ANEXO C
MODELADO DE HEGCON-PS

ANÁLISIS DE REQUERIMIENTOS

Se definirán en torno a los objetivos del sistema a diseñar.

OBJETIVO PRINCIPAL

Desarrollar una Aplicación distribuida para gestionar y controlar políticas de seguridad dentro de la Red de Datos de la Universidad del Cauca mediante el cual se brinde un nivel más alto de protección frente a la debilidad en la administración de los servicios que la Red ofrece actualmente.

OBJETIVOS ESPECÍFICOS

- Realizar el Modelo Conceptual (Análisis, Diseño y Prototipado) del Sistema Gestor-Agente a través del cual se gestionarán y controlarán Políticas de Seguridad de orden técnico en los equipos terminales de la Red de Datos.

- Definir la Sintaxis necesaria para llevar a cabo la transacción de directivas de seguridad y de información entre el Gestor y el Agente de tal manera que el control de Políticas de Seguridad se haga de forma dinámica.

- Establecer bajo un patrón de clasificación específico las Políticas de orden técnico cuyo control se pueda llevar a cabo a través de los Agentes instalados en cada equipo de la Red.

- Implementar un sistema flexible a posteriores desarrollos según avance o evolucione la normatividad y políticas de administración que regularán la prestación de servicios por parte de la Red de Datos.

- Realizar un estudio de prueba de como la implantación de este proyecto puede facilitar las labores de administración y prestación de servicios, además de la reducción de costos que se derivan de las funciones de administración, operación y mantenimiento de la Red de Datos de la Universidad del Cauca.

DESCRIPCIÓN HEGCON-PS

El propósito principal consiste en la gestión y control de políticas de seguridad en una red informática de forma remota. La aplicación se divide en dos módulos principales.

EL GESTOR

Corresponde a una Aplicación Software de mayor jerarquía instalado en la posición del Servidor mediante el cual el Administrador de red puede gestionar las políticas de seguridad que se desean controlar por medio de los Agentes de Control.

Las funciones principales del Gestor serán: Adicionar, eliminar y modificar políticas; mantener la información correspondiente a Usuarios_Responsables o encargados de llevar a cabo ciertas funciones de seguridad sobre la instalación y mantenimiento de los Agentes de Control en cada equipo terminal; Realizar operaciones de control sobre cualquiera de los Agentes; Verificar cuando un Agente ha sido instalado o desinstalado y realizar el procedimiento adecuado; Actualizar la **SIB** (Security Information Base) del Gestor con todos los eventos reportados en cada **SIB** de los Agentes (imagen); Intercambiar la llave pública del Gestor con cada uno de los Agentes y establecer conexiones seguras; generar reportes dinámicos de acuerdo a las solicitudes del Administrador.

EL AGENTE

Corresponde a una Aplicación Software de menor jerarquía instalada en la posición de cada uno de los equipos que conforman la intranet y que está encargado de controlar las distintas políticas gestionadas a través del módulo de gestión, para lo cual su principal interacción es con el sistema operativo de cada equipo terminal de la red (para llevar a cabo el desarrollo piloto de este proyecto se ha determinado trabajar sobre el entorno operativo de Windows 98 considerado como la plataforma estándar de la mayoría de los equipos que conforman la Red de Datos de la Universidad del Cauca. En desarrollos posteriores a este proyecto esta previsto se amplíe la aplicación a los otros tipos de entornos como Windows 95/NT/Me/2000/Xp, y Linux). El Agente correrá de forma paralela con el Sistema Operativo como un Hilo o "demonio" de tal manera que no afecte el rendimiento ni la eficiencia de los proceso de la máquina y hará uso del registro de Sistema Operativo para llevar a cabo las correspondientes operaciones de control.

Las funciones principales de los Agentes de Control serán: Actualizar la **SIB** (Security Information Base) del Agente con todos los eventos y políticas infringidas; Cada Agente intercambia su llave pública con el Gestor y establece conexiones seguras; Actualizar la **SIB** del Agente por cada operación del gestor; Desplegar mensajes informativos por cada una de las políticas infringidas y mostrar las sanciones pertinentes; Controlar de forma dinámica que se cumplan las políticas definidas por la administración de la red a través del módulo de gestión.

POLÍTICAS PILOTO A IMPLEMENTAR

A continuación se hace una mención de las políticas a implementar. Se debe tener en cuenta que la implementación de estas políticas se enfoca en el diseño de un protocolo de comunicación entre el gestor y el agente, capaz de interpretar las directivas suministradas por el agente y cargar dichas políticas para llevar a cabo su ejecución sobre el entorno operativo en el cual se encuentra instalado el agente.

- Control sobre el Software Instalado en los Equipos Terminales de la Red, el Software licenciado, el Software autorizado por las directivas institucionales, y el Software que debilita la Protección de la Red.

- Mecanismos de Protección contra Virus Informáticos y programas que vulneran el sistema. Dentro de este ítem se considera la verificación de instalación de programas antivirus en cada uno de los equipos terminales, revisión de actualizaciones y ejecución remota en caso de una emergencia de infección de la Intranet.

- Restricción y control de visitas a sitios Web no autorizados. De acuerdo a una base de datos instalada con el módulo de gestión, los Agentes de control podrán actualizar su propia base de datos para evitar el uso indebido de los servicios de internet como la visita a sitios con contenido ocioso y sitios con scripts y ejecutables conocidos que podrían vulnerar la seguridad de la Intranet.

- Control de los recursos compartidos (carpetas e impresoras). Debido a las vulnerabilidades que estos ofrecen, su uso debería ser controlado, y estas operaciones estarían sujetas a autorizaciones que el Administrador de la Red otorgaría a través de los Agentes de control.

En la figura 1 se describe gráficamente como se comportaría el sistema una vez implantado en la intranet.

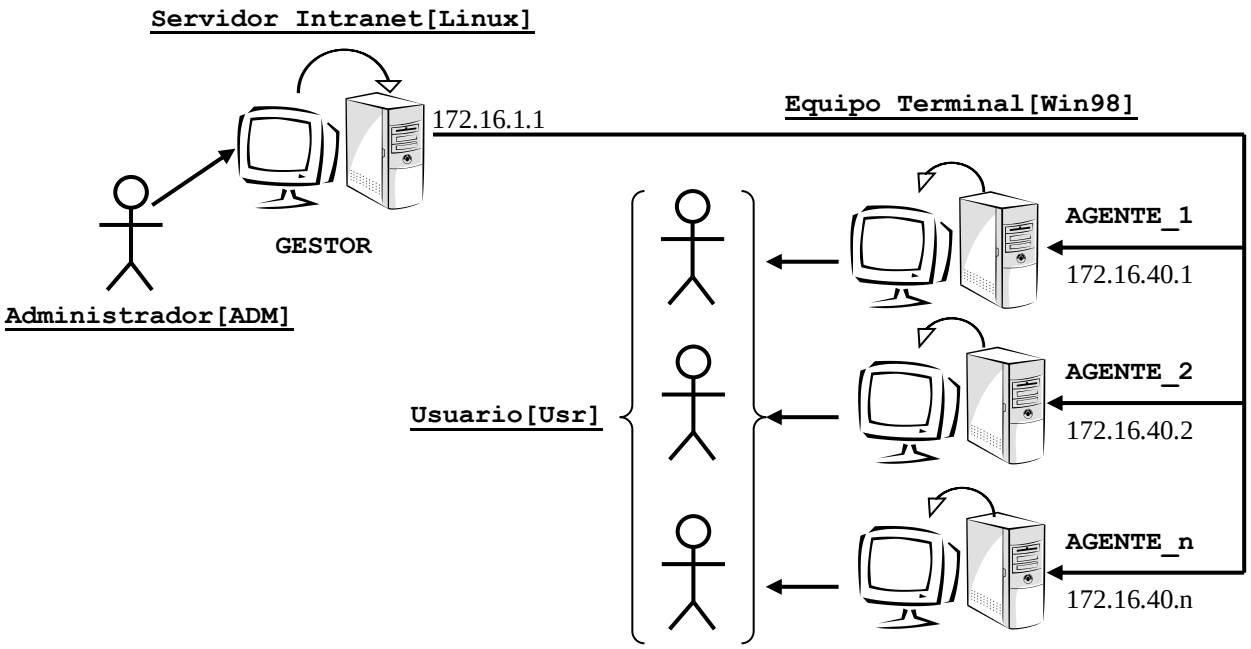


Figura 1. Comportamiento del sistema implementado en intranet.

MODELO DE CASOS DE USO DE ALTO NIVEL (ABSTRACTOS)

IDENTIFICACIÓN DE ACTORES DEL SISTEMA

De acuerdo con la descripción del proyecto HEGCON-PS se tiene

ADM: Administrador del sistema, encargado de interactuar con el módulo de gestor para llevar a cabo las funciones de gestión de información de Políticas, Usuarios y Agentes. Además de las correspondientes funciones de operación del gestor y mantenimiento del sistema.

RESPONSABLE: Usuario de cierta jerarquía dentro de la infraestructura de la Red de Datos (Docentes Encargado, Monitores de sala, Auxiliares de la Red, Laboratoristas) el cual está autorizado para realizar ciertas operaciones (Instalación de Agentes, suministro de información, reporte de fallas, operaciones de mantenimiento) para facilitar la labor del sistema HEGCON-PS.

USR: Usuario, que interactúa con el Sistema Operativo del equipo terminal, pero que recibe información desplegada por el Agente, y además cumple o infringe las Políticas de seguridad.

SO: Sistema Operativo del Equipo Terminal, que interactúa con el Agente de Control suministrando la información necesaria para determinar si se están cumpliendo o no las Políticas de Seguridad proporcionadas a través del Gestor.

Por efectos del modelamiento de la aplicación distribuida, para llevar a cabo una descripción completa de los requerimientos de cada módulo (Gestor y Agente), cada componente se tomará como un Actor para modelar los casos de uso del otro módulo.

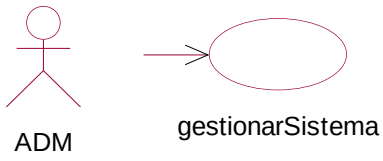
GESTOR: Es el módulo que interactúa con el Agente para establecer comunicación, intercambio de información (entrega nueva información correspondiente a las Políticas de

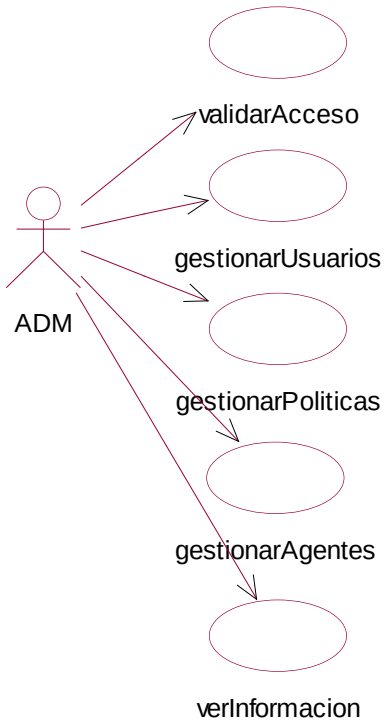
Seguridad y la operación del Agente y recibe información del Agente sobre del Sistema Operativo, Hardware, Software y Políticas infringidas), y operaciones que el Agente debe realizar sobre el Sistema.

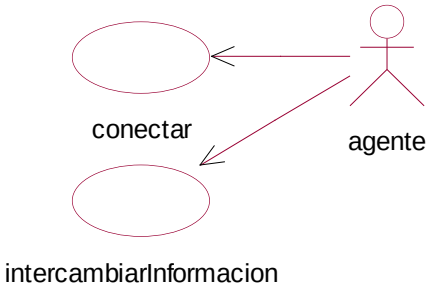
AGENTE: Módulo software que interactúa con el Gestor para establecer comunicación, intercambio de información, y además lleva a cabo funciones de control sobre el Sistema Operativo.

Mediante este modelo se representa de forma general las interacciones entre el sistema y los actores. Se aclara que los módulos que componen la aplicación distribuida serán modelados de forma autónoma e independiente, por lo cual las interacciones recíprocas se representarán mediante la convención establecida actor-sistema. Se realizarán dos niveles de abstracción para dar mas claridad a la forma como funciona el sistema.

- **GESTOR**


ADM
gestionarSistema


validarAcceso
gestionarUsuarios
ADM
gestionarPoliticas
gestionarAgentes
verInformacion


conectar
agente
intercambiarInformacion

‣ DESCRIPCIÓN DE LOS CASOS DE USO

Para esta descripción se usará la notación estándar que corresponde a los casos de uso de alto nivel (abstractos) establecida por UML.

Caso de Uso	validarAcceso
Actor	ADMinistrador (ADM) *Iniciador*
Tipo	Primario
Descripción	El ADM solicita acceso al sistema. El sistema despliega la interfaz de acceso con los campos de texto para introducir los datos de ADM y los botones de confirmación/cancelación. El ADM introduce sus datos y confirma la operación. El sistema captura los datos y los compara con los almacenados en la base de datos, luego notifica al ADM el estado de usuario, si su acceso es válido o si los datos no autorizan el acceso al sistema (datos incorrectos, usuarios no válidos o deshabilitados).

Caso de Uso	gestionarUsuarios
Actor	ADMinistrador (ADM) *Iniciador*
Tipo	Secundario
Descripción	Por defecto, el sistema se instala con un ADM capaz de acceder a los procesos y métodos y realizar configuraciones y modificaciones del sistema. En el caso de varias personas con el mismo rol de ADM, el sistema permite que estos usuarios sean gestionados y su información se mantendrá en la base de datos. Cada Usuario que tiene el rol de ADM posee su propio identificador (Login) y contraseña de acceso (Password). El ADM por defecto (ADM Maestro), está encargado de adicionar, modificar y eliminar los demás Usuarios ADM que se validarán dentro del sistema.

Caso de Uso	gestionarPolíticas
Actor	ADMinistrador (ADM) *Iniciador*

Tipo	Primario
Descripción	Una vez accedido al sistema, el ADM tiene la opción de desplegar la GUI mediante la cual se realiza la gestión de políticas en el módulo GESTOR. El ADM tiene la opción de adicionar una nueva política a gestionar introduciendo los parámetros correspondientes al contenido sintáctico de dicha política. Esta será almacenada en la base de datos. De la misma manera el ADM puede modificar los parámetros correspondientes a una política anteriormente insertada, o llegado el caso eliminarla. Todos los cambios realizados sobre los datos que constituyen la estructura de las políticas se reflejarán en la base de datos.

Caso de Uso	gestionarAgentes
Actor	ADMinistrador (ADM) *Iniciador*
Tipo	Primario
Descripción	Los Agentes serán gestionados por el mismo módulo de gestión de forma automática, sin embargo existe la posibilidad de que el ADM acceda al GESTOR para realizar la gestión manual de los Agentes, llegado el caso de operaciones de mantenimiento de un Agente de Control específico, o en algún tipo de emergencia de seguridad, o dado el caso de conflicto donde se haga necesario realizar algún tipo de operación sobre algún Agente. Este caso de uso permite modificar o desactivar un Agente de Control de forma remota, además permite adicionar, modificar o eliminar la información de un Agente específico en la base de datos del GESTOR. El ADM o ADM Maestro son los únicos usuarios en la capacidad de realizar dichas operaciones a través de una GUI específica para las labores de gestión sobre los Agentes, en la cual se despliegan las correspondientes opciones de gestión. Todos los cambios se reflejarán en la base de datos del GESTOR.

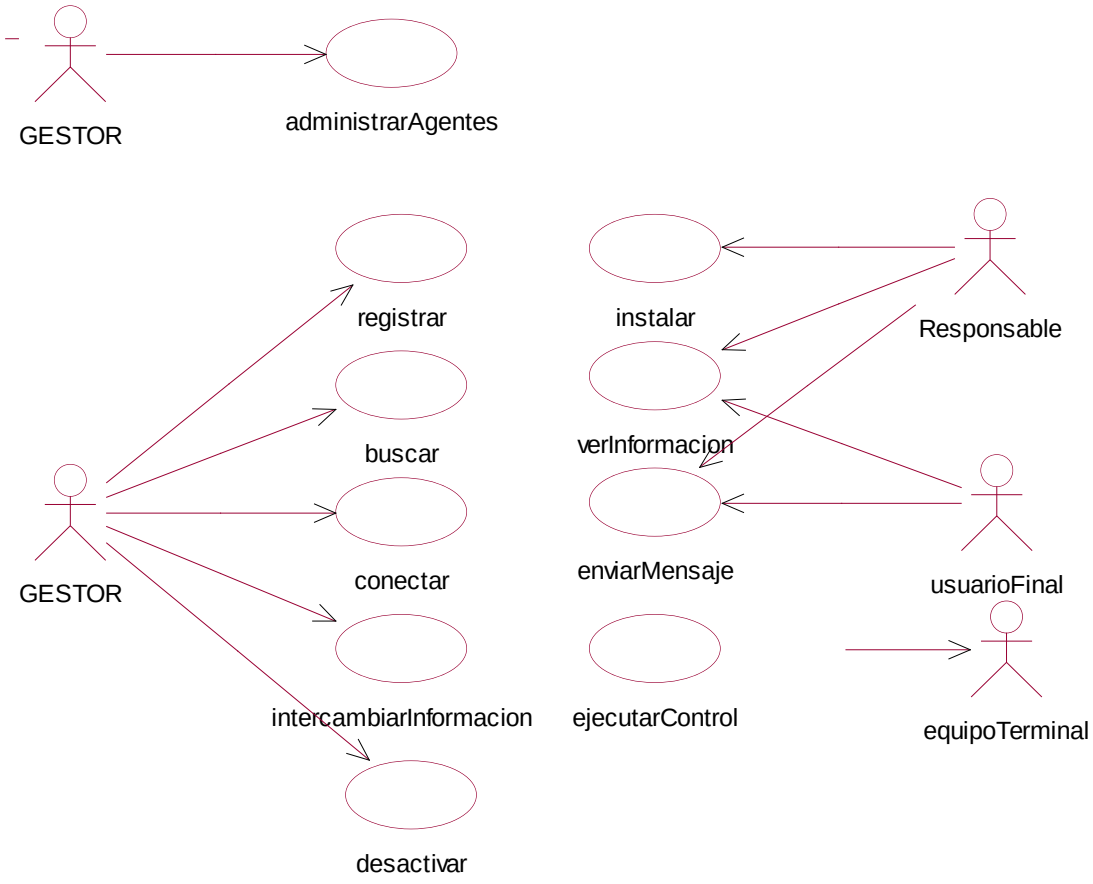
Caso de Uso	verInformacion

Actor	ADMinistrador (ADM) *Iniciador*
Tipo	Opcional
Descripción	El ADM puede revisar la información del estado del sistema que desplegará según la opción seleccionada por el ADM la información correspondiente a las políticas (estructura, última actualización, fecha de creación, sanciones, contenido, grupo aprobador, estado de la política, nivel de seguridad), información de la red y configuración de agentes de control (reportes estadísticos, políticas infringidas, agentes instalados, estado, ubicación física, usuarios de soporte como monitores o laboratoristas encargados de la sala o del equipo), información del servidor, administrador. Esta información le permite al ADM tener datos concretos sobre los cuales se pueden estipular la implementación de nuevas políticas o directrices del uso de los servicios prestados por la Red de Datos.

Caso de Uso	conectar
Actor	Agente
Tipo	Primario
Descripción	En algún momento establecido, el Agente de Control hace una llamada al GESTOR, de forma periódica de tal manera que se permita tener un canal de comunicación a través del cual se lleve a cabo el intercambio de información. El Agente envía una llamada ACK, y el GESTOR responde con un SYN/ACK, luego se establece la conexión. Para establecer una conexión segura para la transferencia de información se hará uso de un sistema de cifrado de llave pública y privada que serán intercambiadas entre el Módulo de Control y el Módulo de Gestión. No siempre es el Agente quién da inicio a este caso de uso, pues dada la necesidad, puede ser el GESTOR quién de forma automática busque a los Agentes para establecer conexiones y realizar alguna operación específica sobre ellos. Esto significa que esta operación de conexión se puede establecer de forma bidireccional dentro de la aplicación distribuida.

Caso de Uso	intercambiarInformacion
Actor	Agente
Tipo	Primario
Descripción	Como se trata de una aplicación distribuida donde cada módulo se desempeña de forma autónoma, y el funcionamiento en general se puede considerar asíncrono, el Agente en un momento determinado es quién hace uso del canal de conexión establecido anteriormente para llevar a cabo el intercambio de información, sin depender necesariamente de que sea el GESTOR quién siempre impulse esta operación.

- **AGENTE**



- DESCRIPCIÓN DE LOS CASOS DE USO

Caso de Uso	registrar
Actor	GESTOR
Tipo	Primario
Descripción	Una vez instalado un agente de control en un equipo terminal, el Agente busca establecer una conexión con el Gestor para notificar su posición, datos del equipo, datos del Usuario Responsable, datos de configuración de red, inventario software y hardware. Toda esta información permite al

	Gestor registrar al Agente dentro de la base de información y validarlo como elemento activo dentro del sistema.

Caso de Uso	buscar
Actor	GESTOR
Tipo	Primario
Descripción	En un momento determinado, el Gestor podrá establecer un rastreo de los Agentes de Control, para establecer conexión (o conexiones de forma simultánea) y realizar operaciones sobre los Agentes.

Caso de Uso	conectar
Actor	GESTOR
Tipo	Primario
Descripción	Una vez encontrado el Agente con el que se desea establecer una comunicación o intercambio de información, se debe establecer una conexión de tipo seguro, haciendo recurso de cifrado de datos por medio de llave pública y privada, y mediante el cual se establece un canal para que se realicen las respectivas operaciones por parte del Gestor hacia el Agente. El iniciador de este caso de uso puede ser el Gestor o el Agente de Control indistintamente, ya que la aplicación se basa en componentes que se desempeñan de forma autónoma, asíncrona y la transacción de la información puede ser bidireccional.

Caso de Uso	Intercambiar Información
Actor	GESTOR
Tipo	Primario
Descripción	Una vez establecida la conexión, el Gestor enviará y recibirá datos desde el Agente de Control. Esta información varía según la operación específica que el Gestor vaya a realizar sobre el Agente de Control (información sobre políticas, sobre los mismos Agentes). Mediante este caso de uso se

	podrá transferir y recibir información entre los Agentes y el Gestor.

Caso de Uso	desactivar
Actor	Gestor *Iniciador*
Tipo	Secundario
Descripción	En condiciones específicas (fuera de control, pruebas autorizadas sobre el equipo terminal), el Gestor estará en la capacidad de dejar inactivo un Agente con el fin de realizar una actividad específica sobre el equipo terminal. Esta operación debe ser sometida a evaluación y aprobación por parte del ADM quién es el que da la autorización correspondiente para llevar a cabo dicha función a través del Gestor.

Caso de Uso	instalar
Actor	Responsable *Iniciador*
Tipo	Primario
Descripción	El Usuario Responsable de la instalación del Agente en el equipo(s) terminal(es) debe proporcionar la información correspondiente con la cual el Agente desarrolla su perfil de configuración. Una vez instalado el Agente de Control estará listo para correr de forma paralela con el sistema operativo.

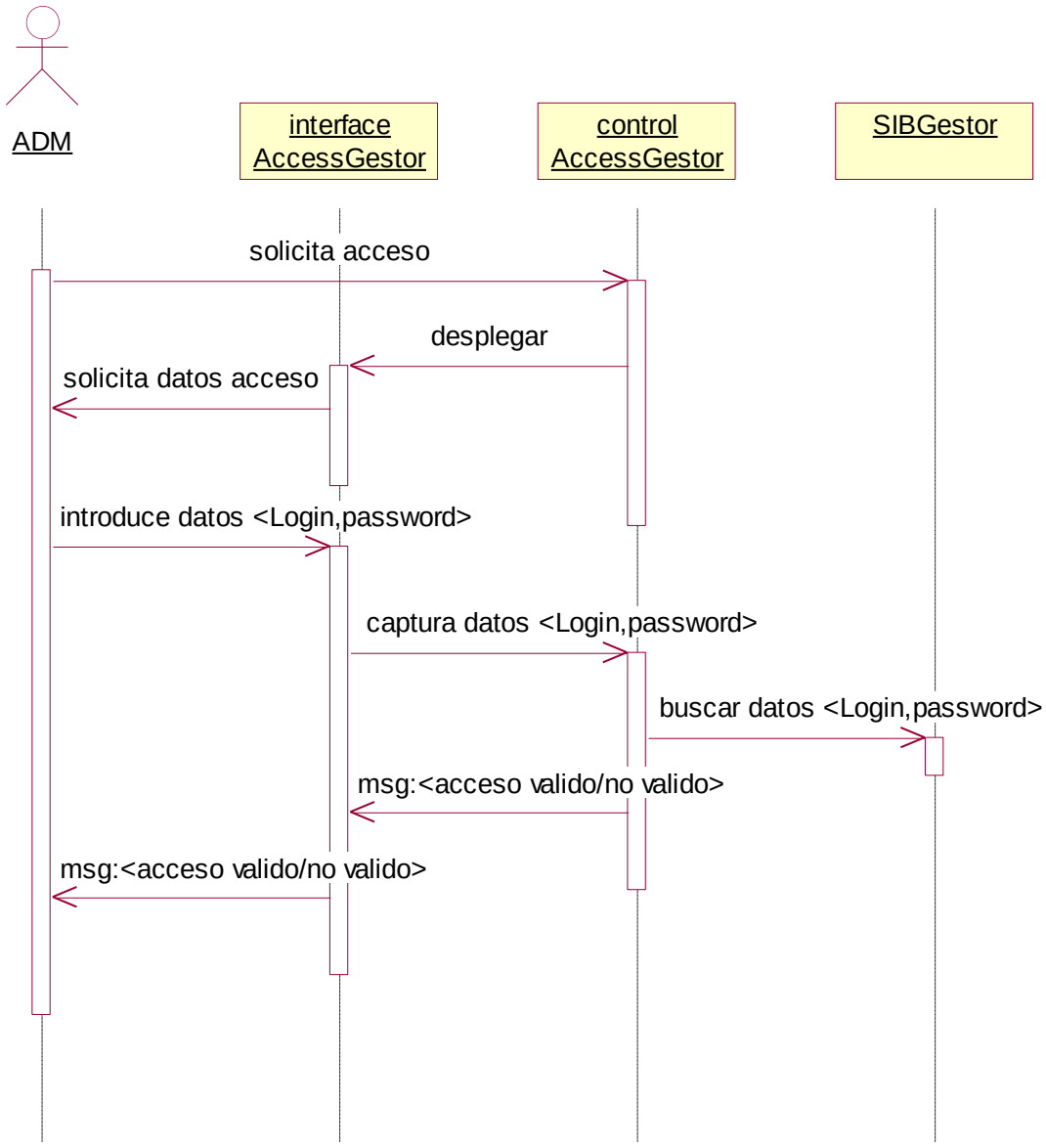
Caso de Uso	Ver Información
Actor	Responsable, Usuario_Final
Tipo	Secundario
Descripción	Cualquier usuario estará en la posibilidad de visualizar la información de contenido respecto a las políticas (significado, explicación, nivel de protección, sanción) que en ese momento se han aprobado e implementado desplegando una interfaz visual similar a las clases de ayuda de software, con la diferencia que esta información se modificará de forma dinámica.

Caso de Uso	Enviar Mensaje
Actor	Responsable, Usuario_Final
Tipo	Secundario
Descripción	En caso de alguna anomalía, sugerencia, necesidad de soporte técnico, problema o conflicto donde el usuario final o el responsable requieran información adicional, se podrá activar una opción de mensajería mediante la cual se puede enviar un E-mail desde la posición del Agente de Control, el cual se transferirá al módulo de Gestión para que el ADM brinde la respuesta oportuna.

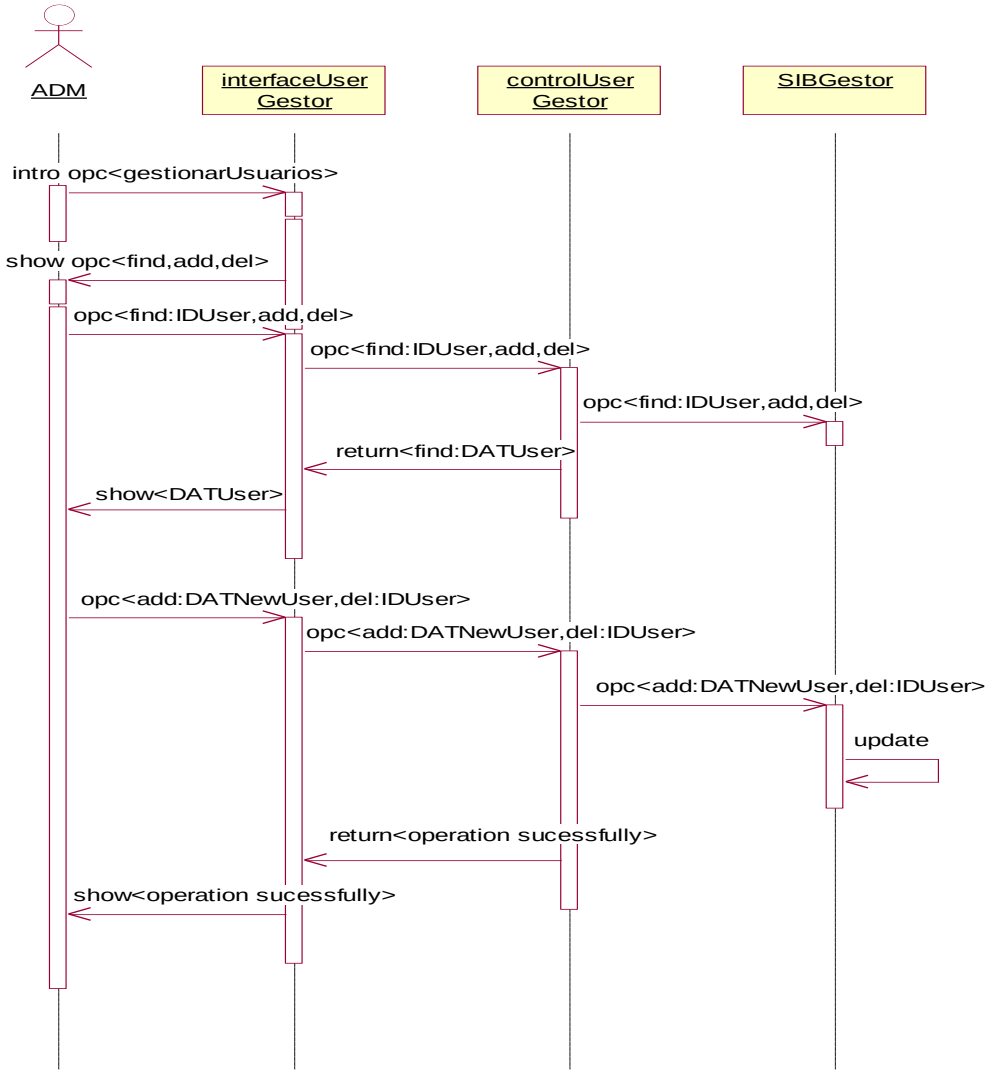
Caso de Uso	Ejecutar Control
Actor	Equipo Terminal
Tipo	Primario
Descripción	Este caso de uso representa la interacción del Agente de Control con el Sistema Operativo del equipo terminal, y del cual se obtendrá, modificará, adicionará o eliminará la información necesaria para llevar a cabo el control de las políticas implementadas por el ADM a través del Módulo Gestor.

DIAGRAMAS DE SECUENCIA GESTOR

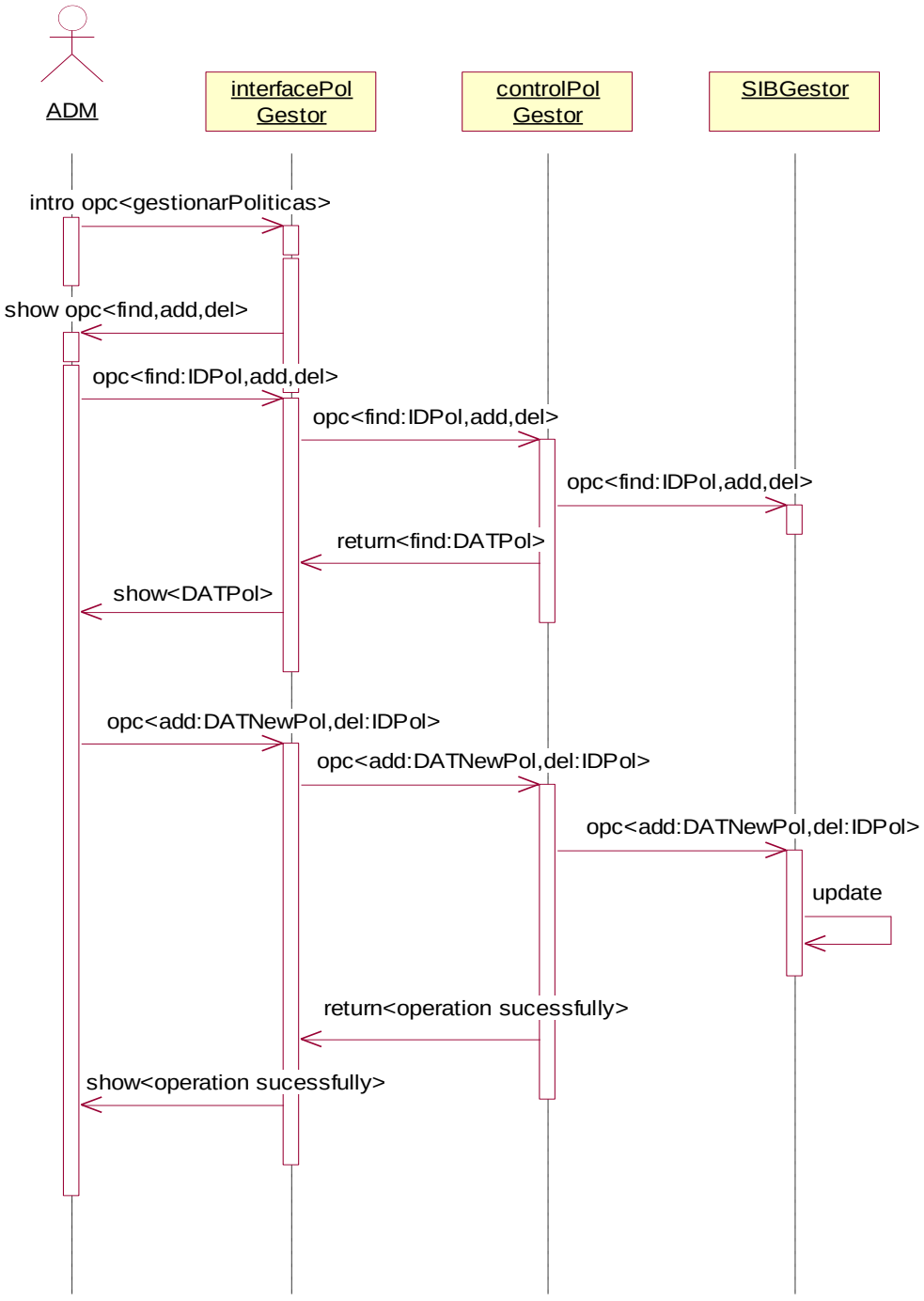
- ValidarAcceso



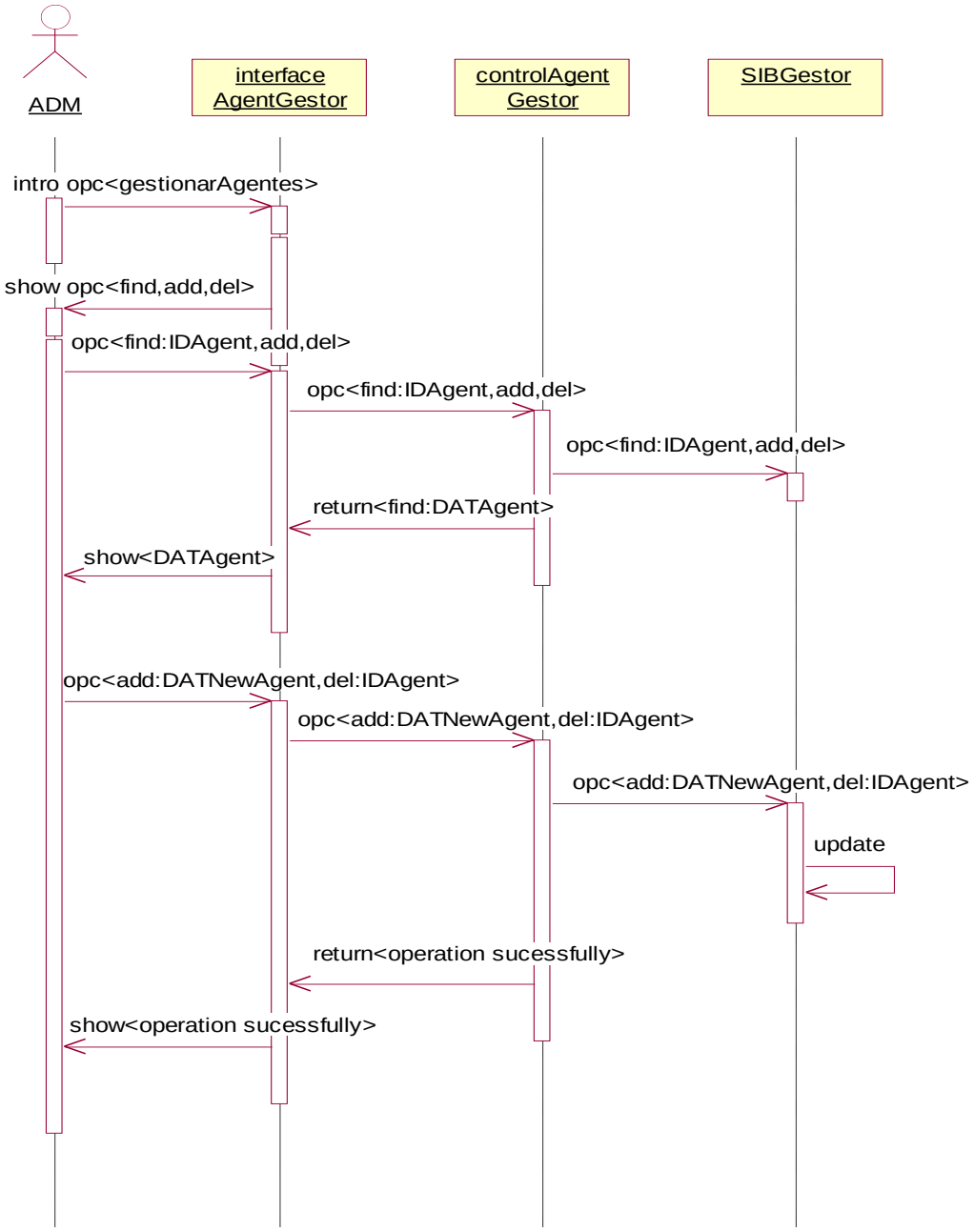
- GestionarUsuarios



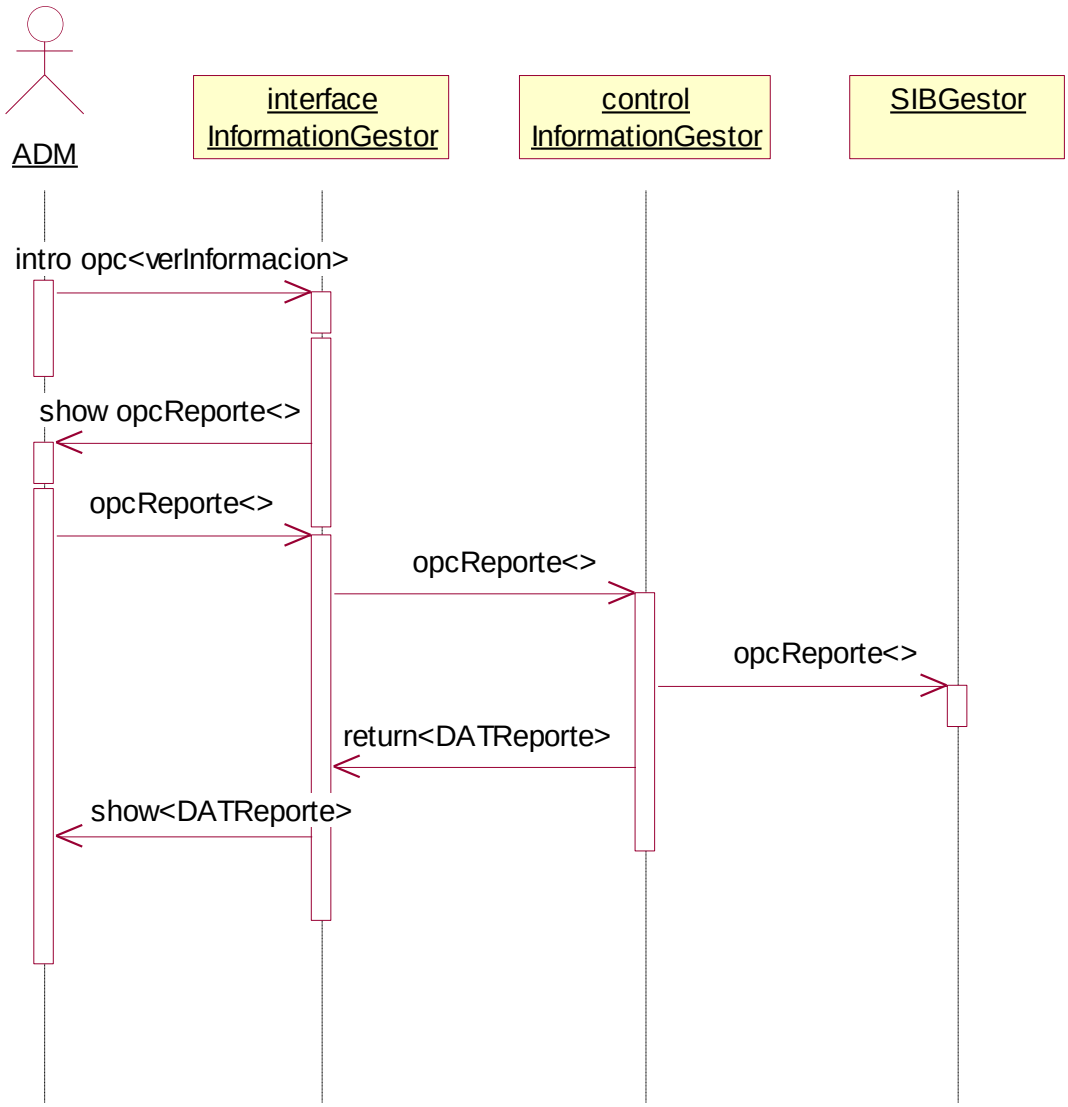
- GestionarPoliticas



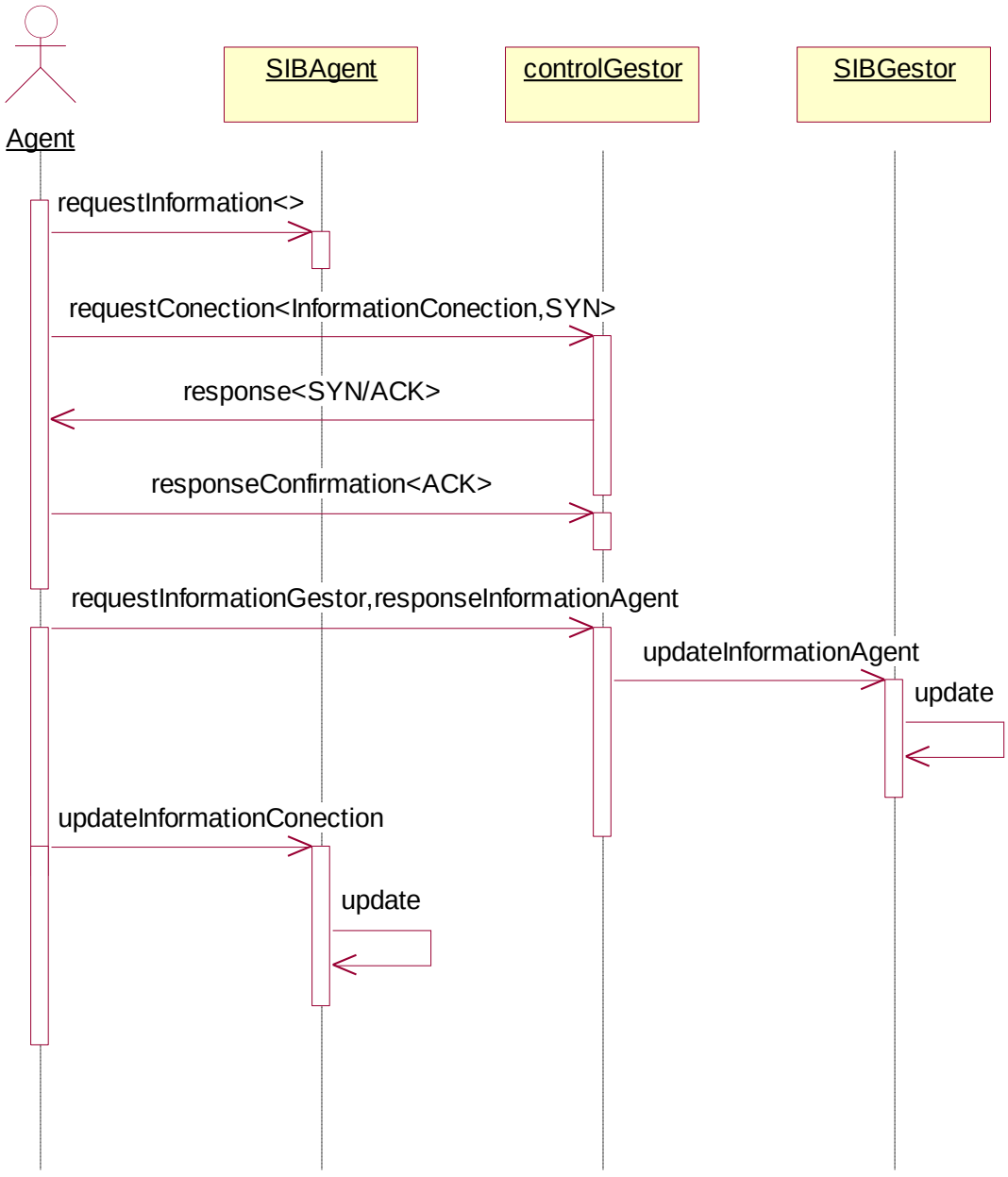
- GestionarAgentes



- Ver Información

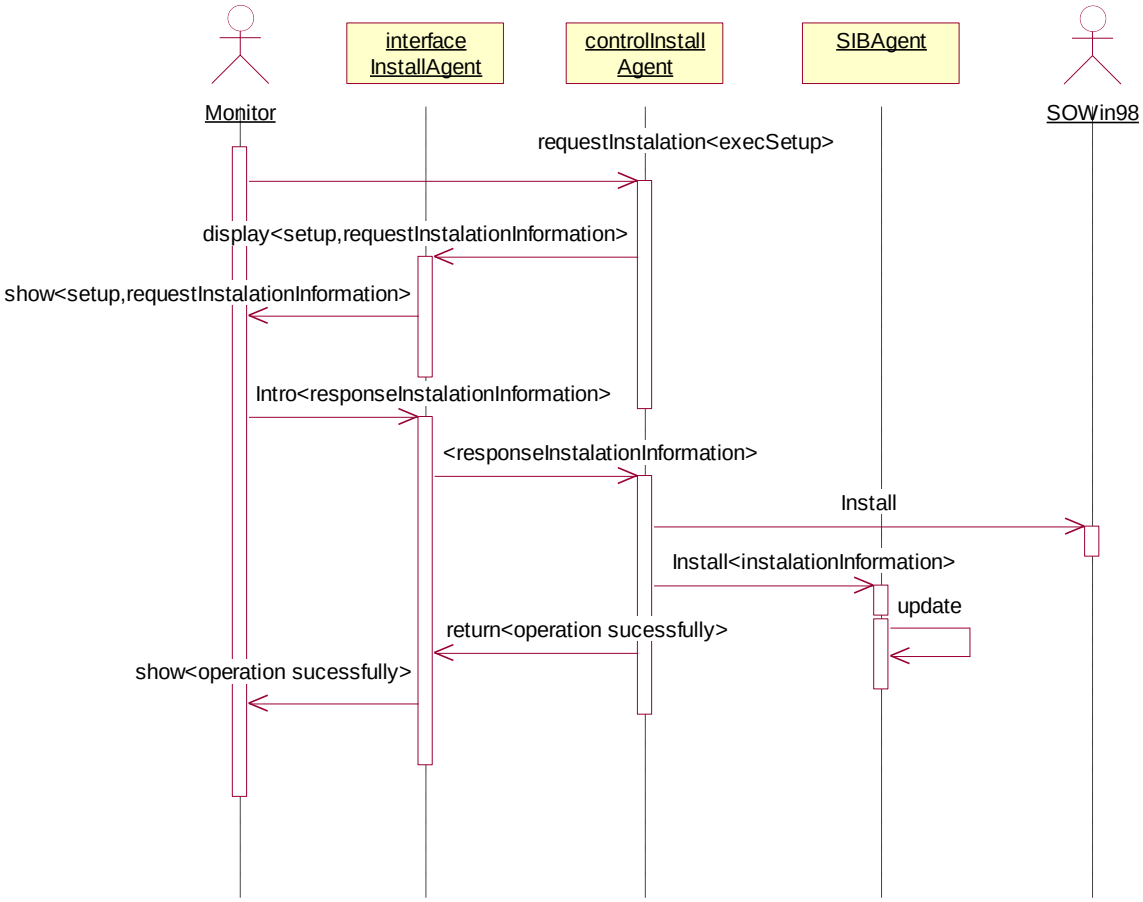


- conectar-intercambiar Información

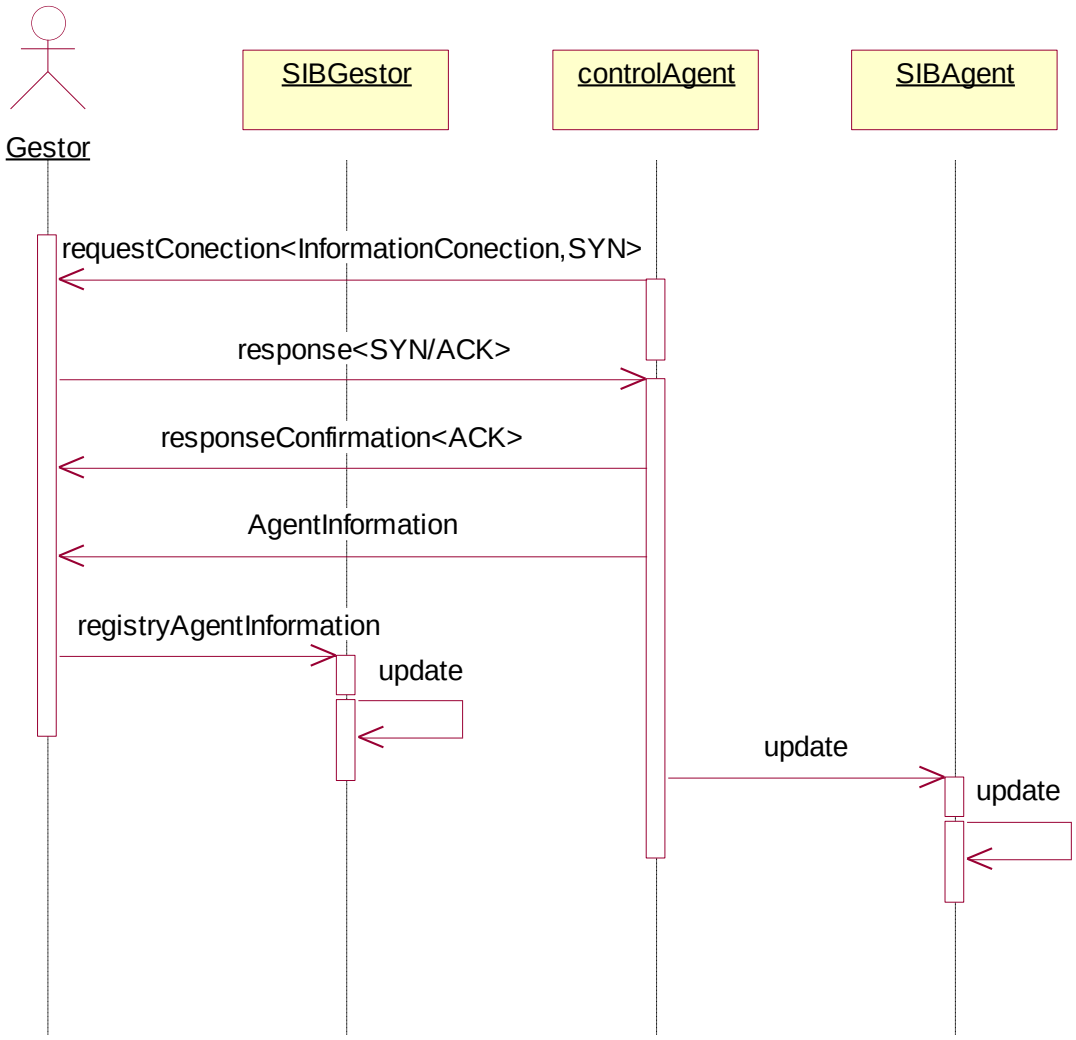


DIAGRAMAS DE SECUENCIA AGENTE

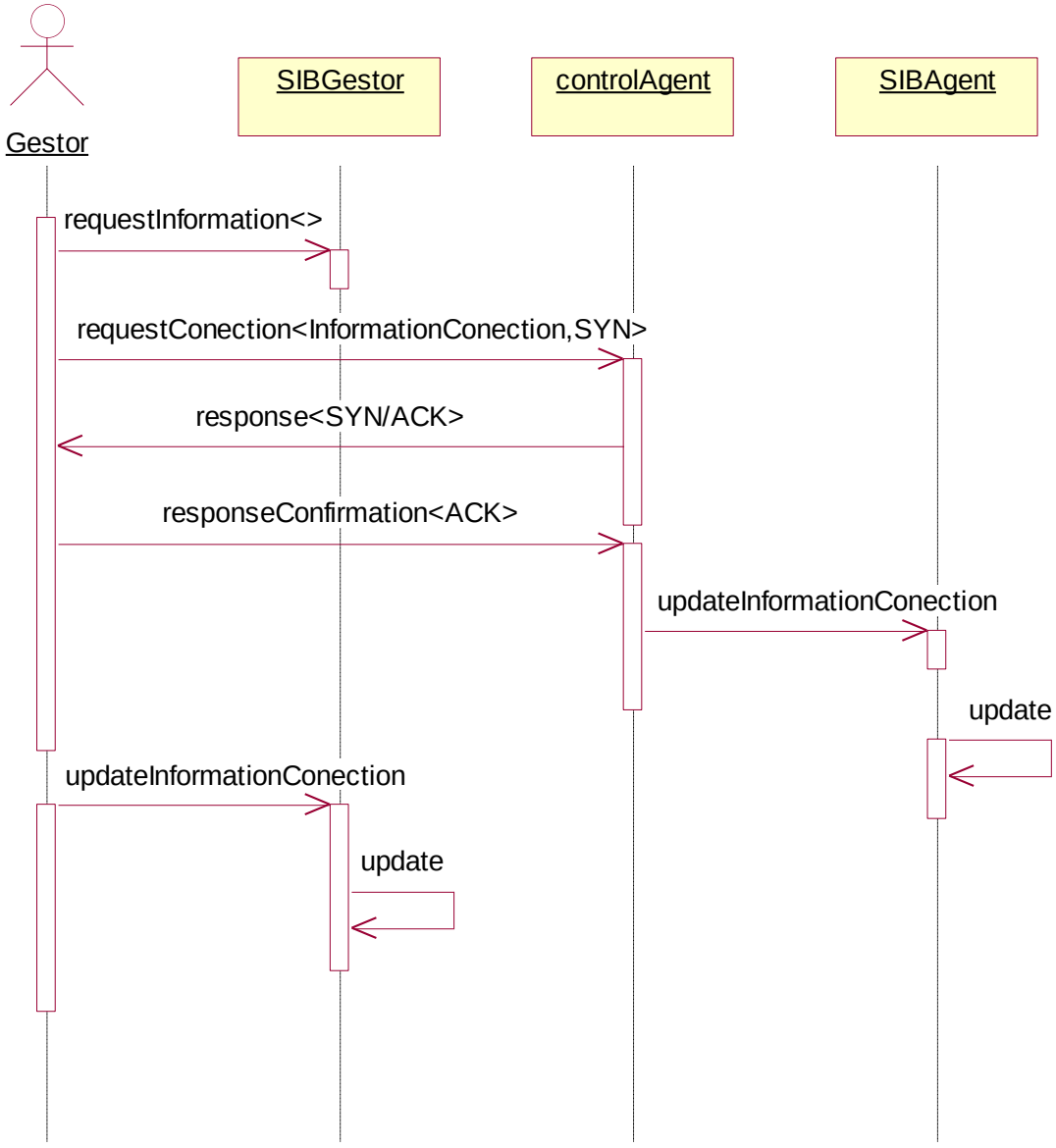
- Instalar



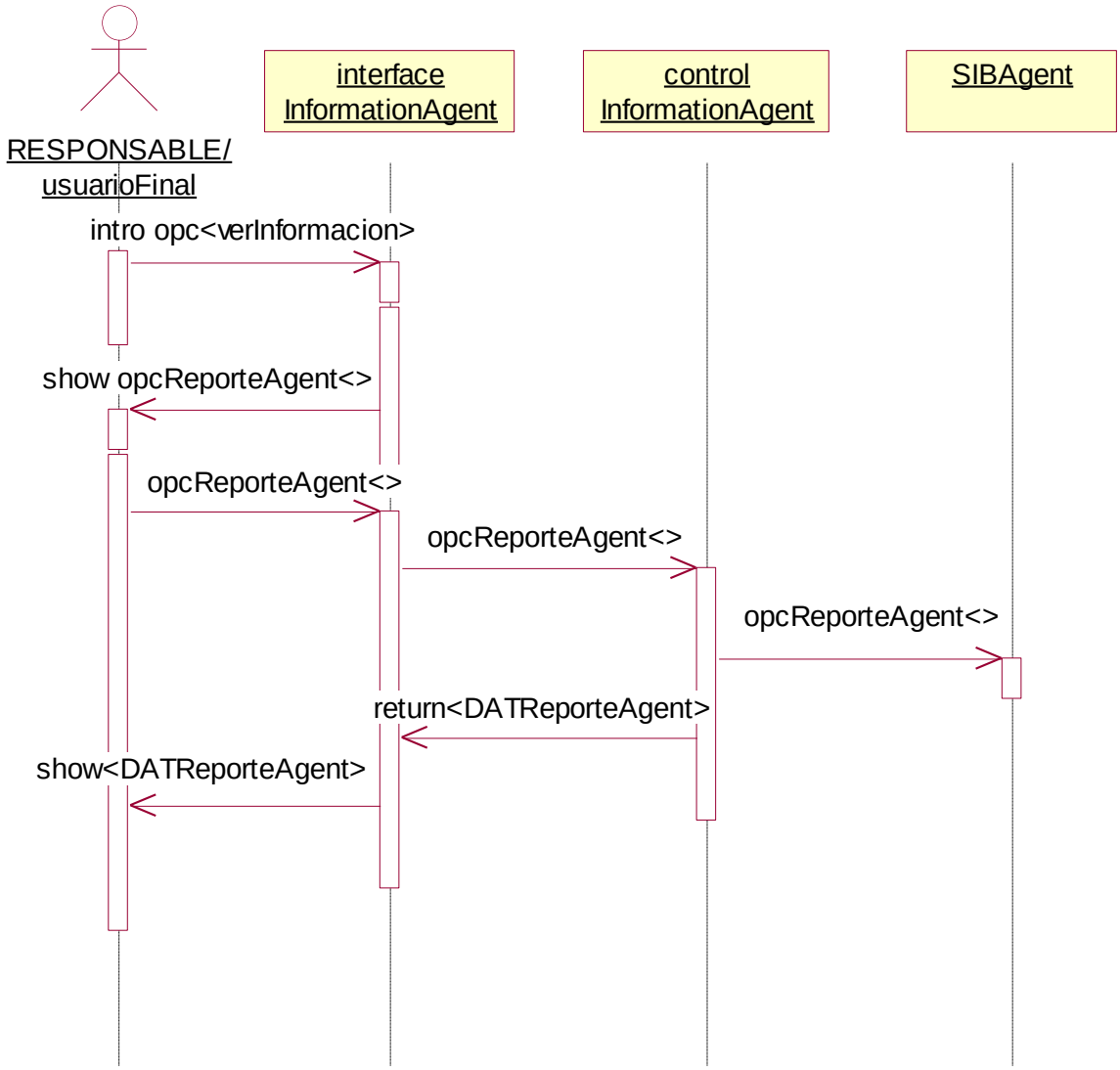
- Registrar


Gestor
SIBGestor
controlAgent
SIBAgent
requestConection<InformationConection,SYN>
response<SYN/ACK>
responseConfirmation<ACK>
AgentInformation
registryAgentInformation
update
update
update

- Conectar-intercambiar Información



- Ver Información Agente



- Enviar Mensaje

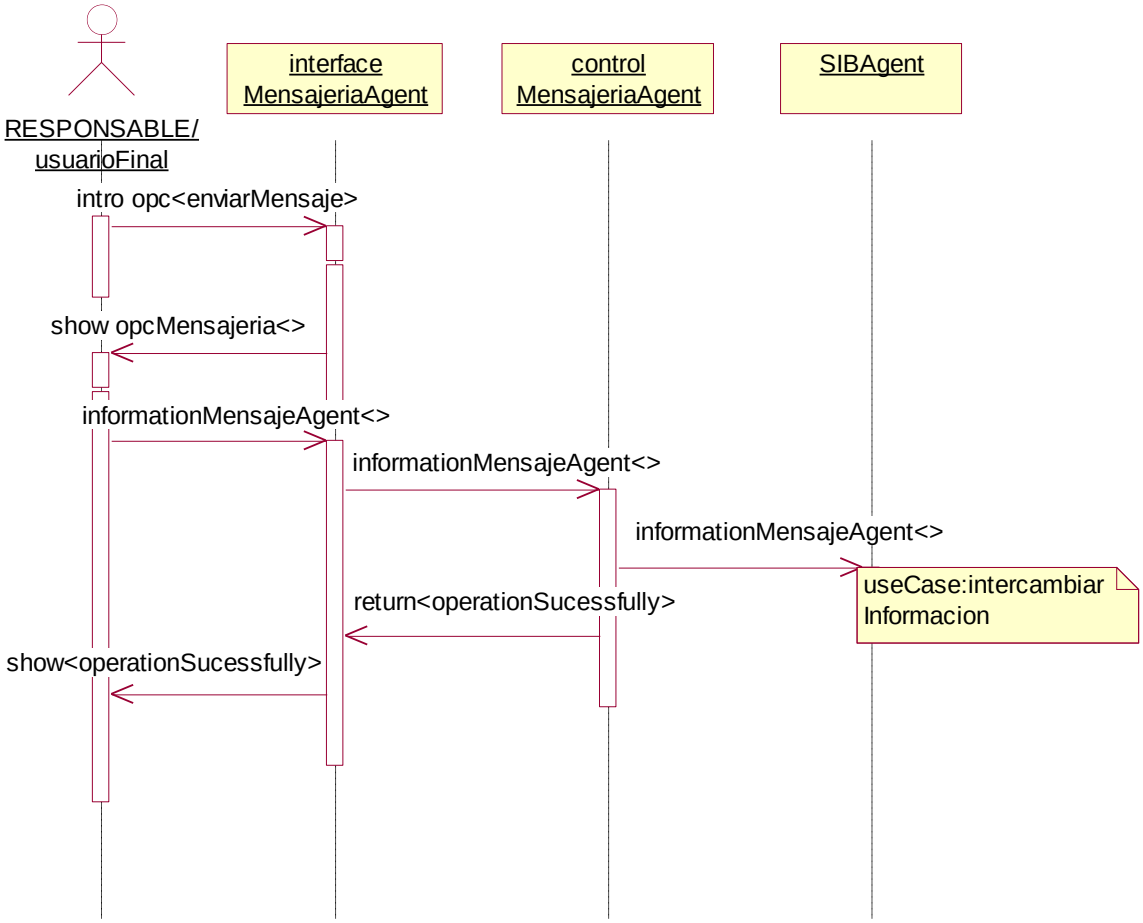


DIAGRAMA DE CLASES HEGCON - PS