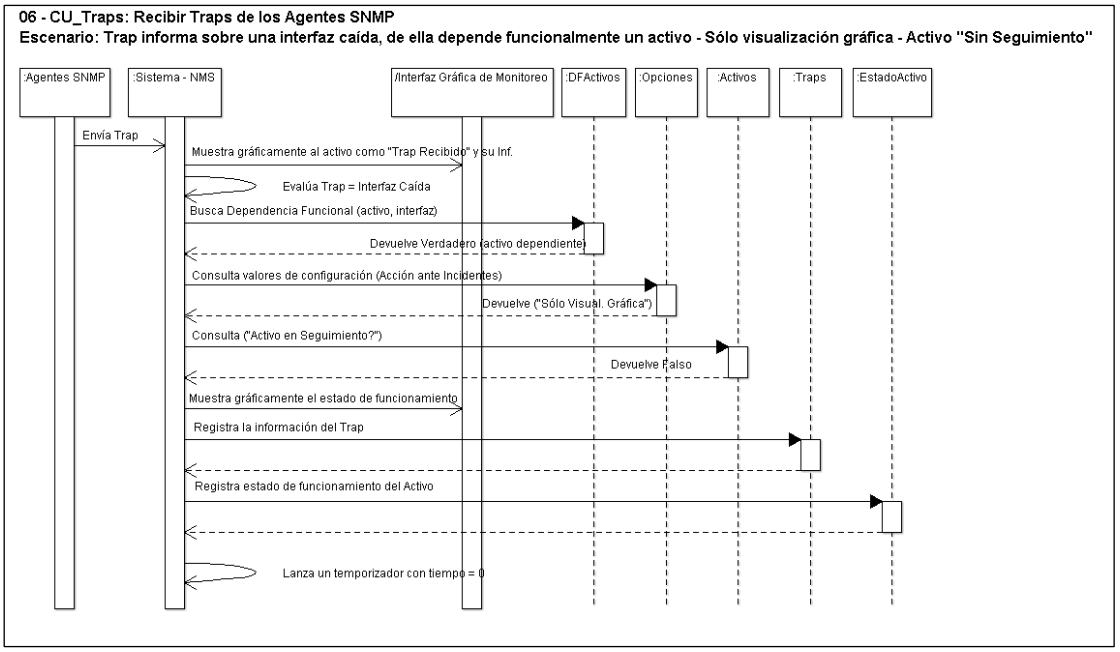


Figura 42. Diagrama de Secuencia Caso de Uso 06 – Escenario 2

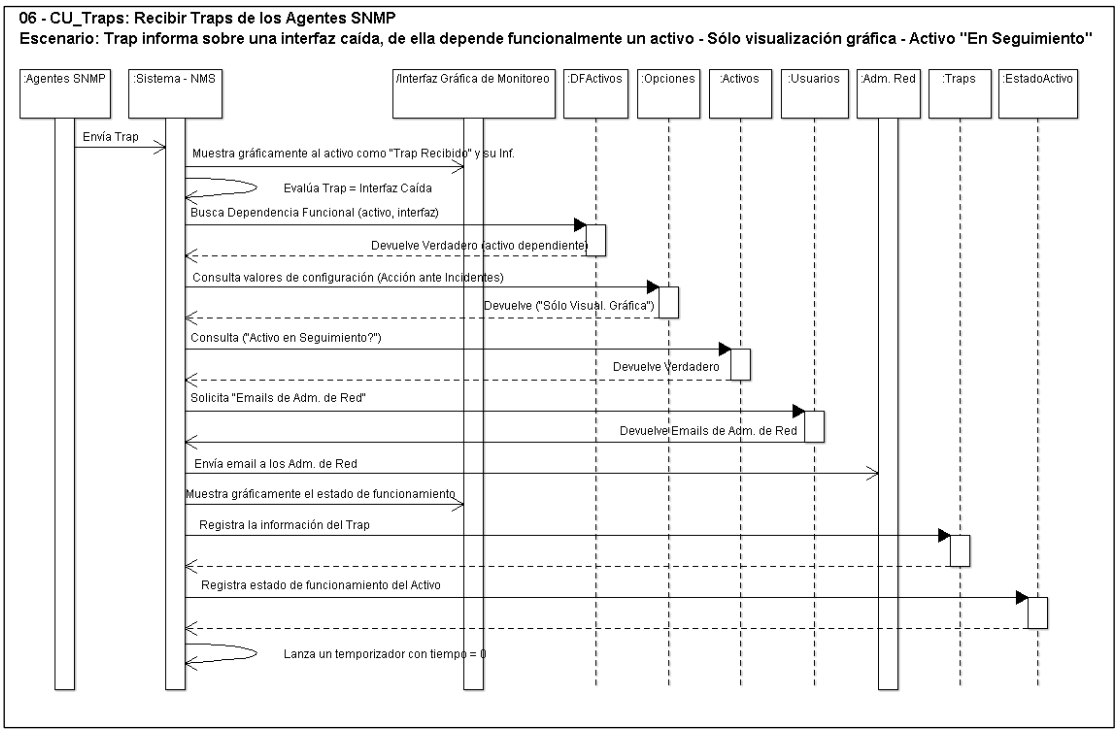


Figura 43. Diagrama de Secuencia Caso de Uso 06 – Escenario 3

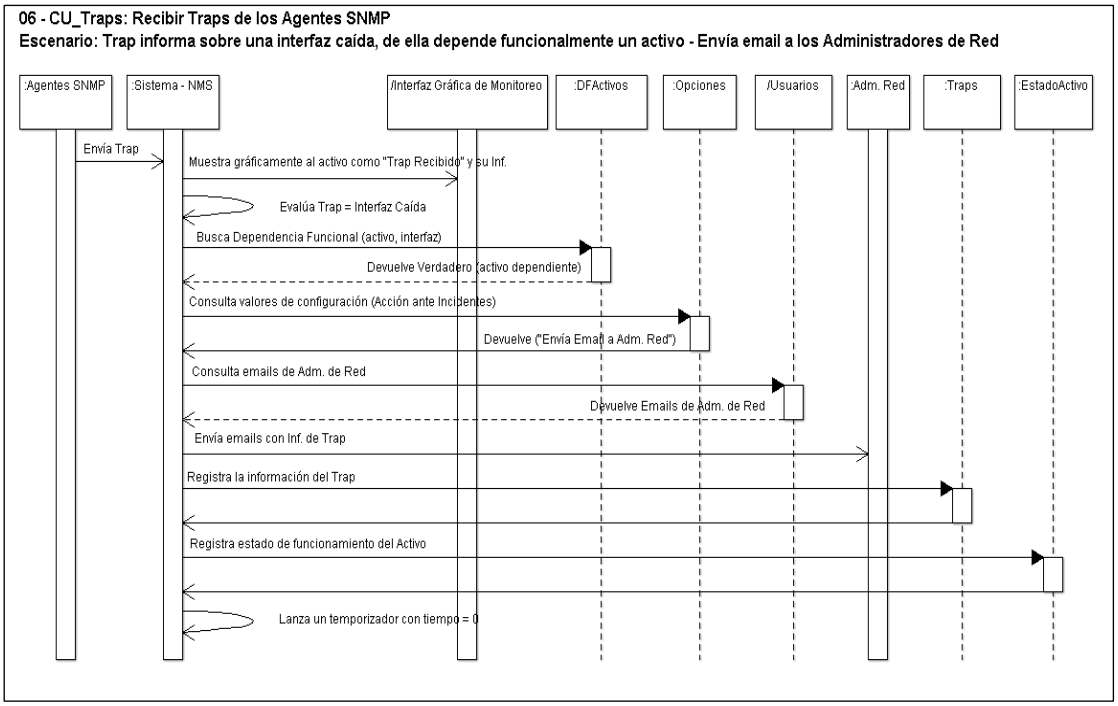


Figura 44. Diagrama de Secuencia Caso de Uso 06 – Escenario 4

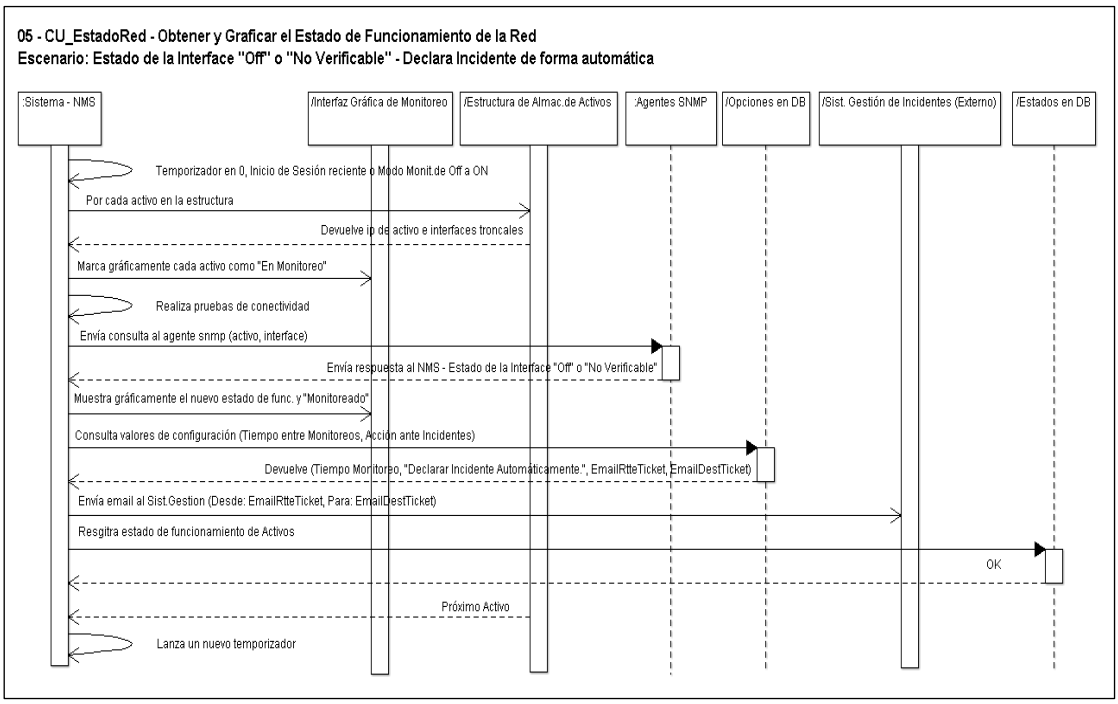


Figura 45. Diagrama de Secuencia Caso de Uso 06 – Escenario 5

9.5.7 Caso de Uso 7: Modo Monitoreo

Tabla 17.
Caso de Uso 7

Identificación	07 - CU_ModoMon
Nombre	Habilitar/deshabilitar modo monitoreo
Descripción:	
El sistema deberá permitir habilitar o deshabilitar el modo monitoreo a los usuarios con perfil de administradores/técnicos de red	
Actores:	
Adm. Red Sistema	
Pre-condición:	
Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD El usuario de la aplicación debe poseer un perfil de Adm. de Red	
Post-condición:	
Monitoreo Activado o desactivado	
Flujo Normal:	
1. Adm. Red: selecciona la opción “Habilitar Monitoreo”. 2. Sistema: establece el Modo Monitoreo en ON y muestra en la interfaz web que el modo monitoreo está ACTIVO. 3. Sistema: cambia la opción del menú a “Deshabilitar Monitoreo”. 4. CU_EstadoRed	
Flujo Alternativo:	
1.1 Adm. Red: selecciona la opción “Deshabilitar Monitoreo”. 1.2 Sistema: establece el Modo Monitoreo en OFF, anula el temporizador en curso y muestra en la interfaz que el modo monitoreo está INACTIVO. 1.3 Sistema: cambia la opción del menú a “Habilitar Monitoreo”. 1.4 Fin	

Diagrama de Secuencia

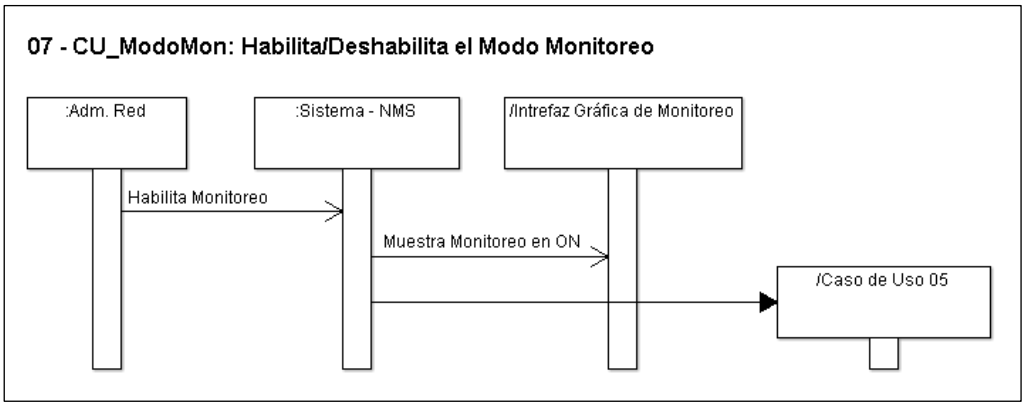


Figura 46. Diagrama de Secuencia Caso de Uso 7 – Escenario 1

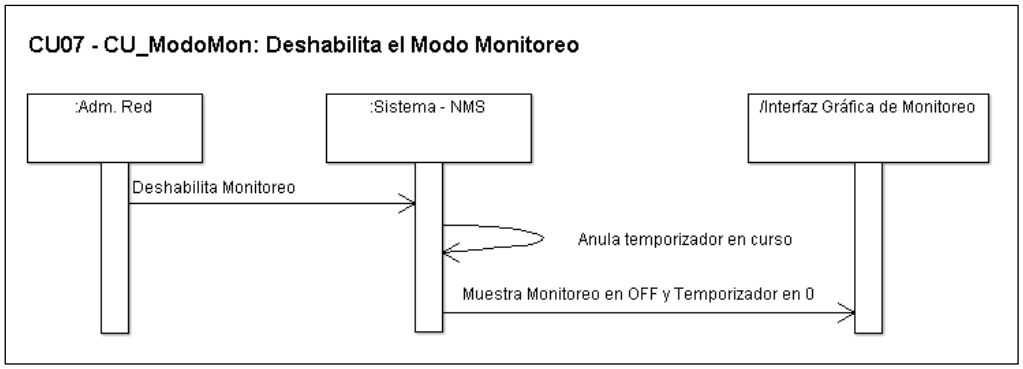


Figura 47. Diagrama de Secuencia Caso de Uso 7 – Escenario 2

9.5.8 Caso de Uso 8: Declarar un activo en Seguimiento

Tabla 18.
Caso de Uso 8

Identificación	08 - CU_ModoSeg
Nombre	Habilita/deshabilita el modo seguimiento de un activo
Descripción:	
El sistema deberá permitir habilitar o deshabilitar el modo "en seguimiento" de un activo, a los usuarios con perfil de administradores/técnicos de red. El modo "en seguimiento" permite que si durante el monitoreo o en la recepción de un trap, se informa de un incidente de un activo declarado en seguimiento, se forzará el envío de un email a los administradores de red independientemente de cualquier otro valor de configuración.	
Actores:	
Sistema Adm. de Red	
Pre-condición:	
Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD El usuario de la aplicación debe poseer un perfil de Adm. de Red	
Post-condición:	
Modo "en seguimiento" de un activo habilitado o deshabilitado.	
Flujo Normal:	
1. Adm. Red: en la interfaz que muestra la dependencia funcional y el estado de activos, se posiciona sobre un activo y presiona el botón derecho del mouse. 2. Sistema: recupera desde la tabla "Activos" el valor del campo "Seguimiento" para ese activo. 3. Sistema: el valor es "Falso" entonces presenta la opción "Declarar activo en seguimiento". 4. Adm. Red: selecciona "Declarar activo en seguimiento". 5. Sistema: establece como verdadero el valor de "Seguimiento" en la tabla "Activos".	
Flujo Alternativo:	
3.1 Sistema: el valor es "Verdadero" entonces presenta la opción "Deshabilitar modo seguimiento". 3.2 Adm. Red: selecciona "Deshabilitar modo seguimiento". 3.3 Sistema: establece como falso el valor de "Seguimiento" en la tabla "Activos". 3.4 Fin.	

Diagrama de Secuencia

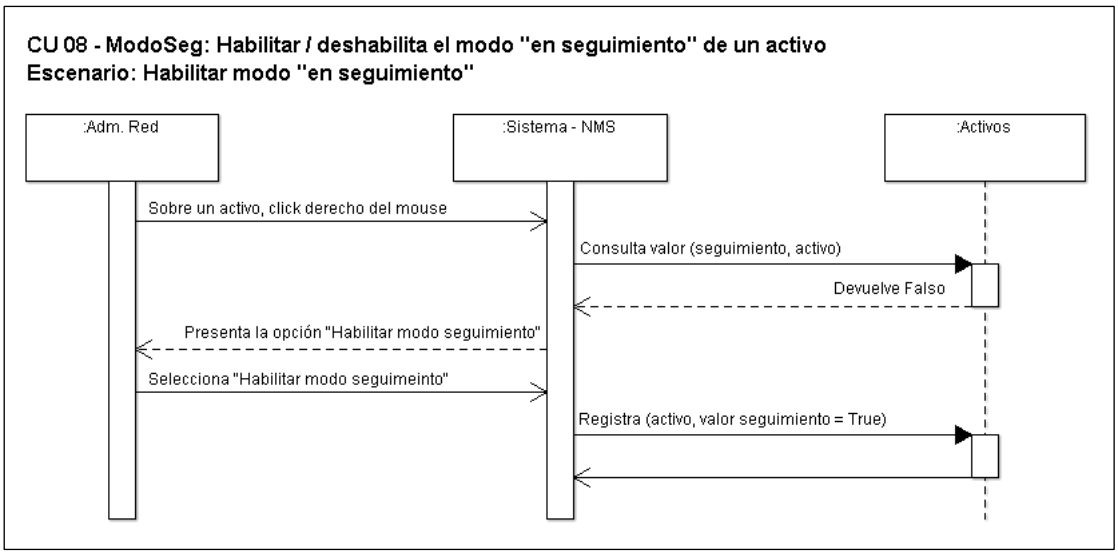


Figura 48. Diagrama de Secuencia Caso de Uso 08 – Escenario 1

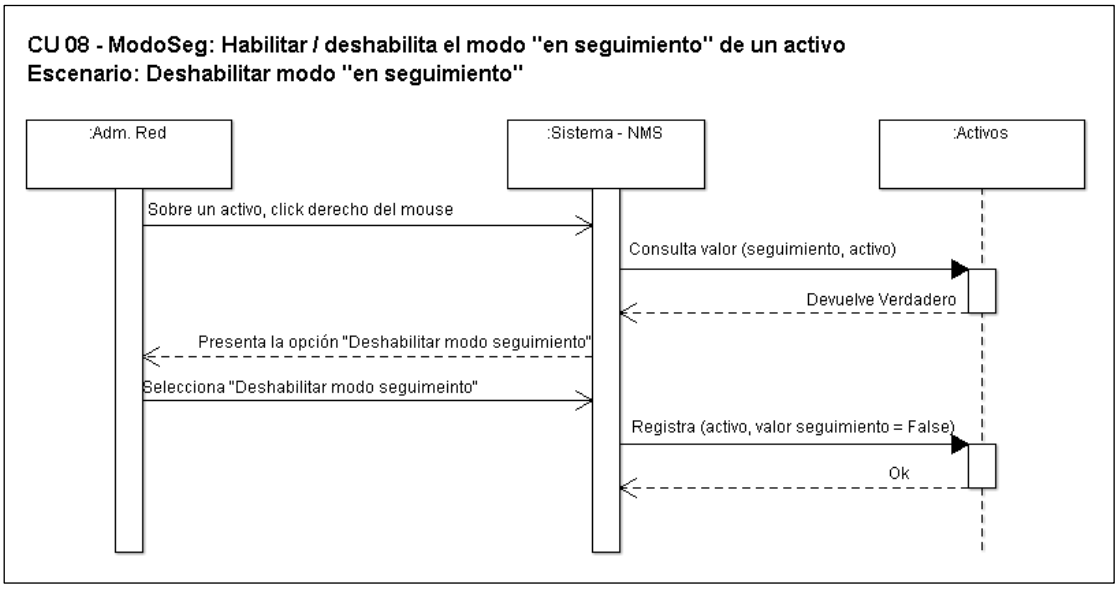


Figura 49. Diagrama de Secuencia Caso de Uso 08 – Escenario 2

9.5.9 Caso de Uso 9: Declarar un incidente manualmente

Tabla 19.
Caso de Uso 9

Identificación	09 - CU_DecIncidente
Nombre	Declarar manualmente un incidente (enviar email a Sistema de Gestión de Incidentes)
Descripción:	
El sistema deberá permitir a un usuario que posea perfil de administrador o técnico de red, seleccionar un activo que presente fallas y declarar de forma manual un Incidente enviando un email al Sistema de Gestión de Incidente con el objetivo de abrir un nuevo ticket de asistencia.	
Actores:	
Adm. Red Sistema	
Pre-condición:	
Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD El usuario de la aplicación debe poseer un perfil de Adm. de Red	
Post-condición:	
Incidente declarado en el Sistema de Gestión de Incidentes (apertura de un nuevo ticket).	
Flujo Normal:	
1. Adm. Red: en la interfaz que muestra la dependencia funcional y el estado de activos, se posiciona sobre el activo que tiene un incidente y presiona el botón derecho del mouse 2. Sistema: recupera desde la base de datos el valor de configuración “Acción ante Incidentes” 3. Sistema: Si el valor de configuración es distinto a “Declarar Automáticamente un Incidente”, indica que el incidente no ha sido declarado automáticamente por el sistema, entonces presenta la opción “Declarar Incidente”. 4. Adm. Red.: selecciona “Declarar Incidente”. 5. Sistema: recupera desde la base de datos los valores de configuración “EmailRtteTicket” y “EmailDestTicket” que contienen los emails remitentes y destino para declaración de incidentes (el remitente es muy importante ya que el sistema asigna el ticket y les envía los emails a los administradores de la unidad donde pertenece el usuario remitente del email). 6. Sistema: envía un email a la dirección del Sistema de Gestión de Incidentes (fuera del alcance de nuestro sistema, el Sistema de Gestión de Incidentes abre un nuevo ticket y lo asigna al administrador de red correspondiente).	
Flujo Alternativo:	
3.1 Sistema: NO presenta la opción “Declarar Incidente”. Fin 4.1 Adm. Red: NO selecciona “Declarar Incidente”. Fin	

Diagrama de Secuencia

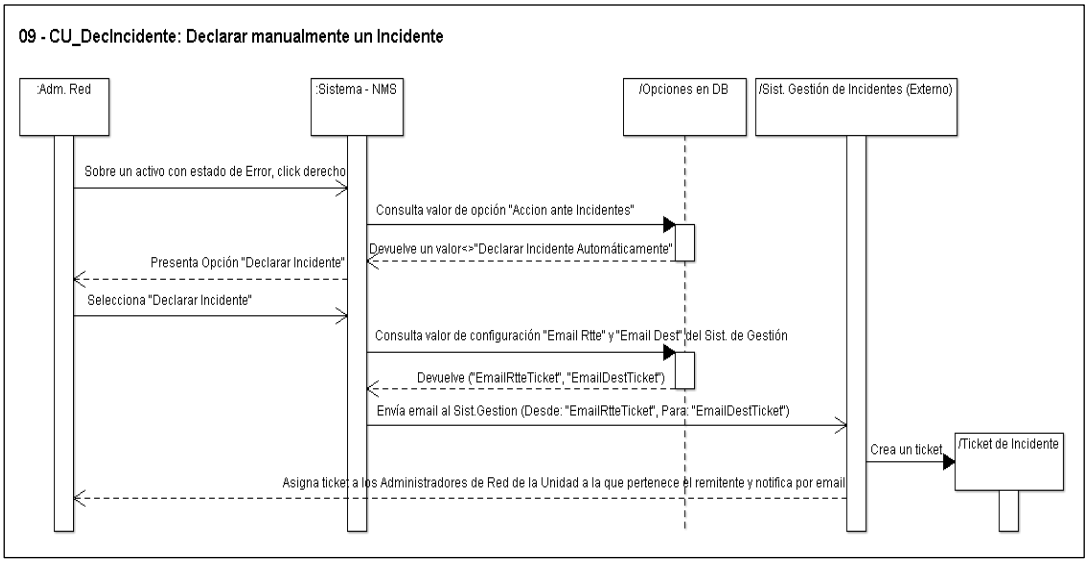


Figura 50. Diagrama de Secuencia Caso de Uso 09

9.5.10 Caso de Uso 10: Reportes de estado de funcionamiento de activos y traps recibidos

Tabla 20.
Caso de Uso 10

Identificación	10 - CU_ReportEF
Nombre	Reportes de estado de funcionamiento de activos y traps recibidos
Descripción:	
El sistema deberá listar, según distintos criterios de selección, los estados de funcionamiento de los activos de red almacenados durante los monitoreos y los traps recibidos.	
Actores:	
Adm. Red. Sistema	
Pre-condición:	
Debe haberse ejecutado exitosamente el Caso de Uso 01 - CU_SesionInAD El usuario de la aplicación debe poseer un perfil de Adm. de Red	
Post-condición:	
Listados de estado de funcionamiento y traps recibidos, preparados para impresión	
Flujo Normal:	
1. Adm. Red: selecciona “Reportes de Estados y Traps”. 2. Sistema: muestra un formulario con campos editables para definir el criterio de selección y presenta dos opciones “Listar” y “Cancelar”. 3. Adm. Red.: define el criterio de selección y opta por “Listar”. 4. Sistema: realiza la búsqueda en las tablas de “Estados de Activos” y “Traps” y lista los estados y traps que concuerden con el criterio de selección indicado por el usuario, en una página nueva y con un formato adecuado para impresión. 5. Fin.	
Flujo Alternativo:	
3.1 Adm. Red: selecciona “Cancelar”. Vuelve a la página anterior. Fin	

Diagrama de Secuencia

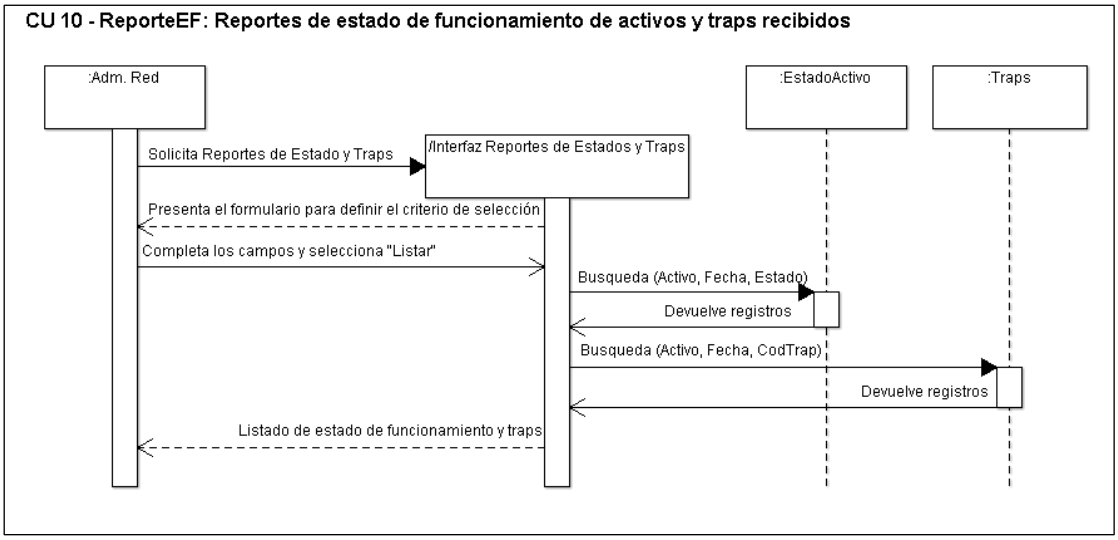


Figura 51. Diagrama de Secuencia Caso de Uso 10

9.6 Diagrama de Clases

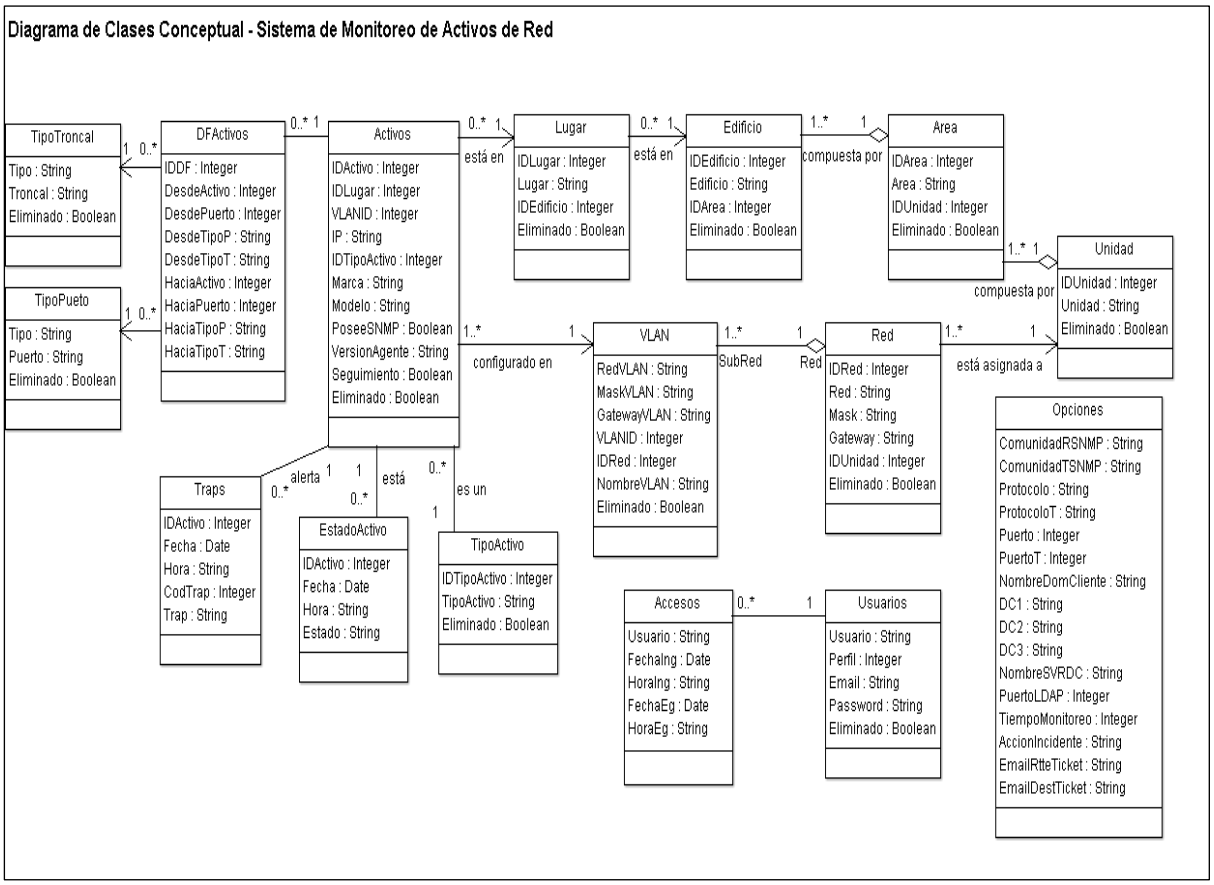


Figura 52. Diagrama de Clases

9.7 Diagrama de Estados

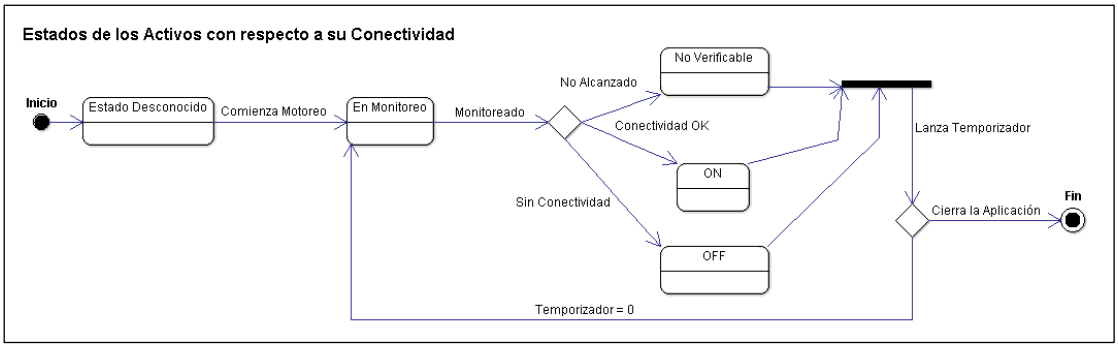


Figura 53. Diagrama de Estados

9.8 Diagrama de Despliegue

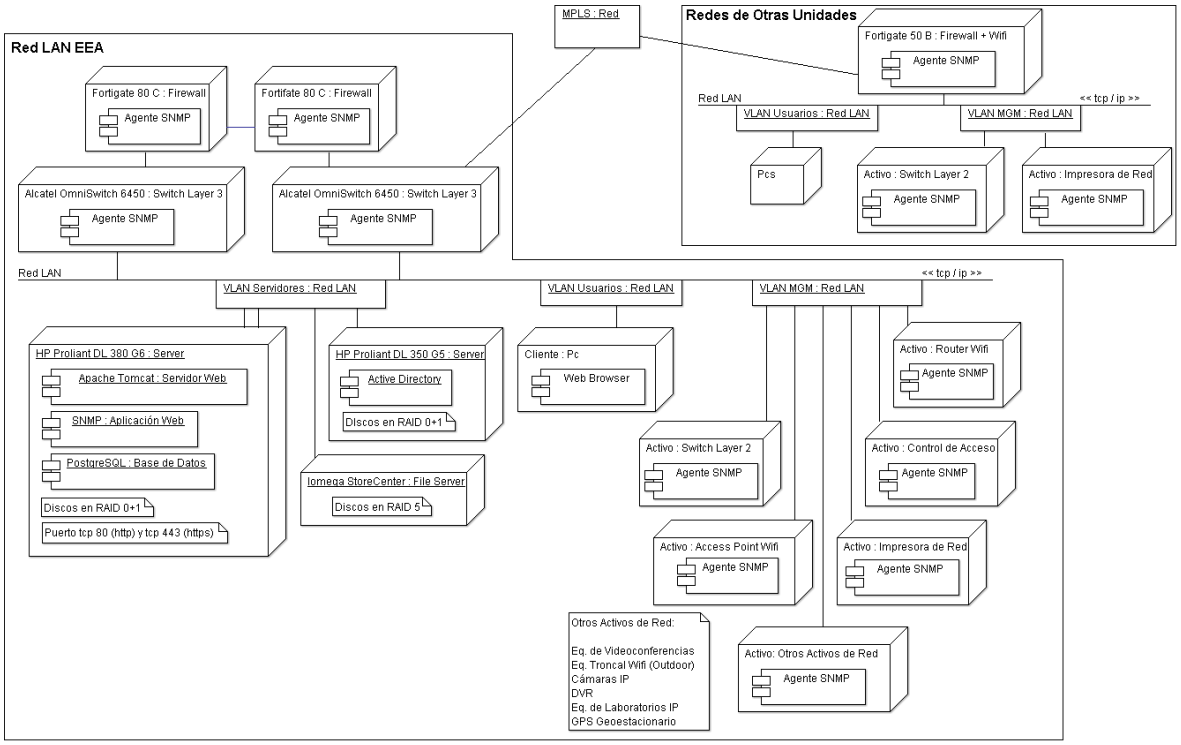


Figura 54. Diagrama de Despliegue

9.9 Ingreso de Datos

Para ingresar los datos de áreas, edificios, lugares y los distintos tipos de activos, puertos y troncales se utilizaron las interfaces disponibles para Altas (Caso de Uso 03).

Para ingresar los datos de activos, redes, vlans y unidades, se importó la información desde las planillas de cálculo existentes en la documentación de la red, suministradas por el administrador durante el relevamiento de datos. Se adaptaron las columnas de la planilla de cálculo y se exportaron los archivos al formato “csv”, formato que delimita con comas las columnas de las planillas (coincidente con los campos). La base de datos PostgreSQL posee una utilidad de importación de archivos “csv” y permite definir distintos delimitadores.

Un caso particular ocurrió con el ingreso de datos para la dependencia funcional de los activos ya que esta información sólo estaba documentada en archivos de presentación. Con la información de los activos ya ingresada en la base y observando los archivos de presentación se pasó la información a una planilla de cálculo y finalmente se la ingresó de

forma manual utilizando la interface de Alta para poder ir seleccionado los activos ya disponibles en el campo.

Las tablas accesos, estado de los activos y traps son para uso del sistema, los datos que allí se ingresan son registrados exclusivamente por él.

Durante el uso del producto, el ingreso de datos se realizará exclusivamente desde las interfaces destinadas a tal fin (Caso de Uso 03).

9.10 Planilla para Casos de Prueba

Tabla 21.
Planilla para Casos de Prueba

Sistema de monitorización de activos de red basado en información de SNMP Planilla para Casos de Prueba					
ID Caso de Prueba		Fecha y Hora			
ID Caso de Uso					
Escenario					
Propósito de la Prueba					
Datos de Entrada					
Resultado/Acción Esperado					
Pasos de Ejecución:	1				
	2				
	3				
	4				
	5				
Resultado/Acción Obtenida					
Estado del Caso de Prueba	Ejecutado:	Resultado Esperado:	SI	Otro Resultado:	
	No Ejecutado / No Finaliza:				
	Error:	Descripción:			
Prueba realizada por:					
Observaciones					
Propuestas de mejoras					

9.11 Puesta en funcionamiento del producto

El primer paso fue implementar un servidor web en una virtualización con sistema operativo Windows 2008 Server Standard R2 de un servidor virtualizado con VMWare ESXi.

Para los servicios web, se instaló el Apache Tomcat versión 9.0.0.M8 atendiendo en el puerto 8080 (http) y Java SE Runtime Environment (Server JRE) versión 8u91. Como gestor de Base de Datos se utilizó PostgreSQL versión 9.4.

El servidor se encuentra en la Sala de Servidores del Departamento de Documentación e Informática de la E.E.A. Balcarce. Casi la totalidad de las tareas de implantación del producto se desarrollaron desde la oficina del Administrador de Red ubicada en el mismo edificio, accediendo al servidor mediante Escritorio Remoto habilitado para tal fin.

El servidor está conectado a un switch de capa 3, a una velocidad de 1 Gbps mediante cableado estructurado de categoría 6 y a la vlan 2, red virtual de los servidores. El switch de capa 3 gestiona las vlans y es quien hace posible el acceso desde cualquier otra vlan hacia la de servidores, que es donde se encuentra la aplicación.

Se agregó y desplegó la aplicación en el servidor web y se importó la base de datos del proyecto en el gestor.

A los dispositivos de red se les configuró remotamente el agente SNMP mediante la configuración web y mediante la interface de línea de comandos.

9.12 Capacitación de usuarios y documentación del producto

Existen dos tipos de usuarios del producto: el personal informático de la organización y los usuarios de la red.

Debido a que el personal informático está conformado por profesionales de sistemas y técnicos de redes, la capacitación fue breve. Además, muchos de ellos participaron en el proyecto por lo que se redujo a la presentación del producto final y su funcionalidad. Al final de la misma se discutieron y documentaron las mejoras que se le podría realizar al producto en próximas versiones y quedó plasmado el compromiso de realizarlas. La más importante de destacar es la georreferenciación de los activos.

El resto de los usuarios del producto, los usuarios de la red, son muchos y no están en una misma ubicación. Tomando en cuenta esto y que el producto posee funcionalidades muy sencillas de utilizar para este tipo de usuarios, se puso a disposición en la página web de inicio, el manual del usuario.

10. Conclusiones

El desarrollo de la aplicación web se realizó en el marco del Proceso Unificado que sirvió de guía a las actividades de desarrollo de software desde el inicio hasta la puesta en funcionamiento del producto, logrando de esta forma alcanzar los objetivos planteados para el Proyecto.

El software cumple el rol de un NMS en una arquitectura SNMP revisando frecuentemente el funcionamiento de los dispositivos que, cumpliendo el rol de agentes, le responden y además generan alertas de fallas. Esto hace posible, en el momento de su ocurrencia, la detección de pérdida de conectividad en la red, producto de fallas en las conexiones y/o en el funcionamiento de los dispositivos que la conforman. Al tener en cuenta la dependencia funcional de los activos de la red, permite mostrar gráficamente el alcance del incidente.

Los administradores y técnicos responsables del funcionamiento de las redes de las unidades a su cargo, cuentan ahora con una herramienta útil que permite el monitoreo del funcionamiento de los activos de red, la detección de fallas y la determinación del alcance del problema. Esto permite tomar conocimiento de una falla en el mismo momento en que ocurre favoreciendo los tiempos de resolución de incidentes y en consecuencia, reduce el efecto negativo que las interrupciones no programadas producen a las actividades de la organización que son dependientes del correcto funcionamiento la red.

Como recomendación, se propone que la aplicación sea distribuida al resto de los administradores de red de la organización, con el objeto de poseer una herramienta de monitorización del funcionamiento de las redes de otras regiones de las cuales son responsables, ya que la problemática y característica de sus actividades es similar.

Por último, quisiera mencionar que el desarrollo del trabajo final de la licenciatura me permitió ampliar mis conocimientos sobre los componentes activos de una red, su conectividad, los tipos de fallas que presentan y profundizar mis conocimientos sobre el tema de supervisión del funcionamiento de redes y, específicamente, sobre el protocolo simple de administración de redes (SNMP).

11. Bibliografía

Apache Tomcat. *Apache Tomcat – Welcome!* Recuperado el 28, Junio 2016 de http://tomcat.apache.org/

ASP.NET. *ASP.NET - The ASP.NET Site.* Recuperado el 28, Junio 2016 de https://www.asp.net

Bizagi. *Software BPMN para el modelamiento de procesos.* Recuperado el 01, Mayo 2016 de http://www.bizagi.com/es/productos/bpm-suite/modeler

Booch, Grady, Rumbaugh, James y Jacobson, Ivar. (2006). *El Lenguaje Unificado de Modelado* (2ª ed.). Pearson Education

Comer, Douglas E. (1996). *Redes globales de información con Internet y TCP/IP* (3ª ed.). Prentice Hall

Internet Engineering Task Force. *About the IETF*. Recuperado el 01, Noviembre 2015 de https://www.ietf.org/about/

Internet Engineering Task Force. *Index of /rfc.* Recuperado el 01, Noviembre 2015 de https://www.ietf.org/rfc/

Jacobson, Ivar, Booch, Grady y Rumbaugh, James. (2000). *El Proceso Unificado de Desarrollo de Software* (3ª ed.). Addison Wesley

Java. *java.com: Java y Tu.* Recuperado el 28, Junio de 2016 de https://www.java.com

jQuery. *jQuery*. Recuperado el 28, Junio 2016 de https://jquery.com/

Mauro, Douglas R. y Schmidt, Kevin J. (2005). *Essential SNMP* (2ª ed.). O'Reilly

Microsoft. *SQL Server 2016. Microsoft.* Recuperado el 28, Junio 2016 de https://www.microsoft.com/sql

MySQL. *MySQL. The world's most popular open source database*. Recuperado el 28, Junio 2016 de https://www.mysql.com

Nagios. *Nagios. The Industry Standard in IT Infrastructure Monitoring*. Recuperado el 28, Junio 2016 de https://www.nagios.org

NetBeans. *NetBeans IDE - Overview*. Recuperado el 08, Diciembre 2015 de https://netbeans.org/features/index.html

Paessler. *Paessler. The Network Monitoring Company.* Recuperado el 28, Junio de 2016 de https://www.es.paessler.com

PostgreSQL. *PostgreSQL. The world's most advanced open source database*. Recuperado el 28, Junio 2016 de https://www.postgresql.org

ProjectLibre. *Projectlibre open source*. Recuperado el 01, Mayo 2016 de http://www.projectlibre.org/product/projectlibre-open-source

SNMP4J. *SNMP4J – Free Open Source SNMP API for Java*. Recuperado el 12, Mayo 2016 de http://www.snmp4j.org

Stallings, William (2004). *Comunicaciones y Redes de Computadores* (7ª ed.). Pearson Prentice Hall

Tanenbaum, Andrew S. y Wetherall, David J. (2012). *Redes de Computadoras* (5ª ed.). Pearson

Tigris.org. *argouml.tigris.org*. Recuperado el 08, Diciembre 2015 de http://argouml.tigris.org

Apéndice A: Guía de entrevista - Personal de Recursos Humanos y Asistente Operativo de Dirección

Sobre la organización

Con respecto a su estructura organizacional ¿Cómo clasificaría a la Estación Experimental como tipo de organización: jerárquica, matricial o mixta? Detalle las razones.

¿Cuántas unidades conforman la EEA? ¿Cómo es la dependencia jerárquica entre las unidades?

¿Cómo es la estructura organizativa de la EEA y cuáles son las áreas que la conforman? Solicitar organigrama.

Sobre las funciones de las áreas

¿Cuáles son las funciones de cada área y qué servicios brindan?

Apéndice B: Guía de entrevista - Personal del Grupo de Soporte Técnico

Sobre el grupo

¿Cuántas personas conforman su grupo y cuáles son sus funciones?

¿Cuál es la formación de las personas que lo conforman?

Sobre las actividades

¿Qué actividades realizan y qué servicios brindan?

¿Qué políticas corporativas de TI regulan las actividades del grupo?

¿Qué procesos o procedimientos utilizan para la realización de las actividades? ¿Fueron desarrollados por informáticos de la unidad o por Gerencia de Informática? ¿Están aprobados por alguna Resolución o Disposición?

¿Realizan plan de actividades y de inversiones? ¿Con qué frecuencia?

Sobre el software que utilizan

Para la administración de las actividades específicas de Soporte Técnico ¿poseen una aplicación del tipo Mesa de Ayuda que integre a los distintos componentes que debe administrar (hardware, software, responsables, licencias, carga patrimonial, incidentes, resolución, entre otros)? ¿Cuál?

En caso de no poseer una aplicación integral, ¿qué base de datos o software adquirido o desarrollado utilizan para administrar cada uno de los componentes?

Apéndice C: Guía de entrevista - Grupo de Sistemas de Información

Sobre el grupo

¿Cuántas personas conforman su grupo y cuáles son sus funciones?

¿Cuál es la formación de las personas que lo conforman?

Sobre las actividades

¿Qué actividades realizan y qué servicios brindan?

¿Qué políticas corporativas de TI regulan las actividades del grupo?

¿Qué procesos o procedimientos utilizan para la realización de las actividades? ¿Fueron desarrollados por informáticos de la unidad o por Gerencia de Informática? ¿Están aprobados por alguna Resolución o Disposición?

¿Realizan plan de actividades y de inversiones? ¿Con qué frecuencia?

Sobre los servidores y servicios

¿Cuántos servidores tienen implementados y qué servicios brinda cada uno?

¿Cuántos servidores están virtualizados? ¿Qué software de virtualización utilizan?

¿Qué sistemas operativos y versiones utilizan en los servidores?

¿Disponen de capacidad de recursos de procesamiento, memoria y disco suficiente para alojar nuevas aplicaciones?

Sobre el software para desarrollo y bases de datos

¿Qué metodologías de desarrollo utilizan?

¿Qué ambiente de desarrollo integrado utilizan?

¿Qué lenguajes de programación utilizan?

¿Qué gestores de bases de datos utilizan para las aplicaciones que desarrollan?

Apéndice D: Guía de entrevista - Grupo de Infraestructura y Servicios de Red

Sobre el grupo y sus funciones

¿Cuántas personas conforman su grupo y cuáles son sus funciones?

¿Cuál es la formación de las personas que lo conforman?

Sobre las actividades

¿Qué actividades realizan y qué servicios brindan?

¿Qué políticas corporativas de TI regulan las actividades del grupo?

¿Qué procesos o procedimientos utilizan para la realización de las actividades? ¿Fueron desarrollados por informáticos de la unidad o por Gerencia de Informática? ¿Están aprobados por alguna Resolución o Disposición?

¿Realizan plan de actividades y de inversiones? ¿Con qué frecuencia?

Sobre las redes

¿Cuántas redes tienen a cargo? ¿Qué dimensión tiene cada una, aproximadamente?

Describa las características de las redes (topología, infraestructura, medios de transmisión, tipos de troncales, tipos de cableados, activos de red, tipos de enlaces, anchos de banda, redes virtuales, etc)

¿Posee documentación de la red? En caso afirmativo solicitarla.

Sobre los servidores y servicios

¿Cuántos servidores tienen implementados y qué servicios brinda cada uno?

¿Cuántos servidores están virtualizados? ¿Qué software de virtualización utilizan?

¿Qué sistemas operativos y versiones utilizan en los servidores?

¿Disponen de capacidad de recursos de procesamiento, memoria y disco suficiente para alojar más servicios?

Cont. Guía de entrevista al personal del grupo de Infraestructura y Servicios de Red

Sobre el funcionamiento de la red

¿Cómo es el proceso actual del control de funcionamiento de la red y sus activos? ¿Quiénes son los responsables? ¿Está documentado? En caso afirmativo, solicitarlo.

¿Poseen una aplicación del tipo Mesa de Ayuda que permita al usuario solicitar asistencia ante una falla en los servicios y que integre a los distintos componentes que debe administrar (activos, usuarios, resolución de incidente, inventario de activos, entre otros)? ¿Cuál?

¿A través de qué otros medios o métodos se descubre que hay una falla u ocurrió un incidente en la red o en un activo de red?

Una vez que se toma conocimiento del incidente, describa cuáles son los pasos que se realizan y por quién, para descubrir el alcance de la falla, dónde está la falla, qué dispositivo o medio físico falló y los pasos para solucionarlo.

¿Qué comandos o aplicaciones utiliza para realizar pruebas de funcionamiento de red?

¿Cuál sería para ustedes la forma de optimizar el control del funcionamiento de la red y sus activos?

¿Qué funcionalidades desearían que un sistema de monitorización del funcionamiento de la red y sus activos les brinde?

Apéndice E: Guía para el Relevamiento de los dispositivos activos de las redes de las 12 unidades administradas por el grupo de redes de Informática de la EEA Balcarce

Unidad:

CERBAS		EEA Balcarce		AER Mar del Plata	
AER Tandil		AER Necochea		AER Olavarría	
AER Cte. N. Otamendi		AER Balcarce		AER Lobería	
AER Laprida		AER Benito Juárez		AER. Gral Lamadrid	

Edificio:
Ublicación:
Red para acceder al dispositivo: **LAN ____** **MPLS ____**

Tipo de Dispositivo:

Firewall		Firewall + AP Wifi		Switch Layer 3	
Switch Layer 2		Router Wifi		AP Wifi	
Equipo de Troncal Wifi		Impresora de Red		Eq. de Videoconferencia	
Estación Permanente GPS		Eq. de Laboratorio		Cámara IP	
Controles de Acc. Puertas		Servidor		Otro: _____	

Si es un servidor: **Sistema Operativo _____** **Versión _____**

ID Activo: _ _ _ **Depende del activo: A: _ _ _ - B: _ _ _**

Cantidad de Puertos:

Fibra Optica (SFP)	MGBics Conectados	Ethernet WAN	Ethernet LAN	Ethernet Stack/LAN	Combo FO (SFP)/Eth	Ethernet DMZ	Consola	USB

Puerto Troncal (802.1Q)

Puerto	Hacia Disp.	Puerto	Hacia Disp.	Puerto	Hacia Disp.	Puerto	Hacia Disp.

Cantidad de señales wifi:

Red y VLAN:

IP	Máscara de Red	Gateway	VLAN Host	VLAN Name

SNMP

¿Implementa SNMP?	Versión 1	Versión 2	Versión 3	Configurable a través de:		
				Web	CLI (Telnet)	S.O.

Apéndice F: Análisis de datos y representación gráfica

Se relevaron los activos de las 12 redes que administra el grupo de redes de la EEA, encontrándose un total de 153 dispositivos.

Dispositivos de Red por Unidad

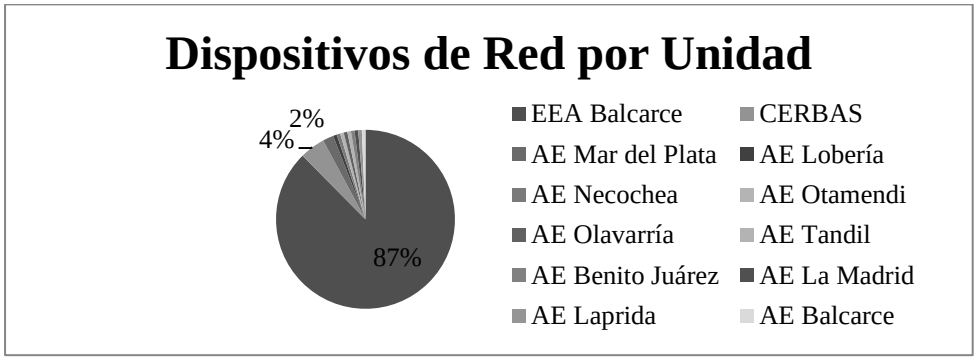


Gráfico 1: Dispositivos de Red por Unidad. Fuente propia

Como se puede ver en el Gráfico 1, el 87.58% de los dispositivos de red corresponden a la EEA Balcarce, el 4,58 % al CERBAS, el 1.96% a la AER Mar del Plata y cada una de las 9 unidades restantes sólo posee cada uno el 0.65% del total de activos.

Tipos de Dispositivos de Red

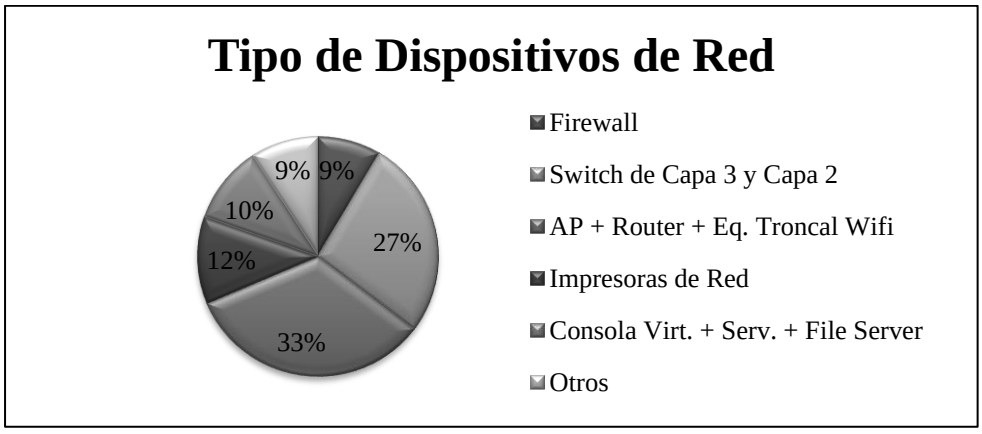


Gráfico 2: Tipos de Dispositivos de Red. Fuente propia

Como podemos apreciar en el Gráfico 2, el 33,33% pertenece a equipamiento con wifi (sumando puntos de acceso, router y equipos troncales), el 26.80% son switchs (contemplando de capa2 y capa 3), el 11.76% impresoras de red, 10,46% de servidores

(virtualizados, sin virtualizar, consolas de virtualización y equipos file server), 8.50% son firewalls, quedando el 9.15% restante para otros dispositivos (controles de puertas de acceso, equipos de laboratorios, cámaras IP, equipos de videoconferencia y estación permanente de GPS).

Red a utilizar para acceder al Dispositivo

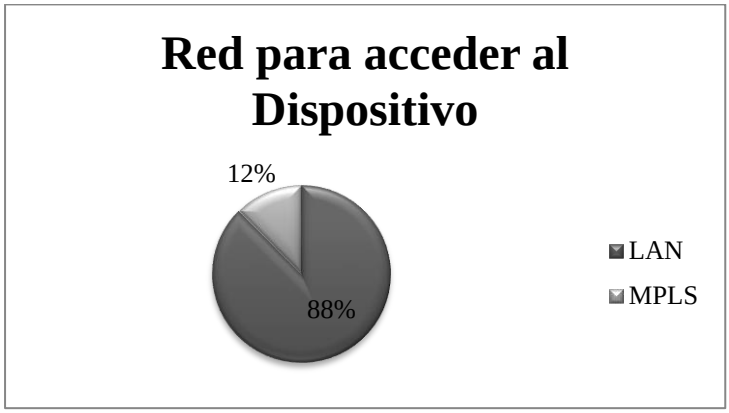


Gráfico 3: Red para acceder al Dispositivo. Fuente propia

El Gráfico 3 nos muestra que el 87.58% es accesible a través de la misma red de la aplicación y el 12.42% a través de la MPLS.

Variedad de Fabricantes

Se utilizan en la red dispositivos de 29 fabricantes distintos

Poseen agentes SNMP

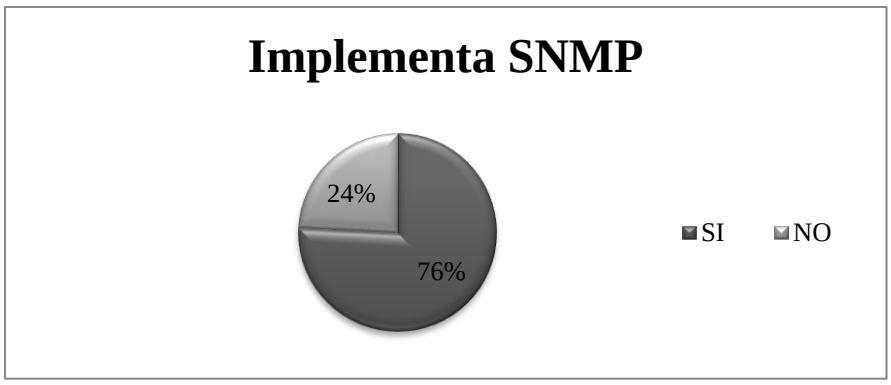


Gráfico 4: Dispositivos que implementan SNMP. Fuente propia

De acuerdo al Gráfico 4, el 75.82% de los dispositivos implementan agentes de SNMP. El 24.18% restante abarca tanto a los equipos que no poseen agente SNMP como a los que no pudo accederse por distintos problemas de red.

Versiones de SNMP

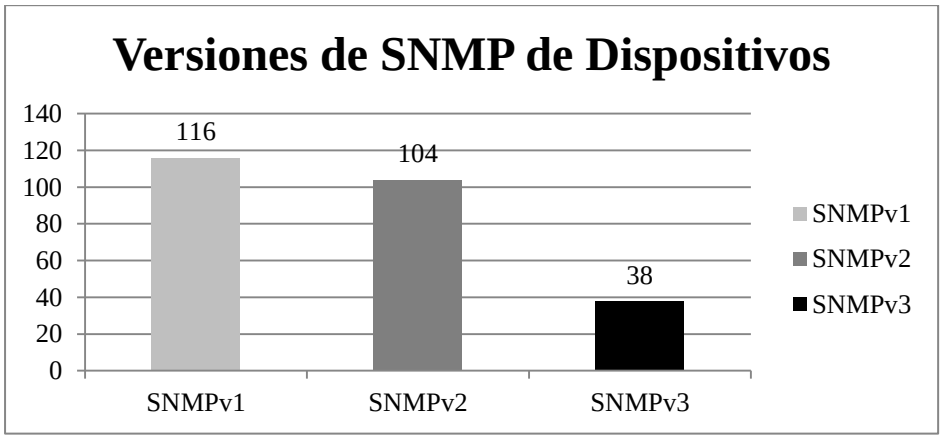
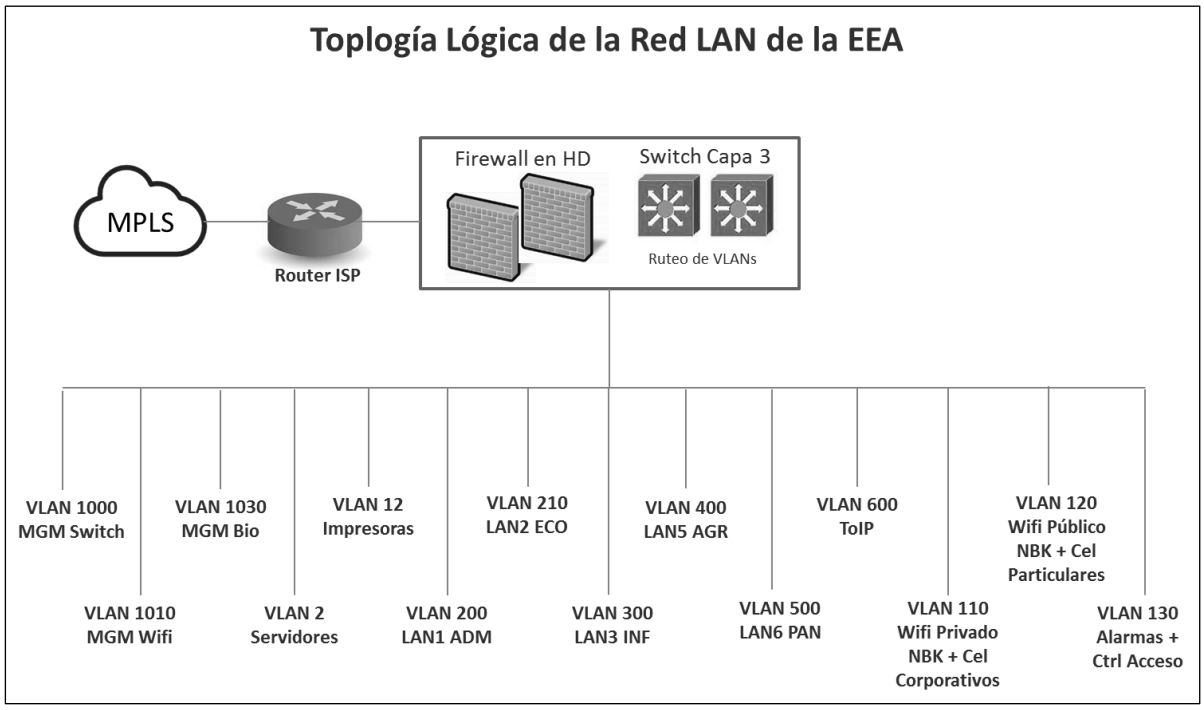
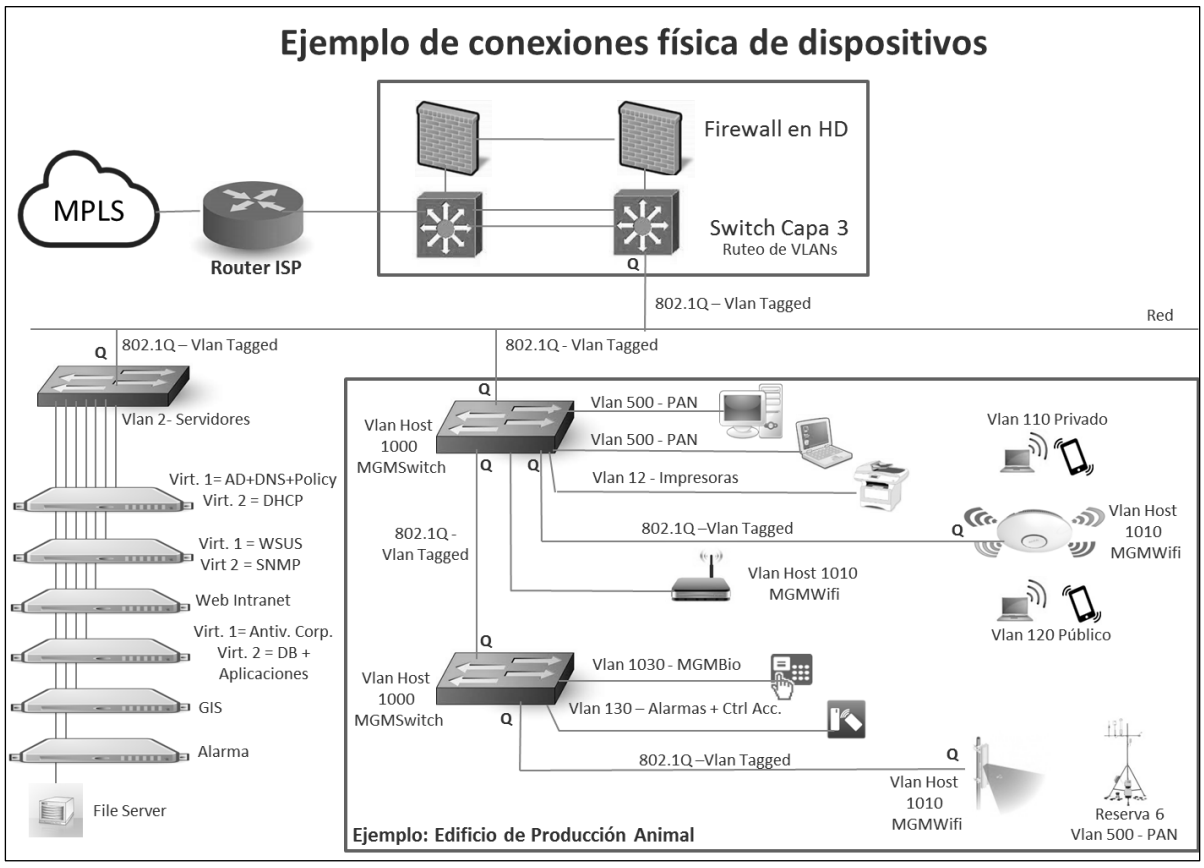


Gráfico 5: Versiones de SNMP implementadas por los Dispositivos. Fuente propia

De los 116 equipos que implementan agentes SNMP, el 100% implementan SNMPv1, el 89.66% posee SNMPv2 y sólo el 32.76% posee SNMPv3, como muestra el Gráfico 5.

Apéndice G: Topología lógica, redes virtuales (VLans) y conexión física de dispositivos





Apéndice H: Listado de RFCs de la IETF citadas

Tabla 22.
Listado de RFCs citadas

RFC	Título
1155	Structure and Identification of Management Information for TCP/IP-based Internets
1157	A Simple Network Management Protocol (SNMP)
2576	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
2578	Structure of Management Information Version 2 (SMIv2)
3410	Introduction and Applicability Statements for Internet Standard Management Framework
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
3413	Simple Network Management Protocol (SNMP) Applications
3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
3417	Transport Mappings for the Simple Network Management Protocol (SNMP)
3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

ANEXO E – FORMULARIO DESCRIPTIVO DEL TRABAJO FINAL DE GRADUACION

AUTORIZACIÓN PARA PUBLICAR Y DIFUNDIRTESIS DE POSGRADO O GRADOA LA UNIVERIDAD SIGLO 21

Por la presente, autorizo a la Universidad Siglo21 a difundir en su página web o bien a través de su campus virtual mi trabajo de Tesis según los datos que detallo a continuación, a los fines que la misma pueda ser leída por los visitantes de dicha página web y/o el cuerpo docente y/o alumnos de la Institución:

Autor-tesista *(apellido/s y nombre/s completos)*	ARCURI, Edgardo Antonio
DNI *(del autor-tesista)*	17.502.046
Título y subtítulo *(completos de la Tesis)*	Sistema de monitorización de activos de red basado en información de SNMP.
Correo electrónico *(del autor-tesista)*	edgarcuri@hotmail.com
Unidad Académica *(donde se presentó la obra)*	Universidad Siglo 21
Datos de edición: *Lugar, editor, fecha e ISBN (para el caso de tesis ya publicadas), depósito en el Registro Nacional de Propiedad Intelectual y autorización de la Editorial (en el caso que corresponda).*	

Otorgo expreso consentimiento para que la copia electrónica de mi Tesis sea publicada en la página web y/o el campus virtual de la Universidad Siglo 21 según el siguiente detalle:

Texto completo de la Tesis *(Marcar SI/NO)*[1]	SI
Publicación parcial *(Informar que capítulos se publicarán)*	

Otorgo expreso consentimiento para que la versión electrónica de este libro sea publicada en la en la página web y/o el campus virtual de la Universidad Siglo 21.

Lugar Fecha: Balcarce, 10 de abril de 2017

	Edgardo Antonio Arcuri
Firma autor-tesista	**Aclaración autor-tesista**

Esta Secretaría/Departamento de Grado/Posgrado de la Unidad Académica: _____certifica que la tesis adjunta es la aprobada y registrada en esta dependencia.

Firma Autoridad	Aclaración Autoridad

Sello de la Secretaría/Departamento de Posgrado

[1] Advertencia: Se informa al autor/tesista que es conveniente publicar en la Biblioteca Digital las obras intelectuales editadas e inscriptas en el INPI para asegurar la plena protección de sus derechos intelectuales (Ley 11.723) y propiedad industrial (Ley 22.362 y Dec. 6673/63. Se recomienda la NO publicación de aquellas tesis que desarrollan un invento patentable, modelo de utilidad y diseño industrial que no ha sido registrado en el INPI, a los fines de preservar la novedad de la creación.