1. Personal Vinculado al Proyecto

1.1 Director de Proyecto

Castellón Apellido Paterno	Mansilla Apellido Materno	Jimena Nombre	10704992 C.I.
1 Grupo de Taller III	Ingeniería Informática Carrera	Ciencias y Tecnología Facultad	
46691170 Teléfono	79265126 Celular	jimecas.53@gmail.com Correo electrónico	Firma

1.2 Participantes equipo de trabajo (señale categoría: Director, Tutor, Asesores)

Categoría	Nombres y Apellidos	Profesión	C.I.	Firma
DIRECTOR	Jimena Ruth Castellón Mansilla	Universitario	10704992	
TUTOR	Marcelo Céspedes	Ing. Electrónico		

1.3 Equipo de trabajo de: Empresas/Instituciones/Organizaciones participantes/cooperantes

Nombre:			
Dirección:		**Telf. Oficina:**	
Nombres y Apellidos	**Cargo**	**C.I.**	**Firma**

1.4 Actividades previstas para los integrantes del equipo de investigación

Responsable *	Actividades
DIRECTOR	Debe realizar un seguimiento constante del cumplimiento a tiempo de las actividades que conlleva el proyecto para evitar retrasos. Cumplir con las fechas de presentaciones en el proceso de desarrollo del proyecto.
TUTOR	Colaborar con la investigación. Orientar en el desarrollo del Sistema Informático que contiene el Proyecto. Coadyuvar con la preparación del estudiante para la defensa.

2. Descripción del Proyecto

2.1. Resumen Ejecutivo del Proyecto

La infraestructura de una Organización debe ser adecuada, ya que si los ambientes son adecuados, el personal trabajará de manera más cómoda y satisfactoria, lo que hará que sean eficientes en las diferentes laborales que desempeñan en la organización a la cual pertenecen, coadyuvando de manera positiva a la actividad principal a la cual se dedica la Organización, ya sea la prestación de servicios que se consideran necesarios para el desarrollo de fines productivos, personales, políticos y sociales o la elaboración de productos industriales.

Un aspecto importante a resaltar, es la seguridad con la que debe contar la infraestructura; tanto para el personal, como para los inmuebles que se encuentran dentro de la misma.

En algunas organizaciones se utilizan equipos de alto costo o de manejo delicado, como también se maneja información confidencial, y que en caso de pérdida o daño ocasiona un grave problema, es por eso que existen áreas restringidas donde sólo personal selecto y autorizado puede ingresar y en las cuales el acceso es restringido y debe ser debidamente controlado como parte de una medida de seguridad.

El uso de las TIC para solucionar este tipo de problemas, como lo es de la inseguridad actual en la infraestructura de una Organización, es una de las mejores alternativas a ser propuesta; ya que con su uso llegamos a automatizar la mayor cantidad de procesos, utilizando tecnología de punta y de costo accesible, obteniendo como resultado que éstos se realicen en mucho menor tiempo a comparación de realizarlos manualmente, además de garantizar mayor seguridad a la infraestructura.

El control automatizado es el mantenimiento de un valor deseado dentro de una cantidad o condición, midiendo el valor existente, comparándolo con el valor deseado, y utilizando la diferencia para proceder a reducirla. En esta ocasión, en el control automatizado el lazo

exigido se dará cuando identifique la tarjeta RFID (tarjeta de identificación) por el lector de la misma y la apertura automatizada de ambientes.

El propósito principal del Proyecto es mejorar el Control de acceso del Personal a las áreas restringidas de la infraestructura de una Organización.

El primer paso a seguir es la Elaboración y acondicionamiento de un modelo de normas de restricciones y funciones que debe regir sobre el total del personal de la Organización, el cual se elaborará por medio de Asambleas Internas.

Gracias al Modelo mencionado anteriormente, se desarrollará un sistema que autorizará oportunamente el acceso automatizado, por medio de la asignación de una tarjeta de identificación única (tecnología RFID) a cada miembro del personal; la cual estará debidamente configurada de acuerdo a su rol y según el modelo de normas de restricciones, mostrando a qué áreas tendrá permiso de acceso el usuario, dicha tarjeta al ser reconocida abrirá automáticamente la puerta de cada ambiente y en el caso de ser forzada alguna de estas puertas, se activará una alarma.

La tecnología a ser aplicada en este sistema que automatizará el control, serán las tarjetas RFID o tarjetas de identificación de radiofrecuencia, debido a la seguridad que presenta actualmente y la adaptabilidad que posee para este Proyecto, además de ser una innovación tecnológica que va tomando fuerza en diferentes sectores. Una gran ventaja es que estas tarjetas no necesitan contacto físico como ser introducidas a una ranura; solo con aproximarla a cierta distancia del lector, la tarjeta reconoce el código y es validada.

Posteriormente se aplicarán ciertas estrategias de socialización; como talleres y conferencias donde se dará a conocer en una primera instancia el Proyecto en general con sus componentes como lo son: El modelo de normas de restricciones, el Sistema de Control Automatizado desarrollado y el uso de su nueva tecnología para posteriormente poder medir de alguna manera el éxito del Proyecto finalizado.

Según las investigaciones realizadas previamente antes de formular este Proyecto, actualmente existen algunos sistemas ya desarrollados para el control de acceso en organizaciones de países vanguardistas en tecnología como lo son Japón, China, Estados Unidos y algunos países Latinoamericanos, la tecnología más utilizadas por éstos son los biométricos con huella digital o tarjetas que tienen que ser introducidas a una ranura para ser reconocidas, pero estos sistemas cuentan con muchos requisitos para poder ser implementados en distintas infraestructuras, además de ser económicamente no muy accesibles, lo que como consecuencia, genera que no muchas organizaciones se animen a implementarlas.

2.2. Descripción y Fundamentación del Proyecto (qué y por qué)

Este Proyecto pretende contribuir a mejorar la seguridad de la infraestructura de una Organización, es por eso que tiene como objetivo general: Mejorar el control del acceso del Personal a áreas restringidas de la misma, en el cual los procesos relacionados serán automatizados. Por lo que, para que este objetivo general sea exitoso, será necesario que la organización involucrada cuente con sus normas de restricciones bien definidas; esto se logrará gracias a las asambleas mensuales que se llevarán a cabo para definir estos aspectos de seguridad; además de contar con una mejor administración del personal por parte del Director de Recursos Humanos. Las áreas restringidas contarán con mayor seguridad ya que, se evaluará la posibilidad de aumentar el presupuesto que este destinado para este aspecto muy importante, haciendo el uso de nuevas tecnologías. El proceso de registro del personal será más ágil por que contará con nueva tecnología, sobre la cual se realizará la debida investigación para estar bien informados sobre la aplicación de la misma. Estas distintas actividades relacionadas coadyuvarán a cumplir el objetivo general del proyecto.

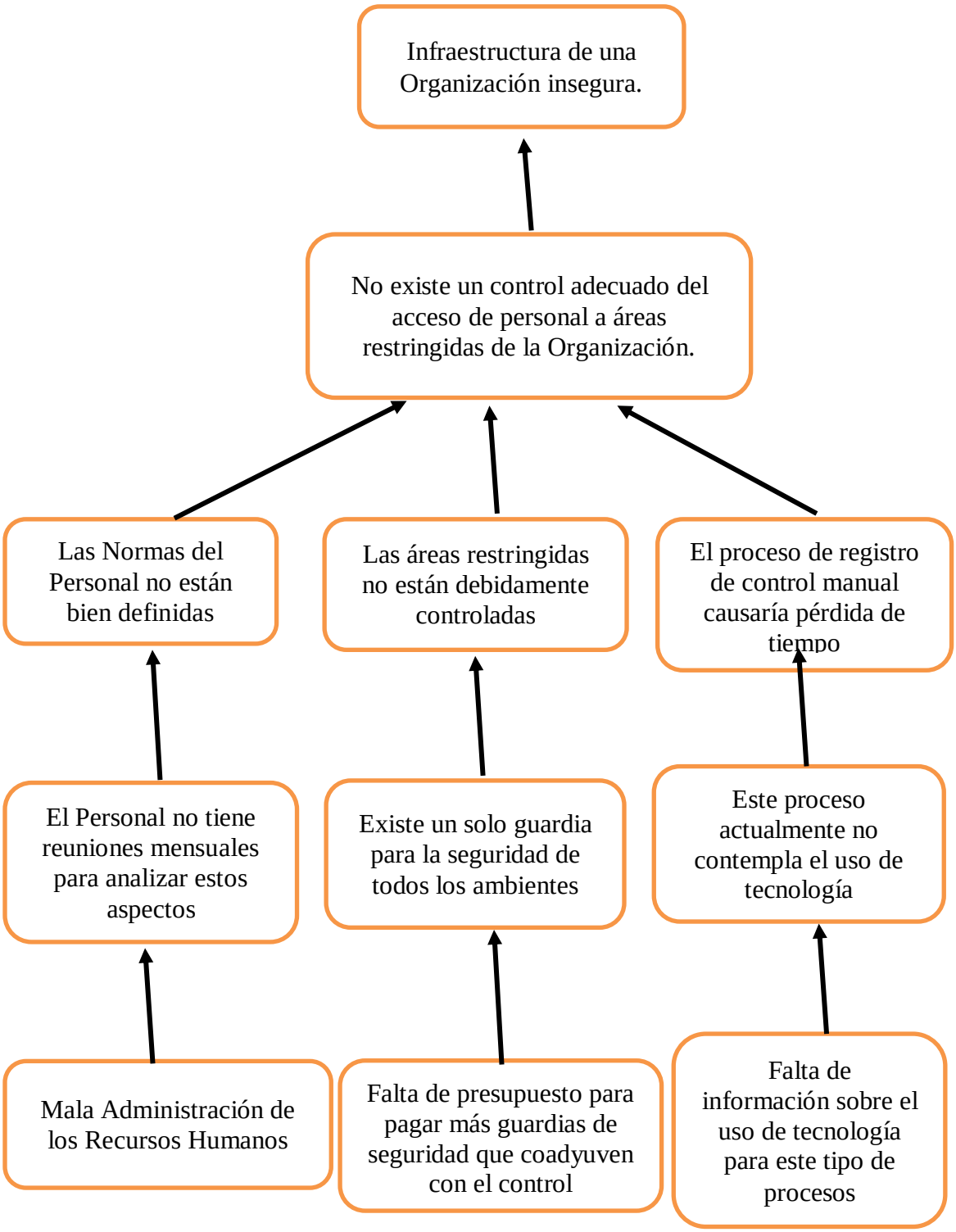
Se vio necesario realizar este Proyecto ya que no hay un buen control de acceso de personal a determinadas áreas restringidas de una Organización, lo cual provoca la inseguridad en la infraestructura de la misma.

La inseguridad en la infraestructura, es causado a su vez por varios factores como ser, la falta de normas de restricción para el personal bien definidas por parte de la Organización, debido a que el Personal no tiene asambleas mensuales en las cuales puedan tocar estos temas como lo es la seguridad en la infraestructura, lo que denota que existe quizá una mala Administración de los Recursos Humanos.

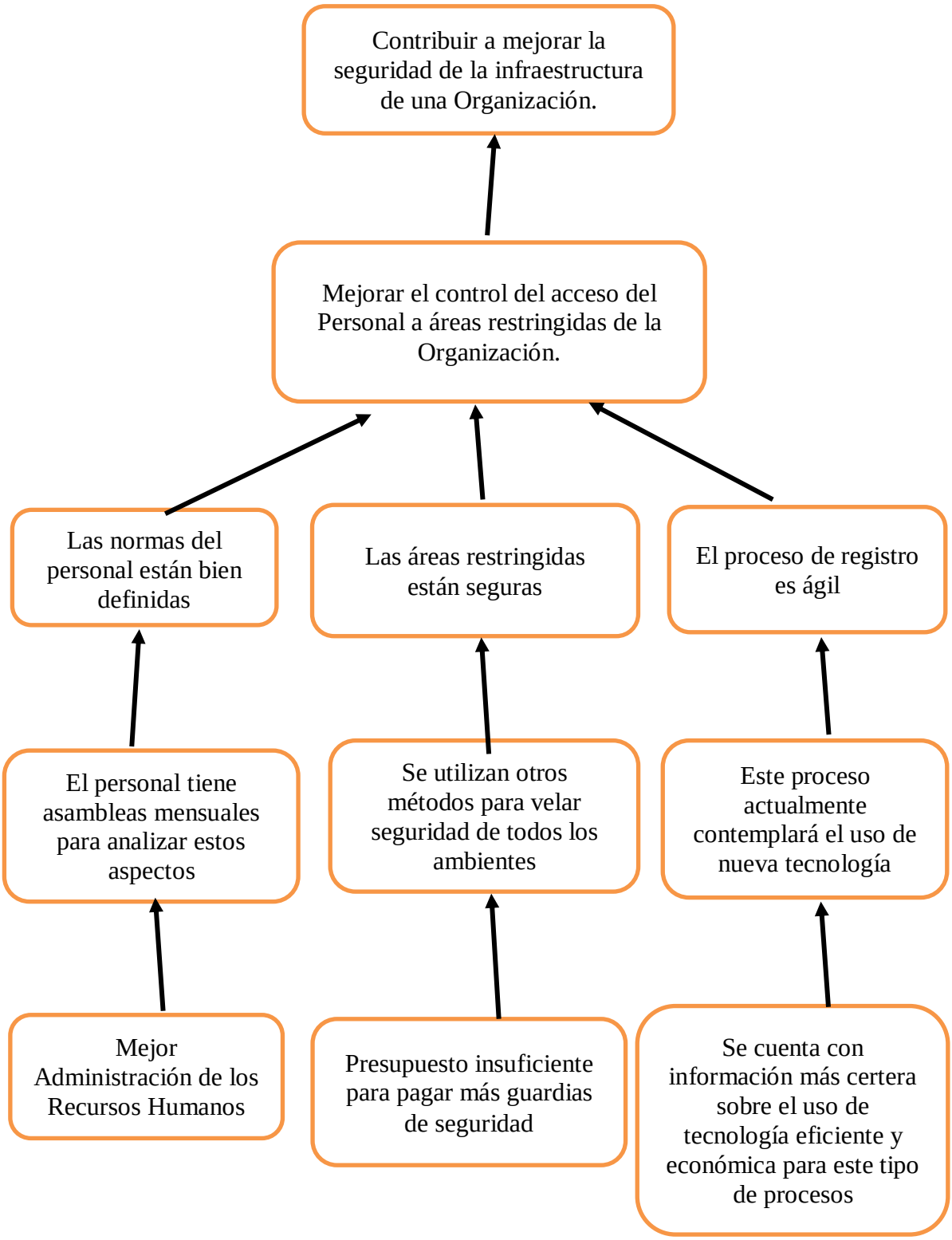
El uso personal de un guardia para velar el aspecto de seguridad en la infraestructura es una estrategia caduca; además que no se cuenta con el presupuesto suficiente para reforzar este aspecto. El proceso de registro del personal para tratar de realizar un control de accesos no cuenta actualmente con el uso de tecnología, quizá por falta de información sobre ello, lo que hace que este proceso sea lento y poco eficiente causando pérdida de tiempo.

a) Análisis de Causas del Problemas

ARBOL DE PROBLEMAS



b) Análisis de objetivos
ARBOL DE OBJETIVOS



d) Situación planteada Con y Sin Proyecto

Situación Sin Proyecto	Situación Con Proyecto
Las áreas restringidas de la Organización actualmente no se encuentran debidamente seguras con relación al personal que ingresa y sale de las mismas. Quizá esto se debe a que el personal no se encuentra debidamente informado a qué áreas pueden tener acceso según los roles que cumplen en la Organización lo que provoca cierta inseguridad y susceptibilidad en cuanto a posible pérdida de documentación o artefactos de valor que se encuentran en ciertas áreas.	Se ha mejorado en un gran porcentaje el control de acceso del personal a áreas restringidas de la infraestructura de la Organización, gracias a que el personal ahora se encuentra debidamente informado sobre el acceso que tienen según sus roles a diferentes áreas de la infraestructura, esto también se ha visto reflejado por medio de la satisfacción expresada por todo los funcionarios de la misma, los cuales alegan que gracias a este proyecto, al mismo tiempo que generó una mejor seguridad para la infraestructura de la Organización, también lo hizo para el personal que trabaja en las mismas instalaciones.

2.3. Objetivos

2.3.1 Objetivo General (Propósito)

Mejorar el Control seguro y eficiente de acceso del Personal a áreas restringidas de una Organización mediante la utilización de nuevas TIC, a costos accesibles en el corto plazo.

2.3.2 Objetivos Específicos (Componentes)

- Elaborar un modelo genérico de normas de ingreso a infraestructuras restringidas.
- Desarrollar un sistema para el control de acceso del personal a áreas restringidas de una Organización.
- Implementar estrategias de socialización para dar a conocer; tanto el modelo de norma creado, como el producto resultante del Proyecto y la nueva tecnología utilizada para el mismo.

Resumen Narrativo del Proyecto	Indicadores	Medios de Verificación	Supuestos
Fin • Contribuir a mejorar la seguridad de la infraestructura de una Organización.	• A un año de finalizado el Proyecto al menos un 90% de los funcionarios de la organización piloto, expresa su conformidad en cuanto a la seguridad implementada.	• Cuadro satisfactorio que refleja una encuesta hecha a los funcionarios de la Organización.	• Contar con el presupuesto necesario para implementar la nueva tecnología. • Contar con la colaboración del personal de la Organización para brindar la información necesaria para el Proyecto. • Contar con la tecnología adecuada para el Proyecto.
Objetivo General (Propósito) • Mejorar el Control seguro y eficiente de acceso del Personal a áreas restringidas de una Organización mediante la utilización de nuevas TIC, a costos accesibles en el corto plazo.	• Al finalizar el Proyecto, al menos un 90% de los procesos inherentes al Control de áreas restringidas en la Organización han sido automatizados.	• Cuadro comparativo entre el total de procesos identificados y el número de procesos automatizados, avalado por el Docente de Taller III y el Asesor del Proyecto.	• Se tenga un presupuesto para realizar el necesario mantenimiento al Sistema Informático. • Identificar minuciosamente las estrategias a tomar para cumplir el propósito.
Objetivos Específicos (Componentes) • Modelo genérico, de normas de restricción para la infraestructura, elaborado. • Sistema informático para el control de acceso del Personal	• En los primeros dos meses de iniciado el Proyecto, se realizan varias Asambleas con el Personal de donde se obtiene un Manual de Funciones completo. • A los 7 meses de iniciado el Proyecto, se ha desarrollado un Sistema de Control de acceso a	• El Manual de Funciones es entregado y socializado con todo el Personal. • Documento donde se informa sobre la entrega del Sistema Informático,	• Contar con la aceptación positiva del modelo genérico de normas por todos los funcionarios. • Se cuenta con toda la información necesaria para el desarrollo del Sistema, y éste,

a áreas restringidas desarrollado. • Taller de socialización del Modelo genérico de Norma de Restricciones y Sistema Informático.	áreas restringidas, basado en requerimientos expresados bajo la norma IEEE830. • Al finalizar el taller, al menos un 90% del Personal de la Organización tendrá conocimiento sobre estos dos componentes del Proyecto.	avalado por Docente de Taller III y el Asesor del Proyecto. • Lista de los asistentes al taller con respectivos nombre completos, números de carnet y firmas.	al finalizar cuenta con la calidad necesaria. • Se cuenta con la Documentación de la investigación minuciosa y conocimiento necesario para el uso de la nueva tecnología. • Determinar un día en el cual todo el personal de la Organización pueda asistir al taller.
Actividades • Modelo genérico de Normas de restricción para la infraestructura, elaborado. - Relevamiento de datos - Desarrollo del Modelo - Verificación del Modelo - Aprobación del Modelo	**Resumen del Presupuesto:** Servicios Personales 10500.- Servicios No Personales 5000.- Materiales de escritorio 300.- TOTAL 13800.-	• El Proyecto implementado, el Sistema instalado y puesto en marcha. El Propósito del Proyecto ha sido cumplido a cabalidad se tiene un Control mejorado del acceso del Personal a las áreas restringidas de la Organización piloto.	• Definir correctamente el tiempo en que se realizará cada actividad que en conjunto formarán cada uno de los componentes, para que el Proyecto sea finalizado a tiempo con éxito.

• Sistema informático para el control de acceso del Personal a áreas restringidas desarrollado. - Inicio - Elaboración - Construcción - Transición - Capacitación de usuarios para el uso del sistema	**Resumen del Presupuesto:** Levantamiento de Redes 1500.- Sistema Web 28000.- Capacitación 300.- TOTAL 29800.-		

2.4 Marco Lógico del Proyecto

2.5 Metodología de Trabajo

Componente 1: **Modelo genérico de Normas de restricción para la infraestructura, elaborado.**

No existe una metodología bien definida para poder elaborar estos modelos genéricos. Es por eso que nos basaremos en el proceso que se sigue para el diseño de Normas, el cual toma como base las necesidades, tratando de vincular del modo más ordenado y ejecutivo posible, el estado de la tecnología con el factor humano que es el actor principal y para el cual se elaborará dicho documento.

Es importante tomar en cuenta que las Normas deben incluir aquellos aspectos que faciliten el cumplimiento de los objetivos aplicados a la Organización, los que a su vez generarán como utilidad, la reducción de riesgos, mejora de las comunicaciones, optimización de las actividades.

Componente 2: **Sistema Informático para el Control de acceso del Personal a áreas restringidas.**

La metodología que se usará con el Sistema Informático de este Proyecto es RUP (Proceso Racional Unificado) el cual constituye la metodología estándar más utilizada para el análisis, diseño, implementación y documentación de Sistemas.

Se vio muy conveniente trabajar con esta metodología ya que la misma se adapta al contexto y necesidades de cada Organización en la que se aplicará el Sistema.

RUP cuenta con 4 fases principales:

- Inicio: Tiene como propósito definir los objetivos, definir y acordar el alcance del Proyecto con los financiadores, dar a conocer una visión muy general de la arquitectura del software a desarrollar.

- Elaboración: En la fase de elaboración se seleccionan los casos de uso que permiten definir la arquitectura base del Sistema que se desarrollará en esta fase, se realiza la especificación de los casos de uso seleccionados y el primer análisis del dominio del problema, se diseña la solución preliminar.

- Construcción: El propósito de esta fase es completar la funcionalidad del Sistema, para ello se deben clarificar los requisitos pendientes, administrar los cambios de acuerdo a las evaluaciones realizadas por los usuarios y se realizan las mejoras para el Proyecto.

- Transición: El propósito de esta fase es asegurar que el software esté disponible para los usuarios finales, ajustar los errores y defectos encontrados en las pruebas de aceptación, capacitar a los usuarios y proveer el soporte técnico necesario. Se debe verificar que el producto cumpla con las especificaciones entregadas por las personas involucradas en el Proyecto.

b) Cronograma de Actividades

Nº	Actividad	Nº días	M1	M2	M3	M4	M5	M6	M7	M8
1.	Componente 1: Modelo genérico de Normas para la restricción de la infraestructura. (Elaborado)									
1.1.	Relevamiento de información	20	X							
1.2	Desarrollo del Modelo	15		X						
1.3	Verificación del Modelo	10		X						
1.4	Aprobación del Modelo	5		X						
2.	Componente 2: Sistema informático para el Control de acceso del Personal a áreas restringidas.(Desarrollado)									
2.1	Inicio	20			X					
2.2	Elaboración	20				X				
2.3	Construcción	130				X	X	X	X	
2.4	Transición	15								X
2.5	Capacitación	2								X
3.	Taller de Socialización	1								X

2.6 RESULTADOS ESPERADOS

- Modelo genérico de Normas de restricción para la infraestructura, elaborado.

  Este Modelo de Normas que será aprobado por la Autoridad máxima de la Organización ayudará que todos los funcionarios de la misma estén respectivamente informados sobre las áreas en las cuales pueden acceder, conforme al rol o función que cumplen en la Organización, lo que no dará lugar a confusiones en este aspecto en un futuro.

- Sistema informático para el control de acceso de personal a áreas restringidas desarrollado.

  Este Sistema brindara mayor seguridad a la infraestructura de la Organización piloto, por medio del control de acceso a diferentes áreas de cada empleado de acuerdo a sus respectivas normas ya establecidas. También el administrador del sistema podrá obtener ciertos reportes sobre los movimientos de los diferentes empleados.

2.7 Transferencia de resultados

a) Grupo de beneficiarios de los resultados

Todos los funcionarios de la Organización desde el Director o Gerente de la Organización hasta los funcionarios que pertenecen a la misma.

2.8 Bibliografía consultada

Que es RUP (Concepto)
El RUP no es un sistema con pasos firmemente establecidos, sino un conjunto de metodologías adaptables al contexto y necesidades de cada organización.
https://es.wikipedia.org/wiki/Proceso_Unificado_de_Rational

Como elaborar una Norma, qué metodología se puede usar.
www.codeinep.org/norma.doc

Labores de un asesor o tutor
http://www.saber.ula.ve/bitstream/123456789/31485/1/articulo3.pdf

Sobre los modelos de lectores de RFID para el Proyecto
http://www.kimaldi.com/productos/sistemas_rfid/controles_de_acceso_rfid/lector_rfid_uhf_para_el_control_de_acceso_stid_gat

Que es RFID (Conceptos, Funcionalidades, Características)
http://www.egomexico.com/tecnologia_rfid

RFID con Arduino para control de accesos
http://miarduinounotieneunblog.blogspot.com.es/2016/02/control-de-acceso-con-el-modulo-rfid.html

Trabajando un módulo RFID con arduino UNO
http://hetpro-store.com/TUTORIALES/modulo-lector-rfid-rc522-rf-con-arduino/

Tipos de tarjetas RFID
https://es.wikipedia.org/wiki/RFID

Definición de la Infraestructura de una Organización en general.
http://www.definicionabc.com/general/infraestructura.php

Control Automatizado – Definición , características
https://es.wikipedia.org/wiki/Ingenier%C3%ADa_de_control

INDICE

1. INTRODUCCIÓN

La administración adecuada de las instalaciones que forman parte de la infraestructura física de una Organización, está directamente relacionada con el cumplimiento de los objetivos de la misma.

En este documento se presenta un modelo de Normas y Procedimientos a seguir por una Organización; gracias a las cuales se podrán administrar de forma eficaz las áreas denominadas restringidas con las que cuenta la infraestructura física de la Organización.

2. VISION Y MISION DE LA ORGANIZACIÓN

2.1. Visión

La misión define principalmente cuál es la labor o actividad que realizará la Organización, además se puede completar haciendo referencia al público hacia el que va dirigido y con la singularidad, particularidad o factor diferencial, mediante la cual desarrolla su labor o actividad. Para definir la misión de una empresa, una buena ayuda es responder algunas de las siguientes preguntas: ¿Qué hacemos?, ¿cuál es nuestro negocio?, ¿a qué nos dedicamos?, ¿cuál es nuestra razón de ser?, ¿quiénes son nuestro público objetivo?, ¿cuál es nuestro ámbito geográfico de acción?, ¿cuál es nuestra ventaja competitiva?, ¿qué nos diferencia de nuestros competidores?

2.2. Misión

La visión define las metas que se pretende conseguir en el futuro. Estas metas tienen que ser realistas y alcanzables, puesto que la propuesta de visión tiene un carácter inspirador y motivador. Para la definición de la visión de una empresa, una buena ayuda será responder a las siguientes preguntas: ¿Qué quiero lograr?, ¿dónde quiero estar en el futuro?, ¿para quién lo haré?

3. OBJETIVOS

3.1.OBJETIVOS DEL MANUAL

- Presentar una visión de conjunto de la organización administrativa de las instalaciones de la presente Organización.
- Precisar las funciones de cada uno de los componentes administrativos que conforman la administración de las respectivas instalaciones de la Organización, para definir responsabilidades.
- Establecer claramente el grado de autoridad y responsabilidad de las distintas Unidades Administrativas.
- Establecer consistentemente las responsabilidades que obtienen los funcionarios al tener acceso seleccionado a ciertas áreas declaradas como restringidas de la Organización a la que pertenecen.

4. BASE LEGAL

En esta parte del documento se nombrarán las leyes, órdenes ejecutivas o resoluciones correspondientes por las cuales se regula la creación obligatoria de un documento de Normas y Procedimientos, en una Organización en este caso.

5. POLITICAS

En esta parte van las políticas sobre las cuales se encuentra la base de la Organización, en si es la orientación o directriz que siguen los diferentes miembros de la misma.

- Coadyuvar en la aplicación de las tecnologías que favorezcan el mejoramiento continuo de los servicios que brinda la Organización.

- Cumplir y hacer cumplir las leyes, resoluciones, normas y procedimientos relacionados con las operaciones en las instalaciones de la Organización.

6. CONCEPTOS

Área de Acceso Restringido:

Infraestructura:

Base Legal – Se refiere a la Ley, Orden Ejecutiva o Resoluciones que dispongan la creación de un organismo, programa o la asignación de recursos.

Política: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la organización, en ella se contemplan las normas y responsabilidades de cada área de la organización.

7. ORGANIGRAMA GENERAL DE LA ADMINISTRACIÓN DE LA ORGANIZACIÓN

En este organigrama se debe reflejar la organización administrativa por medio de las jerarquías de puestos que existe en la Institución.

8. ÁREAS QUE COMPRENDEN LA INFRAESTRUCTURA

En esta apartado se clasificarán todas las áreas que comprenden la infraestructura, la clasificación iría de acuerdo al nivel de acceso que tendría cada área.

8.1. FUNCIONES DE LAS DIFERENTES ÁREAS DE LA INFRAESTRUCTURA

En esta parte del documento se debe nombrar y escribir una pequeña descripción de cada una de las Áreas o Ambientes que componen la infraestructura física de la Organización o Empresa.

Ejemplo:

Área de Expedientes:

Descripción:

Personal con acceso autorizado:

9. CLASIFICACION DE CARGOS DE LA ORGANIZACIÓN

La Clasificación de los Cargos se hará por jerarquía de acuerdo al organigrama general o detallado de la Organización. Mostrándolo en esta parte del documento como una especie de listado con su respectivo número de identificación según el orden de clasificación.

10. ATRIBUCIONES DE LOS DIFERENTES CARGOS

En este apartado se contará con una descripción pequeña pero clara de lo que es cada cargo y qué rol tienen los diferentes funcionarios que trabajan en la Organización.

Un ejemplo de la descripción sería:

Institución:
Subdirección: “en caso de que la tuviera”
Departamento: “Al que pertenece el cargo”
Área: “Área o áreas a la que pertenece y tendrá acceso la persona que ocupe este cargo”
Nombre del Cargo:
Nivel: “nivel de jerarquía en el que se encuentra el Cargo”.
Reporta a:
Supervisa a:
Horario:

11. GLOSARIO

En esta parte del documento se escribirán todas las palabras, con sus respectivos significados, que posiblemente no sean bien comprendidas por los usuarios a los que va dirigido este documento.

SISTEMA DE CONTROL DE ACCESO DEL PERSONAL A ÁREAS RESTRINGIDAS DE UNA ORGANIZACIÓN

2. OBJETIVO GENERAL. -

El objetivo general de este Proyecto es, desarrollar un Sistema de Control de acceso del Personal a áreas restringidas de un Organización que se puede adaptar a cualquier tipo de Organización de manera sencilla.

3. ALCANCE DEL PROYECTO.

El Proyecto pretende contribuir a mejorar la seguridad de la infraestructura de una Organización, llevando un Control del acceso del Personal a las diferentes áreas denominadas restringidas de la infraestructura, siendo asignada una tarjeta por funcionario para que por medio del reconocimiento de la misma por cada lector le dé el acceso correspondiente a determinada área. Se podrá obtener reportes a tiempo de los diferentes aspectos del sistema.

El alcance del prototipo presentado será solo de la apertura de un area de la infraestructura puesto que el modulo lector RFID utilizado solo tiene el alcance para el control de un area.

4. DESCRIPCION DEL PROBLEMA. -

El sistema automatizado en web que se desarrollará, permitirá realizar el Control de acceso del Personal a áreas restringidas de la infraestructura de una Organización de forma automatizada, lo cual conllevará al registro en el mismo, de todo el personal de la Organización.

Gracias al registro de todo el personal que se hará, se le podrá asignar a cada funcionario una tarjeta de acceso previamente registrada en el Sistema con la que podrá acceder a las áreas permitidas según los roles que cumplan en la Organización.

El Sistema contará con una pantalla de Bienvenida donde se encontrará el logo de la Organización que utilizará el Sistema, por medio de una interfaz pasará a una pantalla de Inicio donde el usuario podrá loguearse, ingresando su login (nombre de usuario) y clave; al validar el Sistema estos datos, ingresará a un menú principal donde se encontrarán los módulos autorizados por el Sistema según el rol del usuario.

El menú principal contará con las siguientes opciones:

- Usuarios: En este módulo se podrá realizar diferentes consultas sobre los usuarios; en caso de un Administrador, éste podrá crear, actualizar, dar de baja a algún usuario y realizar otros procesos a los cuales tendrá acceso por medio de este módulo.
- Roles: En este módulo se podrá realizar consultas sobre los roles existentes en la Organización, el administrador podrá adicionar roles, respectivamente modificarlo, eliminarlos si es el caso y en este Sistema, asignarles las áreas de acceso correspondientes a cada rol.
- Áreas: En este módulo se podrán realizar diferentes consultas sobre las áreas a registrar en el Sistema, el Administrador, podrá añadir las áreas correspondientes a la infraestructura física, también podrá modificar los datos de las mismas y deshabilitarlas si fuera el caso.
- Tarjetas: En este módulo se podrá realizar consultas sobre las tarjetas registradas y habilitadas en el Sistema para poder ser asignadas al personal, el Administrador podrá realizar el registro, actualización y bloqueo en caso de pérdida o licencia de las tarjetas.
- Reportes: En este módulo se podrá crear reportes de todo el sistema como cuántas tarjetas han sido extraviadas o bloqueadas, qué personal ha sido dado de baja y otros.

5 MARCO TEORICO DEL PROYECTO

5.1. Tecnología RFID

La tecnología de radiofrecuencia se desarrolló en 1940, como medio para la identificación de los aviones aliados y enemigos durante la Segunda Guerra Mundial.

Años más tarde evolucionó, logrando así ser utilizada en la industria ferroviaria para el seguimiento de los coches del ferrocarril y para los años 60´s y 70´s, su uso se enfocó en la seguridad de materiales nucleares.

En la actualidad RFID se utiliza principalmente en el rubro de seguridad, como es el caso de los cruces fronterizos, credenciales de identidad, en el control vehicular, identificación de ganado, envío de paquetes, control de equipaje en los aeropuertos y de artículos para renta o préstamo (películas y libros) en videoclubes y bibliotecas, en la industria automotriz, para los procesos de automatización y seguimiento, en el sector agrícola y en el de administración de flora y fauna, para rastrear al ganado y a los animales, así como en el mercado minorista como dispositivo antirrobo.

La Tecnología de Identificación por Radiofrecuencia es un método electrónico que consiste en asignar un código de información a un producto, proceso o persona y usar esta información para identificar o acceder a información adicional al respecto. Los sistemas de identificación por radiofrecuencia consisten generalmente de dos componentes:

■ El ”transponder”, pequeña etiqueta electrónica (tag) que contiene un minúsculo microprocesador y una antena de radio. Esta etiqueta contiene un identificador único que puede ser asociado a una persona o producto.
■ El “lector”, que obtiene el identificador del “transponder”. La tecnología del transponder se basa en la aplicación de un transmisor/receptor encapsulado.

El receptor se puede activar por medio de una batería incorporada (transponder activo) o puede ser alimentado por la señal enviada por el lector (transponder pasivo). El lector genera un campo magnético cuya señal de RF es captada por el receptor del chip. Éste, a su vez activará al transmisor, el cual enviará un mensaje codificado único. Este mensaje es decodificado por el lector y procesado por la computadora.

5.2 Ventajas de la Identificación por Radio Frecuencia(RFID)

A continuación, se describen las principales ventajas de la tecnología de RFID en cuanto a

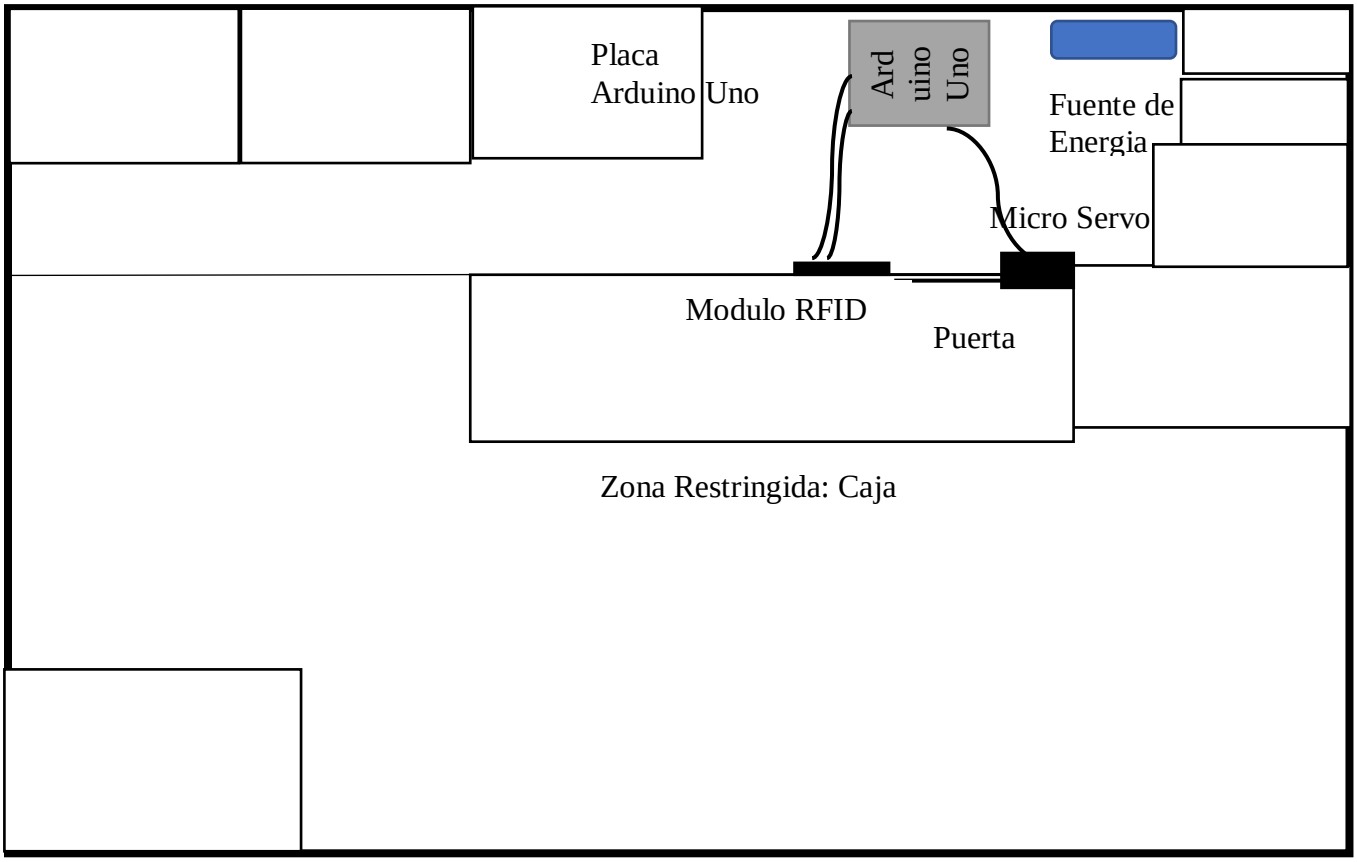
seguridad, línea de vista, velocidad de lectura, mantenimiento, reescritura, entre otras.

- Seguridad. Es una tarjeta que, por su diseño tecnológico, no puede duplicarse fácilmente. Cada una posee un código distinto y no permite que varios usuarios puedan tener una tarjeta duplicada. Es una diferencia fundamental cuando se le compara con los sistemas de banda magnética o código de barras, donde la duplicación de tarjetas es bastante frecuente. Son ideales para situaciones de máxima seguridad y alta tecnología.
- Sin necesidad de alineación o línea vista. De todos es el sistema más ágil y práctico, por varias razones. Una de ellas es que no necesita que la tarjeta sea pasada por una ranura o en el sentido correcto, lo que le da una mayor agilidad y practicidad de uso. Esto garantiza el éxito de la implementación de un sistema nuevo, donde, en general, los usuarios se resisten a ser controlados, pero al ser tan cómodo su uso, brinda una aceptación muy grande por parte de los usuarios.
- Inventarios de alta velocidad. Múltiples dispositivos pueden ser leídos simultáneamente, esto puede ahorrar tiempo si se compara con otras tecnologías, en las que es necesario alinear los dispositivos para leerlos uno por uno.
- Lectores sin mantenimiento. Los lectores son unidades sin partes móviles, lo que garantiza un correcto funcionamiento sin límite de uso y sin que haya que hacerles algún tipo de mantenimiento. También se pueden instalar a la intemperie

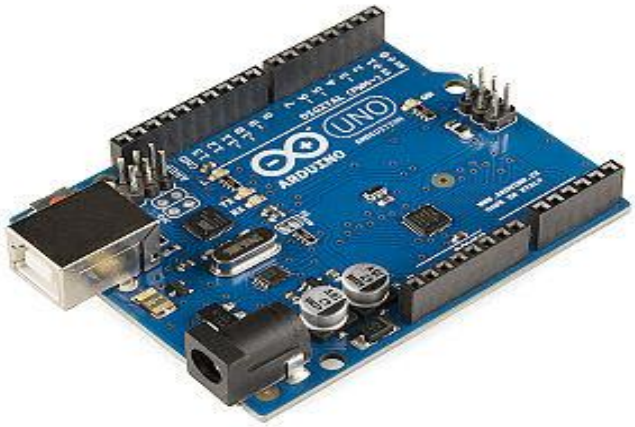
sin que las inclemencias del tiempo, como altas y bajas temperaturas ambientales, los dañen. La distancia de lectura, dependerá del tipo de lector. Los hay con distintos alcances dependiendo de su aplicación. Pueden ir desde 7 cm. a 2 m., siempre hablando de proximidad pasiva.

- Tarjetas sin desgaste. La tarjeta no tiene fricción alguna con el lector, por lo cual no se desgasta y su vida útil es prolongada. Esto permite su reutilización tras asignarlas, al personal de nuevo ingreso. El resultado es la optimización de recursos. Las tarjetas de proximidad vienen de varias formas. La más difundida y estándar es una de plástico bastante rígido, que está preparado para que se le pueda personalizar por medio de una impresión.
- Reescribible. Algunos tipos de etiquetas RFID, pueden ser leídas y escritas en múltiples ocasiones. En caso de que se aplique a componentes reutilizables, puede ser una gran ventaja.
- Factibilidad. El área de aplicación de la tecnología de RFID es muy amplia.
- Otras Tareas. Además de almacenar y transmitir datos, una etiqueta de RFID, puede ser diseñada para desempeñar otras funciones como medir condiciones de humedad o temperatura en el ambiente.

5.3 MODELO DE ESTRUCTURA DEL PROTOTIPO Y SUS DISPOSITIVOS



5.4 PLACA ARDUINO UNO



Una placa de hadware libre y de diseño de libre distribución. Usa su propio entorno de programación y se transferirá datos en este caso utilizando cable usb el cual al mismo tiempo es el que le proporciona fuente de alimentación de energía.

En cuento a su rendimiento la placa Arduino Uno Se basa en un microcontrolador Atmel ATmega320 de 8 bits a 16Mhz que funciona a 5v. 32KB son correspondientes a la memoria flash (0,5KB reservados para el bootloader), 2KB de SRAM y 1KB de EEPROM. En cuanto a memoria es una de las placas más limitadas, pero no por ello resulta insuficiente para casi todos los proyectos que rondan la red. Las salidas pueden trabajar a voltajes superiores, de entre 6 y 20v pero se recomienda una tensión de trabajo de entre 7 y 12v.

Características Técnicas:

- Microcontrolador: ATmega328
- Voltage: 5V
- Voltage entrada (recomendado): 7-12V- (limites): 6-20V
- Voltage entrada - Digital I/O Pins: 14 (de los cuales 6 son salida PWM)
- Entradas Analogicas: 6
- DC Current per I/O Pin: 40 mA

- DC Current parar 3.3V Pin: 50 mA
- Flash Memory: 32 KB (ATmega328) de los cuales 0.5 KB son utilizados para el arranque
- SRAM: 2 KB (ATmega328)
- EEPROM: 1 KB (ATmega328)
- Clock Speed: 16 MHz

5.5 MODULO RFID RC522

El kit de desarrollo RFID RC522 permite comenzar a desarrollar aplicaciones con rfid rápidamente ya que incluye un tag en forma de llavero y otro en forma de tarjeta, además del correspondiente lector RFID. El módulo lector está basado en el circuito integrado MFRC522 de NXP que es un IC especializado en "comunicación sin contacto" o RFID trabajando a una frecuencia de 13.56 Mhz. El lector MFRC522 soporta tags ISO/IEC 14443 A o MIFARE.

El módulo RFID RC522 incluye también la antena para la lectura/escritura de los tags, por lo que todo el diseño de la parte de radiofrecuencia ya se encuentra incluido en el módulo y no es necesario realizar mayor ajuste para una buena comunicación. El usuario solamente debe conectar el módulo mediante la interfaz SPI del microcontrolador de su preferencia, así como a la fuente de alimentación.

El módulo utiliza 3.3V como voltaje de alimentación y se controla a través del protocolo SPI, así como el protocolo UART, por lo que es compatible con casi cualquier micro

controlador, Arduino o tarjeta de desarrollo. El RC522 utiliza un sistema avanzado de modulación y demodulación para todo tipo de dispositivos pasivos de 13.56Mhz.

Características Técnicas:

- Corriente de operación: 13-26mA a 3.3V
- Corrientes de stand by: 10-13mA a 3.3V
- Corriente de sleep-mode: <80uA
- Corriente máxima: 30mA
- Frecuencia de operación: 13.56Mhz
- Distancia de lectura: 0 a 60mm
- Protocolo de comunicación: SPI
- Velocidad de datos máxima: 10Mbit/s
- Dimensiones del módulo: 40 x 60 mm
- Temperatura de operación: -20 a 80º

5.6 TARJETAS RFID

RFID (siglas de Radio Frequency IDentification, en español identificación por radiofrecuencia) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, tarjetas, transpondedores o tags RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio. Las tecnologías RFID se agrupan dentro de las denominadas Auto ID (automatic identification, o identificación automática).

Características Técnicas:

- Proximidad Pasiva (No necesita bateria)
- Material PVC
- No Grabable
- Frecuencia 125 Khz
- Grosor 0.88mm (Imprimible)
- Code 64 bits
- Temperatura -10°C a +50 °C
- Medidas 5.4 x 8.5 cm

Características Generales:

Sólo lectura

Compatible con todos los terminales y lectores de proximidad EM de ZKSoftware

Soporta los formatos de hasta 26 bits de Wiegand.

Cumple con la norma ISO de espesor para impresoras de transferencia térmica.

Compatible con el formato de chip EM4100 chip

En blanco

Las etiquetas RFID son unos dispositivos pequeños, similares a una pegatina, que pueden ser adheridas o incorporadas a un producto, un animal o una persona. Contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID.

Las tarjetas RFID son una llave Incopiable

Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren. Una de las ventajas del uso de radiofrecuencia (en lugar, por ejemplo, de infrarrojos) es que no se requiere visión directa entre emisor y receptor.

5.7 MICROSERVO SG90

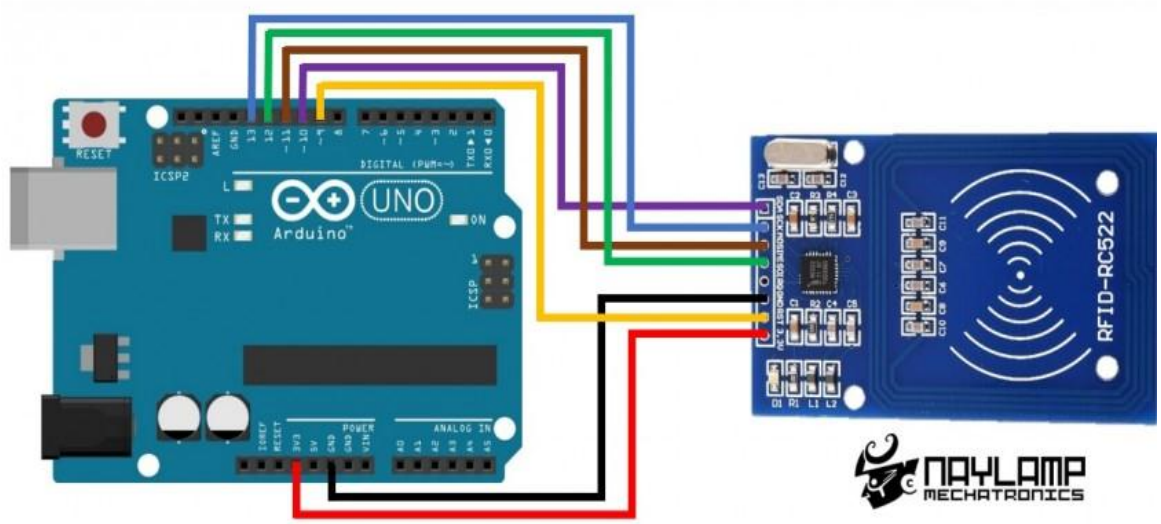
El servo SG90 Tower Pro un servo miniatura de gran calidad y diminutas dimensiones, además es bastante económico. Funciona con la mayoría de tarjetas electrónicas de control con microcontroladores y además con la mayoría de los sistemas de radio control comerciales. Funciona especialmente bien en aeronaves de aeromodelismo dadas sus características de torque, tamaño y peso.

El servo SG90 tiene un conector universal tipo "S" que encaja perfectamente en la mayoría de los receptores de radio control incluyendo los Futaba, JR, GWS, Cirrus, Hitec y otros. Los cables en el conector están distribuidos de la siguiente forma: Rojo =Alimentación (+), Cafe = Alimentación (–) o tierra, Naranja= Señal PWM.

Este tipo de servo es ideal para las primeras experiencias de aprendizaje y prácticas con servos, ya que sus requerimientos de energía son bastante bajos y se permite alimentarlo con la misma fuente de alimentación que el circuito de control. Por ejemplo, si se conecta a una tarjeta arduino, se puede alimentar durante las pruebas desde el puerto USB del PC sin mayor problema.

5.8 CONEXIÓN MODULO RFID RC522 CON ARDUINO UNO

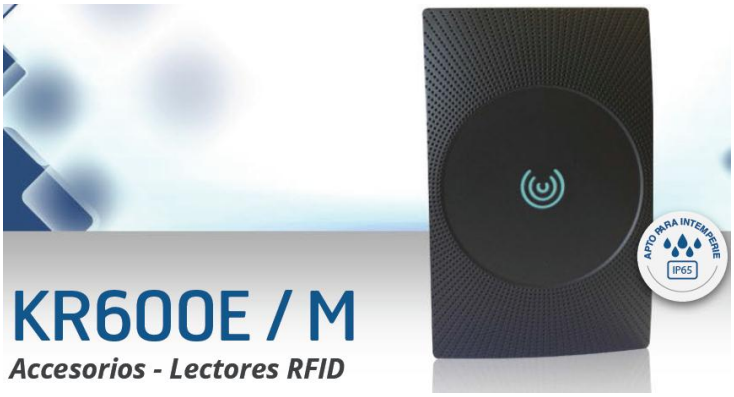
Arduino	RFID RC 522
PIN 10	SDA
PIN 13	SCK
PIN 11	MOSI
PIN 12	MISO
N/A	IRQ
GND	GND
PIN 9	RST
3.3V	3.3V



5.9 DIFERENCIAS ENTRE UN MODULO RC522 Y UN LECTOR RFID KR600M

Características Técnicas del Módulo RC522	Características Técnicas de Lector KR600M
• Lector de tarjetas 13,56MHz • Proximidad Pasiva (No necesita bateria) • Frecuencia 125 Khz • Grosor 0.88mm (Imprimible) • Formato de Lectura Code 64 bits • Temperatura -10°C a +50 °C • Medidas 5.4 x 8.5 cm • Distancia de lectura: 0 a 60mm • Corriente Max: 30mA • Humedad de Operación: -20 a 80ºC	• Lector de tarjetas 13,56 MHz MF • Frecuencia 125 khz • Proximidad EM Marin125 khz / Proximidad MF 13,56 MHz • Formato de lectura 34bit Wiegand (por defecto) • Temperatura -20° C a +65° C • Medidas 75mm x 116mm x 16mm • Índice de protección IP65 • Potencia/Corriente DC 6-14V / Max.70mA • Distancia de lectura: Hasta 5 cm • Corrientes Max: Max.70mA • Humedad de Operación: 10% a 90% de humedad relativa

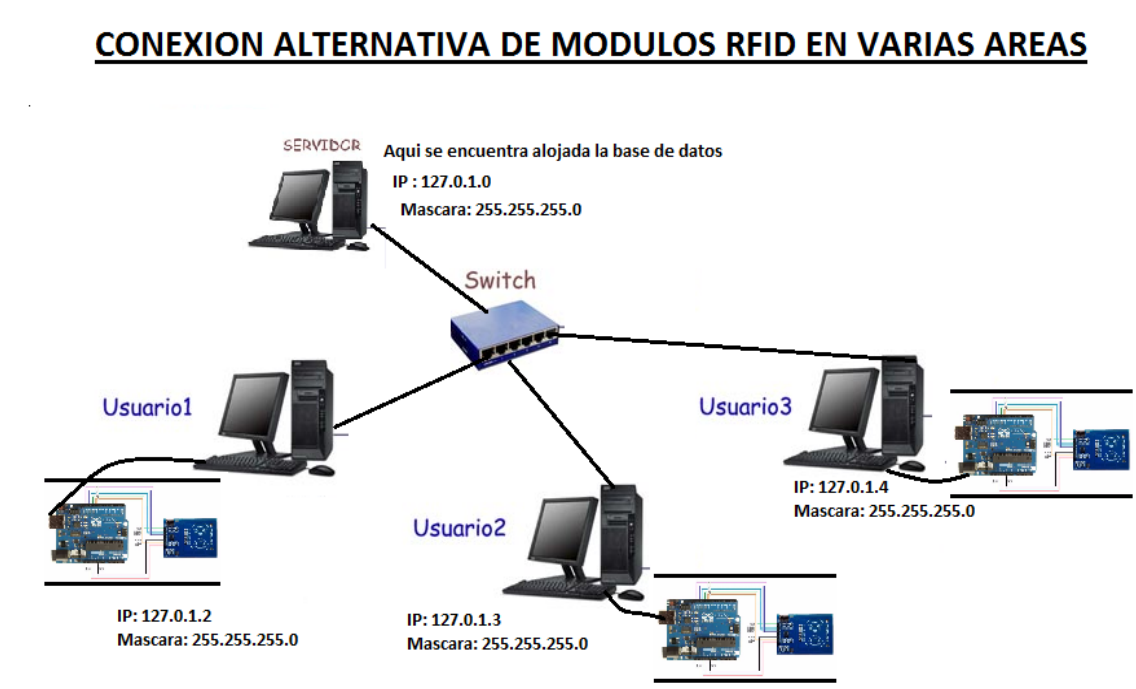
LECTOR RFID MODELO KR600M



La serie de lectores KR es una línea de accesorios principales de los lectores Wiegand externos para todos los dispositivos de control de acceso. Con un diseño elegante y robusto, que son fáciles de conectar e instalar, y ofrecen la posibilidad de controlar una puerta desde ambos lados. El lector identifica tarjetas de proximidad de 13,56 MHz con Wiegand de salida de 34bit.

5.10 CONEXIÓN DE VARIOS MODULOS LECTORES RFID

Diagrama de conexión:



La conexión alternativa que presento aquí para la conexión de estos dispositivos en varias áreas de una Organización está basada en la premisa que el Servidor Principal en donde se encontrará alojada la Base de Datos Principal y el Sistema Web desarrollado compartirá la base de datos dentro de una misma red LAN permitiendo que ingresen a la misma los datos como el código de acceso de una tarjeta RFID y la fecha y hora en la que se la reconoció y accedió a dicha área. Logrando de esta manera el objetivo de poder realizar un control de accesos de todo el personal a las áreas restringidas de una Organización.

Los pasos detallados a seguir para lograr la configuración correcta de la Pc Servidor se encontrarán en descritos en el manual de instalación que va adjunto a este documento.

5.11 METODO DE LECTURA DEL MODULO RC522 EN ARDUINO

```
#include <Servo.h>
Servo miservo;
#include <SPI.h>
#include <MFRC522.h>
#define SS_PIN 10
#define RST_PIN 9
#define SP_PIN 8

MFRC522 rfid(SS_PIN, RST_PIN);
MFRC522::MIFARE_Key key;
const int ledPin=13;
byte entrada;
void setup() {
  //aqui creo la variable del servo//
 miservo.attach(6);
  Serial.begin(9600);
  SPI.begin();
  rfid.PCD_Init();
```

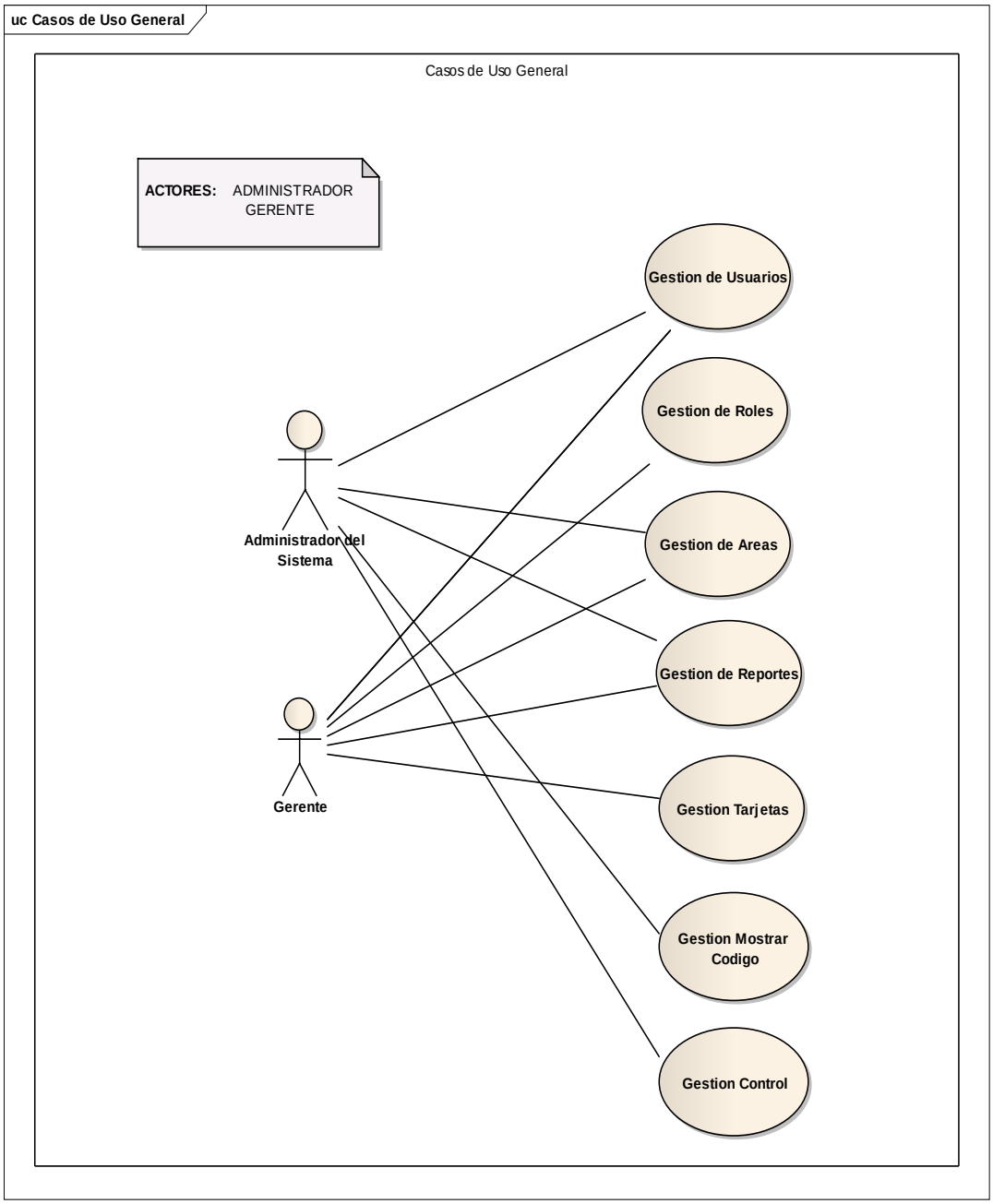
```
}
void cerrar(){
 for(int angulo = 0; angulo < 100; angulo += 1) {   //  un ciclo para mover el servo entre los 0 y los 180 grados
      miservo.write(angulo);             //  manda al servo la posicion
      delay(18);                      //  espera unos milisegundos para que el servo llegue a su posicion
    }
    delay(3000);
 }
 void abrir(){
   for(int angulo = 100; angulo >= 1; angulo -= 1)    {   //  un ciclo para mover el servo entre los 180 y los 0 grados
      miservo.write(angulo);              //  manda al servo la posicion
      delay(18);                      //  espera unos milisegundos para que el servo llegue a su posicion
    }
     delay(3000);
   }

void loop() {
 if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial())
   return;
 MFRC522::PICC_Type piccType = rfid.PICC_GetType(rfid.uid.sak);
 // Serial.println(rfid.PICC_GetTypeName(piccType));
 // Check is the PICC of Classic MIFARE type
 if (piccType != MFRC522::PICC_TYPE_MIFARE_MINI &&  piccType != MFRC522::PICC_TYPE_MIFARE_1K &&  piccType != MFRC522::PICC_TYPE_MIFARE_4K) {
   Serial.println(F("Your tag is not of type MIFARE Classic."));
```

```
    return;
  }
  String strID = "";
  for (byte i = 0; i < 4; i++) {
    strID +=
    (rfid.uid.uidByte[i] < 0x10 ? "0" : "") +
    String(rfid.uid.uidByte[i], HEX) +
    (i!=3 ? ":" : "");
  }
  strID.toUpperCase();
  Serial.println(strID);

//while(strID=="84:0C:88:00"){
    if(strID=="84:0C:88:00" || strID=="F5:60:80:CB" )//{
      //servo se mueve a 180 grados
      abrir();
      cerrar();
      digitalWrite(ledPin,HIGH);
      Serial.println("led encendido");
      //}
      //if(entrada== 78){
        //servo permanece en 90 grados
        //digitalWrite(ledPin,LOW);
        //}
 //  }
  rfid.PICC_HaltA();
  rfid.PCD_StopCrypto1();
}
```

6. DIAGRAMA DE CASOS DE USO GENERAL



6.1 DESCRIPCIÓN:

- Caso de Uso: Gestión Usuarios
  Actor: Gerente y Administrador

Descripción: Su función es registrar todos los datos de los funcionarios de la Organización como usuarios del Sistema, en caso de despido o renuncia, los mismos serán eliminados del Sistema y en caso de licencia serán dados de baja. Se podrá asignar

un rol a cada usuario. Se asignará una cuenta en el Sistema sólo a los usuarios que sea necesario que interactúen con el Sistema.

- Caso de Uso: Gestión Roles
  Actor: Gerente

Descripción: Su función es añadir los roles existentes en la Organización, los mismos podrán ser modificados y eliminados en caso de que ya no existan dentro de la Empresa, también tendrá la función de asignar las áreas correspondientes a las que cada rol podrá tener acceso.

- Caso de Uso: Gestión Áreas
  Actor: Gerente y Administrador

Descripción: Su función es registrar las áreas físicas que existen en la infraestructura de la Organización según un código de área, una descripción o nombre y una ubicación.

- Caso de Uso: Gestión Tarjetas
  Actor: Gerente y Administrador

Descripción: Su función es registrar el código único de todas las tarjetas de acceso disponibles para ser asignadas a los distintos funcionarios de la Organización.

- Caso de Uso: Gestión Reportes
  Actor: Administrador

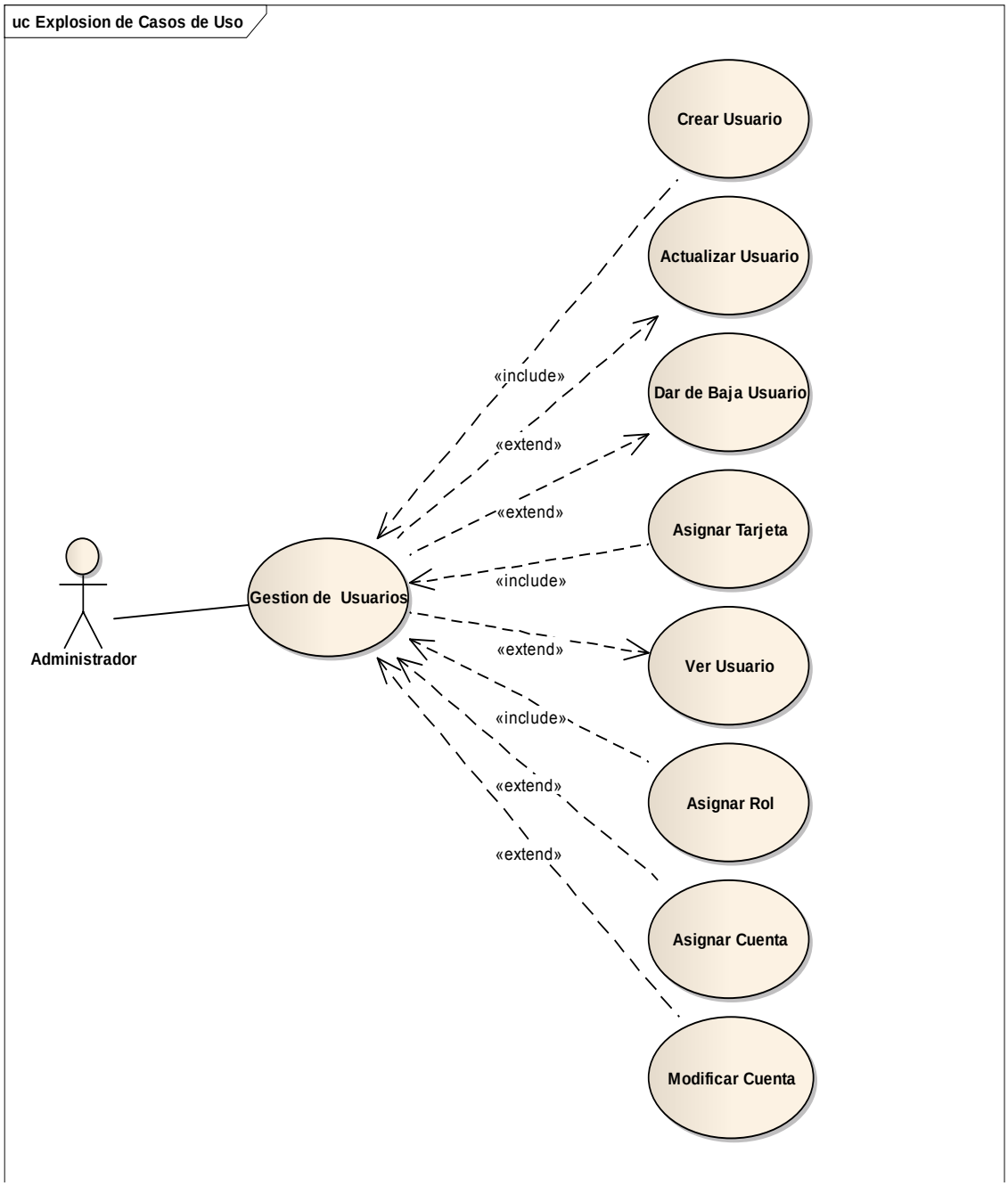
Descripción: Su función es sacar reportes sobre el flujo de acceso que tuvieron las distintas áreas restringidas de la Organización y otro reporte sobre las veces que fue activada las alarmas.

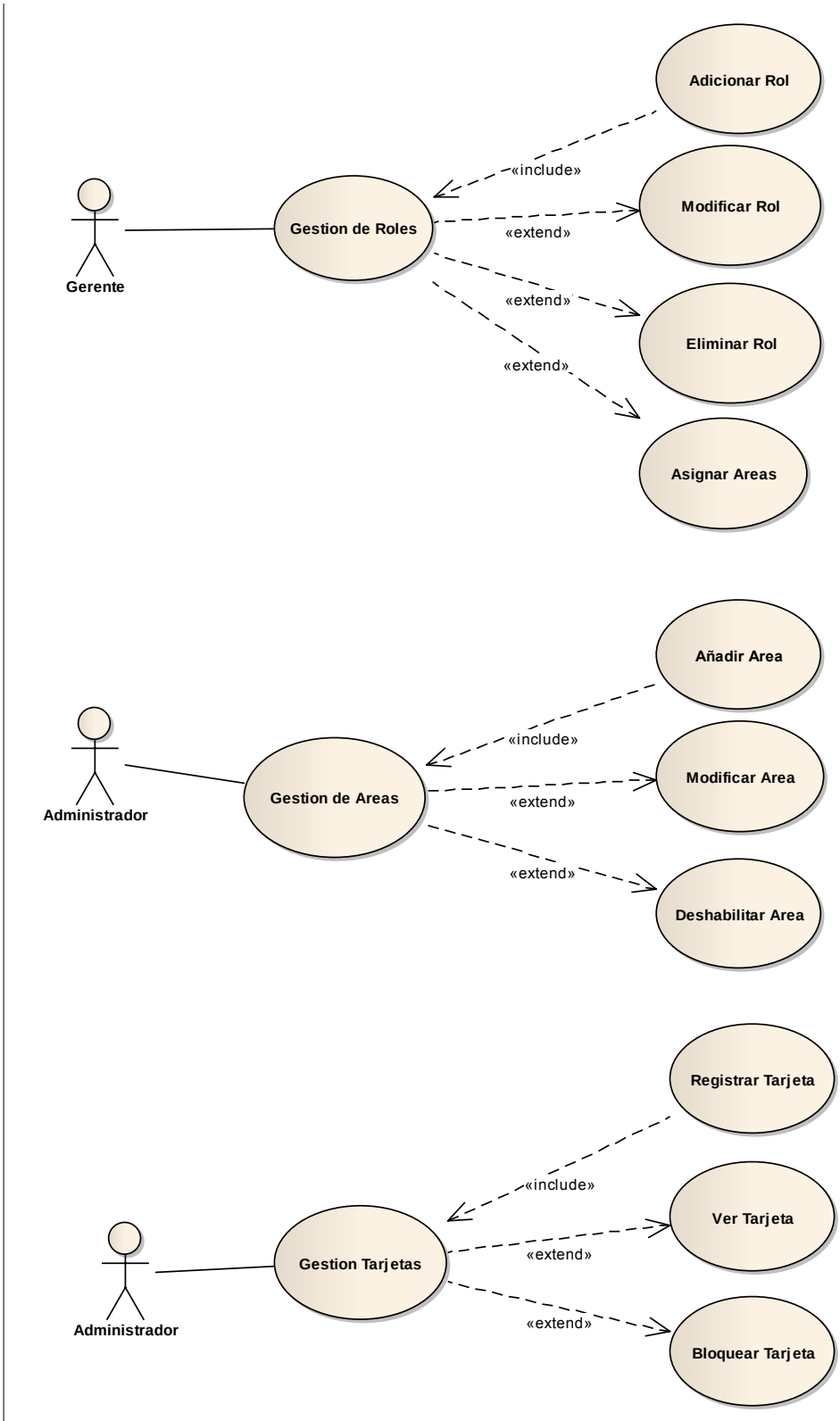
6.2 ACTORES

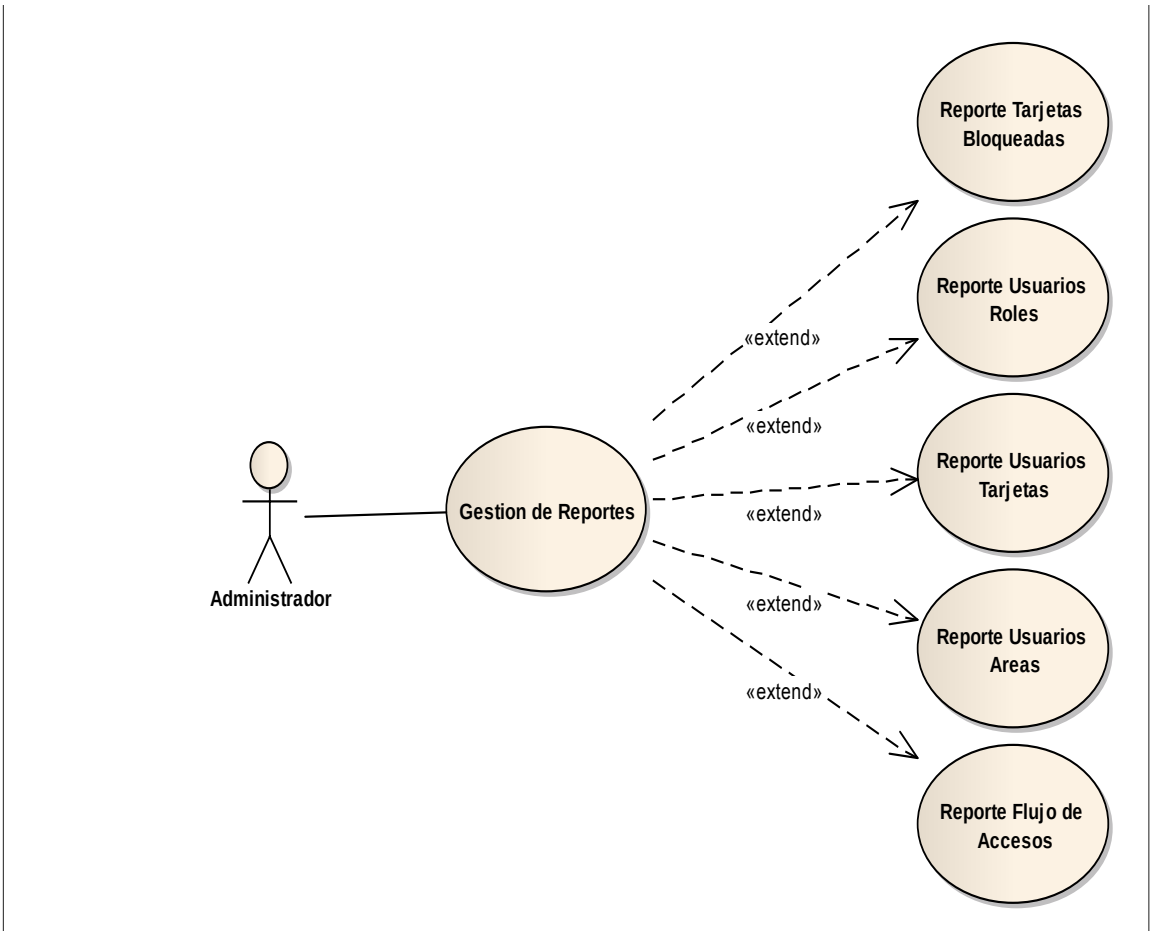
ACTORES PRIMARIOS

- Gerente: Es el dueño de la Organización, éste puede tener acceso a todo el Sistema sin restricción alguna, lo que significa que puede manejar todos los módulos.
- Administrador: Es la persona encargada de administrar el Sistema desde el registro de los usuarios, registro de áreas y de la gestión de reportes; los cuales son presentados al Gerente General de la Organización

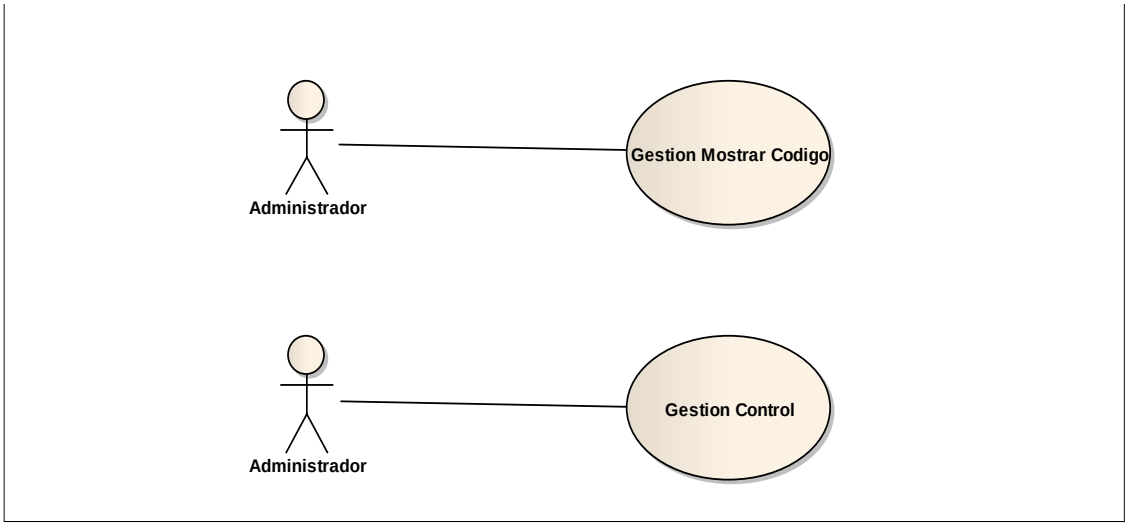
7. EXPLOSION DE CASOS DE USO




Adicionar Rol
«include»
Modificar Rol
Gestion de Roles
«extend»
Gerente
«extend»
Eliminar Rol
«extend»
Asignar Areas
Añadir Area
«include»
Modificar Area
Gestion de Areas
«extend»
Administrador
«extend»
Deshabilitar Area
Registrar Tarjeta
«include»
Ver Tarjeta
Gestion Tarjetas
«extend»
Administrador
«extend»
Bloquear Tarjeta



Casos de Uso de Aplicaciones que Componen el Sistema Principal



8. ESPECIFICACIÓN

8.1 DESCRIPCIÓN DE CASOS DE USO

CREAR USUARIO	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones.
El encargado selecciona una opción del menú.	El Sistema muestra otras opciones incluidas en la anterior pantalla.
El encargado selecciona nuevamente una opción de las que se muestran.	El sistema muestra el formulario de los datos solicitados.
El encargado ingresa los datos en el formulario que se requiere guardar en la base de datos, creando de esta manera un nuevo usuario.	El sistema reconoce y guarda los datos del nuevo usuario en la base de datos y confirma mostrando en un listado de todos los usuarios existentes.

ACTUALIZAR USUARIO	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones.
El encargado selecciona una opción del menú.	El Sistema muestra otras opciones incluidas en la anterior.
El encargado selecciona nuevamente una opción de las que se muestran.	El Sistema muestra el estado de los datos solicitados en un formulario.
El encargado ingresa los datos a modificar en el formulario y posteriormente los guarda en la base de datos.	El Sistema reconoce y guarda los datos en la base de datos.

VER USUARIO	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones.
El encargado selecciona una opción del	El Sistema muestra otras opciones

menú. El encargado selecciona nuevamente una opción de las que se muestran. El encargado puede ver los datos que ha solicitado y salir del formulario.	incluidas en la anterior. El Sistema muestra el estado de los datos solicitados en un formulario editable. El Sistema reconoce la acción y deja de mostrar los datos.

DAR DE BAJA USUARIO	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose. El encargado selecciona una opción del menú. El encargado selecciona nuevamente una opción. El encargado realiza confirmación de baja al usuario seleccionado.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones. El Sistema muestra otras opciones incluidas en la anterior. El Sistema muestra los datos solicitados como resultado de la petición y pide una confirmación para realizar la acción dar de baja. El Sistema reconoce la acción y actualiza la base de datos.

ASIGNAR TARJETA	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose con los datos ya asignados por el sistema por ser el gerente. El encargado selecciona una opción del menú. El encargado selecciona nuevamente una opción. El encargado realiza confirmación de asignación correcta de los datos.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones. El Sistema muestra otras opciones incluidas en la anterior. El Sistema muestra los datos solicitados como resultado de la petición y en este caso se procede a la asignación de una tarjeta a un usuario. El Sistema reconoce la acción y actualiza la base de datos.

ASIGNAR CUENTA	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose con los datos ya asignados por el Sistema por ser el Gerente. El encargado selecciona una opción del menú. El encargado selecciona nuevamente una opción. El encargado realiza confirmación de asignación correcta de los datos.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones. El Sistema muestra otras opciones incluidas en la anterior. El Sistema muestra los datos solicitados como resultado de la petición y en este caso se procede a la asignación de datos para un usuario. El Sistema reconoce la acción y actualiza la base de datos.

MODIFICAR CUENTA	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose. El encargado selecciona una opción del menú. El encargado selecciona nuevamente una opción de las que se muestran. El encargado ingresa los datos a modificar en el formulario y posteriormente los guarda en la base de datos.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones. El Sistema muestra otras opciones incluidas en la anterior. El Sistema muestra el estado de los datos solicitados en un formulario. El Sistema reconoce y guarda los datos en la base de datos.

ASIGNAR ROL	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose con los datos ya asignados por el Sistema por ser el gerente. El encargado selecciona una opción del menú. El encargado selecciona nuevamente una	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones. El Sistema muestra otras opciones incluidas en la anterior. El Sistema muestra los datos solicitados

opción.	como resultado de la petición y en este caso se procede a la asignación de un rol para un usuario.
El encargado realiza confirmación de asignación correcta de los datos.	El Sistema reconoce la acción y actualiza la base de datos.

ADICIONAR ROL	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones.
El encargado selecciona una opción del menú.	El Sistema muestra otras opciones incluidas en la anterior pantalla.
El encargado selecciona nuevamente una opción de las que se muestran.	El Sistema muestra el formulario los datos solicitaron.
El encargado ingresa los datos en el formulario que se requiere guardar en la base de datos, adicionando de esta manera un nuevo rol.	El Sistema reconoce y guarda los datos del nuevo rol en la base de datos y confirma mostrando en un listado de todos los roles ya existentes.

MODIFICAR ROL	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones.
El encargado selecciona una opción del menú.	El Sistema muestra otras opciones incluidas en la anterior.
El encargado selecciona nuevamente una opción de las que se muestran.	El Sistema muestra el estado de los datos solicitados en un formulario.
El encargado ingresa los datos a modificar en el formulario y posteriormente los guarda en la base de datos.	El Sistema reconoce y guarda los datos en la base de datos.

ELIMINAR ROL

ADMINISTRADOR	SISTEMA
El encargado se identifica logueándose.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones.
El encargado selecciona una opción del menú.	El Sistema muestra otras opciones incluidas en la anterior.
El encargado selecciona nuevamente una opción.	El Sistema muestra los datos solicitados como resultado de la petición y pide una confirmación para realizar la acción de eliminar.
El encargado realiza confirmación de eliminar los datos del rol seleccionado.	El Sistema reconoce la acción y actualiza la base de datos.

ASIGNAR ÁREAS	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose con los datos ya asignados por el Sistema por ser el Gerente.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones.
El encargado selecciona una opción del menú.	El Sistema muestra otras opciones incluidas en la anterior.
El encargado selecciona nuevamente una opción.	El Sistema muestra los datos solicitados como resultado de la petición y en este caso se procede a la asignación de las áreas permitidas para el rol que tendrá un usuario.
El encargado realiza confirmación de asignación correcta de los datos.	El Sistema reconoce la acción y actualiza la base de datos.

AÑADIR AREA	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones.
El encargado selecciona una opción del menú.	El Sistema muestra otras opciones incluidas en la anterior pantalla.
El encargado selecciona nuevamente una	El sistema muestra el formulario de los

opción de las que se muestran. El encargado ingresa los datos en el formulario que se requiere guardar en la base de datos, añadiendo de esta manera una nueva área.	datos solicitados. El Sistema reconoce y guarda los datos de la nueva área en la base de datos y confirma mostrando en un listado todas las áreas ya existentes.

MODIFICAR ÁREA	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose. El encargado selecciona una opción del menú. El encargado selecciona nuevamente una opción de las que se muestran. El encargado ingresa los datos a modificar en el formulario y posteriormente los guarda en la base de datos.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones. El Sistema muestra otras opciones incluidas en la anterior. El sistema muestra el estado de los datos solicitados en un formulario. El Sistema reconoce y guarda los datos en la base de datos.

DESHABILITAR AREA	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose. El encargado selecciona una opción del menú. El encargado selecciona nuevamente una opción. El encargado realiza confirmación de deshabilitar el área seleccionada.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones. El Sistema muestra otras opciones incluidas en la anterior. El Sistema muestra los datos solicitados como resultado de la petición y pide una confirmación para realizar la acción dar de baja. El Sistema reconoce la acción y actualiza la base de datos.

REGISTRAR TARJETA

ADMINISTRADOR	SISTEMA
El encargado se identifica logueándose.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones.
El encargado selecciona una opción del menú.	El Sistema muestra otras opciones incluidas en la anterior pantalla.
El encargado selecciona nuevamente una opción de las que se muestran.	El sistema muestra el formulario de los datos solicitados.
El encargado ingresa los datos en el formulario que se requiere guardar en la base de datos, registrando de esta manera el código de una nueva tarjeta.	El Sistema reconoce y guarda los datos de la nueva tarjeta en la base de datos y confirma mostrando en un listado todas las tarjetas ya registradas.

VER TARJETA	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones.
El encargado selecciona una opción del menú.	El Sistema muestra otras opciones incluidas en el menú anterior.
El encargado selecciona nuevamente una opción de las que se muestran.	El Sistema muestra el estado de los datos solicitados en un formulario.
El encargado selecciona en la lista que se muestra la tarjeta de la que quiere ver todos los datos.	El Sistema reconoce la instrucción y muestra los datos solicitados en un formulario no editable.

BLOQUEAR TARJETA	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones.
El encargado selecciona una opción del menú.	El Sistema muestra otras opciones incluidas en la anterior.
El encargado selecciona nuevamente una	El Sistema muestra los datos solicitados

opción. El encargado realiza confirmación de Bloquear la tarjeta seleccionada.	como resultado de la petición y pide una confirmación para realizar la acción de bloquear la tarjeta. El Sistema reconoce la acción y actualiza la base de datos.

REPORTE TARJETAS BLOQUEADAS	
GERENTE	**SISTEMA**
El encargado se identifica logueándose. El encargado selecciona una opción del menú. El encardo puede seleccionar si imprimir o cerrar el formulario.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones. El Sistema muestra el formulario no editable correspondiente con los datos solicitados. El Sistema imprime de forma física el reporte correspondiente con los datos extraídos de la base de datos.

REPORTE USUARIOS ROLES	
GERENTE	**SISTEMA**
El encargado se identifica logueándose. El encargado selecciona una opción del menú. El encargado puede seleccionar si imprimir o cerrar el formulario.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones. El Sistema muestra el formulario no editable correspondiente con los datos solicitados. El Sistema imprime de forma física el reporte correspondiente con los datos extraídos de la base de datos.

REPORTE USUARIOS TARJETA	
GERENTE	**SISTEMA**
El encargado se identifica logueándose.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones.

El encargado selecciona una opción del menú. El encargado puede seleccionar si imprimir o cerrar el formulario.	El Sistema muestra el formulario no editable correspondiente con los datos solicitados. El Sistema imprime de forma física el reporte correspondiente con los datos extraídos de la base de datos.

REPORTE FLUJO DE ACCESOS	
GERENTE	**SISTEMA**
El encargado se identifica logueándose. El encargado selecciona una opción del menú. El encargado puede seleccionar si imprimir o cerrar el formulario.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones. El Sistema muestra el formulario no editable correspondiente con los datos solicitados. El Sistema imprime de forma física el reporte correspondiente con los datos extraídos de la base de datos.

REPORTE USUARIOS AREAS	
ADMINISTRADOR	**SISTEMA**
El encargado se identifica logueándose. El encargado selecciona una opción del menú. El encargado puede seleccionar si imprimir o cerrar el formulario.	El Sistema valida los datos ingresados por el encargado y le ofrece un menú con distintas opciones. El Sistema muestra el formulario no editable correspondiente con los datos solicitados. El Sistema imprime de forma física el reporte correspondiente con los datos extraídos de la base de datos.

GESTION MOSTRAR CODIGO	
ADMINISTRADOR	**SISTEMA**
El encargado hace correr la pequeña aplicación. El encargado pasa la tarjeta por el lector El encargado copia el código para después ser registrado en la base de datos.	La aplicación levanta el escuchador del módulo RFID. La aplicación muestra el dato de la tarjeta en una pantalla. La aplicación cierra la Pantalla

GESTION CONTROL	
ADMINISTRADOR	**SISTEMA**
El encargado hace correr la aplicación o servicio.	La aplicación levanta el escuchador del módulo RFID y el servicio de control de tarjetas.
El encargado pasa la tarjeta por el lector	La aplicación almacena la fecha y el código de la tarjeta.
El encargado copia el código para después ser registrado en la base de datos.	La aplicación cierra la Pantalla

8.3 DESCRIPCIÓN DETALLADA DE CASOS DE USO

CASO DE USO: GESTION DE USUARIOS

Caso de Uso	Gestión Usuarios
Actores	Gerente
Tipo	Básico
Propósito	Permitir gestionar usuarios.
Resumen	El Caso de uso: Gestión usuarios es iniciado por el Gerente (Dueño), el cual estará habilitado para crear, actualizar y dar de baja, asignar cuenta, asignar rol y asignar tarjeta en el Sistema.
Pre-condiciones	El Gerente debe estar previamente registrado en el Sistema y haber iniciado sesión. Debe seleccionar el Módulo "Usuarios", donde visualiza una pantalla con un listado de Usuarios y sus detalles.
Post-condiciones	Usuarios autorizados y que tengan una cuenta para la manipulación del sistema.
Flujo Principal	Se ejecuta el Caso de uso: Gestión de Usuarios. Dependiendo de las opciones seleccionadas por el usuario.
Subflujos	Se muestra la Pantalla: Usuarios, con los datos de todos los usuarios registrados en el Sistema. El usuario puede seleccionar entre las siguientes opciones: "crear", "actualizar", "ver" "dar de baja"," asignar tarjeta"," asignar rol"," asignar cuenta"," modificar cuenta". S-1 Si la actividad seleccionada es "crear", se muestra la Pantalla Crear Usuario. S-2 Si la actividad seleccionada es "actualizar", se muestra la Pantalla Actualizar Usuario. S-3 Si la actividad seleccionada es "ver", se

	muestra la Pantalla Ver Usuario. S-4 Si la actividad seleccionada es “dar de baja”, se muestra la Pantalla Dar de Baja Usuario. S-5 Si la actividad seleccionada es “asignar cuenta”, se muestra la Pantalla Asignar Cuenta. S-5 Si la actividad seleccionada es “asignar rol”, se muestra la Pantalla Asignar Rol. S-6 Si la actividad seleccionada es “asignar tarjeta”, se muestra la Pantalla Asignar Tarjeta. S-7 Si la actividad seleccionada es “modificar cuenta” se muestra la Pantalla Modificar Cuenta.

CASO DE USO: CREAR USUARIO

Caso de uso	Crear Usuario.
Actores	Gerente
Tipo	Inclusión.
Propósito	Crear nuevos usuarios.
Resumen	El Caso de uso es iniciado por el Gerente; Crea los usuarios que estarán habilitados para el manejo del sistema, además de registrar como usuarios a los funcionarios de la Organización.
Pre-Condiciones	El usuario debe estar previamente registrado en el Sistema y haber iniciado sesión. Debe seleccionar la opción "crear" en (Pantalla Usuarios).
Post-Condiciones	Usuarios con cuenta autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Crear Usuario), donde se carga el formulario para adicionar los datos personales: (Ci, Nombre, Ap. Paterno, Ap. Materno, Dirección, Foto, Teléfono, Sexo, Email). Una vez el formulario es llenado correctamente, se hace clic en el botón "Aceptar" para que se almacenen los datos en la tabla Usuarios. Si se hace clic en el botón "Cancelar" se retorna a (Pantalla Usuarios).
Subflujos	Ninguno.
Excepciones	Si se deja algún Campo vacío, se pone en rojo los Campos de entrada de datos no permitiendo guardar los datos ingresados.

CASO DE USO: ACTUALIZAR USUARIO

Caso de uso	Actualizar Usuario.
Actores	Gerente
Tipo	Extensión.
Propósito	Actualizar un usuario ya existente en el Sistema.
Resumen	El Caso de uso actualiza algún dato de los usuarios que están registrados en el Sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el Sistema y haber iniciado sesión con su respectiva cuenta asignada. Se debe ejecutar previamente el Caso de uso: Crear Usuario para crear un nuevo usuario. Debe seleccionar un usuario de la lista y luego presione la opción "actualizar".
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Actualizar Usuario), donde se carga el formulario para actualizar los datos personales: (Ci, Nombre, Ap. Paterno, Ap. Materno, Dirección, Foto, Teléfono, Sexo, Email). Una vez el formulario es llenado correctamente se hace clic en el botón "guardar" y se almacenan los datos actualizados en la tabla Usuarios de la Base de datos. Si se hace clic en el botón "cancelar" se retorna a (Pantalla Usuarios).
Subflujos	Ninguno.
Excepciones	Si se deja algún campo vacío, se ponen de color rojo los campos de entrada de datos no permitiendo guardar correctamente los datos en la Base de datos.

CASO DE USO: VER USUARIO

Caso de uso	Ver Usuario.
Actores	Gerente.
Tipo	Extensión.
Propósito	Ver todos los datos de un usuario del Sistema.
Resumen	El Caso de uso: Ver a los usuarios que estarán habilitados para el manejo del Sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el Sistema y haber iniciado sesión. Se debe ejecutar previamente el Caso de uso: Crear usuario para crear un nuevo ingreso. Debe seleccionar un usuario de la lista y luego presione la opción "Ver".
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Ver Usuario), donde se carga el formulario para ver los datos personales: (Ci, Nombre, Ap. Paterno, Ap. Materno, Dirección, Foto, Teléfono, Sexo, Email).Una vez el formulario es llenado correctamente, para ser vistos los datos se hace clic en el botón "salir" y se guardarán nuevamente todos los datos mostrados y se retorna a (Pantalla Usuarios).
Subflujos	Ninguno.
Excepciones	Ninguna.

CASO DE USO: DAR DE BAJA A USUARIO

Caso de uso	Dar de Baja Usuario.
Actores	Gerente.
Tipo	Extensión.
Propósito	Dar de baja a un usuario del Sistema.
Resumen	El Caso de uso da de baja a los usuarios que estarán habilitados para el manejo del Sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el Sistema y haber iniciado sesión. Se debe ejecutar previamente el caso de uso crear usuario para crear un nuevo ingreso. Debe seleccionar un usuario de la lista y luego presione la opción "Dar de Baja".
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Dar de baja Usuario), con el mensaje "¿Está seguro que desea dar de baja a este usuario? Si se presiona "si" cambia de estado del usuario en la tabla Datos de la Base de datos. Si se hace clic en el botón "no" se cancela la operación y se retorna a (Pantalla Usuarios).
Subflujos	Ninguno.
Excepciones	Ninguna.

CASO DE USO: ASIGNAR CUENTA

Caso de uso	Asignar Cuenta
Actores	Gerente.
Tipo	Inclusión.
Propósito	Permitir adicionar los datos login y clave al usuario.
Resumen	El Caso de uso es iniciado principalmente por el Gerente, este Caso de uso tiene la funcionalidad de adicionar un login y clave a los usuarios que estarán autorizados para su ingreso en el Sistema.
Pre-Condiciones	Debe seleccionar la opción "asignar cuenta" en la Pantalla Usuarios.
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Asignar Cuenta), donde se carga el formulario para adicionar los siguientes datos del usuario: (Login, clave), una vez el formulario es llenado correctamente se hace clic en el botón "asignar" y se almacenan los datos en la tabla Datos de la base de datos. Si se hace clic en el botón "cancelar" se retorna a (Pantalla Usuarios).
Subflujos	Ninguno
Excepciones	Si se deja algún campo vacío, el mismo se pone rojo de no estar lleno y por lo tanto no añade los datos.

CASO DE USO: MODIFICAR CUENTA

Caso de uso	Modificar Cuenta
Actores	Gerente
Tipo	Extensión.
Propósito	Modificar los datos de una cuenta ya existente en el Sistema.
Resumen	El Caso de uso modifica algún dato de la cuenta de algún usuario que están registrado en el Sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el Sistema y haber iniciado sesión con su respectiva cuenta asignada. Se debe ejecutar previamente el Caso de uso: Crear Usuario para crear un nuevo usuario. Debe seleccionar un usuario de la lista que tenga una cuenta y luego presione la opción "modificar cuenta".
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Modificar Cuenta), donde se carga el formulario para modificar los datos de la cuenta: (Ci, Login, Contraseña). Una vez el formulario es llenado correctamente se hace clic en el botón "guardar" y se almacenan los datos modificados en la tabla Datos de la Base de datos. Si se hace clic en el botón "cancelar" se retorna a (Pantalla Usuarios).
Subflujos	Ninguno.
Excepciones	Si se deja algún campo vacío, se ponen de color rojo los campos de entrada de datos no permitiendo guardar correctamente los datos en la Base de datos.

CASO DE USO: ASIGNAR TARJETA

Caso de uso	Asignar Tarjeta.
Actores	Gerente.
Tipo	Inclusión.
Propósito	Permitir asignar el código de una tarjeta de acceso al usuario.
Resumen	El caso de uso es iniciado principalmente por el Gerente, este Caso de uso tiene la funcionalidad de asignar el código de una tarjeta física a los usuarios registrados en el Sistema.
Pre-Condiciones	Debe seleccionar la opción "asignar tarjeta" en la Pantalla Usuarios.
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Asignar Tarjeta), donde se carga el formulario para asignar los siguientes datos del usuario: (Ci, Código de tarjeta), una vez el formulario es llenado correctamente se hace clic en el botón "asignar" y se almacenan los datos en la tabla Datos de la base de datos. Si se hace clic en el botón "cancelar" se retorna a (Pantalla Usuarios).
Subflujos	Ninguno
Excepciones	Si se deja algún campo vacío, el mismo se pone rojo de no estar lleno y por lo tanto no añade los datos.

CASO DE USO: ASIGNAR ROL

Caso de uso	Asignar Rol
Actores	Gerente.
Tipo	Inclusión.
Propósito	Permitir asignarle un rol ya existente en el Sistema a un usuario.
Resumen	El Caso de uso es iniciado principalmente por el Gerente, este Caso de uso tiene la funcionalidad de asignar un rol a cada uno de los usuarios registrados en el sistema.
Pre-Condiciones	Debe seleccionar la opción "asignar rol" en la Pantalla Usuarios.
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Asignar Rol), donde se carga el formulario para añadir los siguientes datos del usuario: (Ci, Rol), una vez el formulario es llenado correctamente se hace clic en el botón "asignar" y se almacenan los datos en la tabla Datos de la base de datos. Si se hace clic en el botón "cancelar" se retorna a (Pantalla Usuarios).
Subflujos	Ninguno
Excepciones	Si se deja algún campo vacío, el mismo se pone rojo de no estar lleno y por lo tanto no añade los datos.

CASO DE USO: GESTION DE ROLES

Caso de Uso	Gestión de Roles
Actores	Gerente
Tipo	Básico
Propósito	Permitir gestionar roles.
Resumen	El Caso de uso; Gestión de roles es iniciado por el Gerente; el cual estará habilitado para adicionar, modificar, eliminar y asignar áreas en el Sistema.
Pre-condiciones	El Gerente debe estar previamente registrado en el Sistema y haber iniciado sesión. Debe seleccionar el Módulo "Roles", donde visualiza una pantalla con un listado de Roles y sus detalles.
Post-condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se ejecuta el Caso de uso: Gestión de Roles. Dependiendo de las opciones seleccionadas por el usuario.
Subflujos	Se muestra La Pantalla Roles con las características de todos los Roles registrados en el Sistema. El usuario puede seleccionar entre las siguientes opciones: "adicionar", "modificar", "eliminar"," asignar áreas". S-1 Si la actividad seleccionada es "adicionar" se muestra la Pantalla: Adicionar Rol. S-2 Si la actividad seleccionada es "modificar" se muestra la Pantalla: Modificar Rol. S-3 Si la actividad seleccionada es "eliminar" se muestra la Pantalla: Eliminar Rol. S-4 Si la actividad seleccionada es "asignar área" se muestra la Pantalla: Asignar Áreas.

CASO DE USO: ADICIONAR ROL

Caso de uso	Adicionar Rol.
Actores	Gerente
Tipo	Inclusión.
Propósito	Adicionar nuevos roles.
Resumen	El Caso de uso es iniciado por el Gerente, el cual adiciona los roles que estarán habilitados en el Sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el sistema y haber iniciado sesión. Debe seleccionar la opción "adicionar" en (Pantalla Roles).
Post-Condiciones	Usuarios autorizados para la manipulación del sistema.
Flujo Principal	Se muestra (Pantalla Adicionar Rol), donde se carga el formulario para adicionar los datos correspondientes: (Idrol, Nombre, Jerarquía, Descripción). Una vez el formulario es llenado correctamente se hace clic en el botón "Aceptar" para que se almacenen los datos en la tabla Roles. Si se hace clic en el botón "Cancelar" se retorna a (Pantalla Roles).
Subflujos	Ninguno.
Excepciones	Si se deja algún campo importante vacío, se pone en rojo los campos de entrada de datos no permitiendo guardar los datos ingresados.

CASO DE USO: MODIFICAR ROL

Caso de uso	Modificar Rol.
Actores	Gerente
Tipo	Extensión.
Propósito	Modificar un rol ya existente en el Sistema.
Resumen	El Caso de uso modifica algún dato de los roles que están registrados en el manejo del Sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el Sistema y haber iniciado sesión. Se debe ejecutar previamente el caso de uso Adicionar Rol para modificar un rol. Debe seleccionar un rol de la lista y luego presione la opción "modificar".
Post-Condiciones	Usuarios autorizados para la manipulación del sistema.
Flujo Principal	Se muestra (Pantalla Modificar Usuario), donde se carga el formulario para modificar los datos de un rol: (Idrol, Nombre, Jerarquía, Descripción). Una vez el formulario es llenado correctamente se hace clic en el botón "guardar" y se almacenan los datos actualizados en la tabla Roles de la Base de datos. Si se hace clic en el botón "cancelar" se retorna a (Pantalla Roles).
Subflujos	Ninguno.
Excepciones	Si se deja algún campo vacío, se ponen de color rojo los campos de entrada de datos no permitiendo guardar correctamente los datos en la Base de datos.

CASO DE USO: ELIMINAR ROL

Caso de uso	Eliminar Rol.
Actores	Gerente.
Tipo	Extensión
Propósito	Eliminar un rol que está registrado en el Sistema.
Resumen	El Caso de uso elimina los roles que estarán registrados en el sistema.
Pre-Condiciones	Debe seleccionar un rol de la lista y luego presionar la opción "eliminar" en (Pantalla Roles).
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Eliminar Rol), con el mensaje "Está seguro que desea eliminar este Rol". Si se presiona "Si" se eliminan los datos de la tabla Roles de la base de datos. Si se hace clic en el botón "No" se cancela la operación y se retorna a (Pantalla Roles).
Subflujos	Ninguno.
Excepciones	Ninguna.

CASO DE USO: ASIGNAR AREAS

Caso de uso	Asignar Áreas
Actores	Gerente.
Tipo	Inclusión.
Propósito	Permitir asignar distintas áreas ya existentes en el Sistema a un determinado rol.
Resumen	El Caso de uso es iniciado principalmente por el Gerente, este caso de uso tiene la funcionalidad de asignar áreas a cada uno de los roles registrados en el Sistema.
Pre-Condiciones	Debe seleccionar la opción "asignar áreas" en la Pantalla Roles.
Post-Condiciones	Usuarios autorizados para la manipulación del sistema.
Flujo Principal	Se muestra (Pantalla Asignar Áreas), donde se carga el formulario para añadir los siguientes datos del rol: (Idrol, id_a), una vez el formulario es llenado correctamente se hace clic en el botón "Guardar" y se almacenan los datos en la tabla Rol-Áreas de la base de datos. Si se hace clic en el botón "Cancelar" se retorna a (Pantalla Roles).
Subflujos	Ninguno
Excepciones	Si se deja algún campo vacío, el mismo se pone rojo de no estar lleno y por lo tanto no añade los datos.

CASO DE USO: GESTION DE AREAS

Caso de Uso	Gestión de Áreas
Actores	Gerente
Tipo	Básico
Propósito	Permitir Gestionar Áreas.
Resumen	El Caso de uso: Gestión de Áreas es iniciado por el Gerente; el cual estará habilitado para adicionar, modificar, eliminar y asignar áreas en el Sistema.
Pre-condiciones	El Gerente debe estar previamente registrado en el Sistema y haber iniciado sesión. Debe seleccionar el Módulo "Áreas", donde visualiza una pantalla con un listado de Áreas y sus detalles.
Post-condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se ejecuta el Caso de uso: Gestión de Áreas. Dependiendo de las opciones seleccionadas por el usuario.
Subflujos	Se muestra La Pantalla Área con las características de todos los Roles registrados en el Sistema. El usuario puede seleccionar entre las siguientes opciones: "añadir", "modificar", "deshabilitar". S-1 Si la actividad seleccionada es "añadir" se muestra la Pantalla: Añadir Área. S-2 Si la actividad seleccionada es "modificar" se muestra la Pantalla: Modificar Área. S-3 Si la actividad seleccionada es "deshabilitar" se muestra la Pantalla: Deshabilitar Área.

CASO DE USO: AÑADIR AREA

Caso de uso	Añadir Área
Actores	Gerente
Tipo	Inclusión.
Propósito	Añadir nuevas áreas.
Resumen	El Caso de uso es iniciado por el Gerente; el cual añade las áreas que estarán habilitadas en el Sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el Sistema y haber iniciado sesión. Debe seleccionar la opción "añadir" en (Pantalla Áreas).
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Añadir Área), donde se carga el formulario para registrar los datos correspondientes: (id_a, nombre_a, numpiso, descripción). Una vez el formulario es llenado correctamente se hace clic en el botón "Aceptar" para que se almacenen los datos en la tabla Áreas. Si se hace clic en el botón "Cancelar" se retorna a (Pantalla Áreas).
Subflujos	Ninguno.
Excepciones	Si se deja algún campo importante vacío, se pone en rojo los campos de entrada de datos no permitiendo guardar los datos ingresados.

CASO DE USO: MODIFICAR ÁREA

Caso de uso	Modificar Área.
Actores	Gerente
Tipo	Extensión.
Propósito	Modificar área ya existente en el Sistema.
Resumen	El Caso de uso modifica algún dato de las áreas que están registradas en el manejo del Sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el Sistema y haber iniciado sesión. Se debe ejecutar previamente el Caso de uso: Añadir un área para modificarla posteriormente. Debe seleccionar un rol de la lista y luego presione la opción "modificar".
Post-Condiciones	Usuarios autorizados para la manipulación del sistema.
Flujo Principal	Se muestra (Pantalla Modificar Área), donde se carga el formulario para modificar los datos de un área: (id_a, nombre_a, numpiso, descripción). Una vez el formulario es llenado correctamente se hace clic en el botón "guardar" y se almacenan los datos actualizados en la tabla Áreas de la Base de datos. Si se hace clic en el botón "cancelar" se retorna a (Pantalla Áreas).
Subflujos	Ninguno.
Excepciones	Si se deja algún campo vacío, se ponen de color rojo los campos de entrada de datos no permitiendo guardar correctamente los datos en la Base de datos.

CASO DE USO: DESHABILITAR AREA

Caso de uso	Deshabilitar Área.
Actores	Gerente.
Tipo	Extensión
Propósito	Deshabilitar un área que está registrado en el Sistema.
Resumen	El Caso de uso deshabilitará un área que estará registrado en el Sistema.
Pre-Condiciones	Se debe ejecutar previamente el Caso de uso "añadir" para registrar una nueva área. Debe seleccionar un área de la lista y luego presione la opción "deshabilitar" en (Pantalla Áreas).
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Deshabilitar Área), con el mensaje "Está seguro que desea deshabilitar esta Área". Si se presiona "Si" se eliminan los datos de la tabla Roles de la base de datos. Si se hace clic en el botón "No" se cancela la operación y se retorna a (Pantalla Área).
Subflujos	Ninguno.
Excepciones	Ninguna.

CASO DE USO: GESTION MOSTRAR CODIGO

Caso de uso	Mostrar Código
Actores	Administrador
Tipo	Básico
Propósito	Obtener los Códigos predeterminados de las Tarjetas
Resumen	El Caso de uso es iniciado por el Gerente o el Administrador; el cual registra las tarjetas de acceso que estarán habilitadas en el Sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el Sistema y haber iniciado sesión y debe haber obtenido el código de la tarjeta utilizando la aplicación del anterior caso de uso descrito. Debe seleccionar la opción "registrar" en (Pantalla Tarjetas).
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Registrar Tarjeta), donde se carga el formulario para registrar los datos correspondientes: (código_da). Una vez el formulario es llenado correctamente se hace clic en el botón "Aceptar" para que se almacenen los datos en la tabla Tarjetas. Si se hace clic en el botón "Cancelar" se retorna a (Pantalla Tarjetas).
Subflujos	Ninguno.
Excepciones	Si se deja algún campo importante vacío, se pone en rojo los campos de entrada de datos no permitiendo guardar los datos ingresados.

CASO DE USO: GESTION DE TARJETAS

Caso de Uso	Gestión de Tarjetas
Actores	Gerente, Administrador
Tipo	Básico
Propósito	Permitir gestionar las tarjetas de acceso.
Resumen	El Caso de uso es iniciado principalmente por el Administrador, pero el Gerente también puede acceder a este módulo, este caso de uso tiene las funcionalidades de registrar, actualizar y bloquear las tarjetas de acceso de la Organización.
Pre-condiciones	Debe seleccionar el modulo "Tarjetas" del menú principal, donde visualiza una pantalla con un listado de las Tarjetas ya registradas.
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se ejecuta gestión de tarjetas y se muestra (Pantalla Tarjetas) con los datos de todas las tarjetas registradas en el Sistema. El usuario puede seleccionar entre las siguientes opciones: "registrar", "ver", "bloquear".
Subflujos	**S-1** Si la actividad seleccionada es "registrar" se muestra la Pantalla: Registrar Tarjeta. **S-2** Si la actividad seleccionada es "ver" se muestra la Pantalla: Actualizar Tarjeta. **S-3** Si la actividad seleccionada es "bloquear" se muestra la Pantalla: Bloquear Tarjeta.
Excepciones	Ninguna.

CASO DE USO: REGISTRAR TARJETAS

Caso de uso	Registrar Tarjeta
Actores	Gerente y Administrador
Tipo	Inclusión.
Propósito	Registrar nuevas tarjetas de acceso.
Resumen	El Caso de uso es iniciado por el Gerente o el Administrador; el cual registra las tarjetas de acceso que estarán habilitadas en el Sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el Sistema y haber iniciado sesión y debe haber obtenido el código de la tarjeta utilizando la aplicación del anterior caso de uso descrito.. Debe seleccionar la opción "registrar" en (Pantalla Tarjetas).
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Registrar Tarjeta), donde se carga el formulario para registrar los datos correspondientes: (código_da). Una vez el formulario es llenado correctamente se hace clic en el botón "Aceptar" para que se almacenen los datos en la tabla Tarjetas. Si se hace clic en el botón "Cancelar" se retorna a (Pantalla Tarjetas).
Subflujos	Ninguno.
Excepciones	Si se deja algún campo importante vacío, se pone en rojo los campos de entrada de datos no permitiendo guardar los datos ingresados.

CASO DE USO: VER TARJETA

Caso de uso	Ver Tarjeta.
Actores	Gerente y Administrador
Tipo	Extensión.
Propósito	Ver los datos de una tarjeta ya registrada en el Sistema.
Resumen	El Caso de uso muestra los datos de las tarjetas que están registradas en el manejo del Sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el sistema y haber iniciado sesión. Se debe ejecutar previamente el caso de uso Registrar Tarjeta para ver una tarjeta. Debe seleccionar una tarjeta de la lista y luego presione la opción "ver".
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Ver Tarjeta) donde se carga el formulario no editable con todos los datos de una tarjeta: (código_da). Si se hace clic en el botón "salir" se retorna a (Pantalla Tarjetas).
Subflujos	Ninguno.
Excepciones	Si se deja algún campo vacío, se ponen de color rojo los campos de entrada de datos no permitiendo guardar correctamente los datos en la Base de datos.

CASO DE USO: BLOQUEAR TARJETA

Caso de uso	Bloquear Tarjeta
Actores	Gerente y Administrador
Tipo	Extensión
Propósito	Bloquear una tarjeta que está registrada en el Sistema.
Resumen	El Caso de uso bloqueará una tarjeta ya registrada en el Sistema, previa presentación de una notificación física ya sea de pérdida o licencia temporal.
Pre-Condiciones	Se debe ejecutar previamente el Caso de uso "registrar" para añadir el código de una nueva tarjeta. Debe seleccionar una tarjeta de la lista y luego presionar la opción "bloquea" en (Pantalla Tarjetas).
Post-Condiciones	Usuarios autorizados para la manipulación del Sistema.
Flujo Principal	Se muestra (Pantalla Bloquear Tarjeta), con el mensaje "Está seguro que desea bloquear esta tarjeta". Si se presiona "Si" el dato estado de la tarjeta pasa de verdadero (true) a falso (false) en la tabla Tarjetas de la base de datos. Si se hace clic en el botón "No", se cancela la operación y se retorna a (Pantalla Tarjetas).
Subflujos	Ninguno.
Excepciones	Ninguna.

CASO DE USO: GESTION DE REPORTES

Caso de uso	Gestión Reportes.
Actores	Gerente, Administrador.
Tipo	Básico.
Propósito	El propósito es ver un informe de lo que realiza la Organización
Resumen	El caso de uso es iniciado principalmente por el Administrador, pero el Gerente también puede acceder a este módulo. El caso de uso visualiza los reportes generados por el sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el sistema y haber iniciado sesión. Debe seleccionar en el menú principal el módulo "Reportes" y seleccionar entre las siguientes opciones: "Tarjetas Bloqueadas", "Usuarios Roles", "Usuarios Tarjetas", "Flujo de Accesos".
Post-Condiciones	Usuarios autorizados para la manipulación del sistema.
Flujo Principal	Se ejecuta gestión Reportes se muestra (Pantalla Reportes) y se continúa con los subflujos.
Subflujos	**s-1** Si la actividad seleccionada es "Tarjetas Bloqueadas" se muestra (Pantalla Reporte Tarjetas Bloqueadas). **s-2** Si la actividad seleccionada es "Usuarios Roles" se muestra (Pantalla Reporte Usuario Roles). **s-3** Si la actividad seleccionada es "Usuarios Tarjetas" se muestra (Pantalla Reporte Usuarios Tarjetas). **s-4** Si la actividad seleccionada es "Flujo de Accesos" se muestra (Pantalla Reporte Flujo de Accesos). **s-5** Si la actividad seleccionada es "Usuarios Áreas" se muestra (Pantalla Reporte Usuarios Áreas).
Excepciones	Ninguna.

CASO DE USO: REPORTE TARJETAS BLOQUEADAS

Caso de uso	Tarjetas Bloqueadas
Actores	Gerente, Administrador.
Tipo	Extensión.
Propósito	Permite ver los datos de las Tarjetas registradas en el sistema que se encuentran bloqueadas.
Resumen	El caso de uso visualiza la lista de todas las tarjetas que han sido bloqueadas en el sistema por el Administrador.
Pre-Condiciones	El usuario debe estar previamente registrado en el sistema. Debe seleccionar "Reportes" y hacer clic en "Tarjetas Bloqueadas" en (Pantalla Reportes).
Post-Condiciones	Usuarios autorizados para la manipulación del sistema.
Flujo Principal	Se muestra (Pantalla Reporte Tarjetas Bloqueadas), Una tabla con los campos: (N, cod_da) donde se cargan todos los datos de las tarjetas registradas en el sistema. Se presiona el botón Imprimir, para imprimir los datos visualizados. Para salir de la pantalla puede escoger la opción cancelar y vuelve a la (Pantalla Reportes).
Subflujos	Ninguno.
Excepciones	Ninguna.

CASO DE USO: REPORTE USUARIOS ROLES

Caso de uso	Usuario Roles
Actores	Gerente, Administrador.
Tipo	Extensión.
Propósito	Permite ver los datos de los Usuarios y sus respectivos roles registrados en el sistema.
Resumen	El caso de uso visualiza la lista de todas los Usuarios y sus Roles que han sido asignados en el sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el sistema. Debe seleccionar "Reportes" y hacer clic en "Usuarios Roles" en (Pantalla Reportes).
Post-Condiciones	Usuarios autorizados para la manipulación del sistema.
Flujo Principal	Se muestra (Pantalla Reporte Usuarios Roles) una tabla con los campos: (N, Nombre, Ap, Am, Nombre de Rol) donde se cargan todos los datos de los usuarios en el sistema. Se presiona el botón Imprimir, para imprimir los datos visualizados. Para salir de la pantalla puede escoger la opción cancelar y vuelve a la (Pantalla Reportes).
Subflujos	Ninguno.
Excepciones	Ninguna.

CASO DE USO: REPORTE USUARIOS TARJETAS

Caso de uso	Usuarios Tarjetas
Actores	Gerente, Administrador.
Tipo	Extensión.
Propósito	Permite ver los datos de las Tarjetas que fueron asignadas a los diferentes Usuarios registrados en el sistema y su estado actual.
Resumen	El caso de uso visualiza la lista de todas las tarjetas que han sido bloqueadas en el sistema por el Administrador.
Pre-Condiciones	El usuario debe estar previamente registrado en el sistema. Debe seleccionar "Reportes" y hacer clic en "Usuarios Tarjetas" en (Pantalla Reportes).
Post-Condiciones	Usuarios autorizados para la manipulación del sistema.
Flujo Principal	Se muestra (Pantalla Reporte Usuarios Tarjetas), Una tabla con los campos: (N, Nombre, Ap, Am, cod_da, estado) donde se cargan todos los datos de las tarjetas y usuarios registrados en el sistema. Se presiona el botón Imprimir, para imprimir los datos guardados. Para salir de la pantalla puede escoger la opción cancelar y vuelve a la (Pantalla Reportes).
Subflujos	Ninguno.
Excepciones	Ninguna.

CASO DE USO: REPORTE USUARIOS AREAS

Caso de uso	Usuarios Areas
Actores	Gerente, Administrador.
Tipo	Extensión.
Propósito	Permite ver los datos de las Áreas que fueron asignadas a los diferentes Usuarios registrados en el sistema.
Resumen	El caso de uso visualiza la lista de todas las áreas que han sido asignadas a sus respectivos usuarios en el sistema por el Administrador.
Pre-Condiciones	El usuario debe estar previamente registrado en el sistema. Debe seleccionar "Reportes" y hacer clic en "Usuarios Áreas" en (Pantalla Reportes).
Post-Condiciones	Usuarios autorizados para la manipulación del sistema.
Flujo Principal	Se muestra (Pantalla Reporte Usuarios Áreas), Una tabla con los campos: (N, Nombre, Ap, Am, Rol, Área) donde se cargan todos los datos de las áreas y usuarios registrados en el sistema. Se presiona el botón Imprimir, para imprimir los datos guardados. Para salir de la pantalla puede escoger la opción cancelar y vuelve a la (Pantalla Reportes).
Subflujos	Ninguno.
Excepciones	Ninguna.

CASO DE USO: FLUJO DE ACCESOS

Caso de uso	Flujo de Accesos
Actores	Gerente, Administrador.
Tipo	Extensión.
Propósito	Permite ver los datos de las Tarjetas, la Fecha y Hora en la que se ingresó a un área.
Resumen	El caso de uso visualiza la lista de todas las tarjetas que han accedido a un área registrada en el sistema.
Pre-Condiciones	El usuario debe estar previamente registrado en el sistema. Debe seleccionar "Reportes" y hacer clic en "Flujo de Accesos" en (Pantalla Reportes).
Post-Condiciones	Usuarios autorizados para la manipulación del sistema.
Flujo Principal	Se muestra (Pantalla Reporte Flujo de Accesos), Una tabla con los campos: (N, Nombre, Ap, Am, cod_da, area) donde se cargan todos los datos de las tarjetas y usuarios registrados en el sistema. Se presiona el botón Imprimir, para imprimir los datos guardados. Para salir de la pantalla puede escoger la opción cancelar y vuelve a la (Pantalla Reportes).
Subflujos	Ninguno.
Excepciones	Ninguna.

9. DIAGRAMAS DE ACTIVIDADES

DIAGRAMA DE ACTIVIDADES: INICIO DE SESION

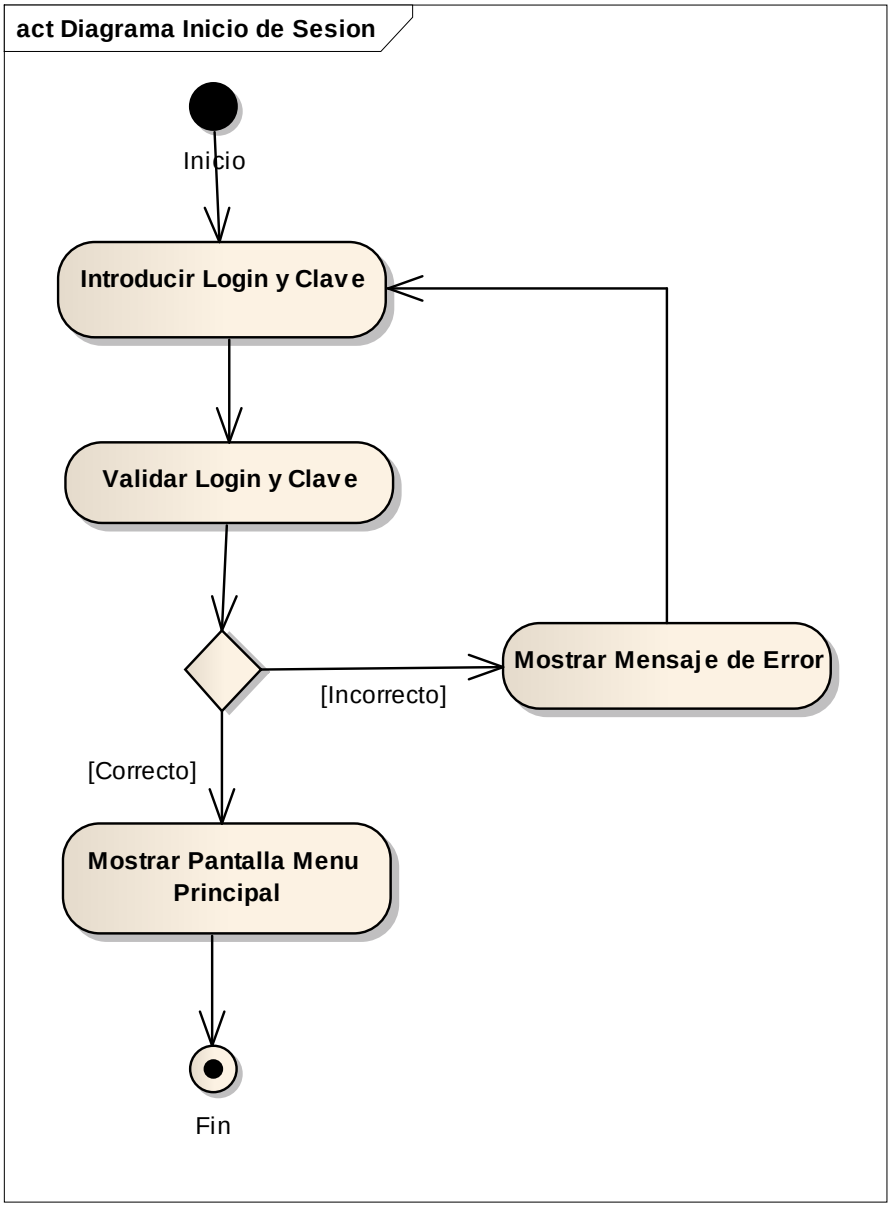


DIAGRAMA DE ACTIVIDADES: CREAR USUARIO

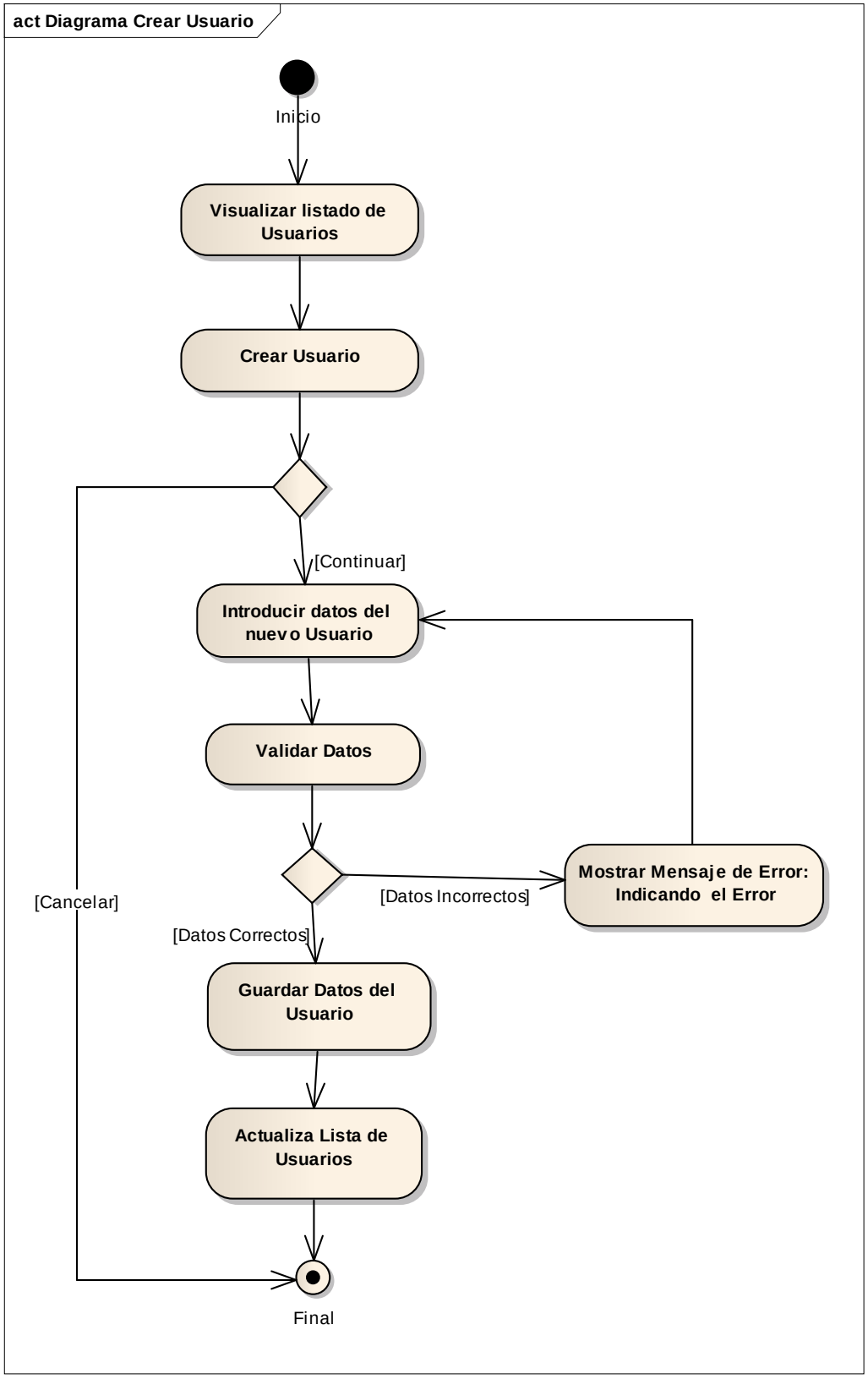


DIAGRAMA DE ACTIVIDADES: ACTUALIZAR USUARIO

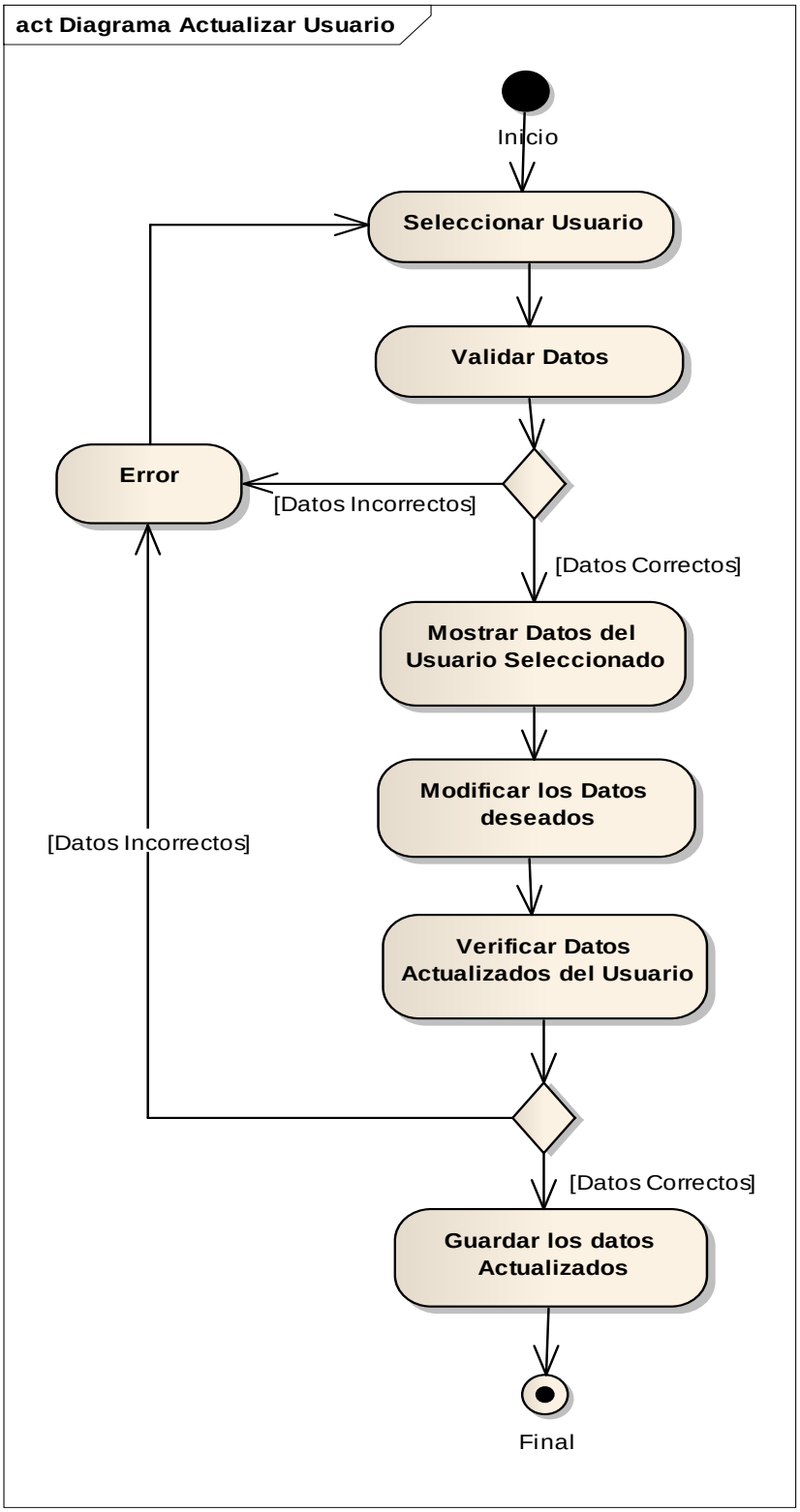


DIAGRAMA DE ACTIVIDADES: DAR DE BAJA USUARIO

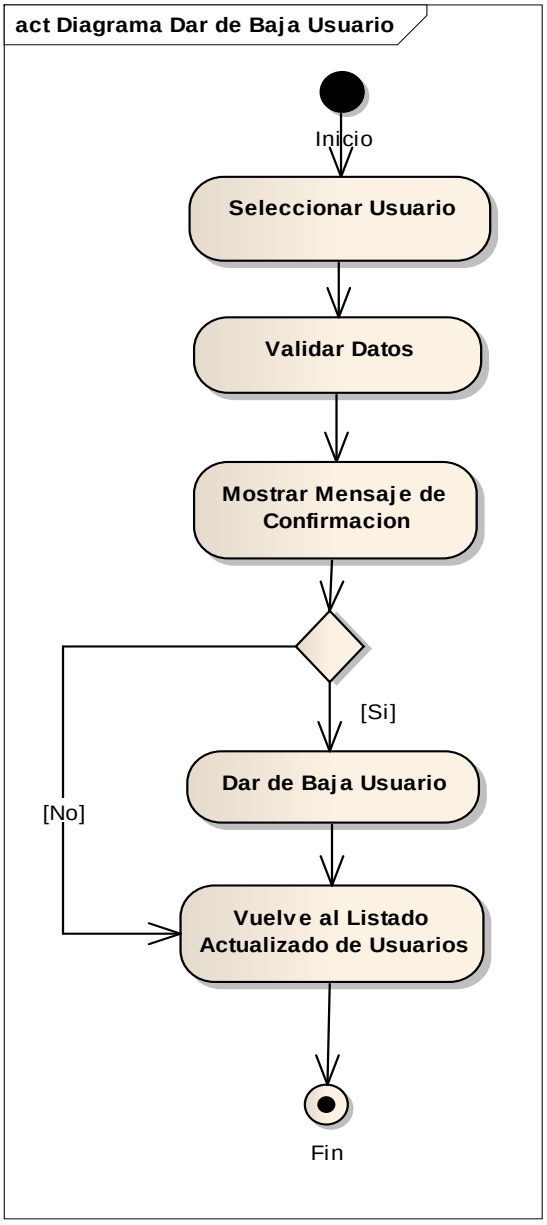


DIAGRAMA DE ACTIVIDADES: VER USUARIO

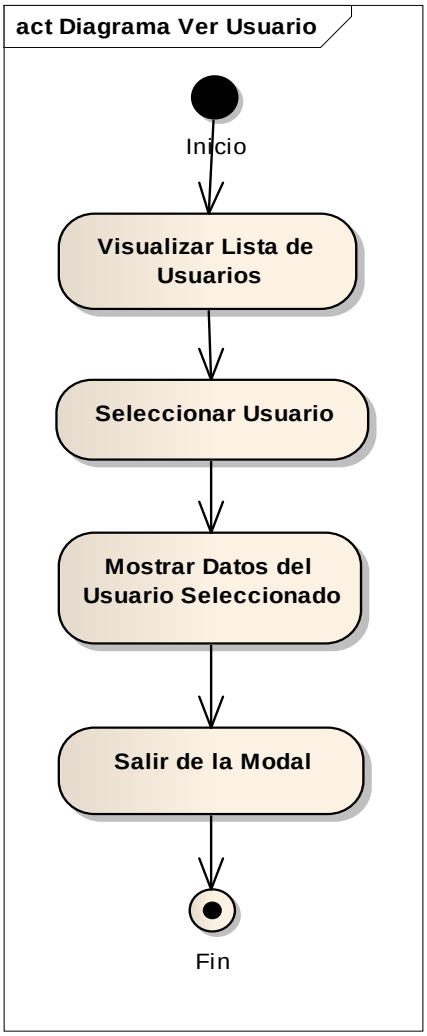


DIAGRAMA DE ACTIVIDADES: ASIGNAR ROL

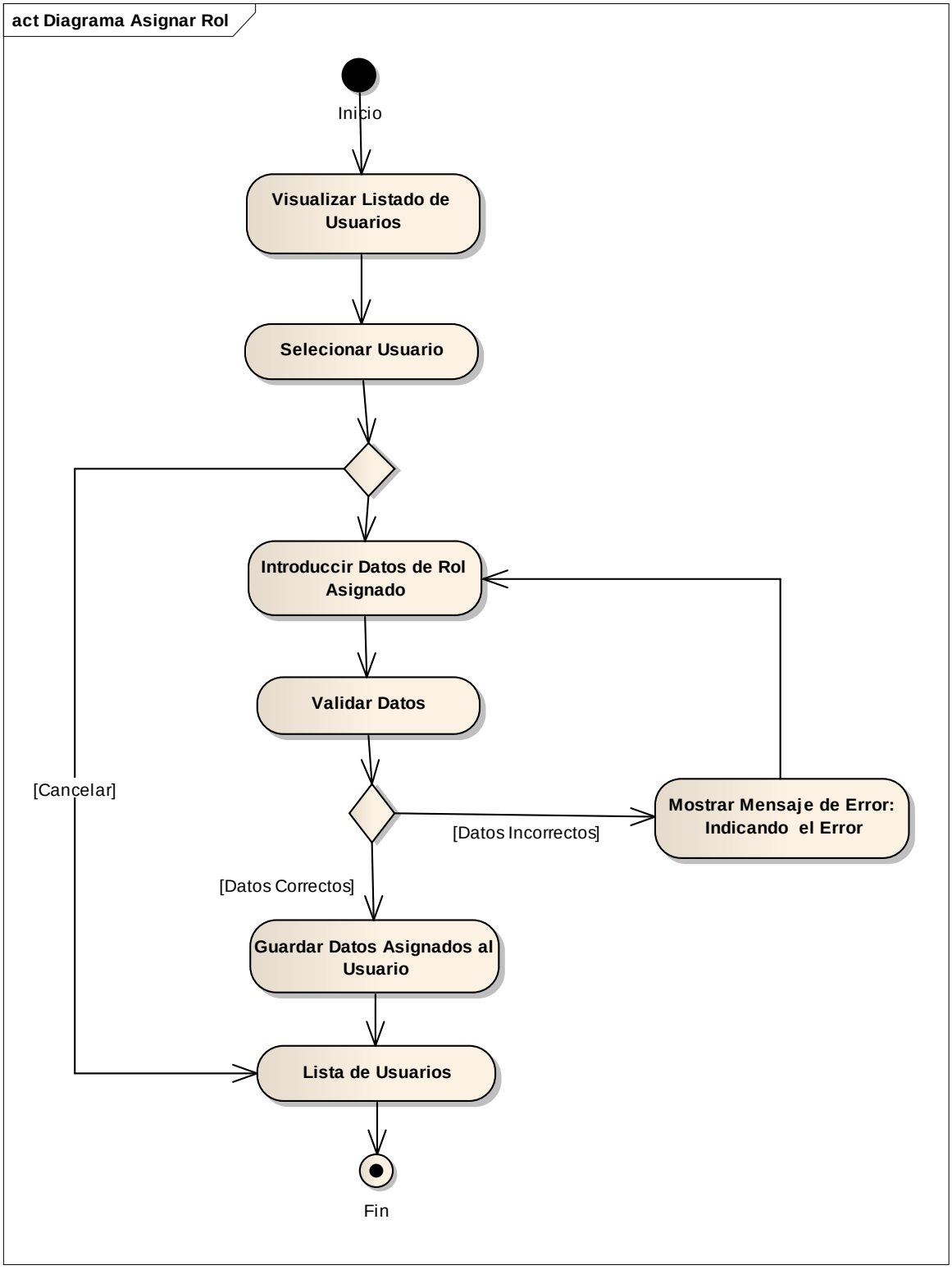


DIAGRAMA DE ACTIVIDADES: ASIGNAR CUENTA

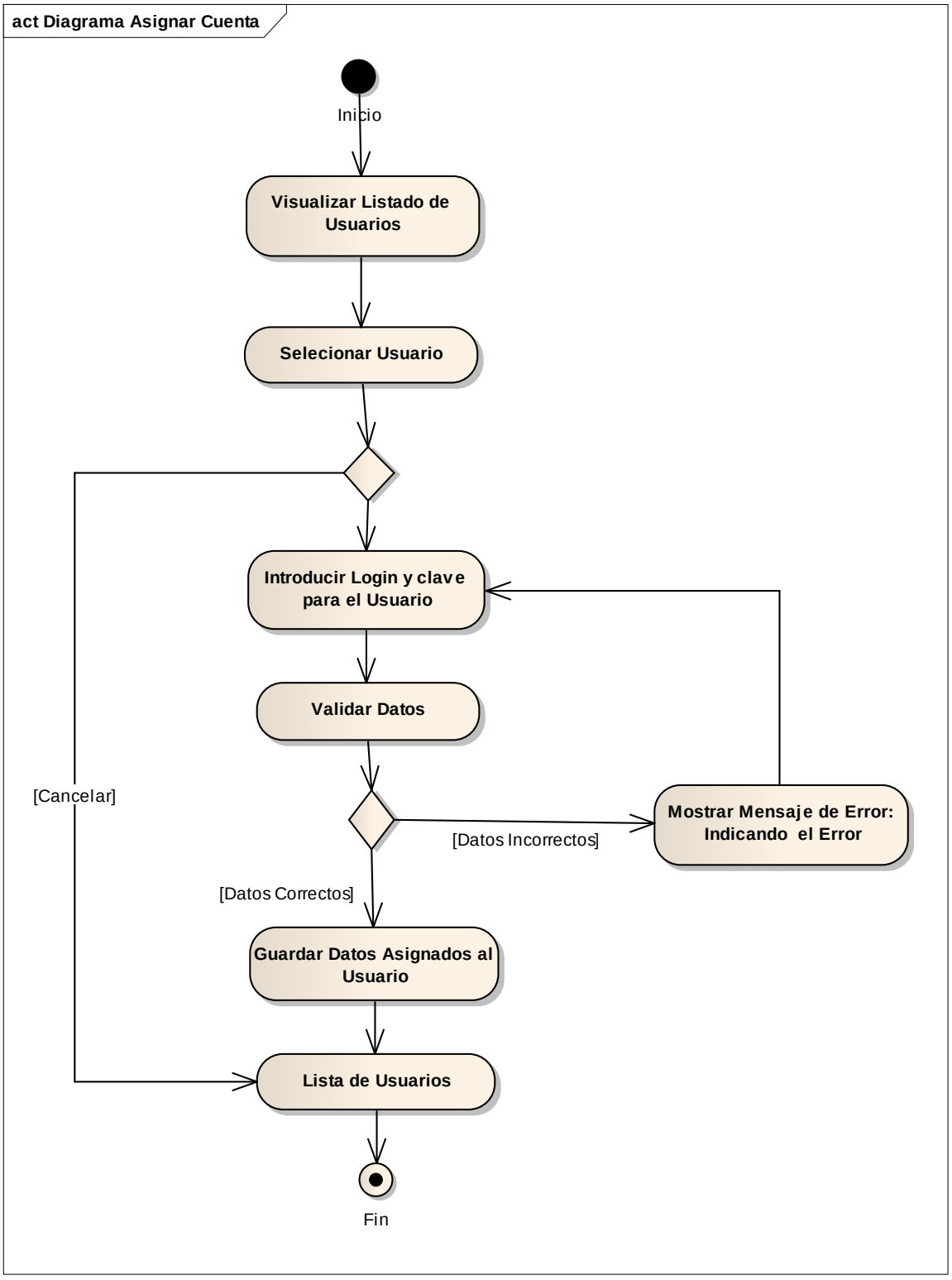


DIAGRAMA DE ACTIVIDADES: MODIFICAR CUENTA

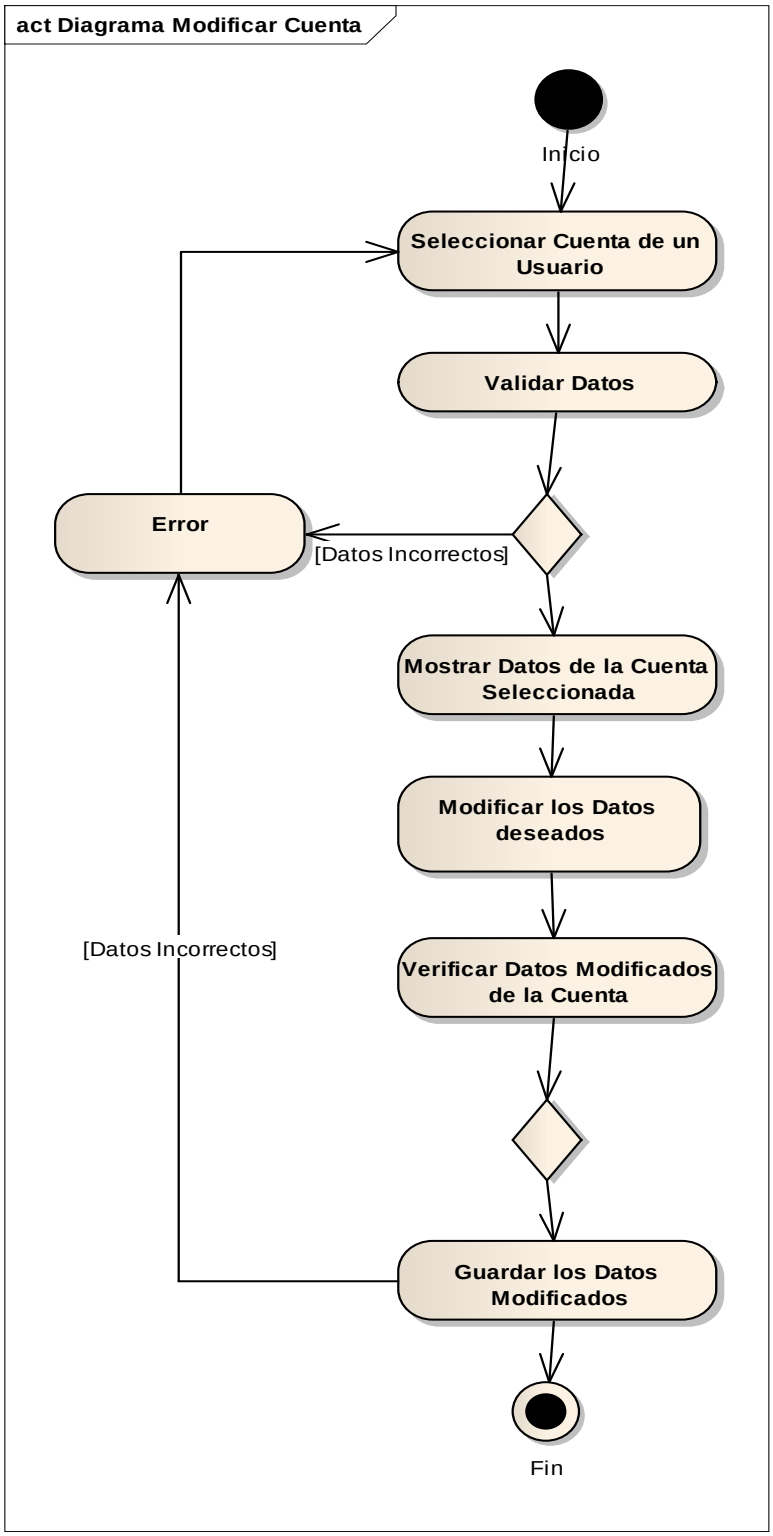


DIAGRAMA DE ACTIVIDADES: ASIGNAR TARJETA

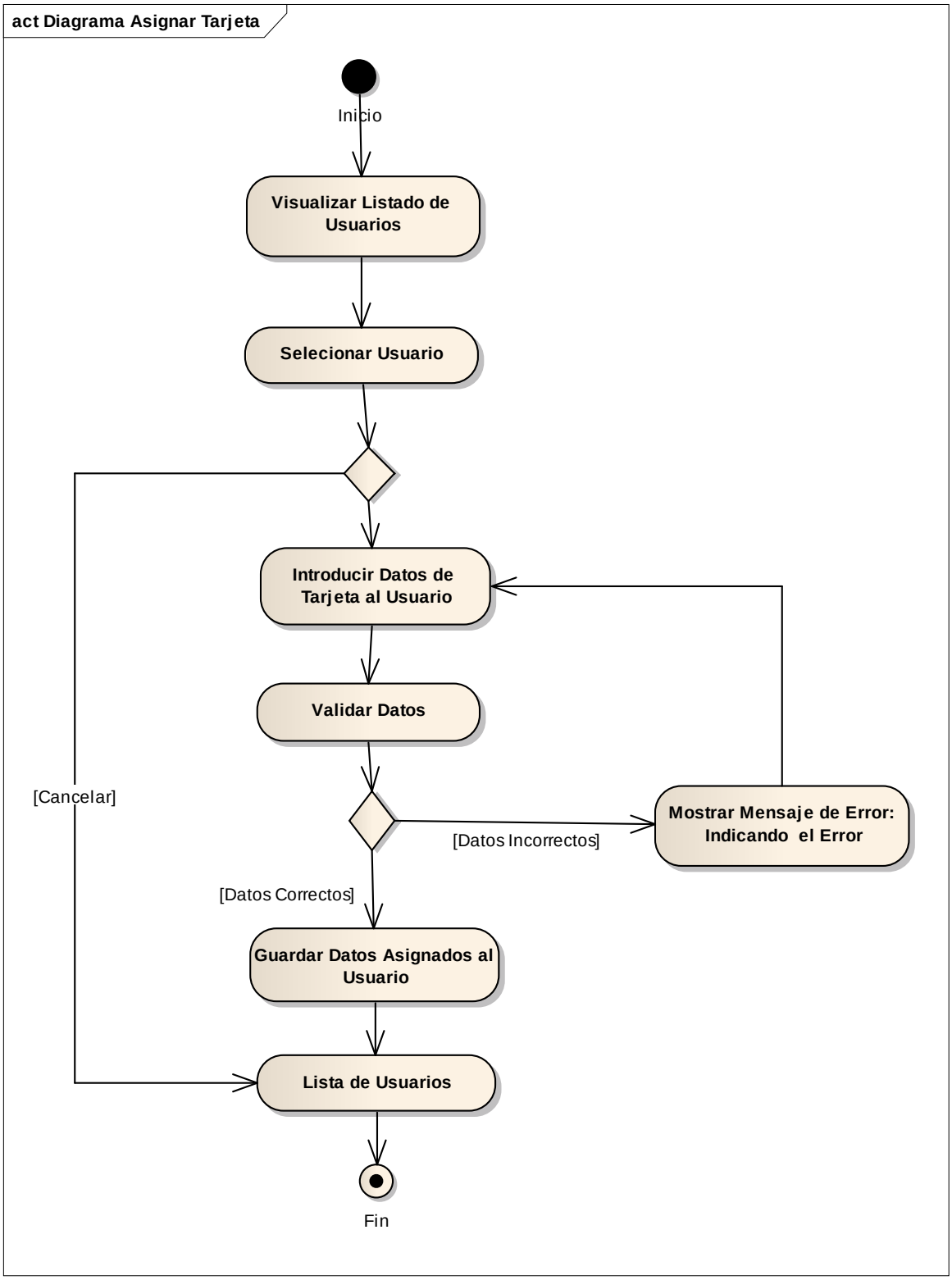


DIAGRAMA DE ACTIVIDADES: ADICIONAR ROL

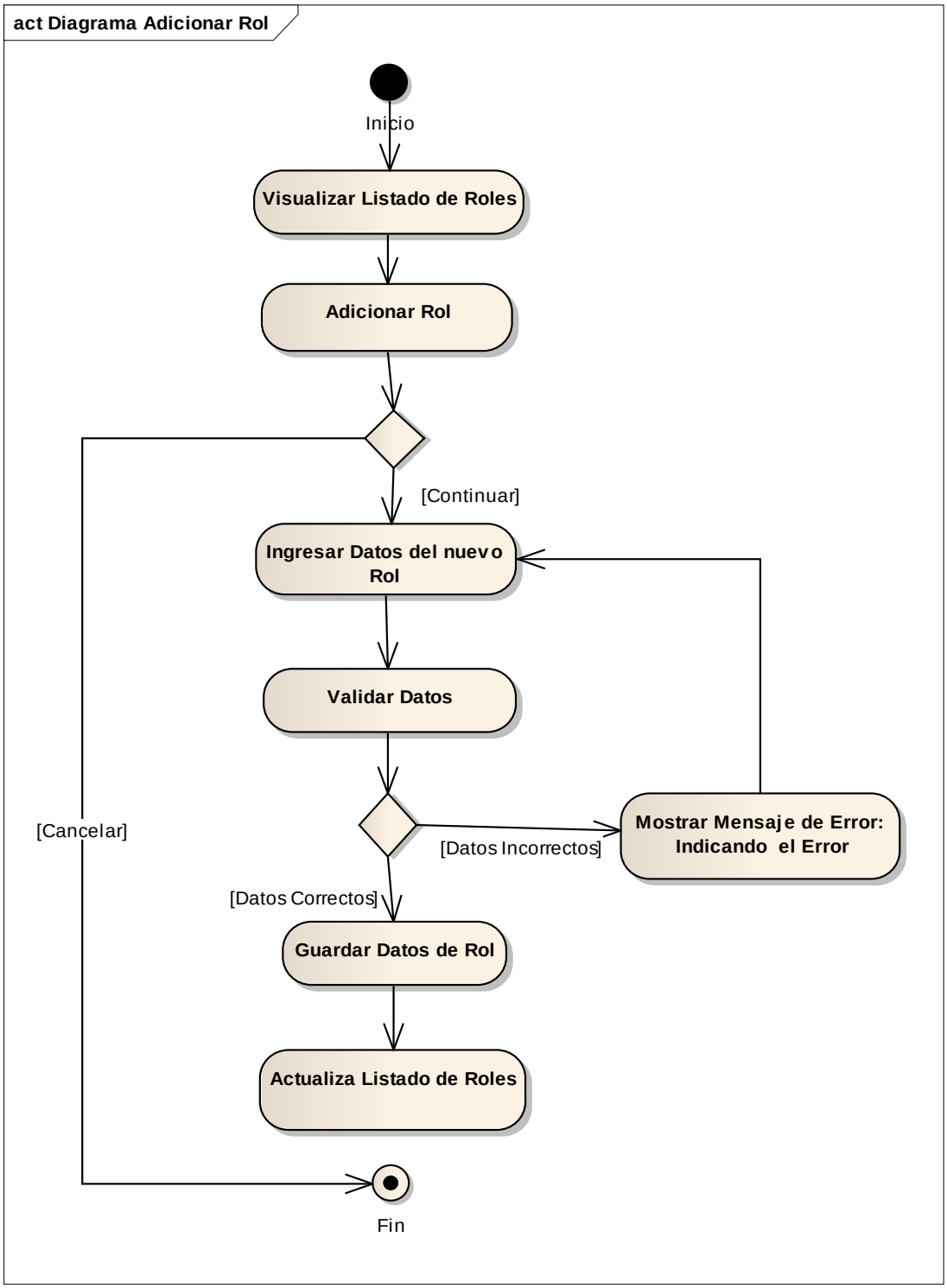


DIAGRAMA DE ACTIVIDADES: MODIFICAR ROL

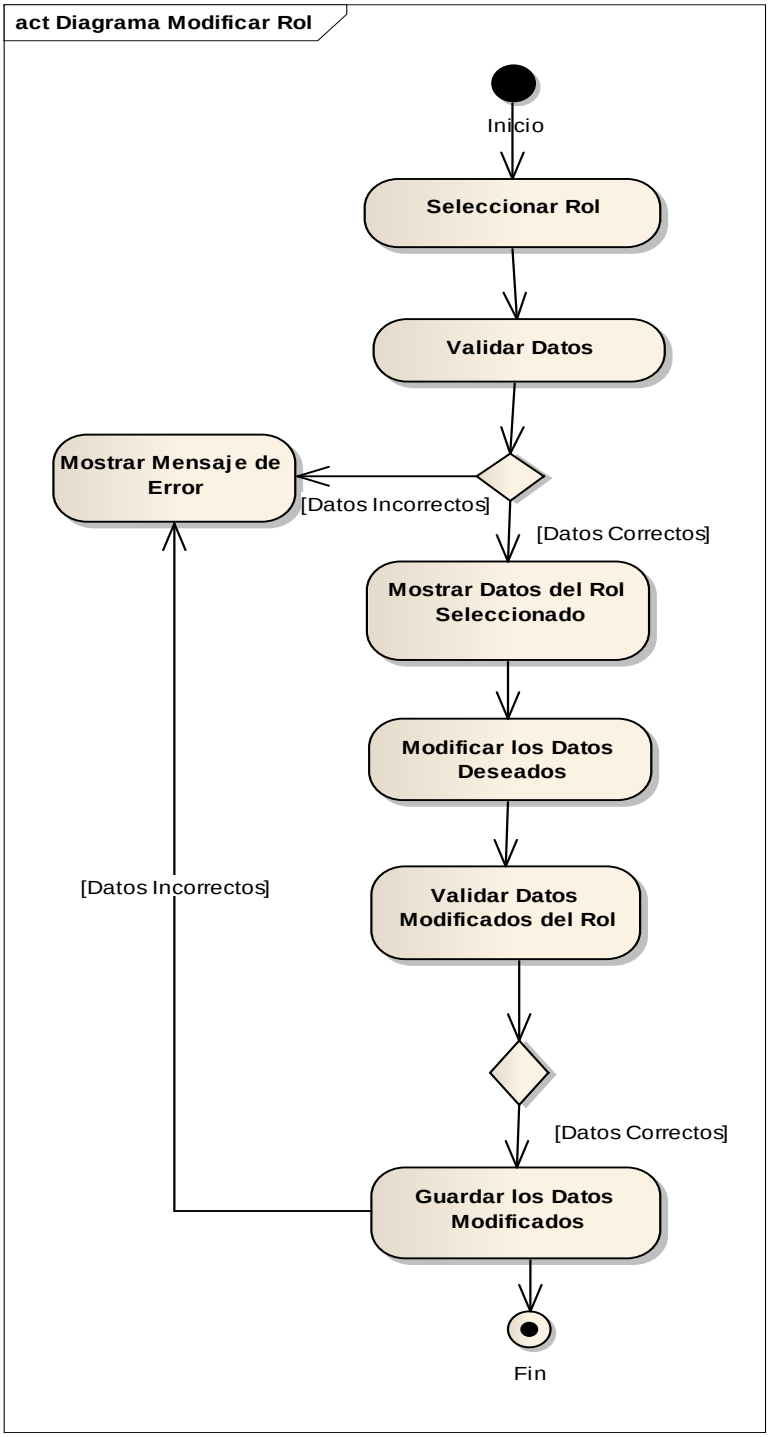


DIAGRAMA DE ACTIVIDADES: ELIMINAR ROL

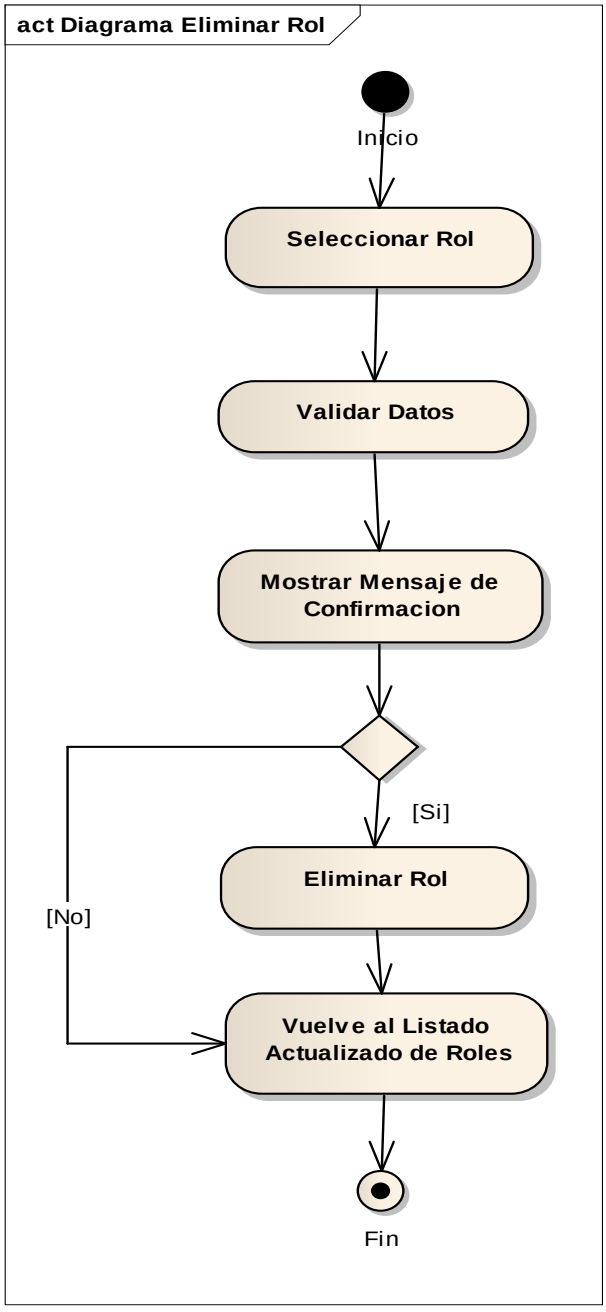


DIAGRAMA DE ACTIVIDADES: ASIGNAR AREA

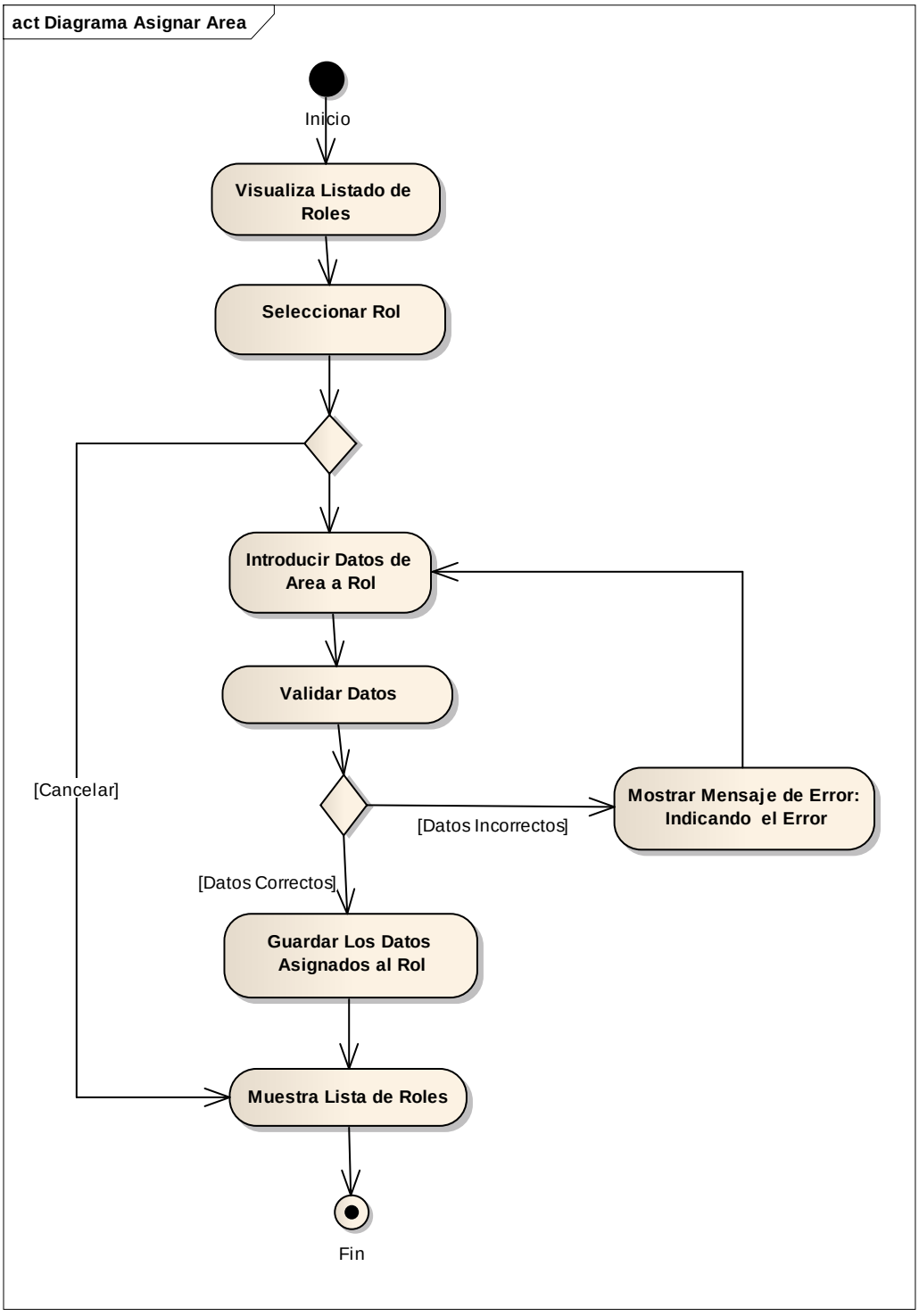


DIAGRAMA DEACTIVIDADES: AÑADIR AREA

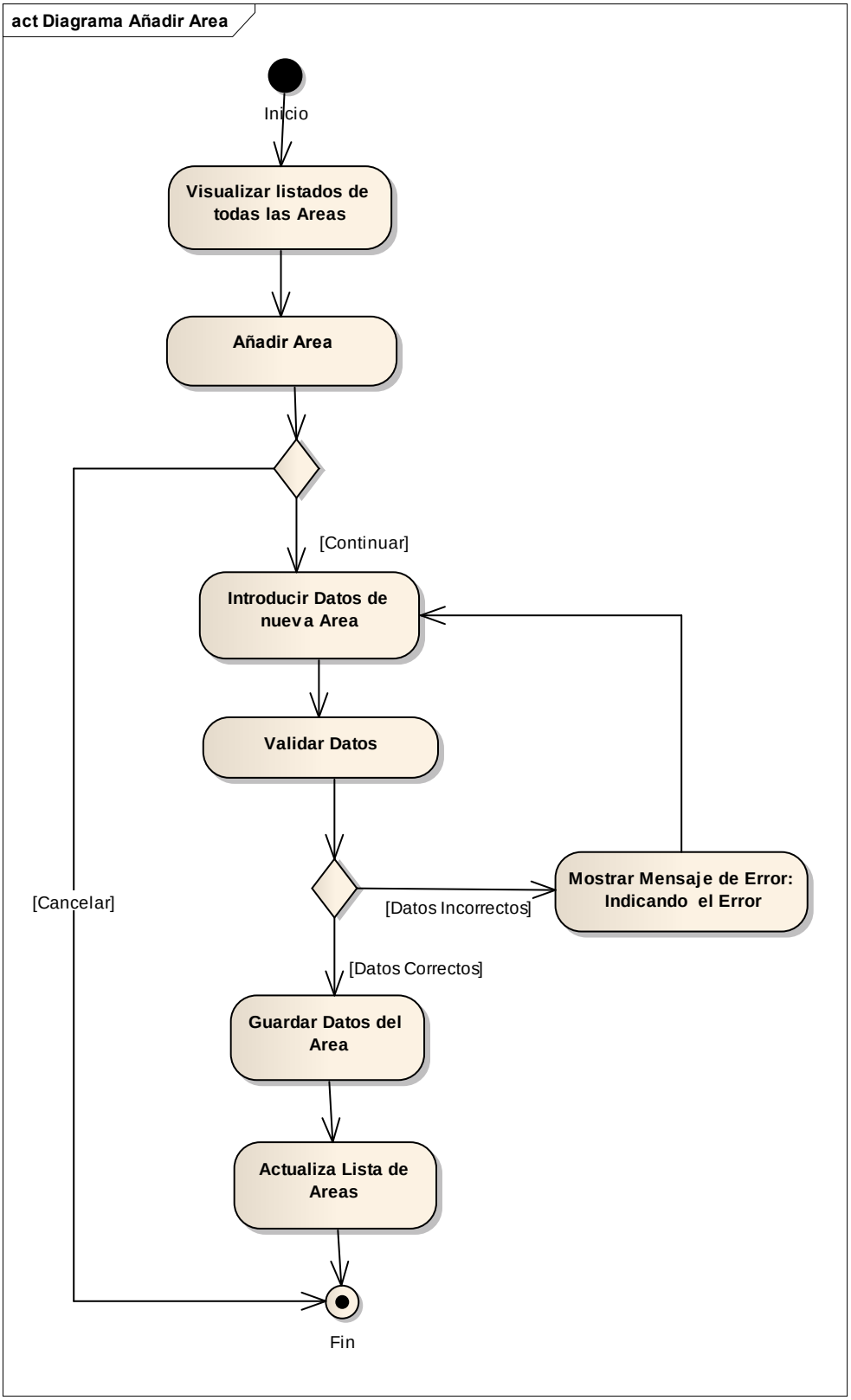


DIAGRAMA DE ACTIVIDADES: MODIFICAR AREA

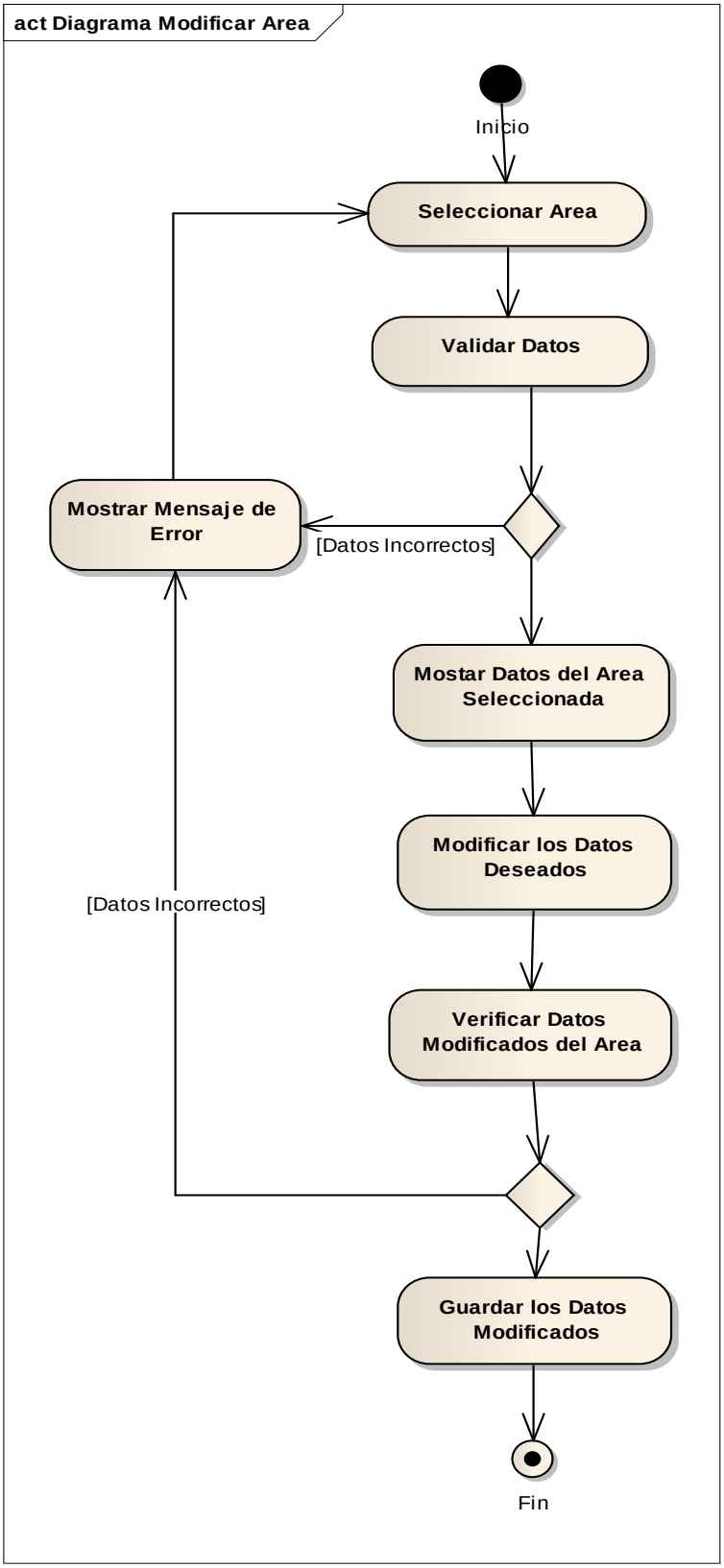


DIAGRAMA DE ACTIVIDADES: DESHABILITAR AREA

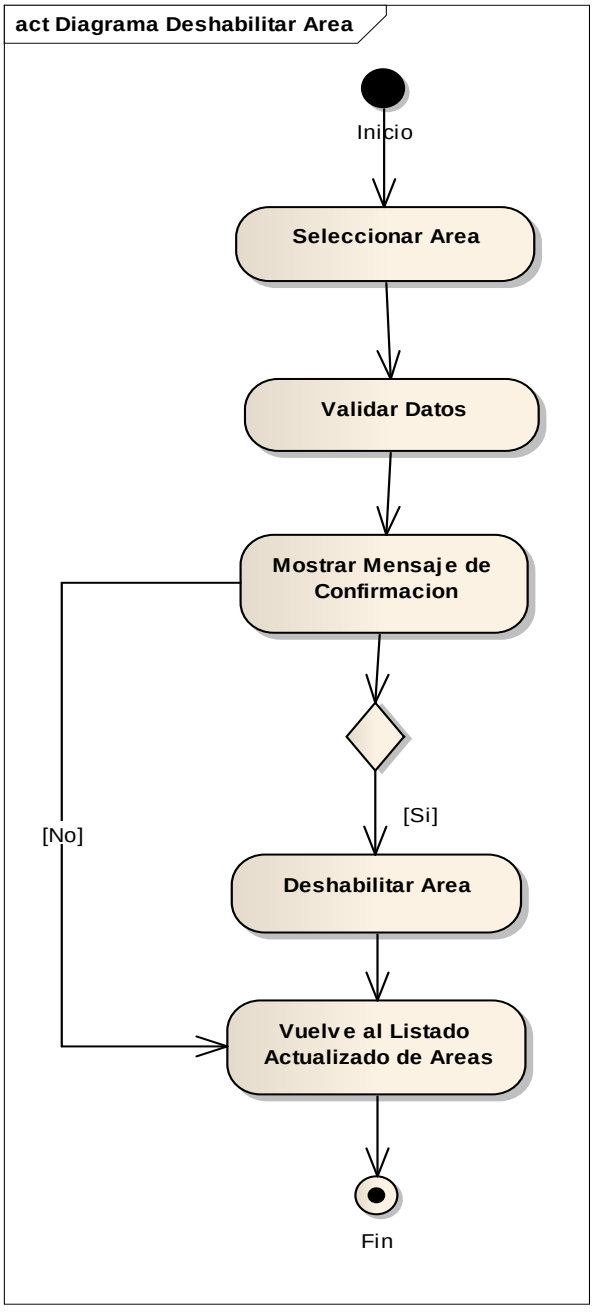


DIAGRAMA DE ACTIVIDADES: REGISTRAR TARJETA

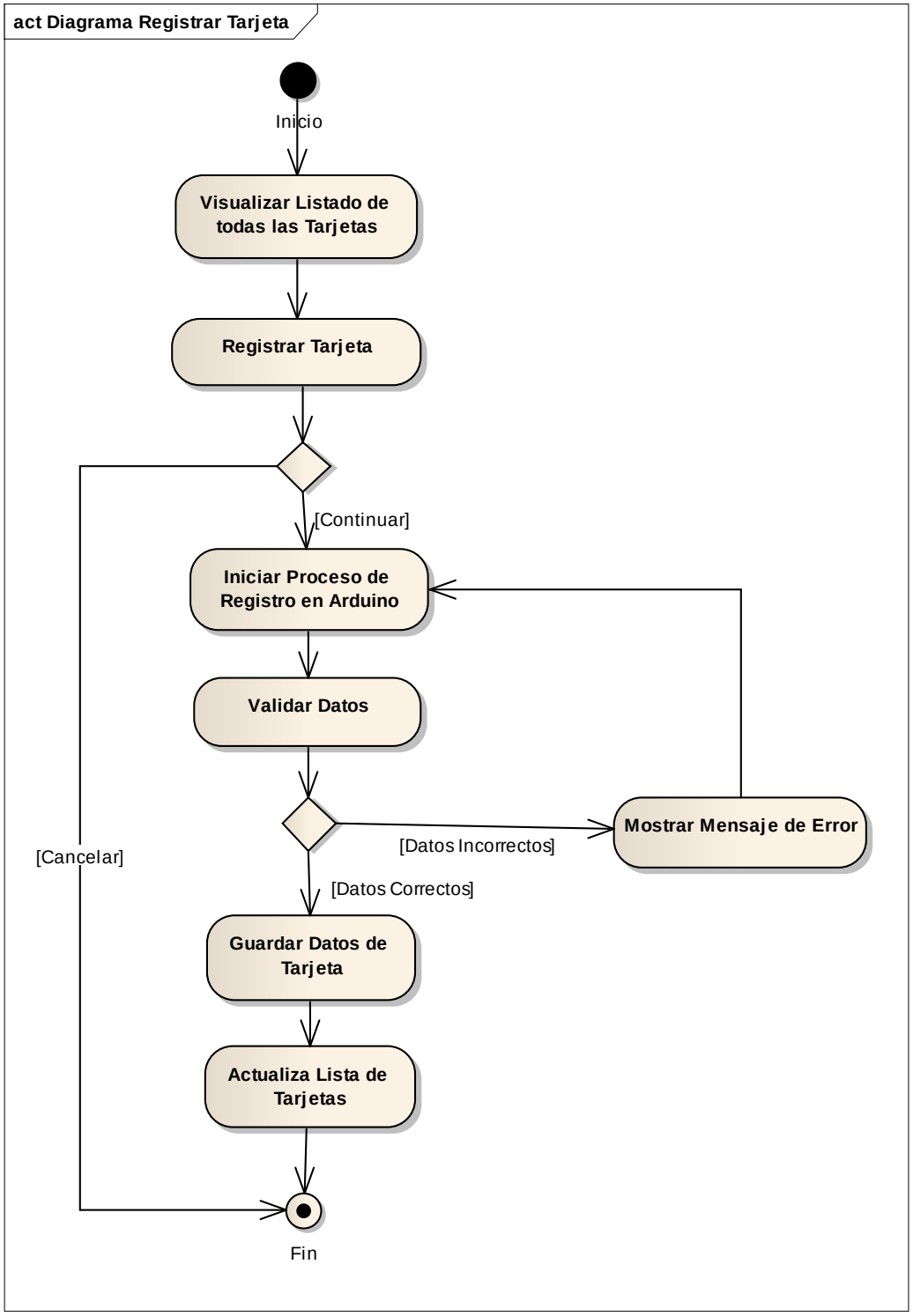


DIAGRAMA DE ACTIVIDADES: VER TARJETA

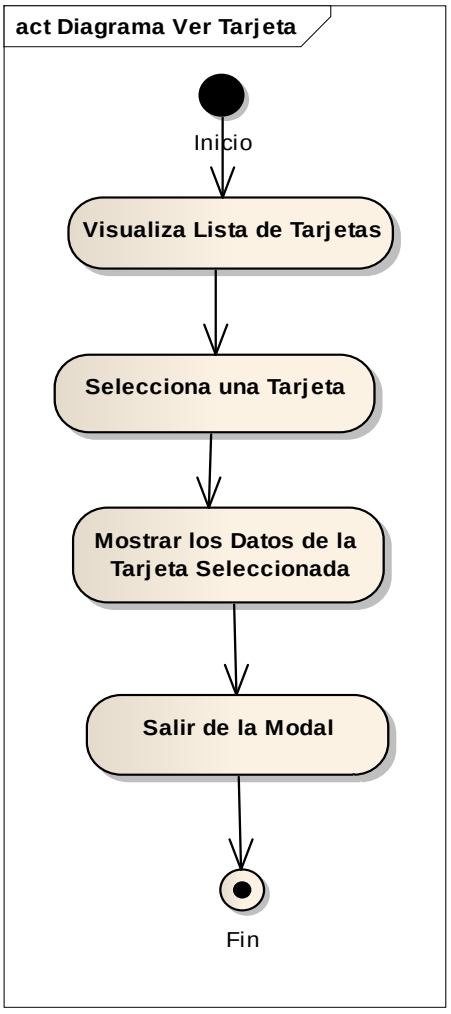


DIAGRAMA DE ACTIVIDADES: BLOQUEAR TARJETA

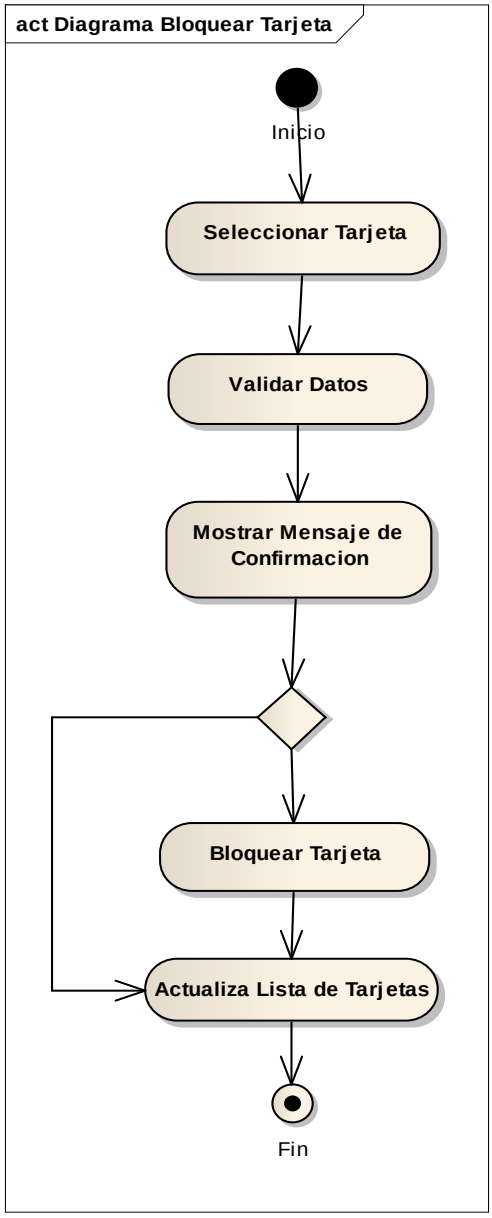


DIAGRAMA DE ACTIVIDADES: REPORTE TARJETAS BLOQUEADAS

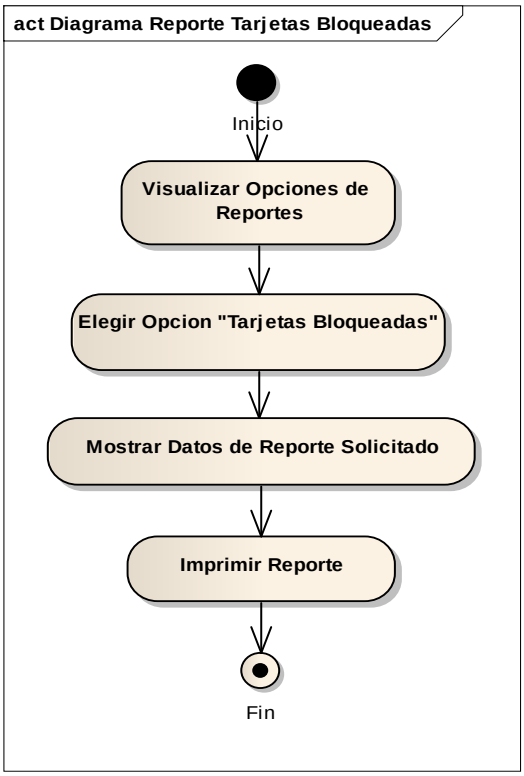


DIAGRAMA DE ACTIVIDADES: REPORTE USUARIOS ROLES

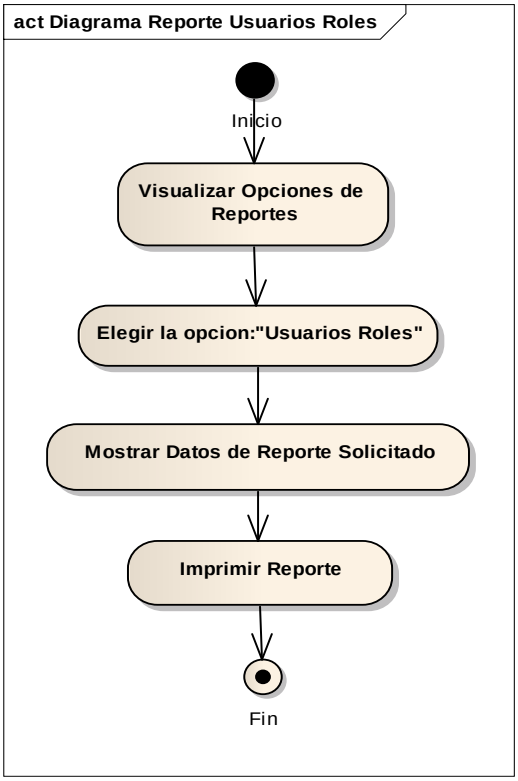


DIAGRAMA DE ACTIVIDADES: USUARIOS TARJETAS

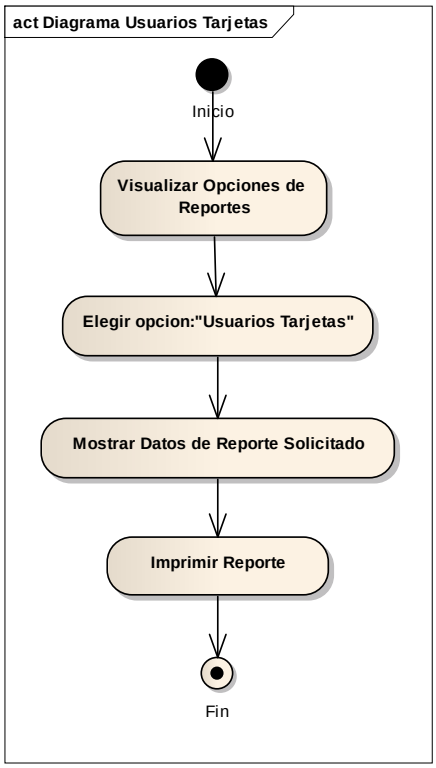


DIAGRAMA DE ACTIVIDADES: FLUJO DE ACCESOS

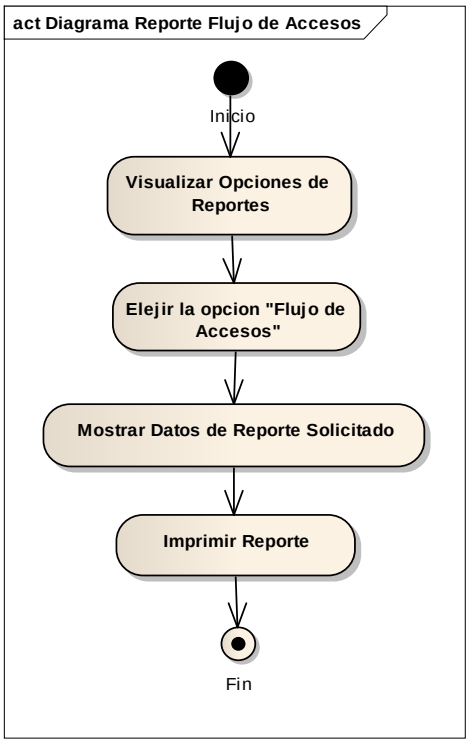


DIAGRAMA DE ACTIVIDADES: LEVANTAR APLICACIÓN MOSTRAR CODIGO

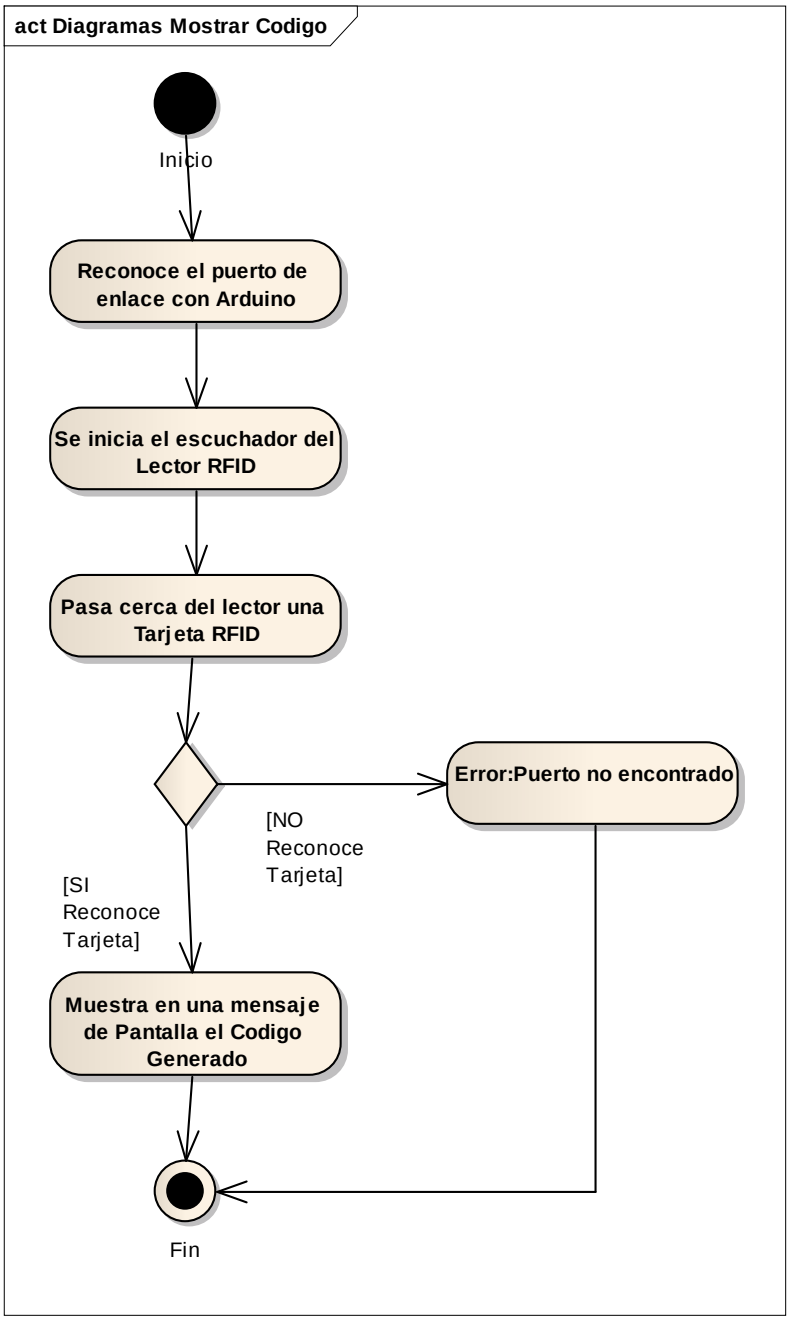
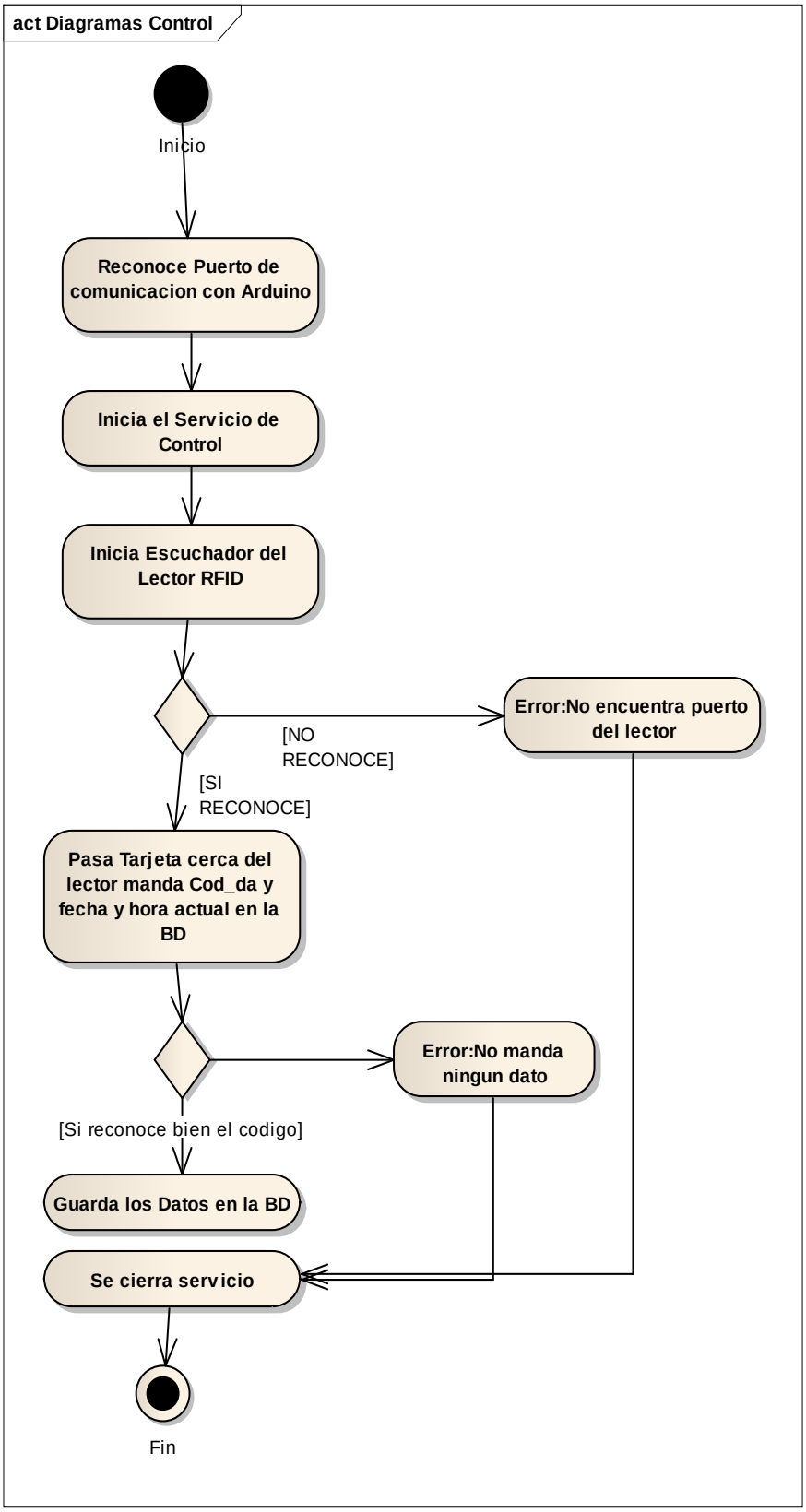


DIAGRAMA DE ACTIVIDADES: INICIAR SERVICIO DE CONTROL



10. DIAGRAMAS DE SECUENCIA

Diagrama de Secuencia: Iniciar Sesión

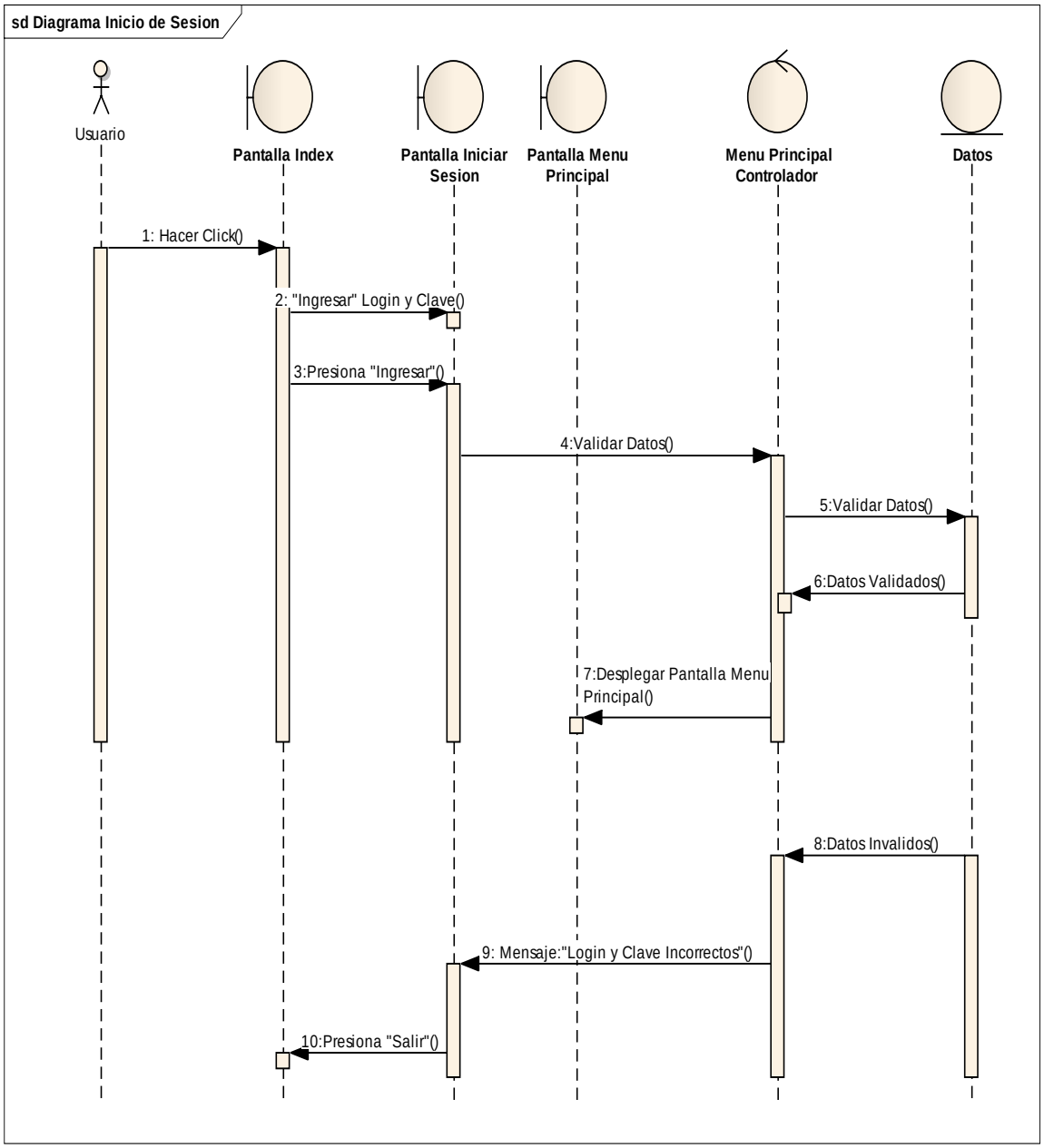


Diagrama de Secuencia: Gestión de Usuarios

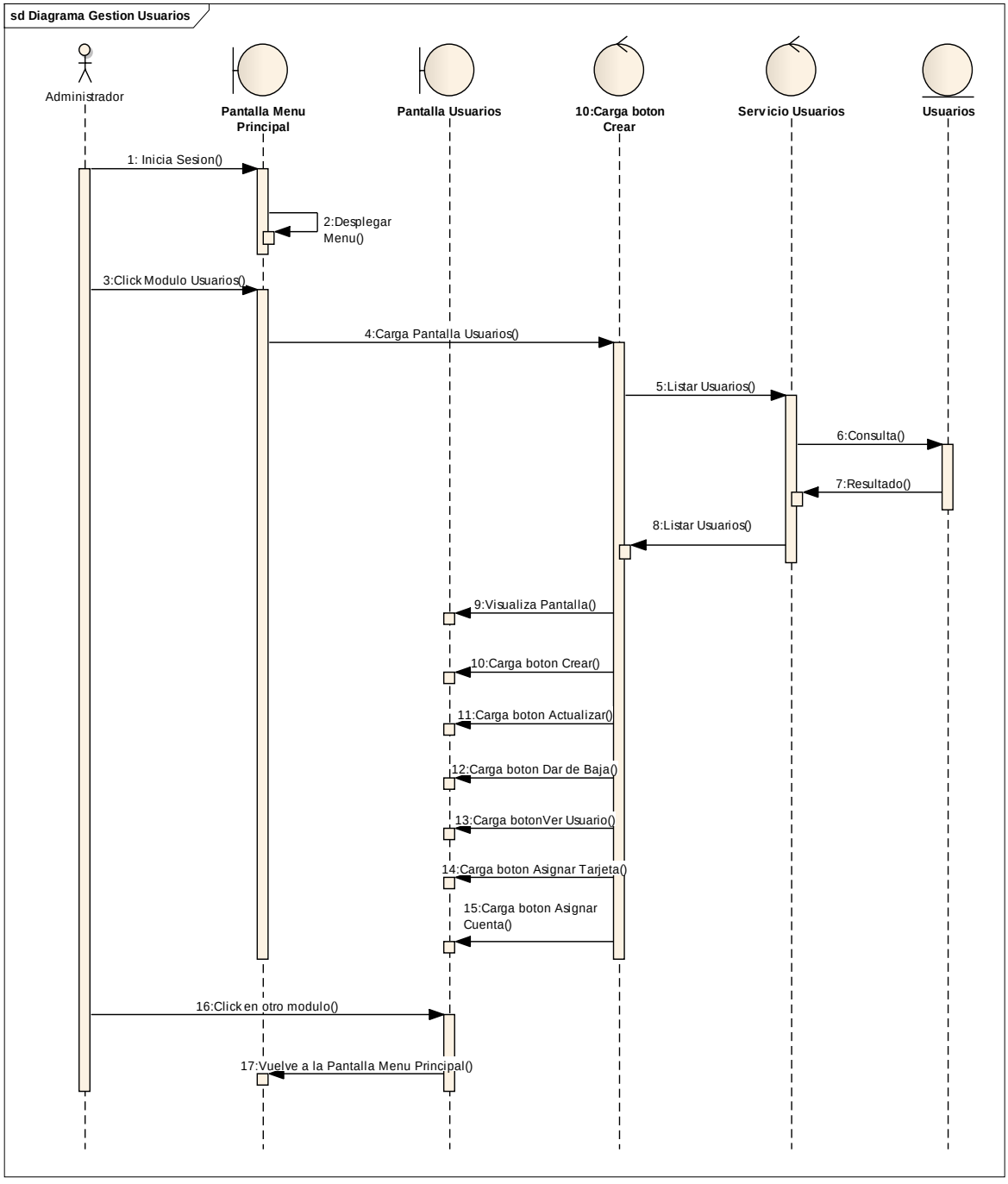


Diagrama de Secuencia: Crear Usuario

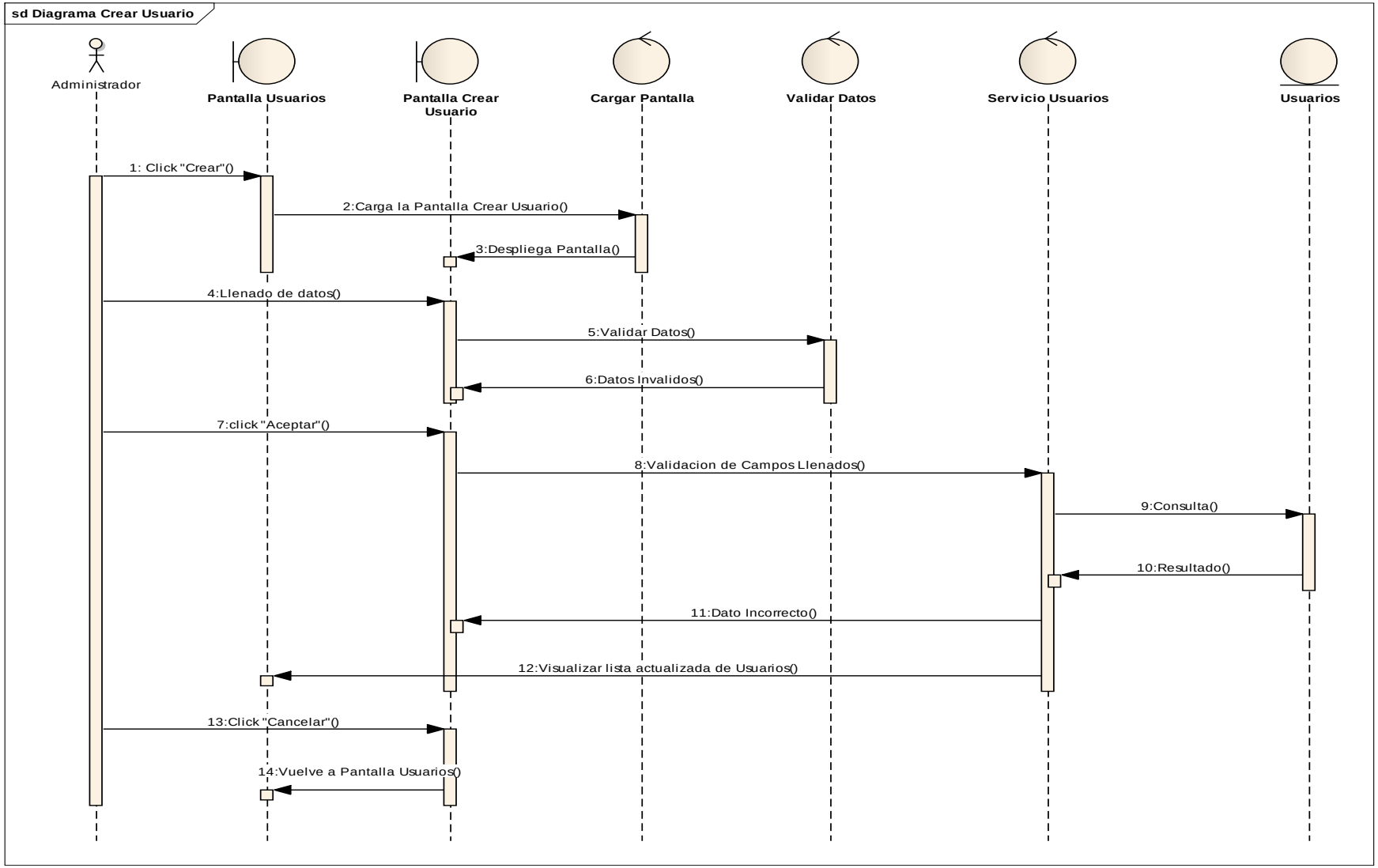


Diagrama de Secuencia: Actualizar Usuario

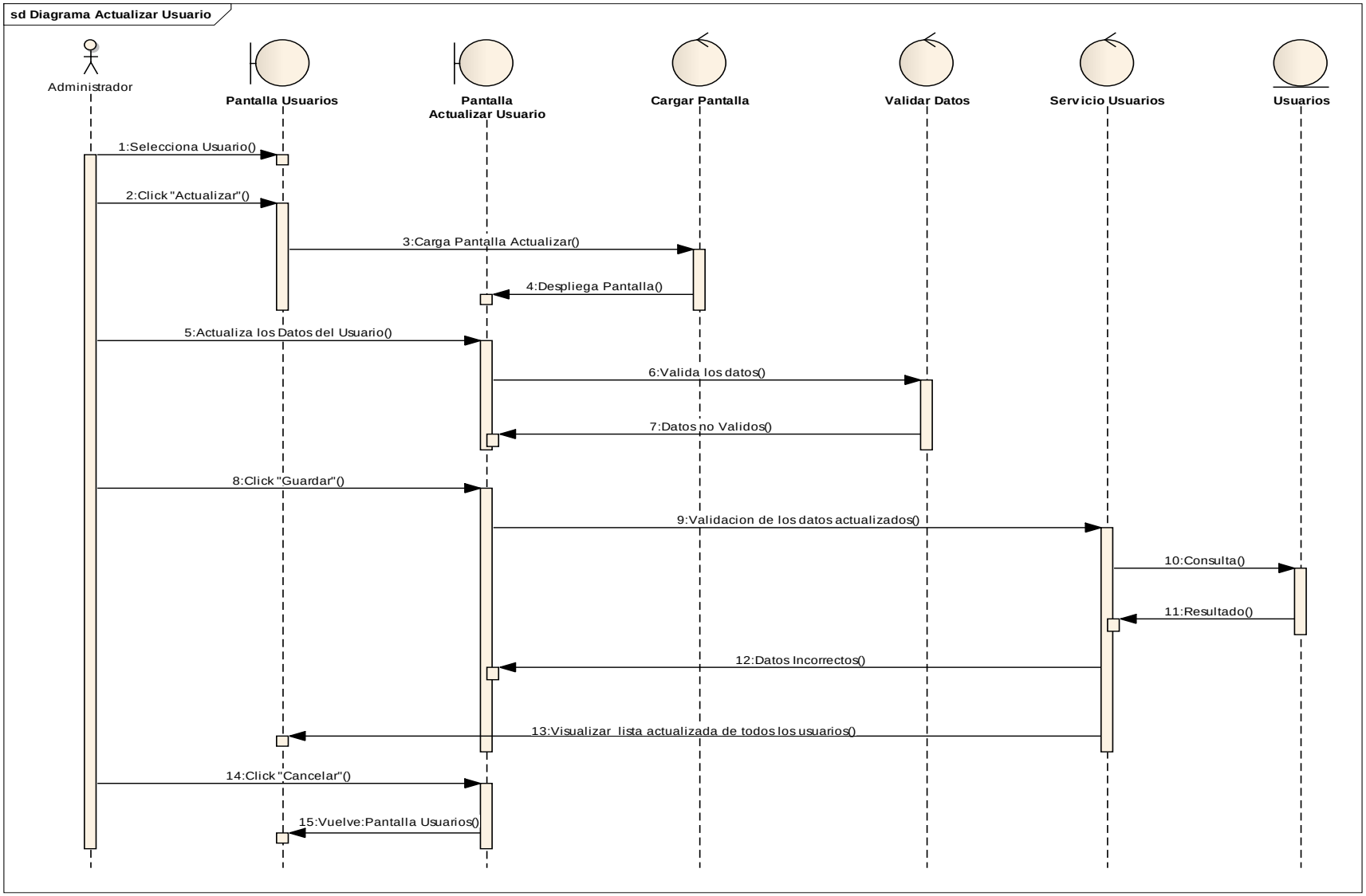


Diagrama de Secuencia: Dar de Baja Usuario

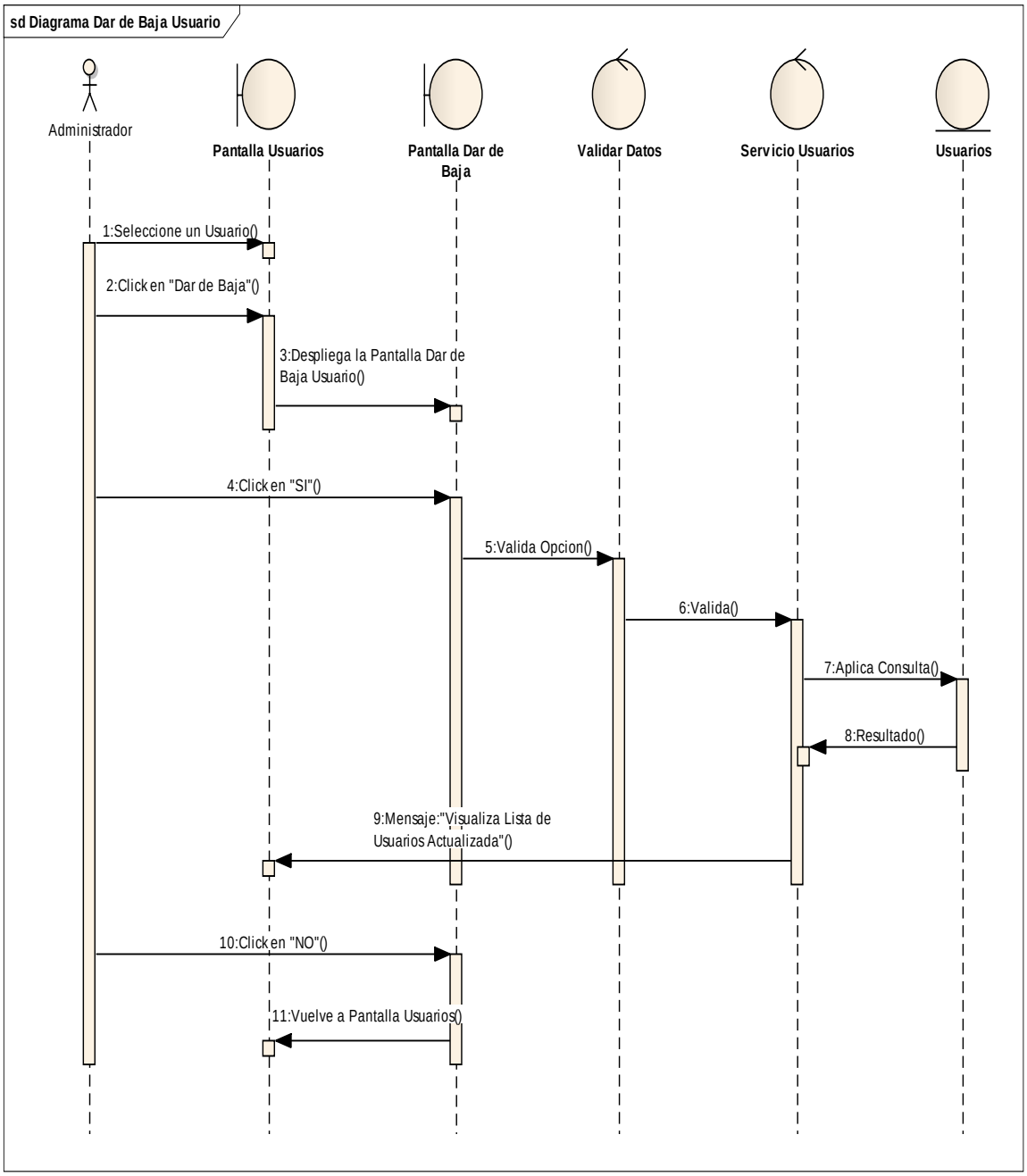


Diagrama de Secuencia: Ver Usuario

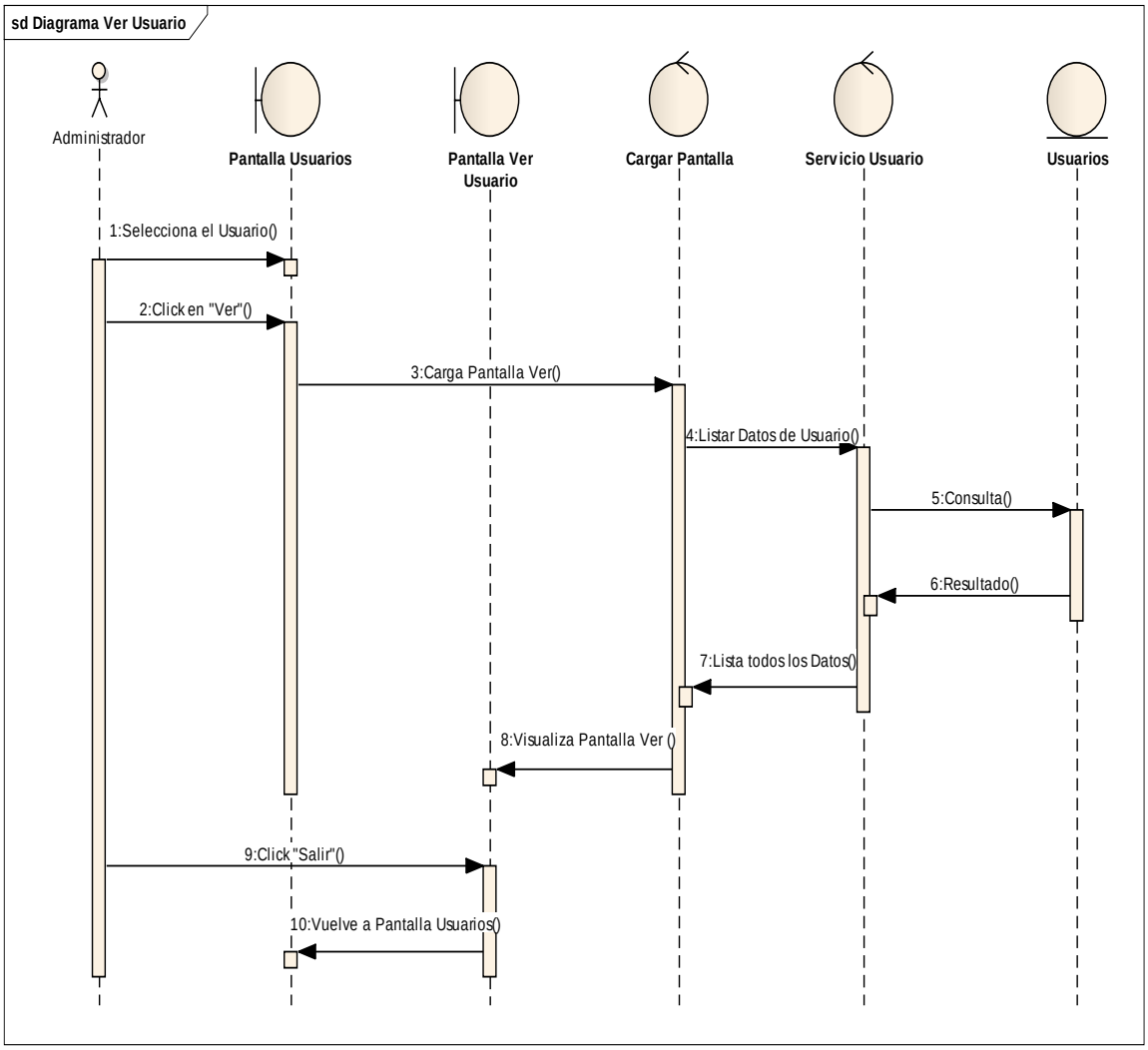


Diagrama de Secuencia: Asignar Cuenta

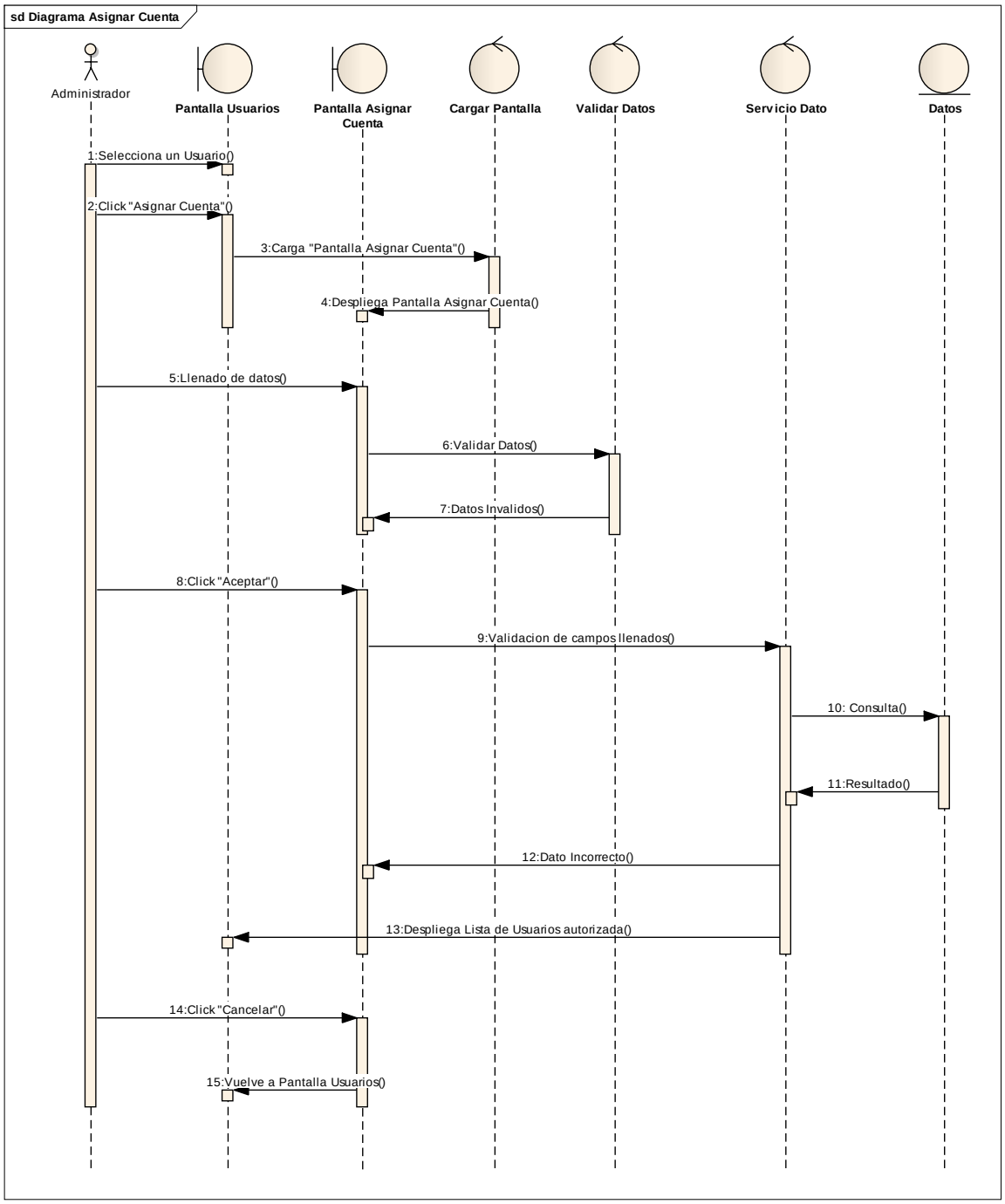


Diagrama de Secuencia: Modificar Cuenta

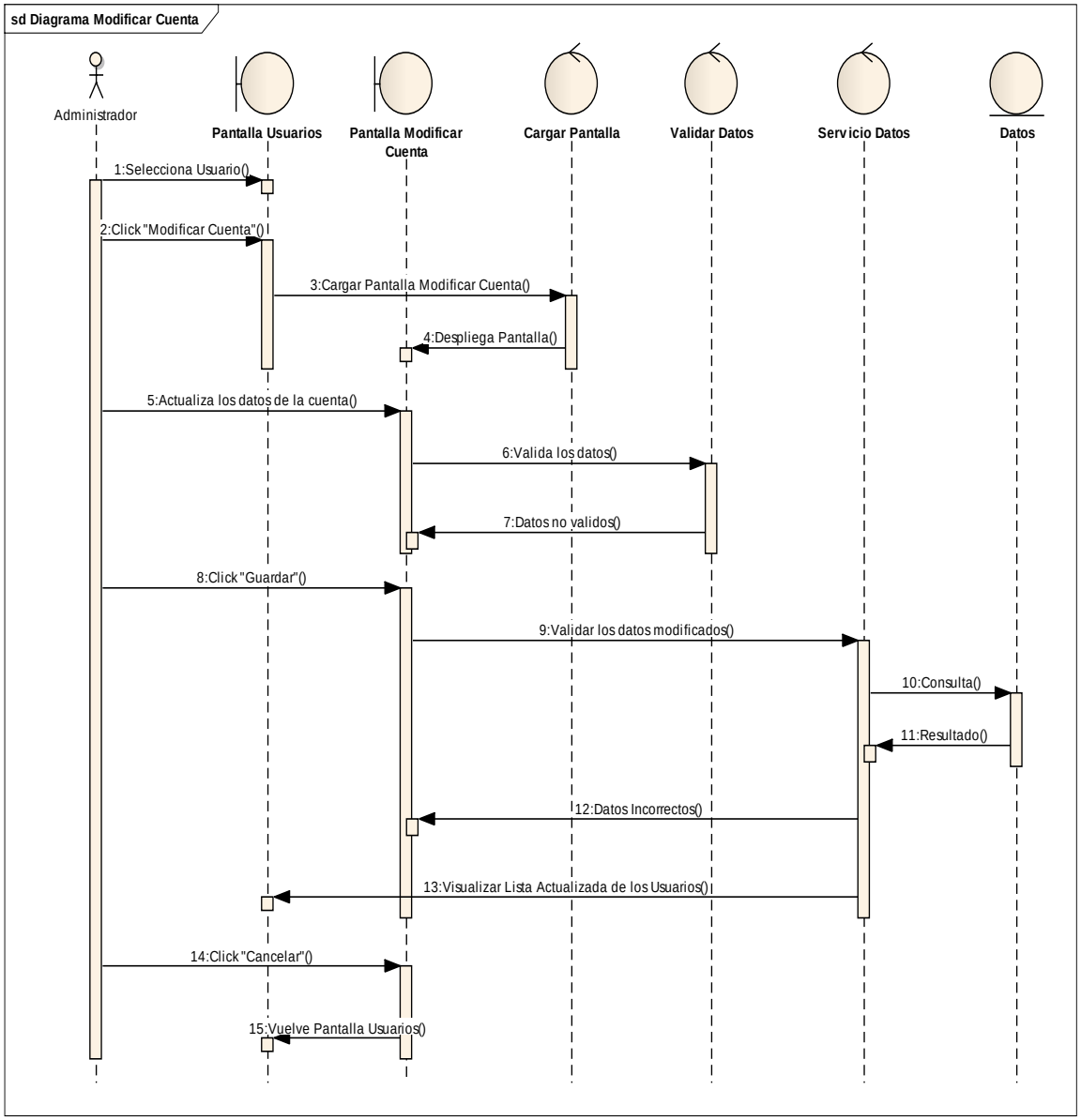


Diagrama de Secuencia: Asignar Rol

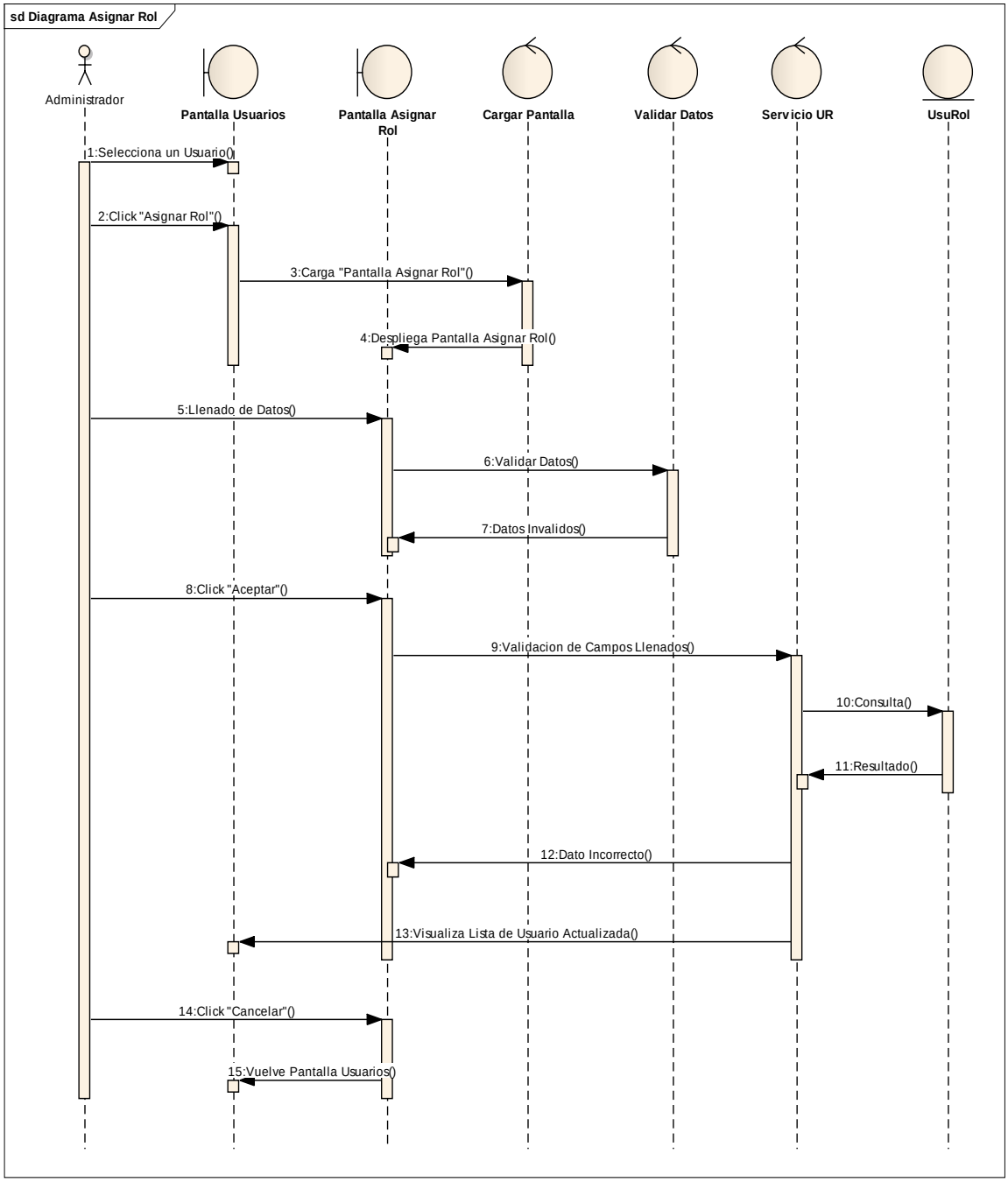


Diagrama de Secuencia: Gestión Roles

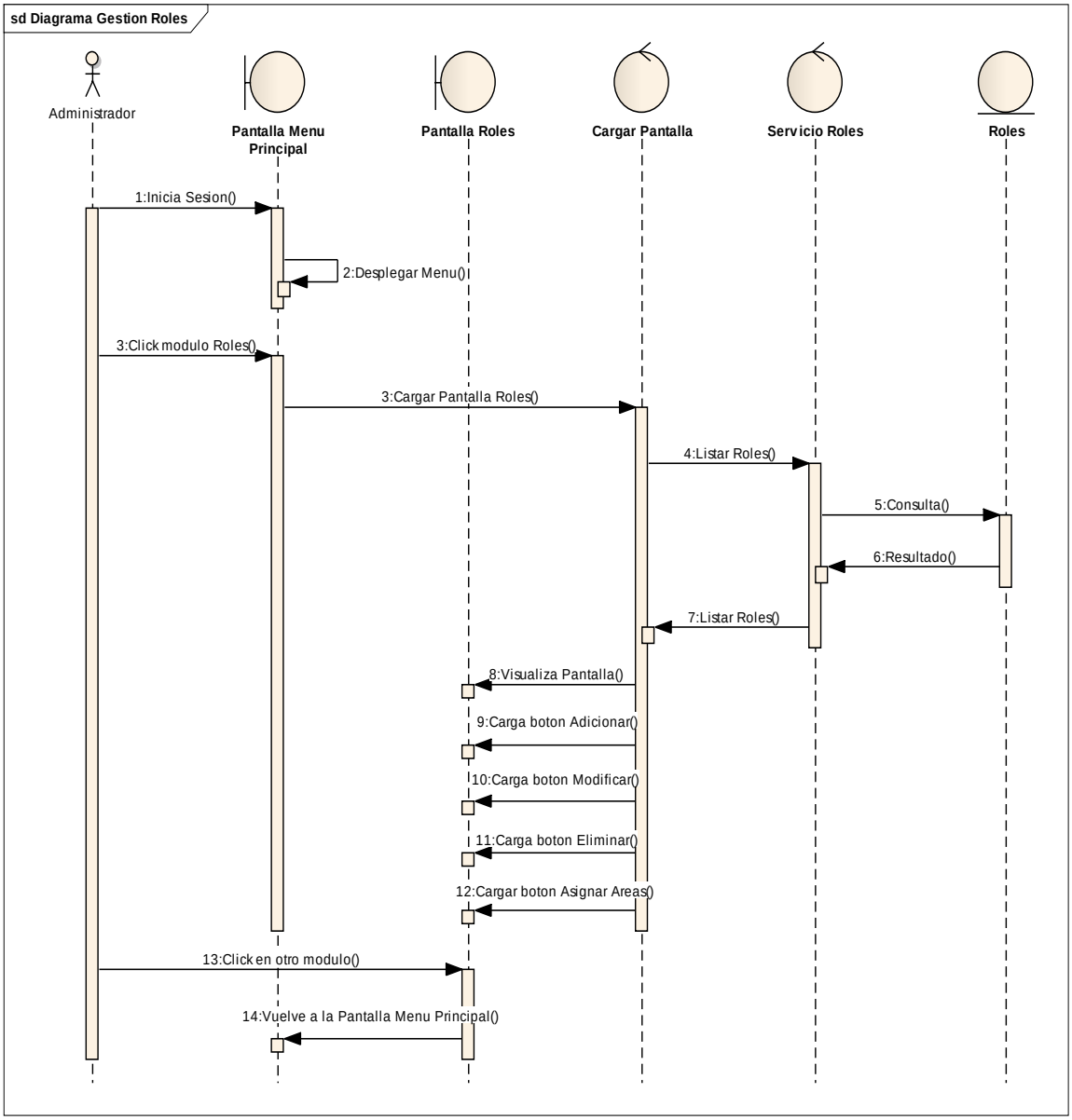


Diagrama de Secuencia: Adicionar Rol

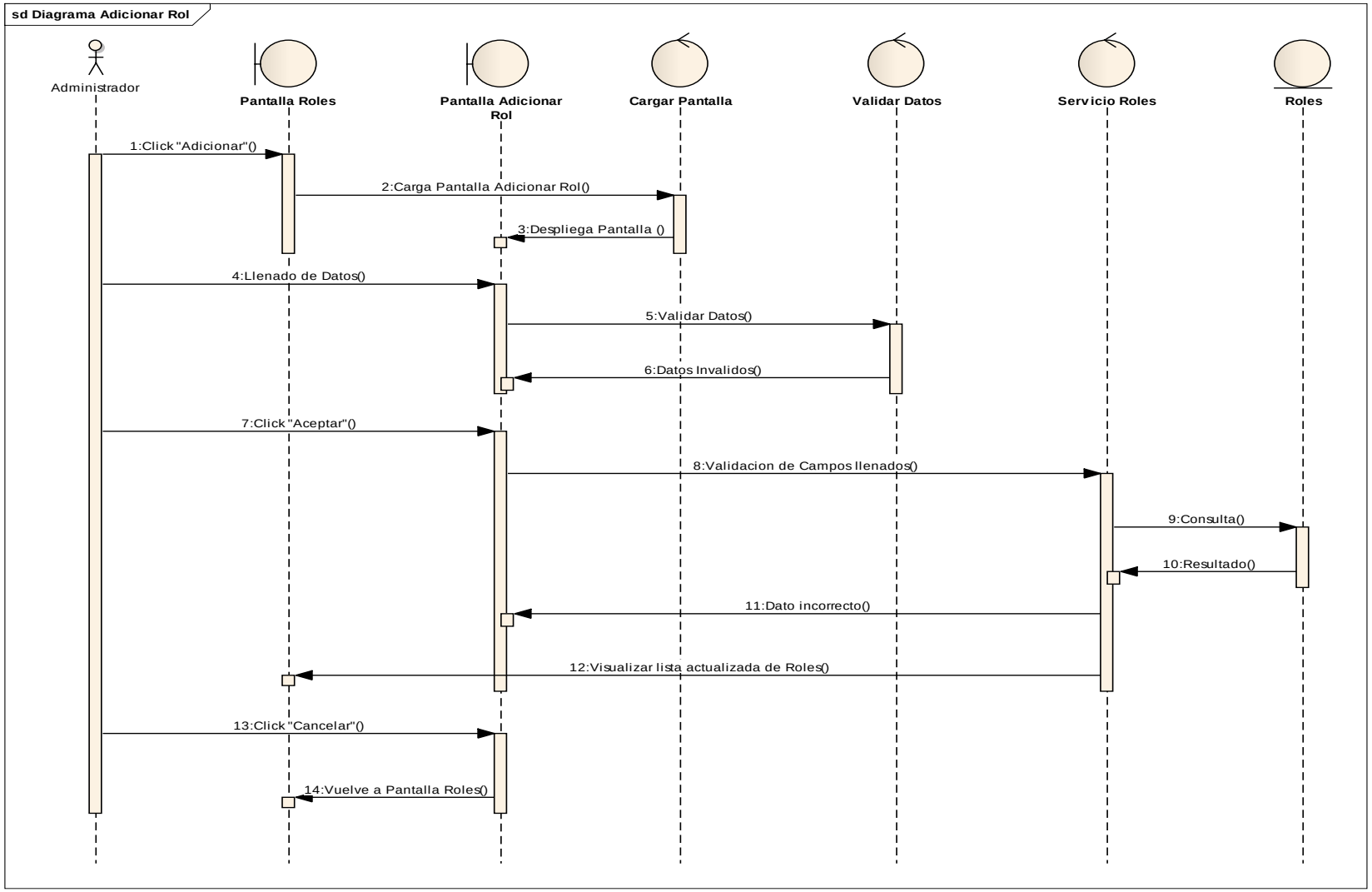


Diagrama de Secuencia: Modificar Rol

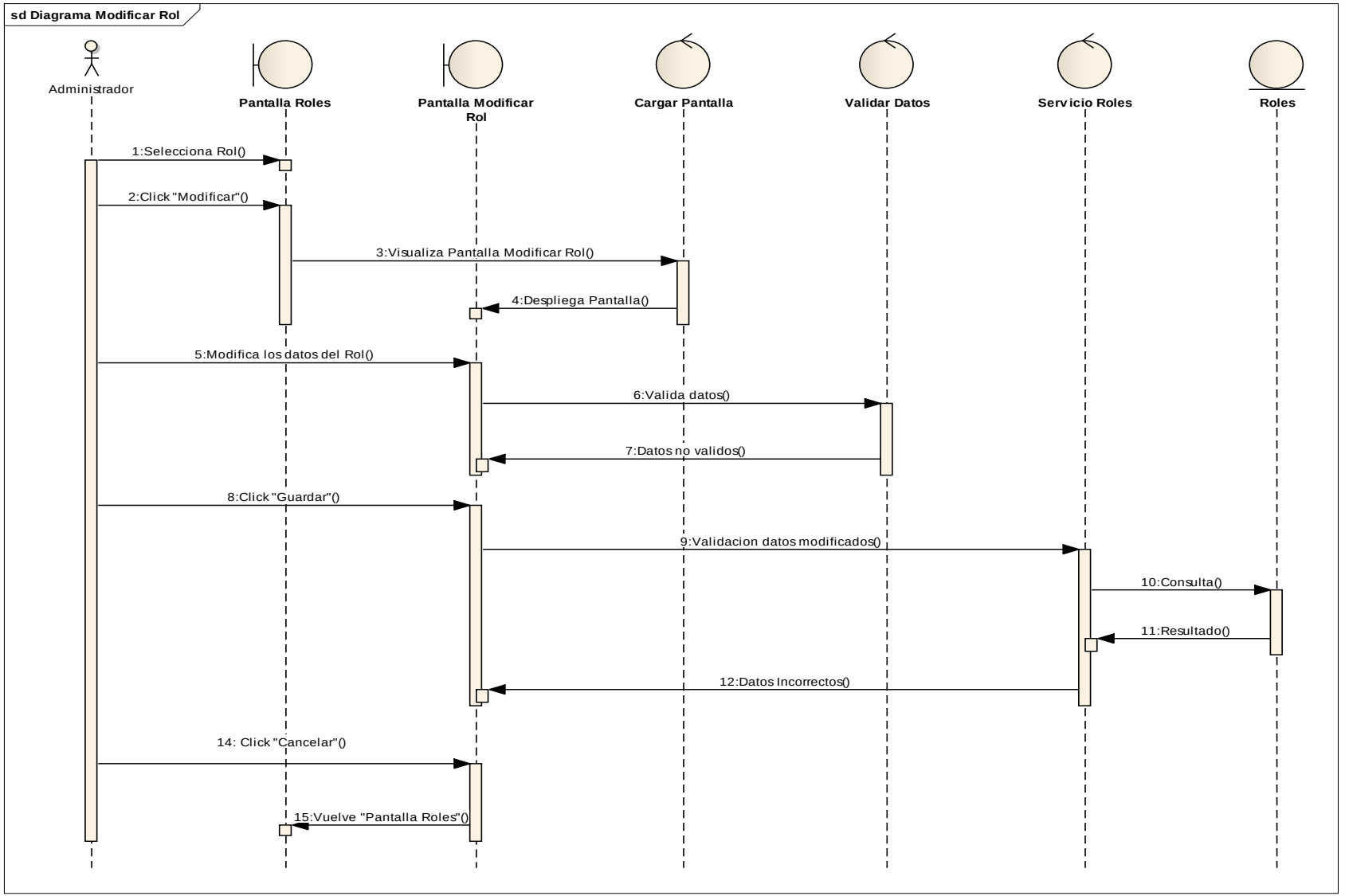


Diagrama de Secuencia: Eliminar Rol

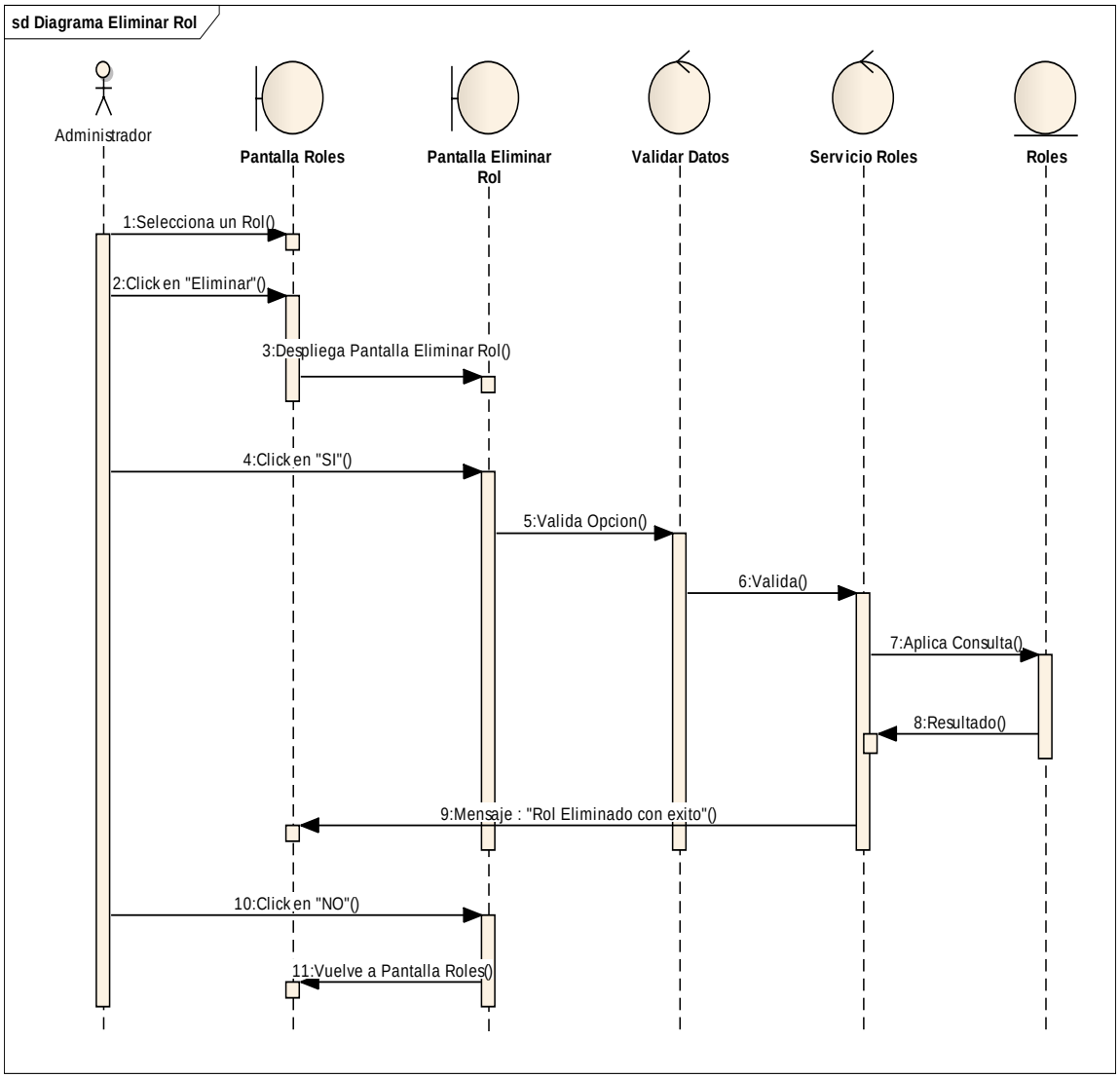


Diagrama de Secuencia: Asignar Área

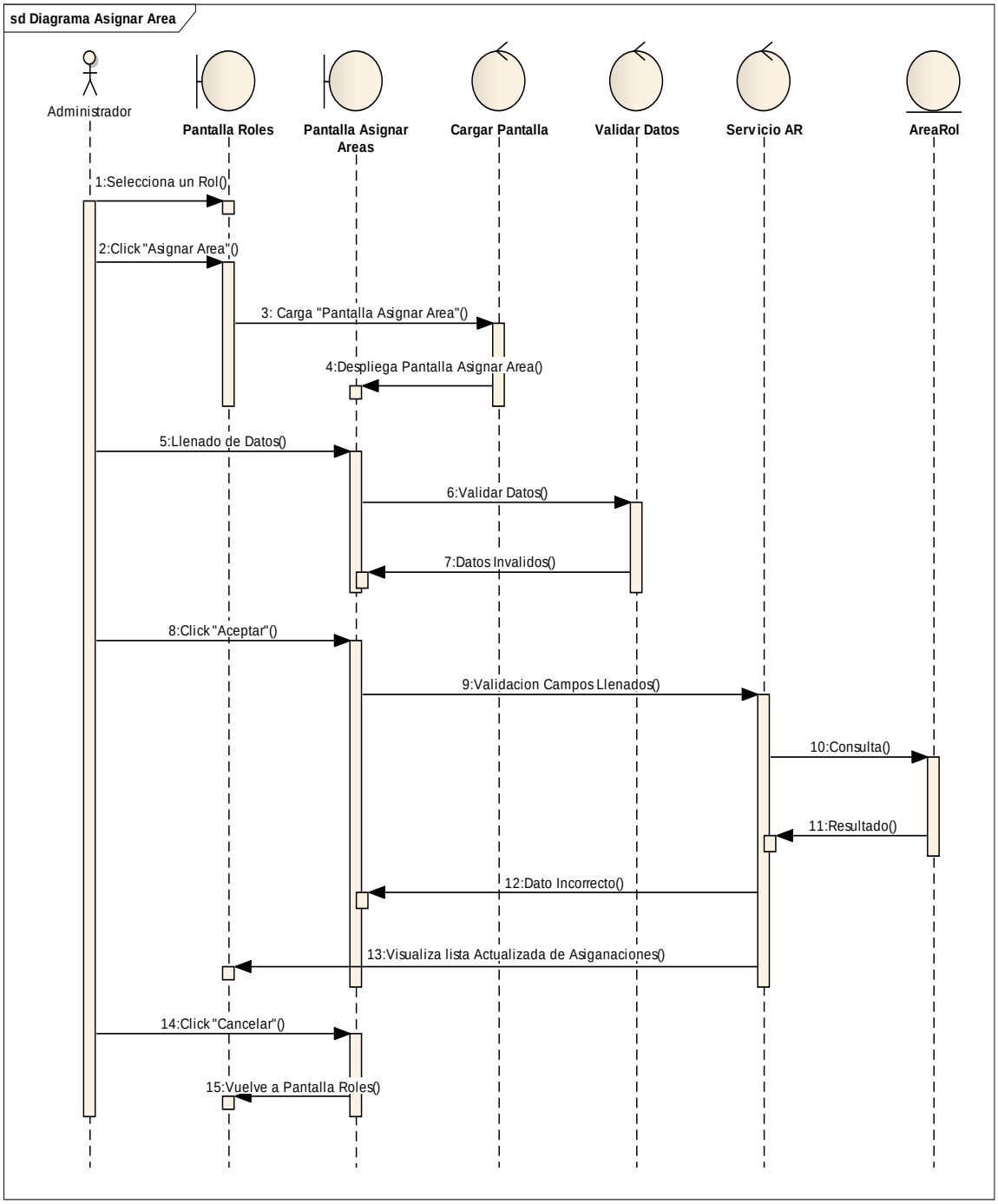


Diagrama de Secuencia: Gestión Áreas

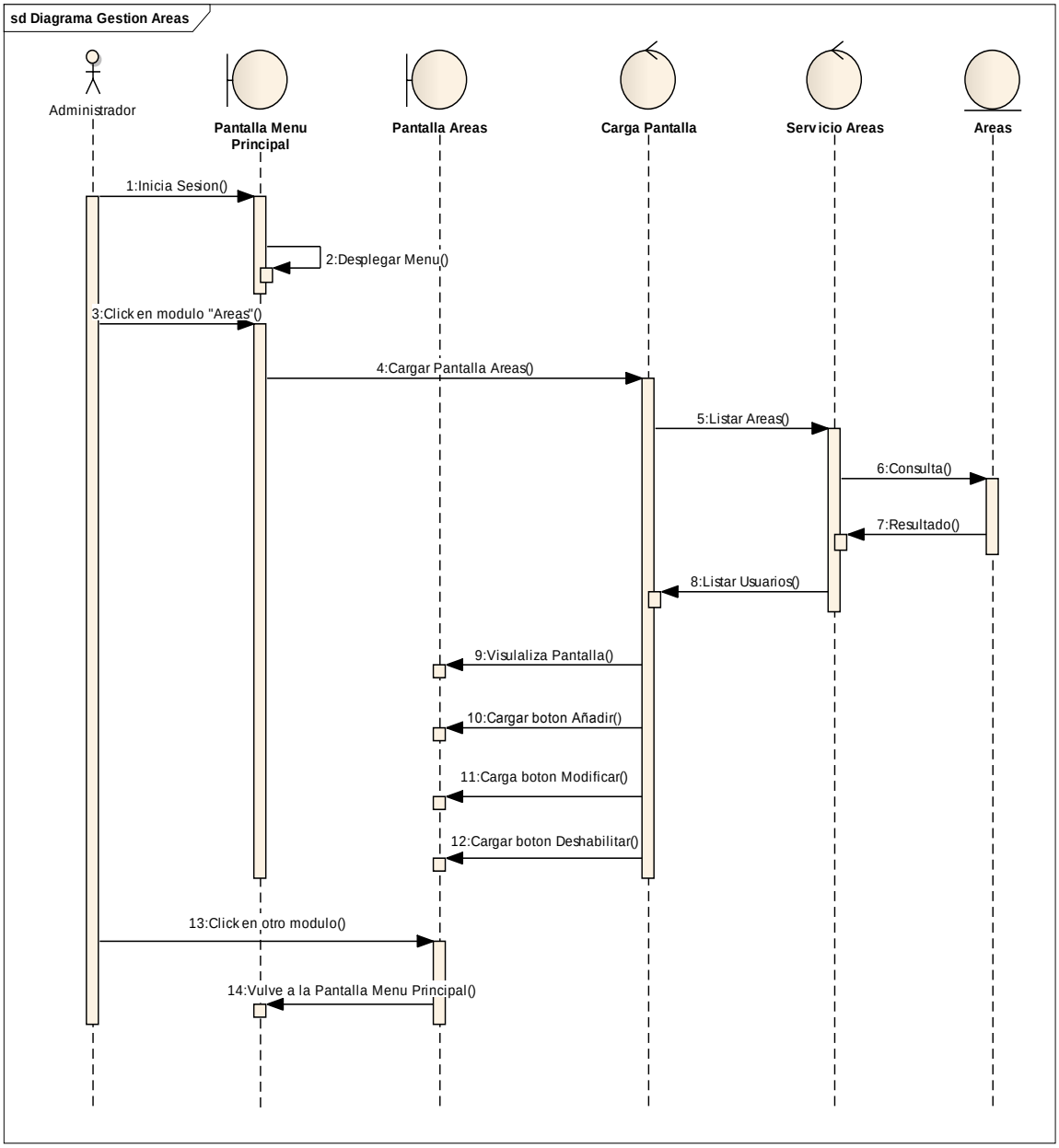


Diagrama de Secuencia: Añadir Área

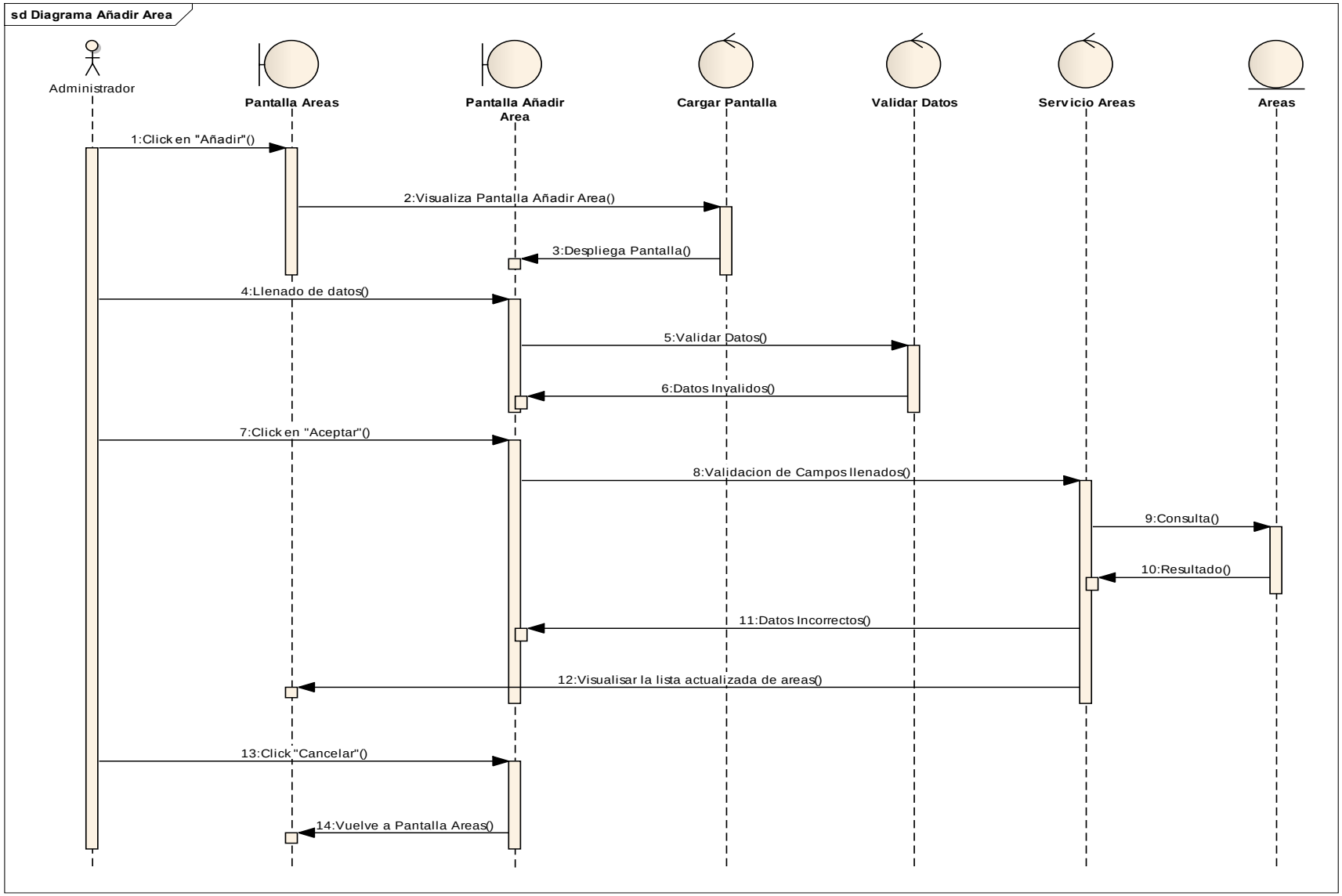


Diagrama de Secuencia: Modificar Área

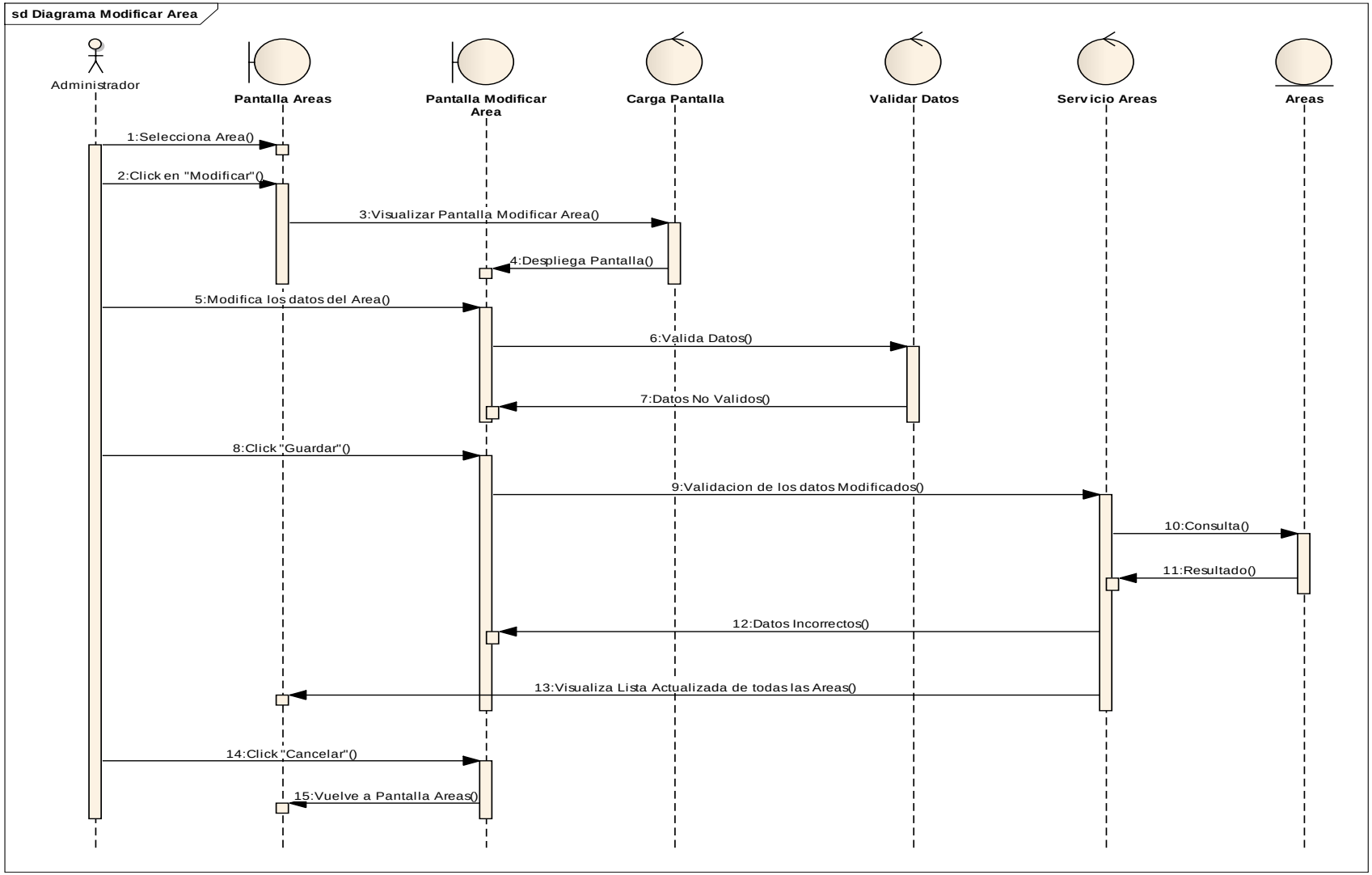


Diagrama de Secuencia: Deshabilitar Área

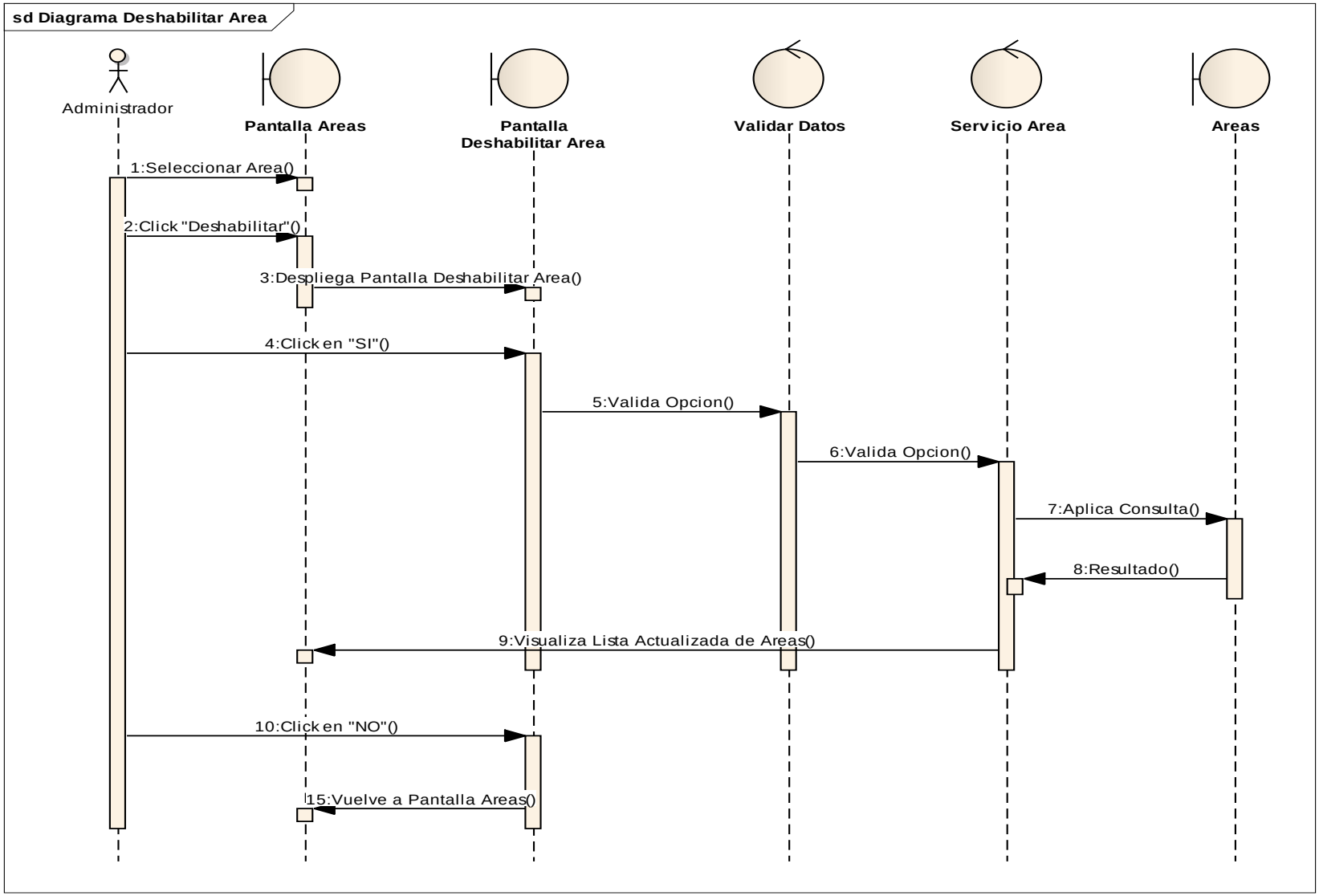


Diagrama de Secuencia: Gestión Tarjetas

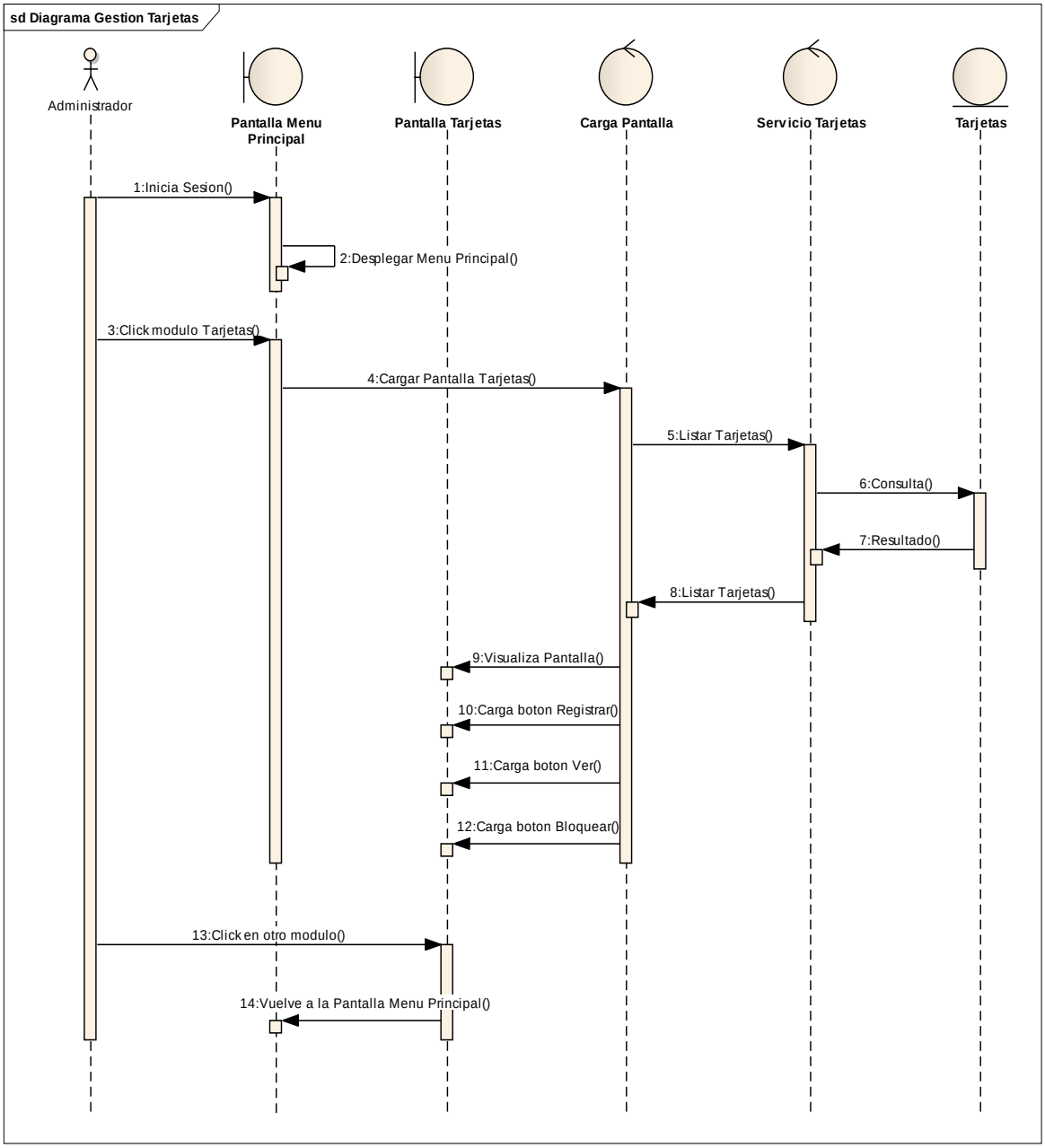


Diagrama de Secuencia: Registrar Tarjeta

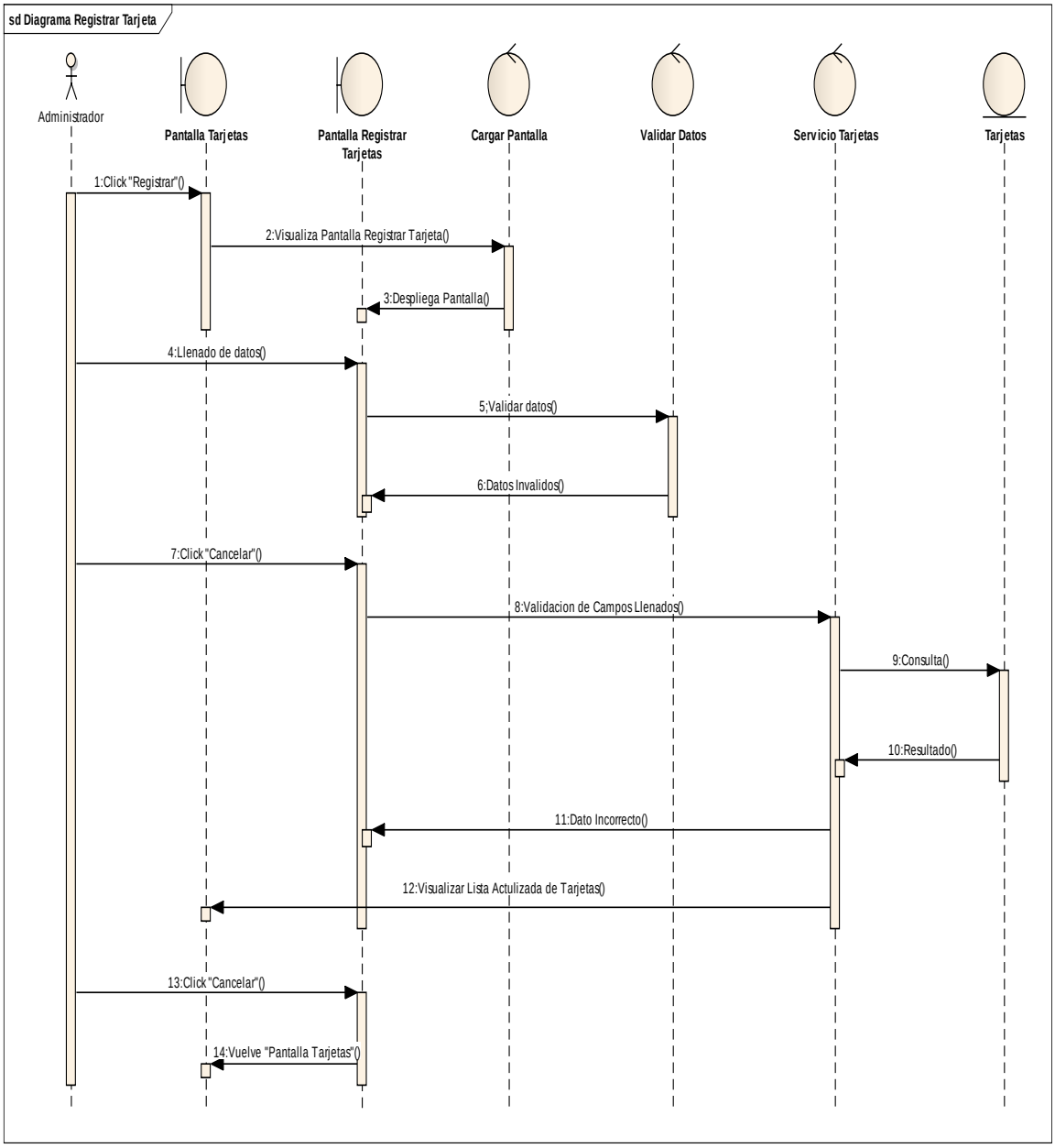


Diagrama de Secuencia: Ver Tarjeta

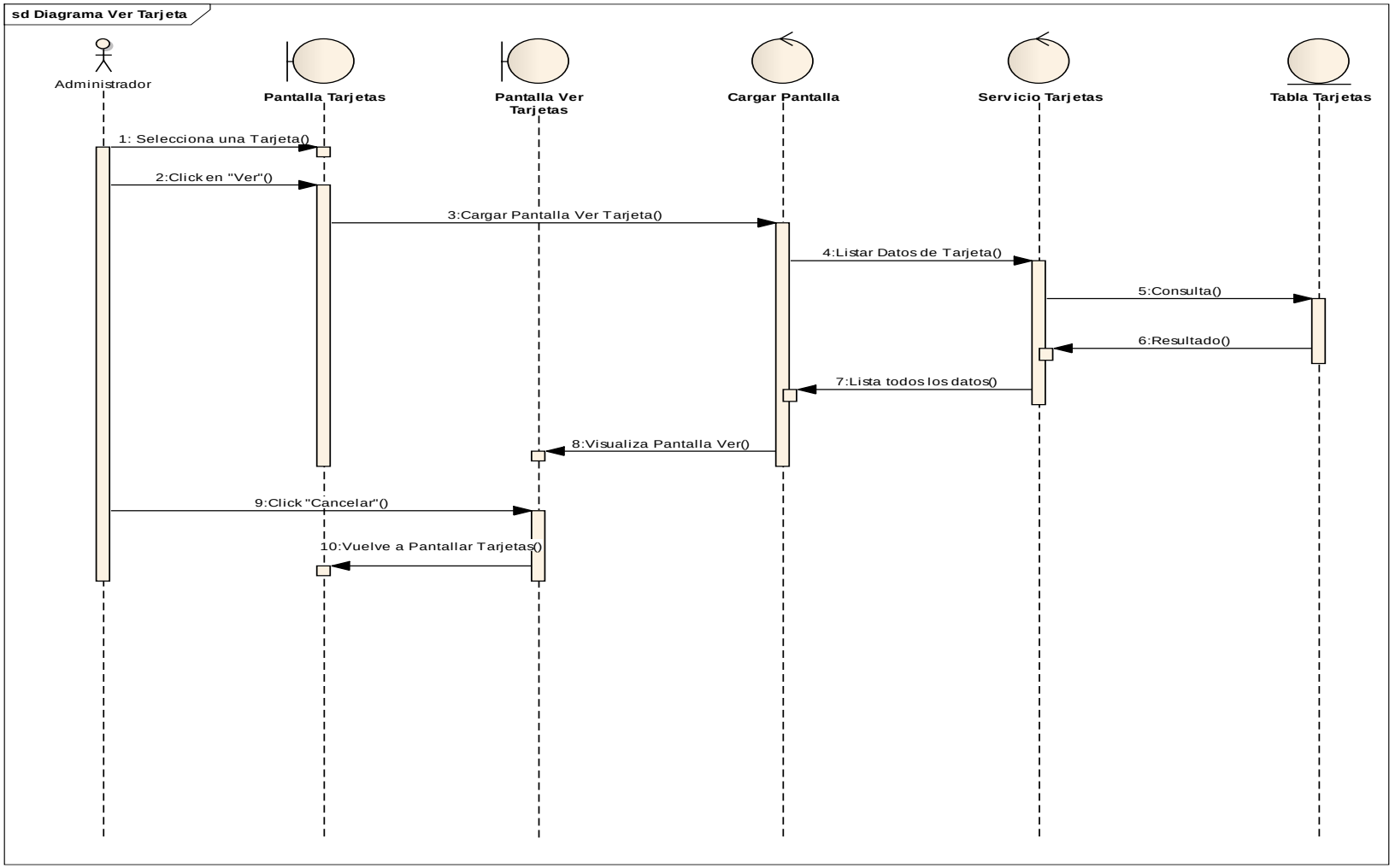


Diagrama de Secuencia: Bloquear Tarjeta

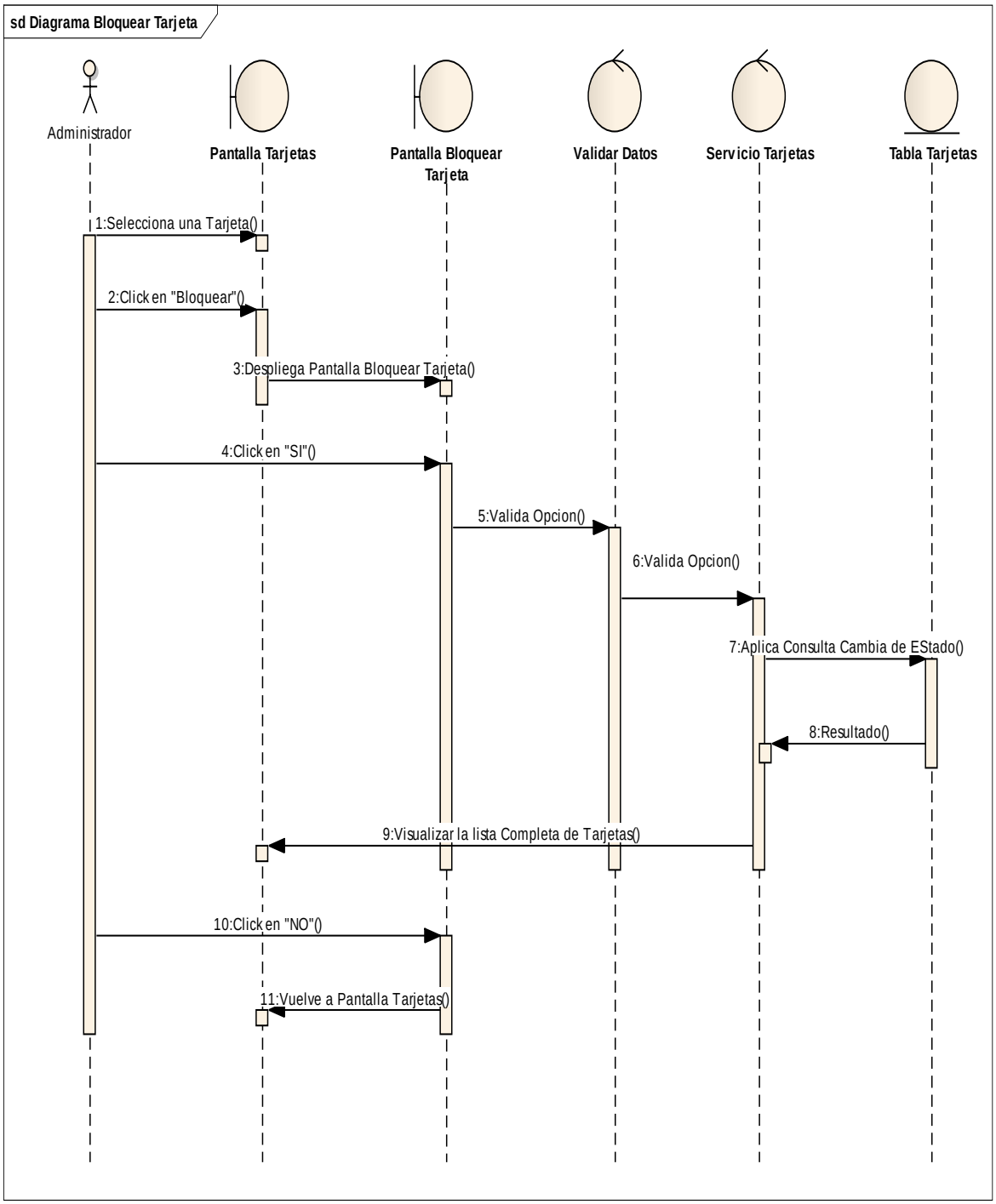


Diagrama de Secuencia: Gestión Reportes

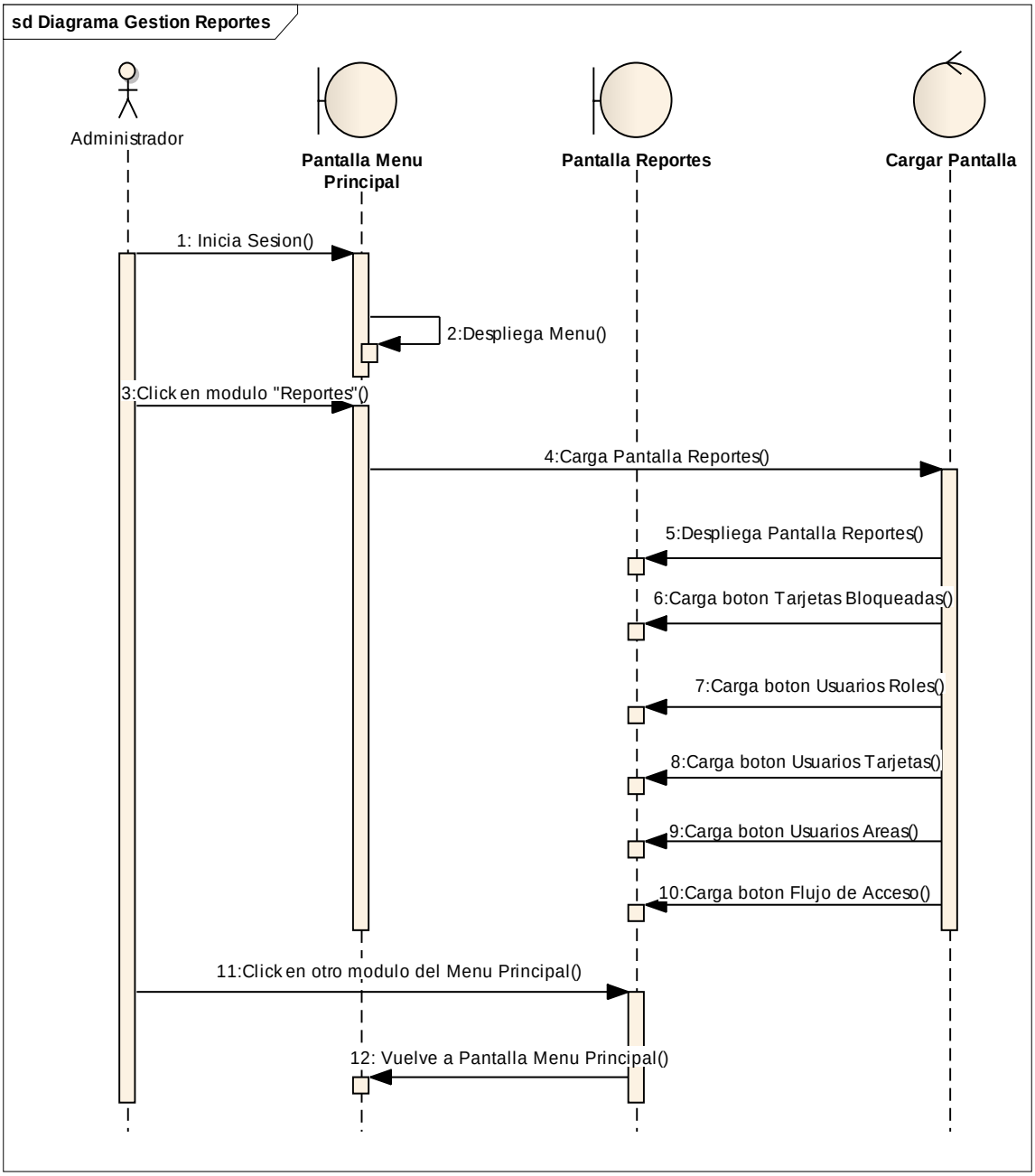


Diagrama de Secuencia: Reporte Tarjetas Bloqueadas

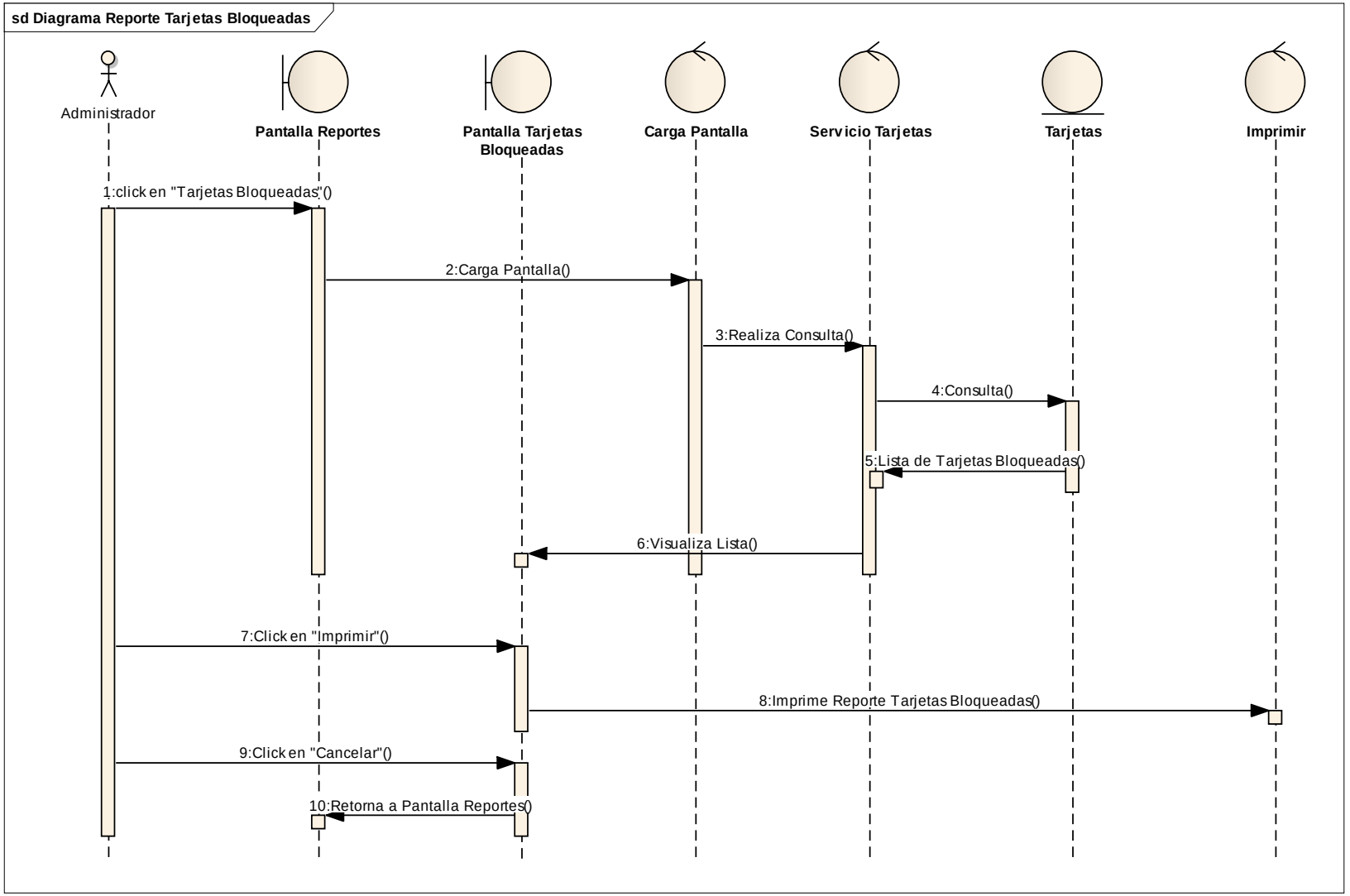


Diagrama de Secuencia: Reporte Usuarios Roles

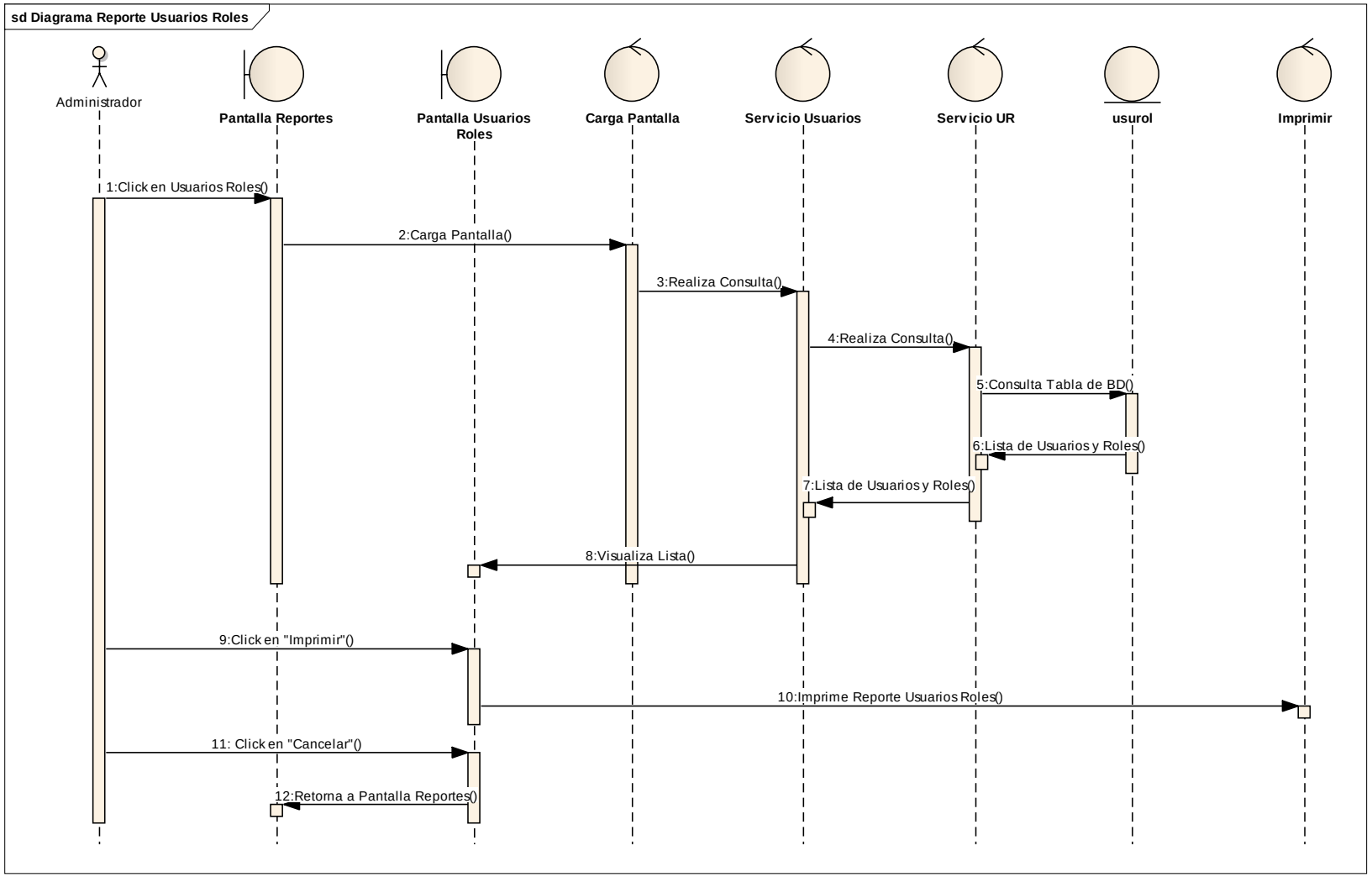


Diagrama de Secuencia: Reporte Usuarios Tarjetas

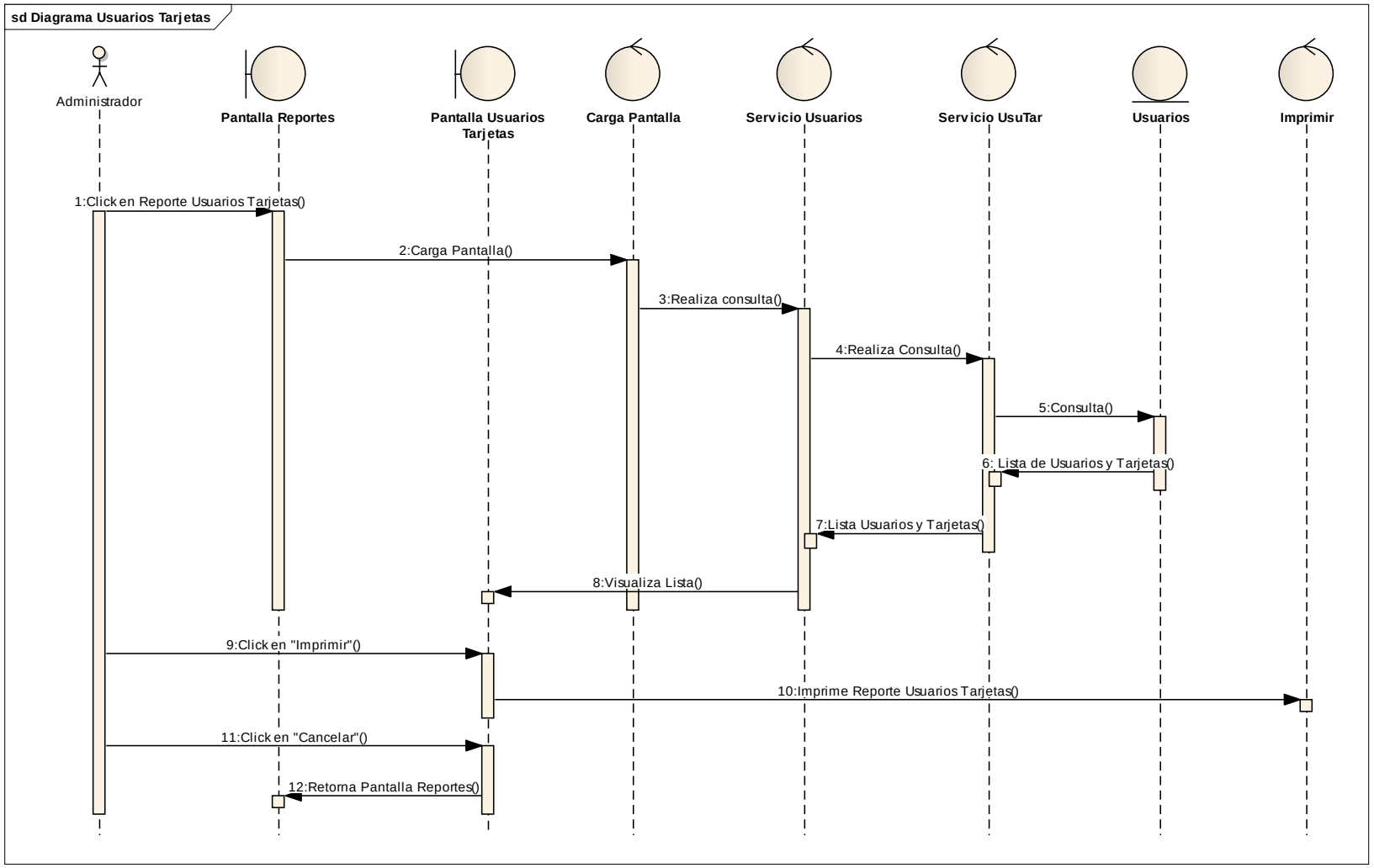


Diagrama de Secuencia: Reporte Usuarios Áreas

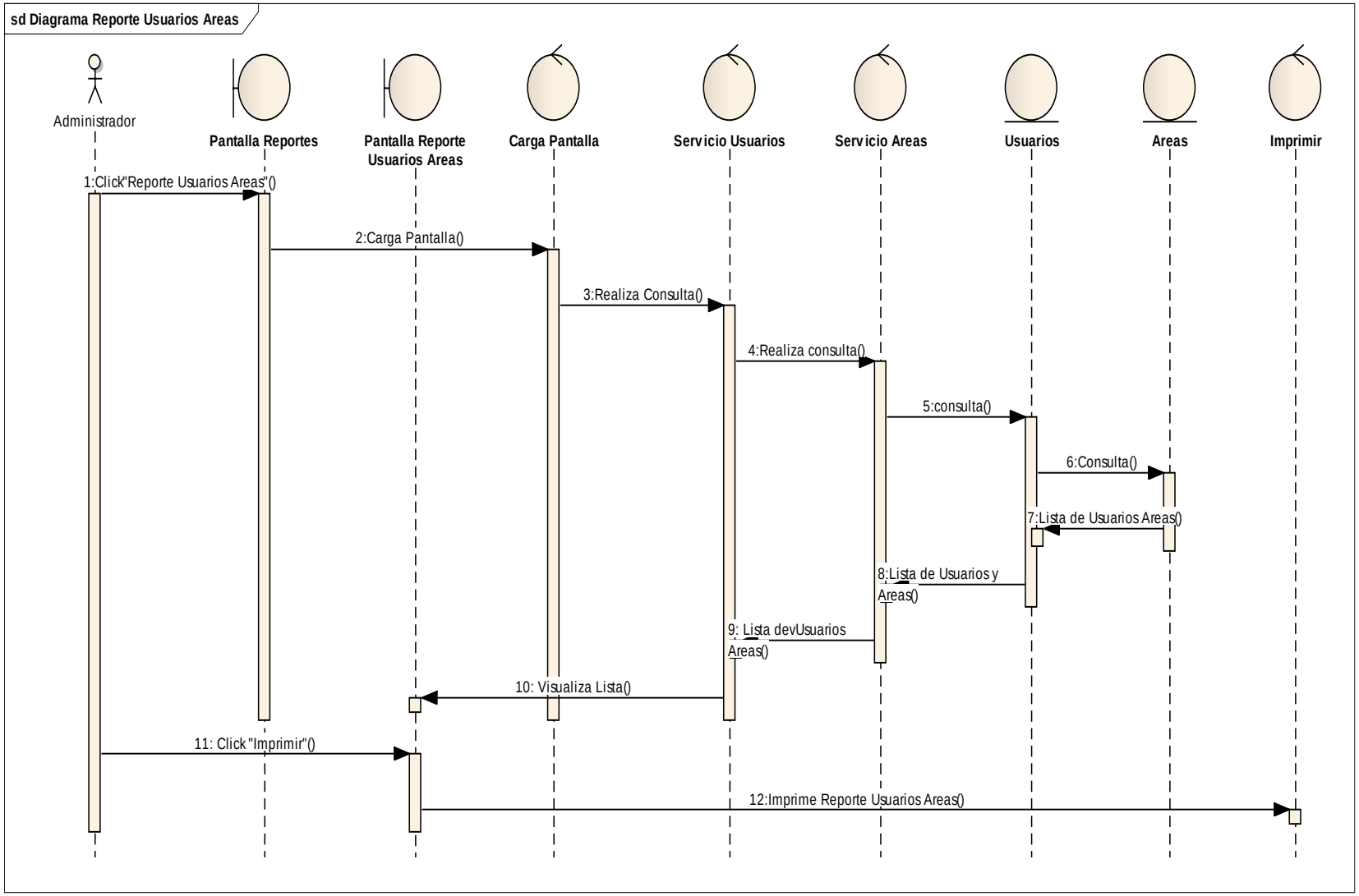
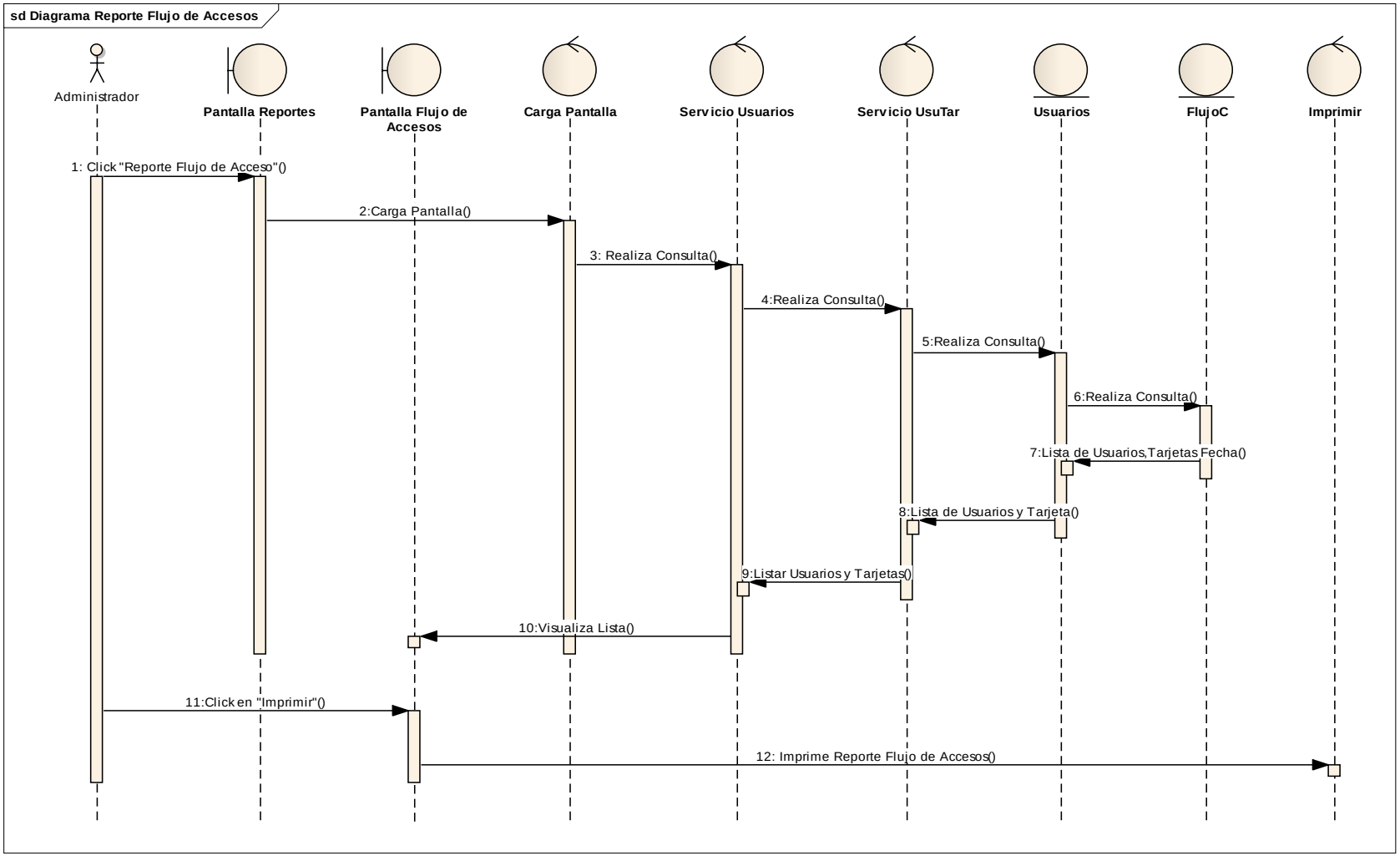


Diagrama de Secuencia: Reporte Flujo de Accesos



11. IDENTIFICACION DE CLASES CANDIDATAS

DESCRIPCION DEL PROBLEMA. -

El Sistema automatizado en web que se desarrollará; permitirá realizar el control de acceso del Personal a áreas restringidas de la infraestructura de una Organización de forma automatizada, lo cual conllevará al registro en el mismo de todo el personal de la Organización.

Gracias al registro de todo el personal que se hará, se le podrá asignar a cada funcionario una tarjeta de acceso previamente registrada en el Sistema con la que podrá acceder a las áreas permitidas según los roles que cumplan en la Organización.

El Sistema contará con una pantalla de Bienvenida donde se encontrará el logo de la Organización que utilizará el Sistema, por medio de una interfaz pasará a una pantalla de Inicio donde el usuario podrá loguearse, ingresando su login (nombre de usuario) y clave; al validar el Sistema estos datos, ingresará a un menú principal donde se encontrarán los módulos autorizados por el Sistema según el rol del usuario.

El menú principal contará con las siguientes opciones:

- Usuarios: En este módulo se podrá realizar diferentes consultas sobre los usuarios; en caso de un Administrador, éste podrá crear, actualizar, dar de baja a algún usuario y realizar otros procesos a los cuales tendrá acceso por medio de este módulo.
- Roles: En este módulo se podrá realizar consultas sobre los roles existente en la Organización, el Administrador podrá adicionar roles, respectivamente modificarlo, eliminarlos si es el caso y en este Sistema, asignarles las áreas de acceso correspondientes a cada rol.
- Áreas: En este módulo se podrá realizar diferentes consultas sobre las áreas a registrar en el Sistema, el Administrador podrá añadir las áreas correspondientes a la infraestructura física; también podrá modificar los datos de las mismas y deshabilitarlas si fuese el caso.
- Tarjetas: En este módulo se podrá realizar consultas sobre las tarjetas registradas y habilitadas en el Sistema para poder ser asignadas al Personal; el Administrador

podrá realizar el registro, actualización y bloqueo en caso de pérdida o licencia de las tarjetas.

- Reportes: En este módulo se podrá crear reportes de todo el Sistema como cuántas tarjetas han sido extraviadas o bloqueadas, qué personal ha sido dado de baja y otros.

11.1 IDENTIFICACIÓN DE CLASES EN EL PROBLEMA PARA EL SISTEMA

Usuarios

Datos

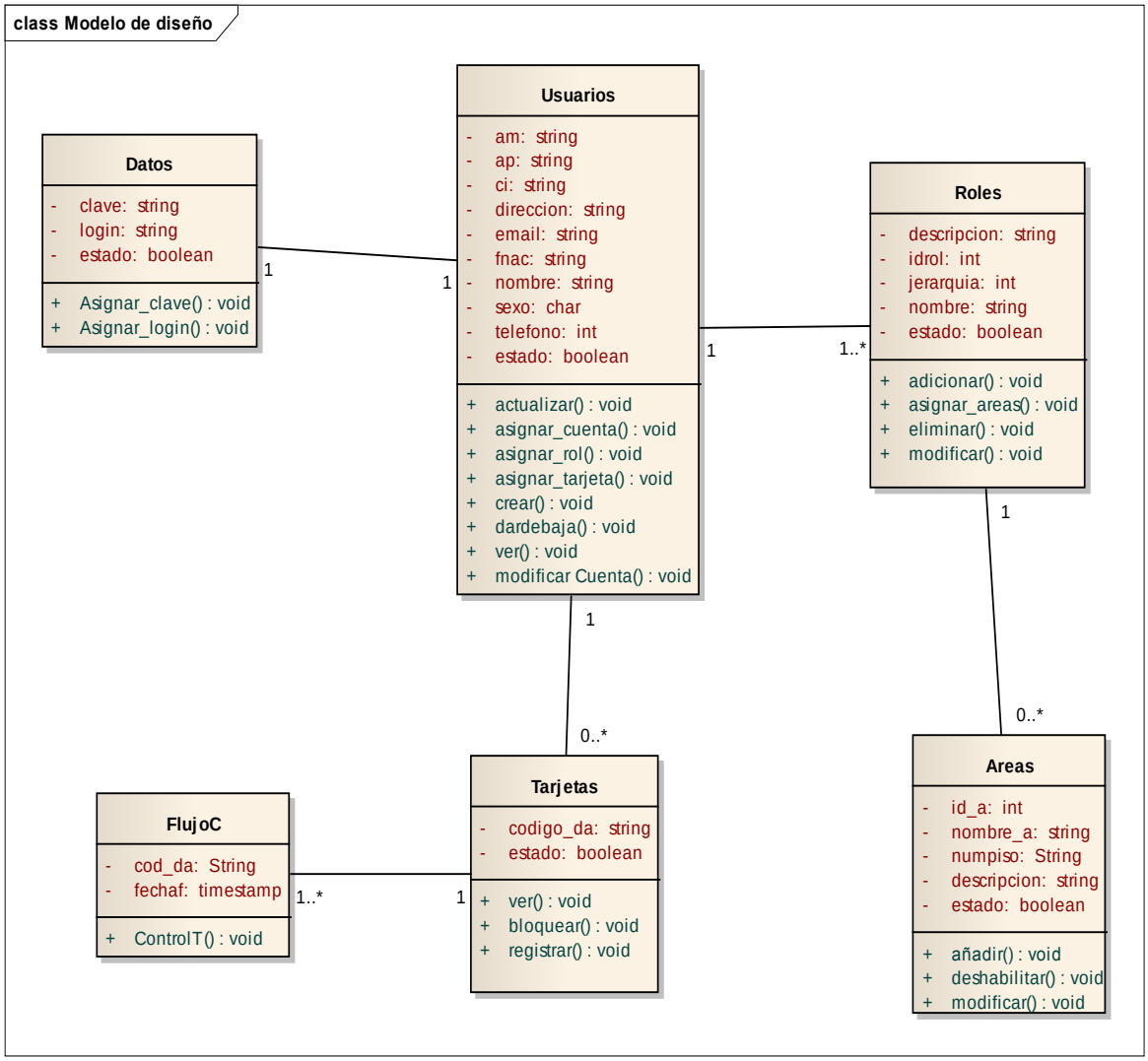
Roles

Áreas

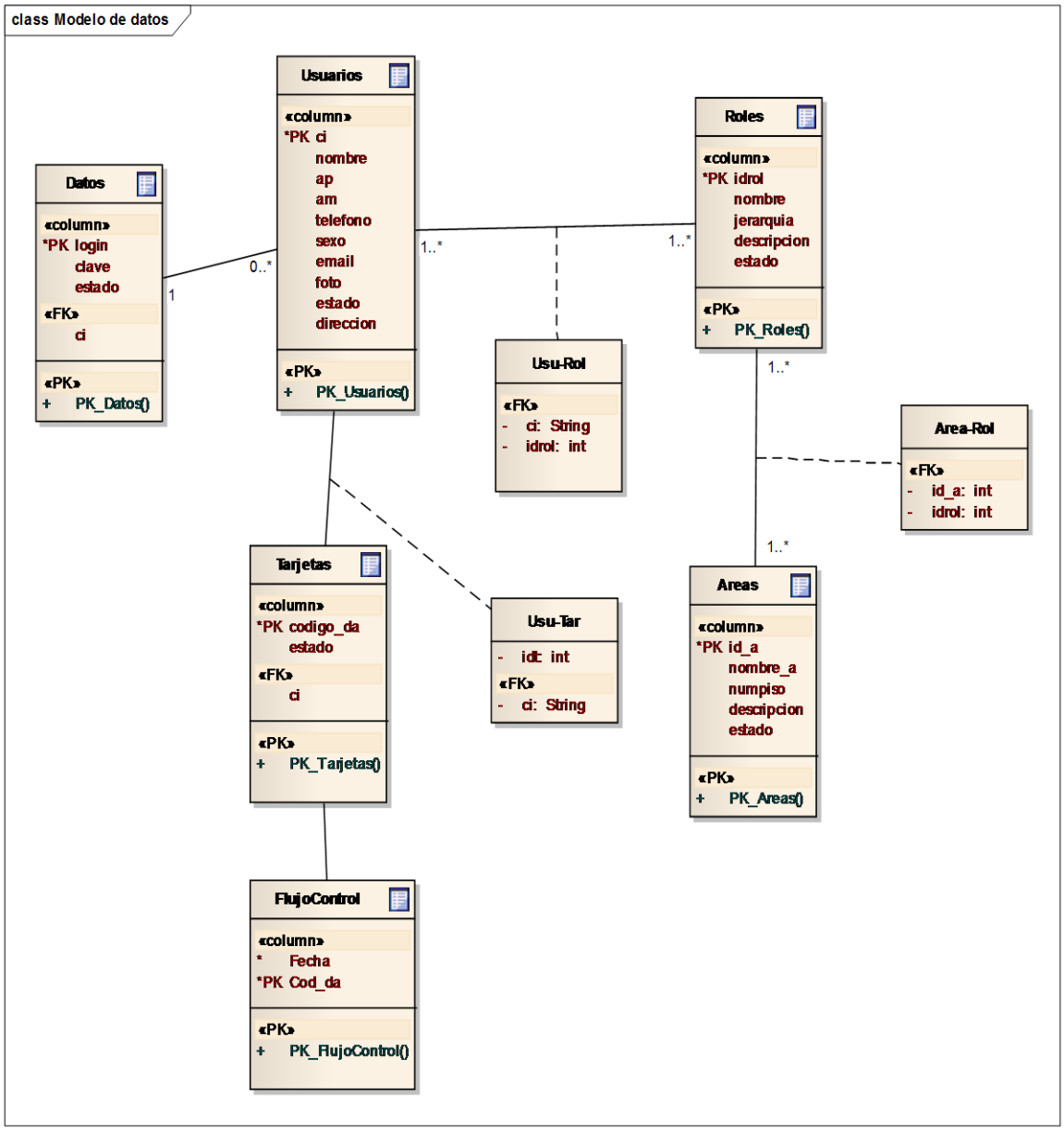
Tarjetas

Reportes

12. DIAGRAMA DE CLASES



13. MODELADO DE LA BASE DE DATOS (MODELO ENTIDAD-RELACIÓN)



13.1 CREACION DE BASE DE DATOS

***** Usuarios *****

```
create table usuarios(
ci varchar (8)not null,
nombre varchar(20) not null,
ap varchar (20) not null,
am varchar (20),
direccion varchar (30) not null,
telefono integer not null,
sexo char(1) not null,
fnac date not null,
email varchar (50),
estado boolean not null default true,
primary key(ci)
);
```

******Roles****

```
create table roles(
idrol serial not null,
nombre varchar(30)not null,
descripcion varchar (50),
jerarquia smallint not null,
estado boolean not null default true,
primary key(idrol)
);
```

******UsuRol******

```
create table usurol(
ci varchar(8) not null,
```

```
idrol serial not null,
primary key(ci,idrol),
foreign key(ci)references usuarios(ci),
foreign key(idrol)references roles(idrol)
);
********Datos***********
create table datos(
ci varchar(8)not null,
login varchar (20) not null,
clave varchar (20)not null,
estado boolean not null default true,
primary key(login),
foreign key(ci)references usuarios(ci)
);

*****Areas*****
create table areas(
id_a integer not null,
nombre_a varchar(20)not null,
descripcion varchar(50),
numpiso varchar(10),
estado boolean default true,
primary key(id_a)
);

********AreaRol*******
create table arearol(
id_a integer not null,
```

```
idrol integer not null,
primary key(id_a,idrol);
foreign key(id_a)references areas(id_a)
foreign key(idrol)references roles(idrol)
);

*****tarjetas******
create table tarjetas(
idt integer not null,
codigo_da varchar(30) not null,
estado boolean default true,
ci varchar(8)not null,
primary key(idt),
foreign key(ci)references usuarios(ci)
);

******UsuTar******
create table usutar(
ci varchar(8) not null,
idt integer not null,
primary key(ci,idt),
foreign key(ci)references usuarios(ci),
foreign key(idt)references tarjetas(idt)
);

*****FlujoC ******
create table flujoc(
fechaf timestamp not null,
```

cod_da varchar(20) not null,

primary key (cod_da),

foreign key(cod_da)references tarjetas(cod_da)

);

13.2 MODELO ENTIDAD RELACIÓN O MODELO RELACIONAL:

TABLA USUARIOS

CI String	Nombre String	Ap String	Am String	Dirección String	Foto String	Sexo Char	Teléfono Int	Email String	Estado Boolean

TABLA DATOS

Login String	Clave String	Estado Boolean	Ci String

TABLA ROLES

Idrol Int	Nombre String	Jerarquía String	Descripción String	Estado Boolean

TABLA USU-ROL

Idrol Int	Ci String

TABLA AREAS

Id_a Int	Nombre_a String	Numpiso Int	Descripción String	Estado Boolean

TABLA ROL-ÁREA

Idrol Int	Id_a Int

TABLA TARJETAS

Codigo_da String	Estado Boolean	Ci String

TABLA USU-TAR

Ci String	Cod_da String

TABLA FLUJOC

Cod_da String	Fechaf Timestamp

13.3 DICCIONARIO DE DATOS MODELO ENTIDAD-RELACIÓN

TABLA USUARIOS

Nombre: Usuarios					
Descripción: Para ingresar o ser reconocido en el Sistema de Control de Acceso, el usuario debe estar registrado en el Sistema.					
Campos					
Atributos	**Tipo**	**Longitud**	**PK**	**FK**	**Descripción**
Ci	**String**	**8**	**X**		**Identificador de usuario**
Nombre	**String**	**20**			**Nombre del usuario**
Ap	**String**	**20**			**Apellido Paterno**
Am	**String**	**20**			**Apellido Materno**
Dirección	**String**	**30**			**Dirección del usuario**
Fnac	**Date**				**Fecha de nacimiento de usuario**
Sexo	**Char**	**1**			**Sexo que tiene el usuario**
Telefono	**Int**	**7**			**Teléfono o celular**
Email	**String**	**50**			**Correo electrónico del usuario**

TABLA DATOS

Nombre: Datos					
Descripción: Para ingresar al Sistema, a cada usuario se le asigna los siguientes datos.					
Campos					
Atributos	**Tipo**	**Longitud**	**PK**	**FK**	**Descripción**
Ci	**Int**	**8**		**X**	**Identificador de usuario**
Login	**String**	**20**	**X**		**Nombre con el que ingresará el usuario**
Clave	**String**	**20**			**Contraseña con la que ingresará al Sistema**
Estado	**Boolean**	**1**			**Si están activos o no los datos**

TABLA ROLES

Nombre: Roles
Descripción: Para encontrarse registrado en el Sistema de Control de Acceso como

funcionario de la Organización debe tener un rol asignado.					
Campos					
Atributos	**Tipo**	**Longitud**	**PK**	**FK**	**Descripción**
Idrol	**Int**	**8**		**X**	**Identificador de un rol**
Nombre	**String**	**30**	**X**		**Nombre del rol**
Jerarquía	**String**	**1**			**Jerarquía según organigrama en el que se encuentra el rol**
Descripción	**String**	**50**			**Descripción breve del rol**
Estado	**Boolean**	**1**			**Si está activo o no el rol**

TABLA USU-ROL

Nombre: Usu-Rol					
Descripción: Relación entre los usuarios y sus roles correspondientes					
Campos					
Atributos	**Tipo**	**Longitud**	**PK**	**FK**	**Descripción**
Ci	**String**	**8**	**X**		**Identificador de usuario**
Idrol	**Int**		**X**		**Identificador de rol**

TABLA AREAS

Nombre: Áreas					
Descripción: Se registran todas las áreas existentes en la infraestructura física de la Organización.					
Campos					
Atributos	**Tipo**	**Longitud**	**PK**	**FK**	**Descripción**
Id_a	**Int**	**4**	**X**		**Identificador de área**
Nombre	**String**	**20**			**Nombre del área a identificar**
Numpiso	**Int**	**1**			**Número de piso en el que se encuentra el área.**
Descripción	**String**	**50**			**Descripción breve del área**
Estado	**Boolean**	**1**			**Si está activa o no el área.**

TABLA ROL_AREA

Nombre: Rol-Área	
Descripción: Relación entre los roles y sus áreas de acceso correspondientes	
Campos	

Atributos	Tipo	Longitud	PK	FK	Descripción
Id_a	Int	4	X		Identificador de área
Idrol	Int	4	X		Identificador de rol

TABLA TARJETAS

Nombre: Tarjetas					
Descripción: Se registran todas las tarjetas habilitadas en el Sistema para ser asignadas a los distintos usuarios y/o funcionarios.					
Campos					
Atributos	Tipo	Longitud	PK	FK	Descripción
Codigo_da	String	20	X		Código predeterminado de tarjeta
Estado	Boolean	1			Si está o no activa la tarjeta

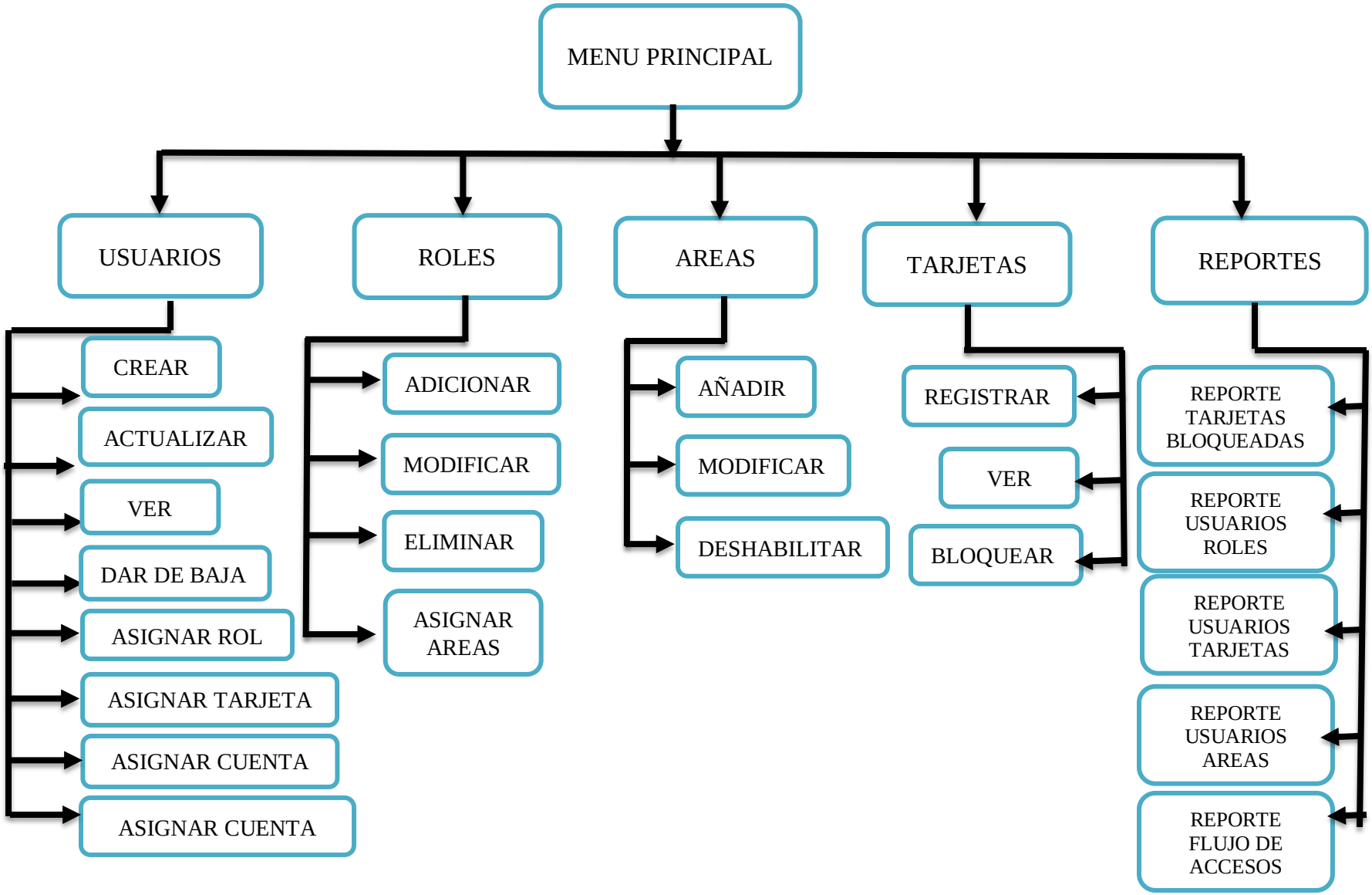
TABLA USU_TAR

Nombre: Usu-Ta					
Descripción: Relación entre los usuarios y sus tarjetas de acceso correspondientes					
Campos					
Atributos	Tipo	Longitud	PK	FK	Descripción
Cod_da	String	20	X		Identificador de tarjeta
Ci	String	8	X		Identificador de usuario

TABLA FLUJOC

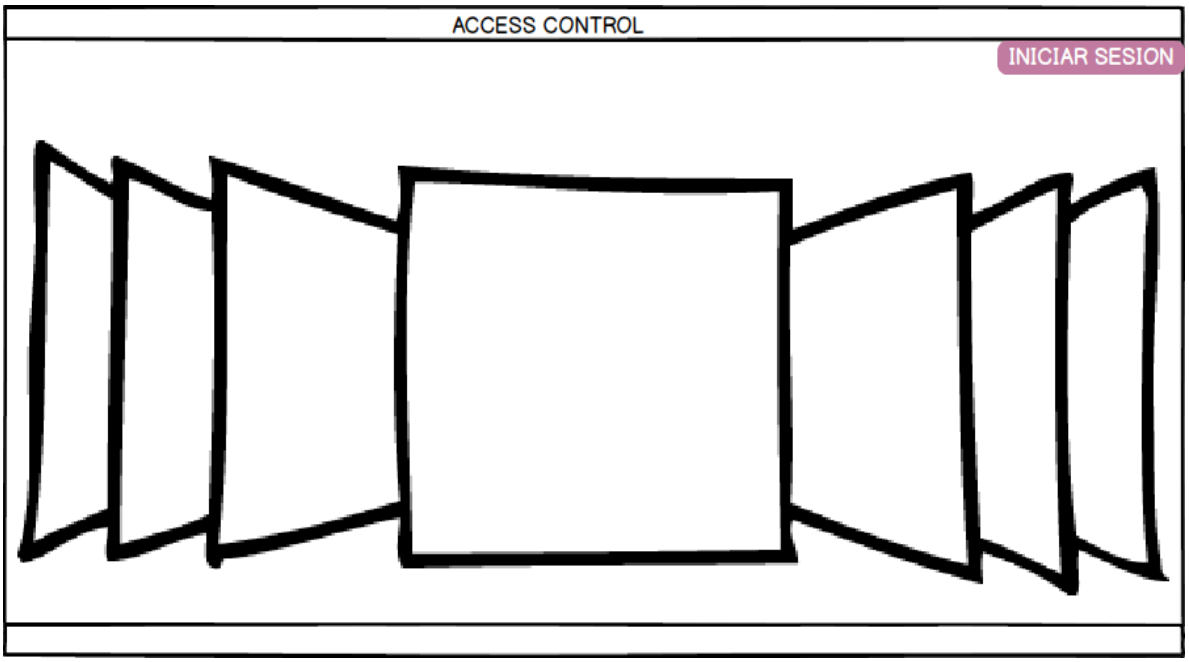
Nombre: FlujoC					
Descripción: Relación entre los las tarjetas y su flujo de accesos al día					
Campos					
Atributos	Tipo	Longitud	PK	FK	Descripción
Cod_da	String	20	X		Identificador de tarjeta
FechaF	Timestamp	6			Fecha y Hora de lectura de tarjeta

14. DIAGRAMA NAVEGACIONAL

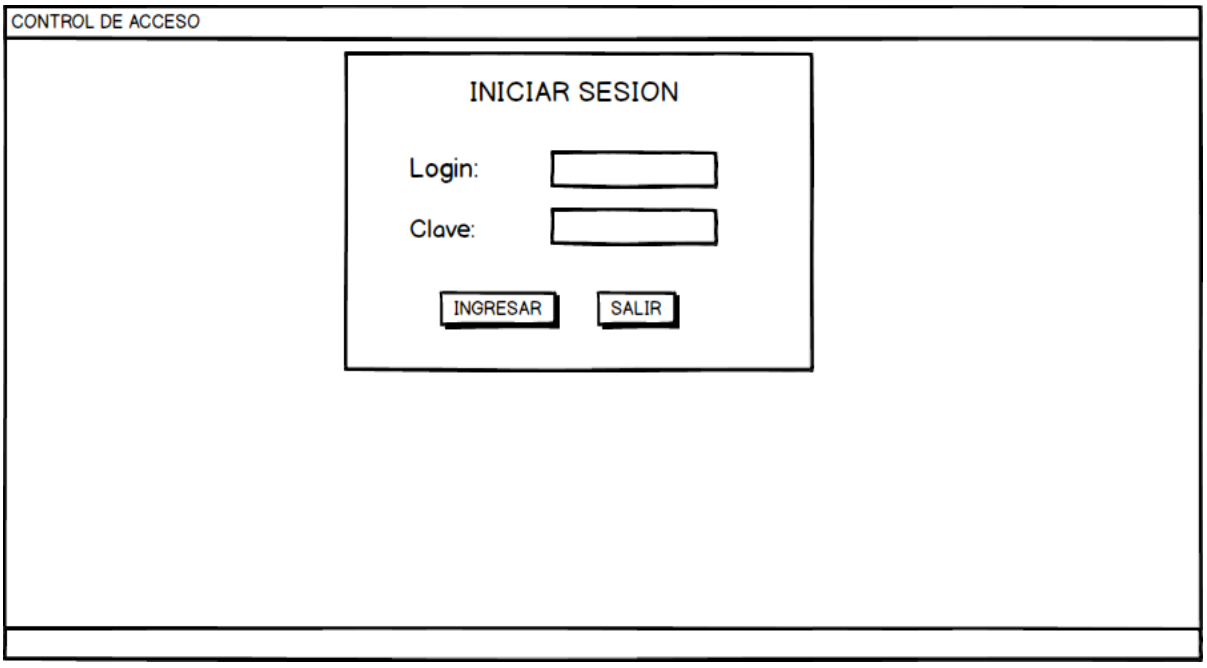


15. INTERFACES BÁSICAS

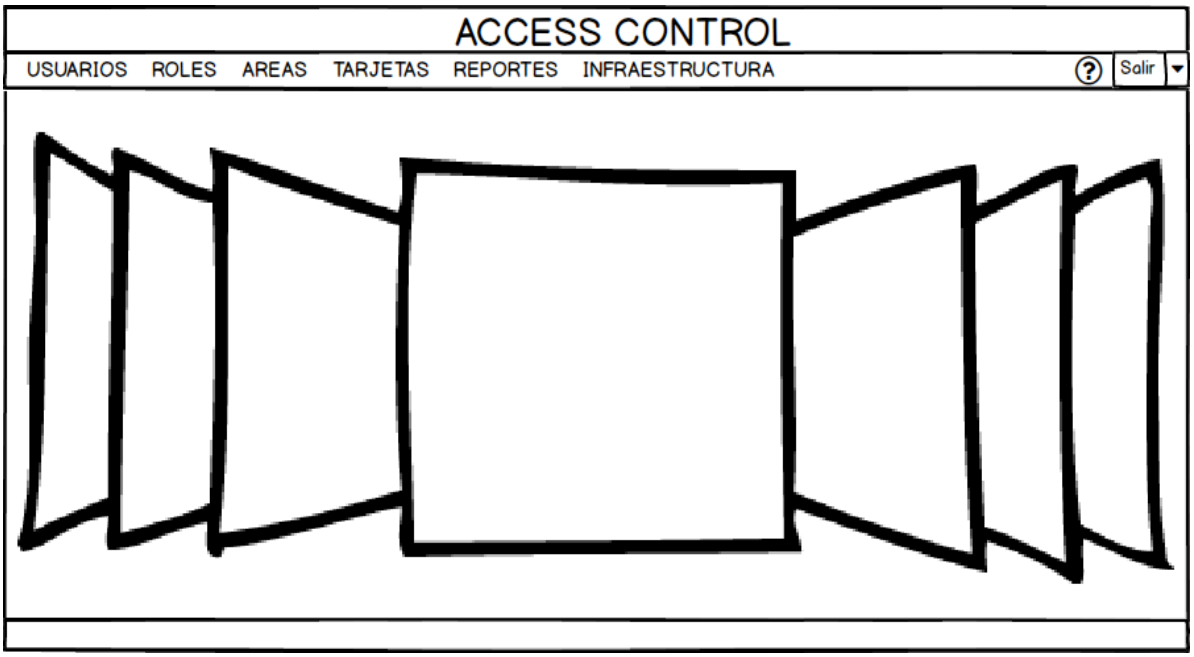
Aquí podemos ver la Pantalla de Bienvenida en la parte central, se puede ver un carrusel de imágenes, todas relacionadas al tema del Sistema.



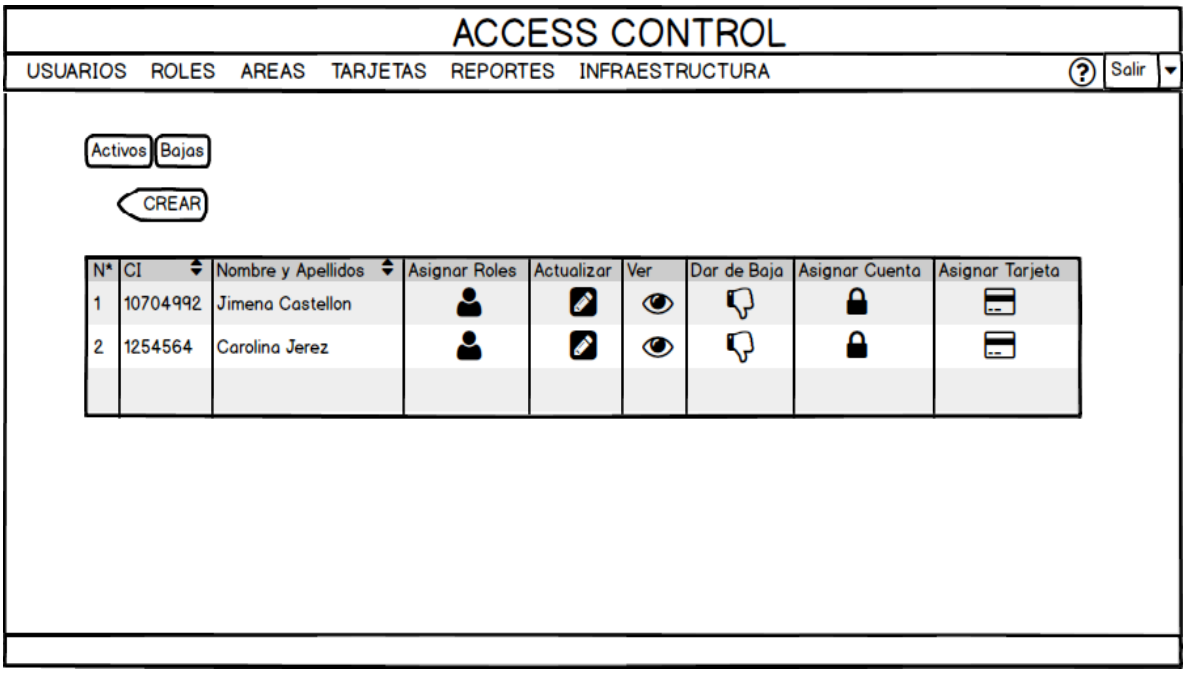
Al hacer clic en el botón: iniciar sesión se desplegará la pantalla modal donde se podrá introducir el login la clave para ingresar al Sistema.



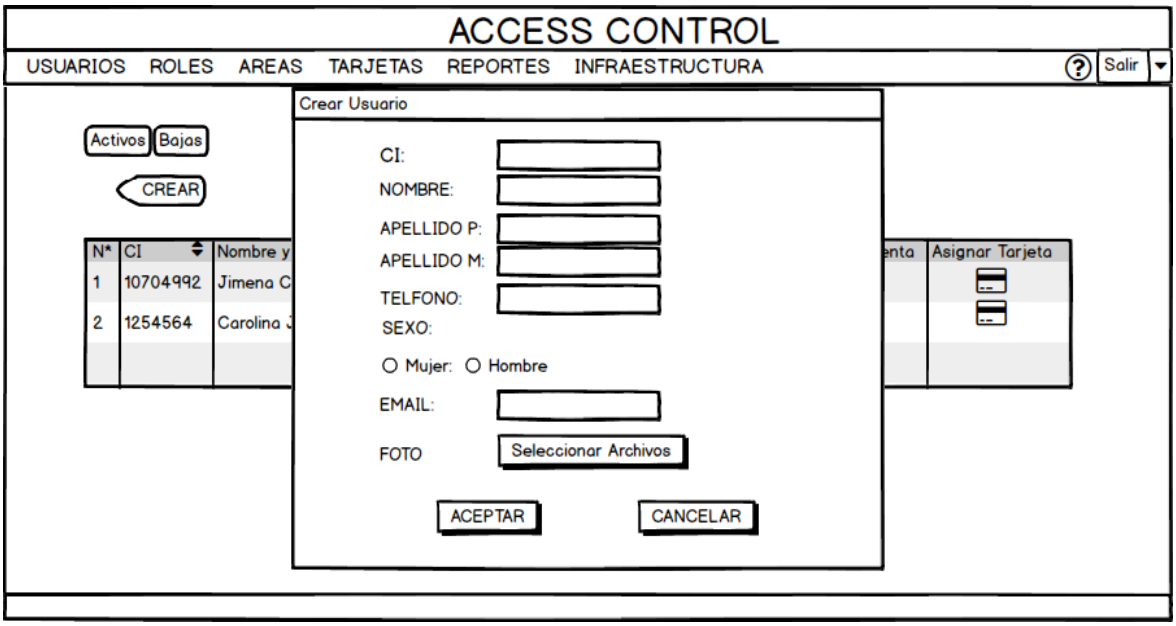
Pantalla Menú principal en donde podemos observar en la parte superior un menú de opciones que tiene el Sistema y en la parte central se puede ver un carrusel de imágenes relacionadas a la temática del Sistema.



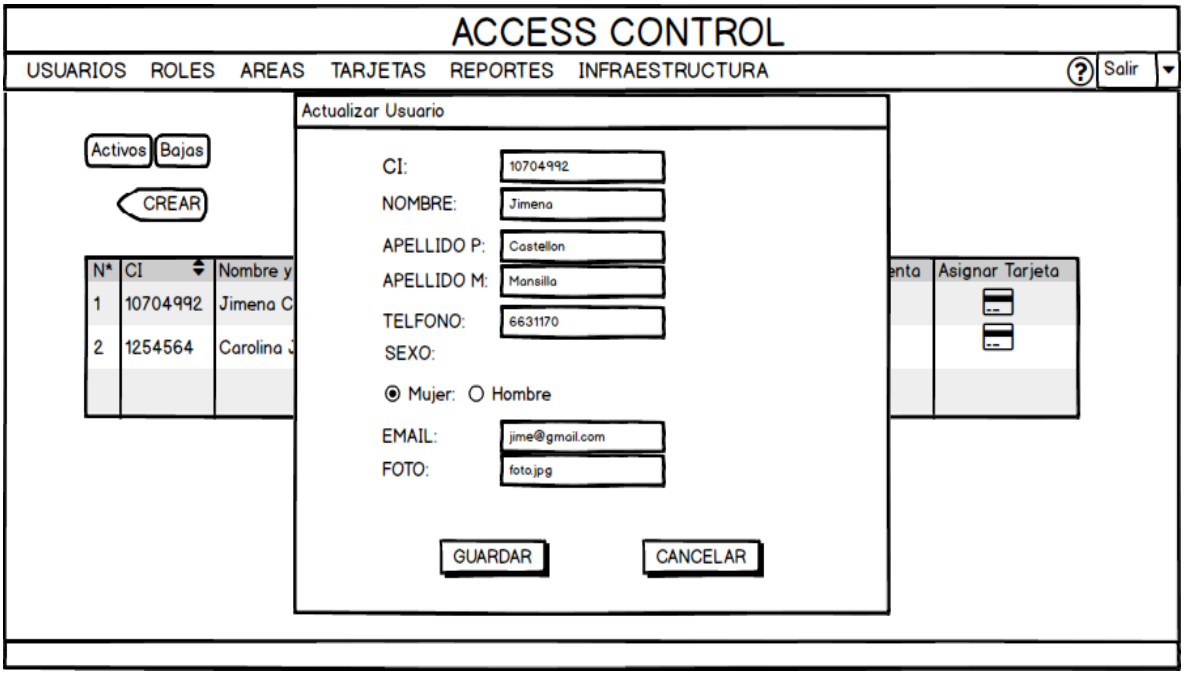
Pantalla Usuarios: En esta pantalla podemos ver los datos de los diferentes usuarios como también las opciones que nos ofrecen como: Crear, actualizar, ver, dar de baja, asignar roles, asignar tarjeta, asignar cuenta.



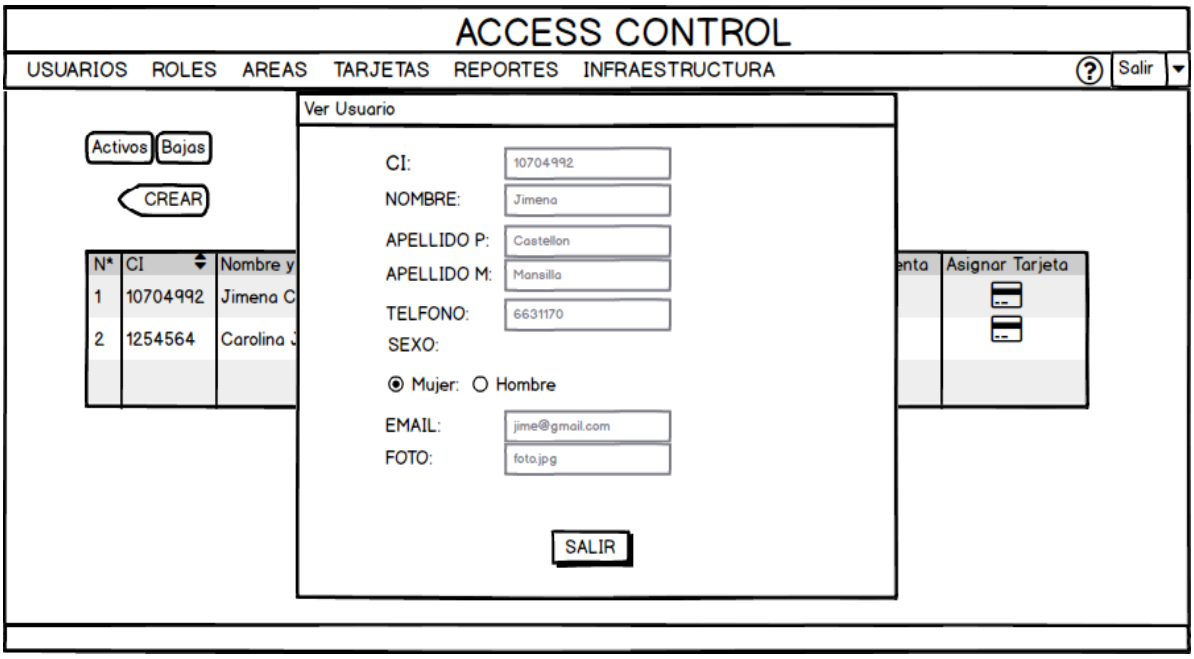
Pantalla Crear Usuario: Aquí podemos crear los usuarios que estén registrados en el Sistema.



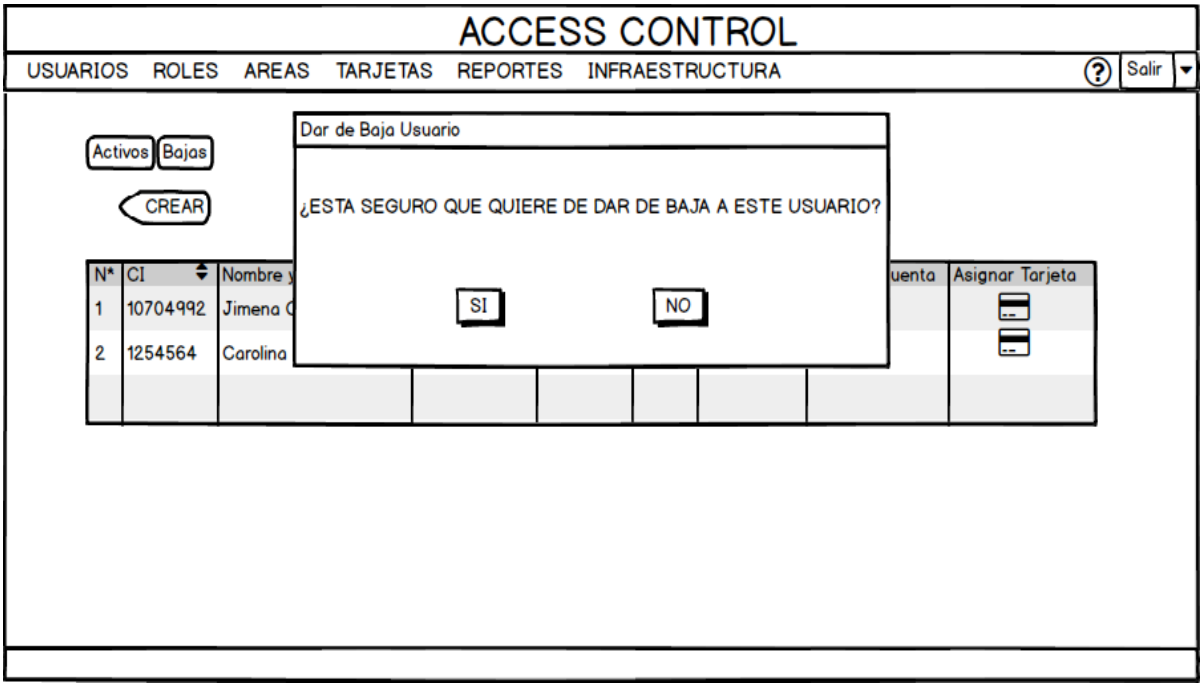
Pantalla Actualizar Usuario: Aquí tenemos la opción de modificar cualquiera de los datos de los usuarios ya registrados en el Sistema.



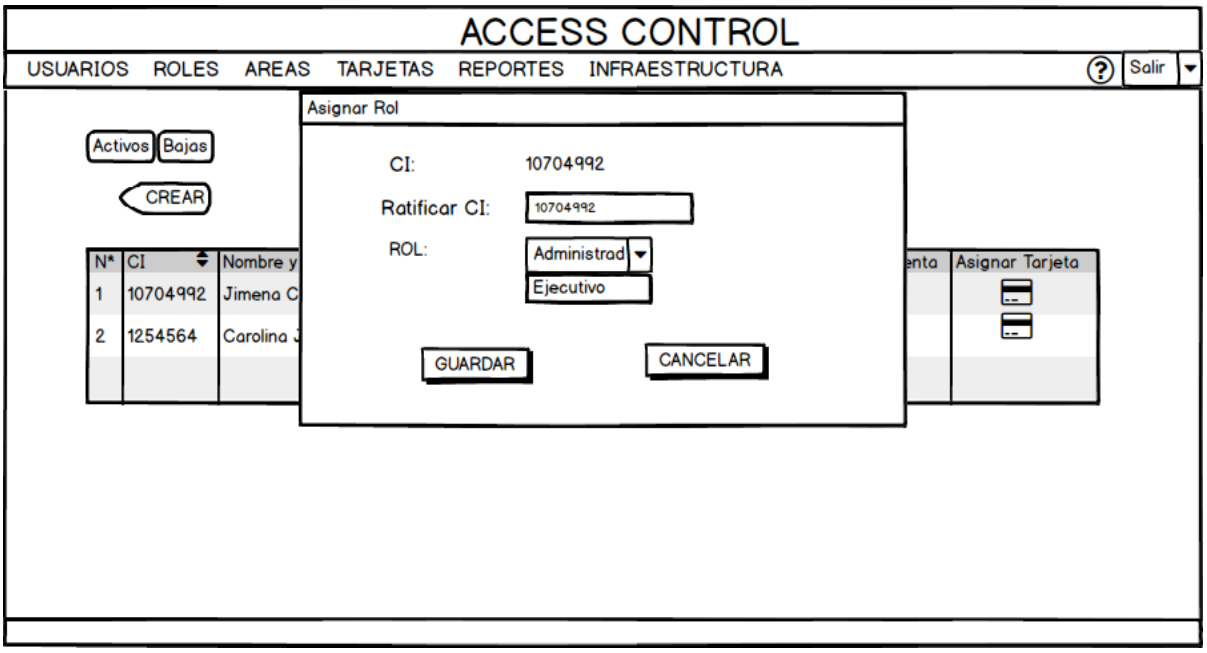
Pantalla Ver Usuario: Aquí podemos ver los datos completos de cualquiera de los usuarios seleccionados.



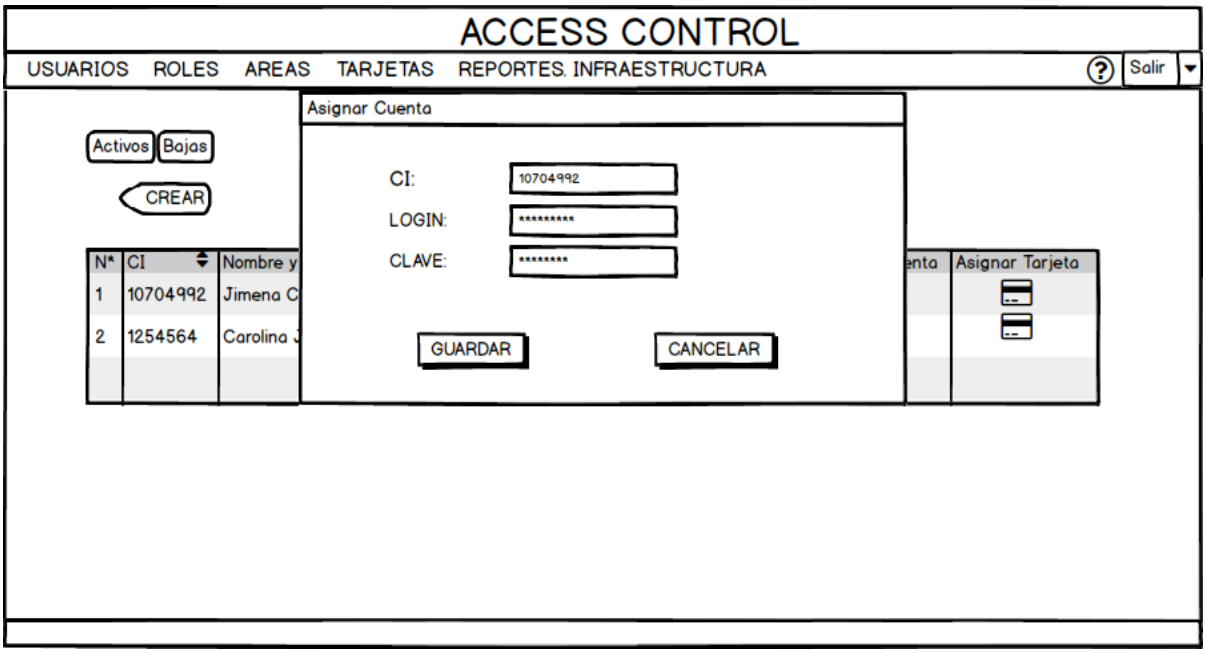
Pantalla Dar de Baja Usuario: Podemos Dar de baja lógicamente a cualquiera de los usuarios registrados.



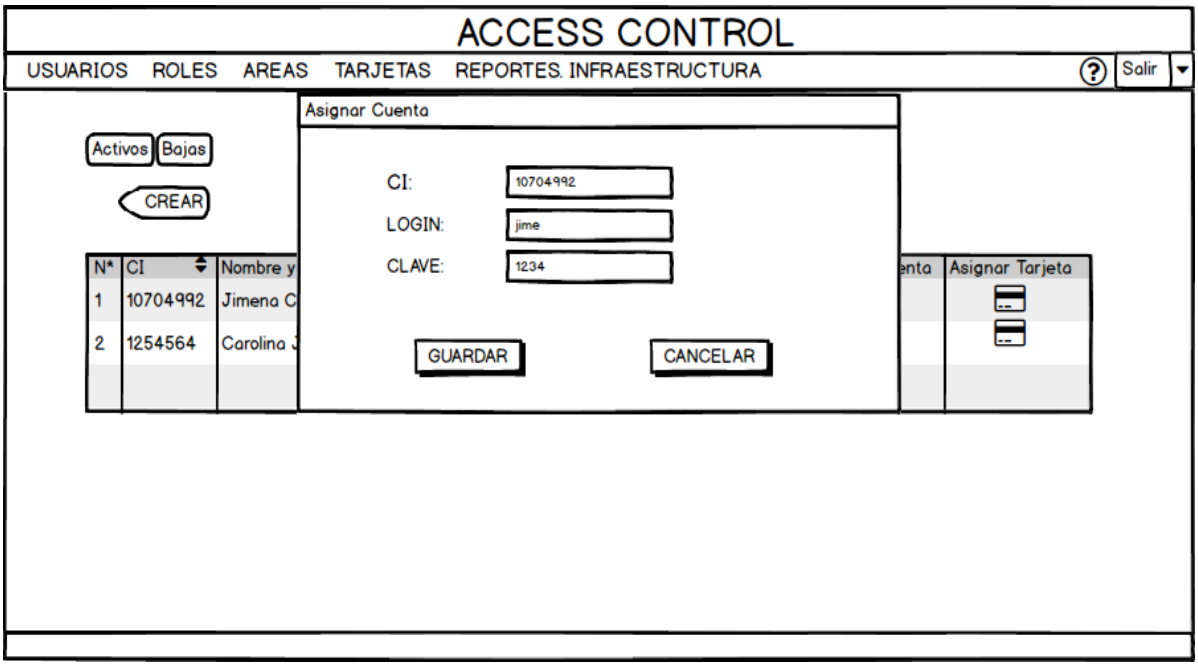
Pantalla Asignar Roles: En esta Pantalla solo el Administrador o Gerente podrá asignar uno o máximo dos roles a un Usuario.



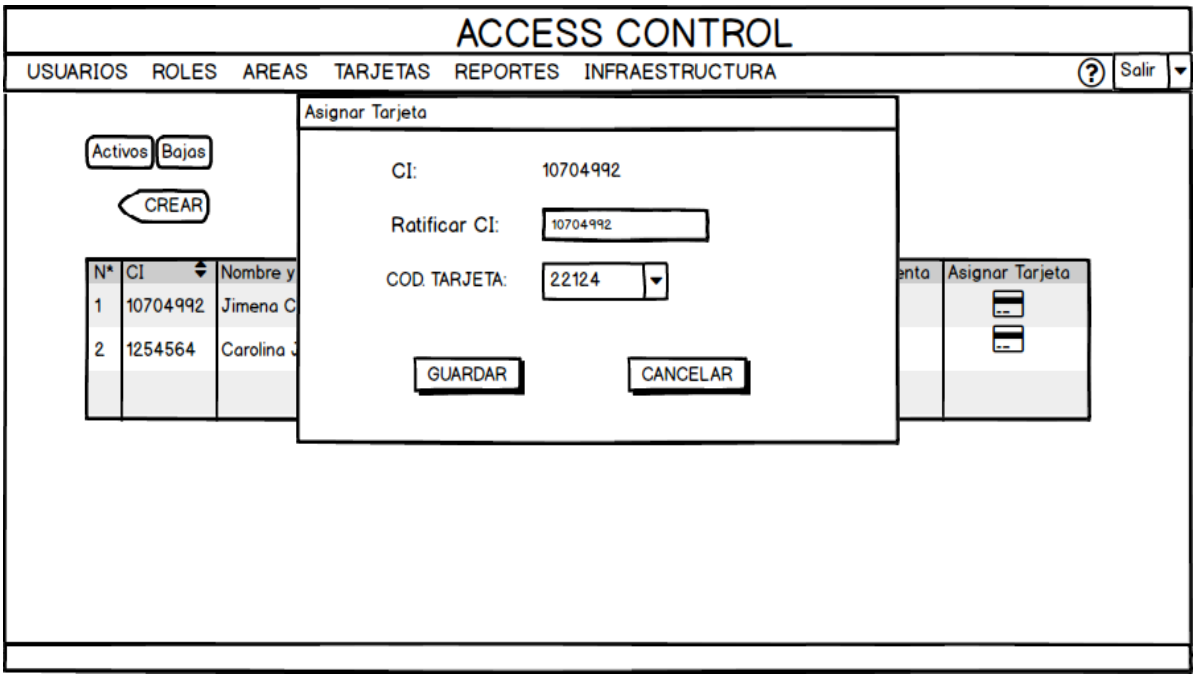
Pantalla Asignar Cuenta: En esta pantalla solo el Administrador podrá asignar los logins y claves sólo a los usuarios que también podrán ingresar al Sistema.



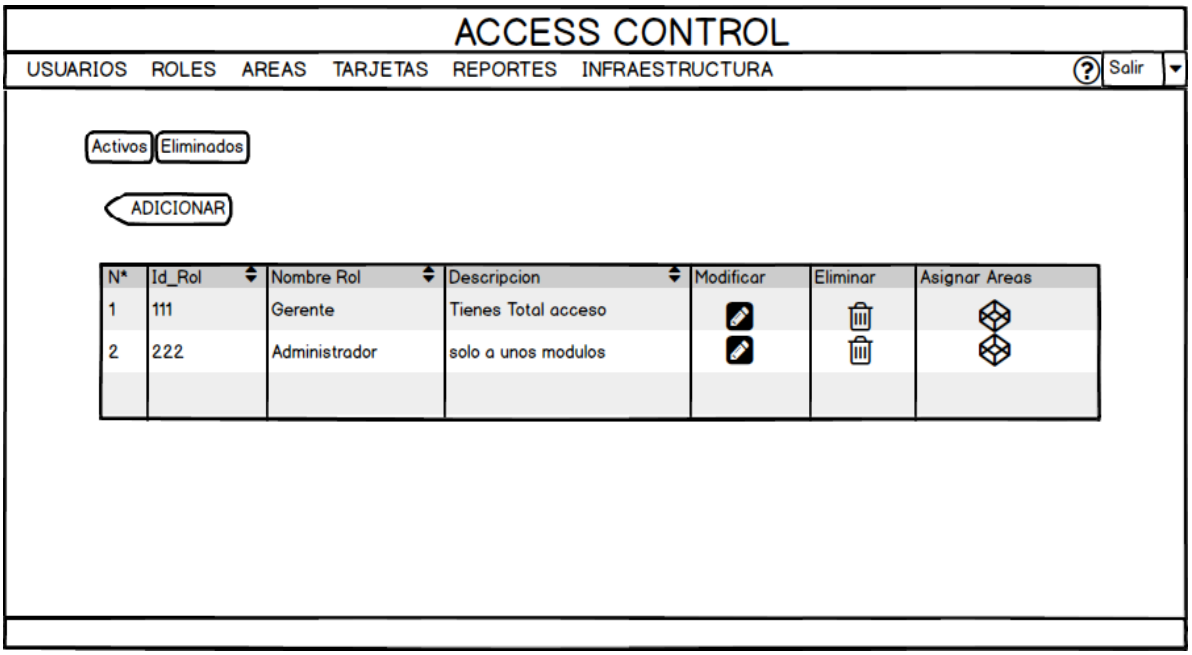
Pantalla Modificar Cuenta: En esta pantalla solo los usuarios que cuenten con una cuenta podrán acceder a modificarla.



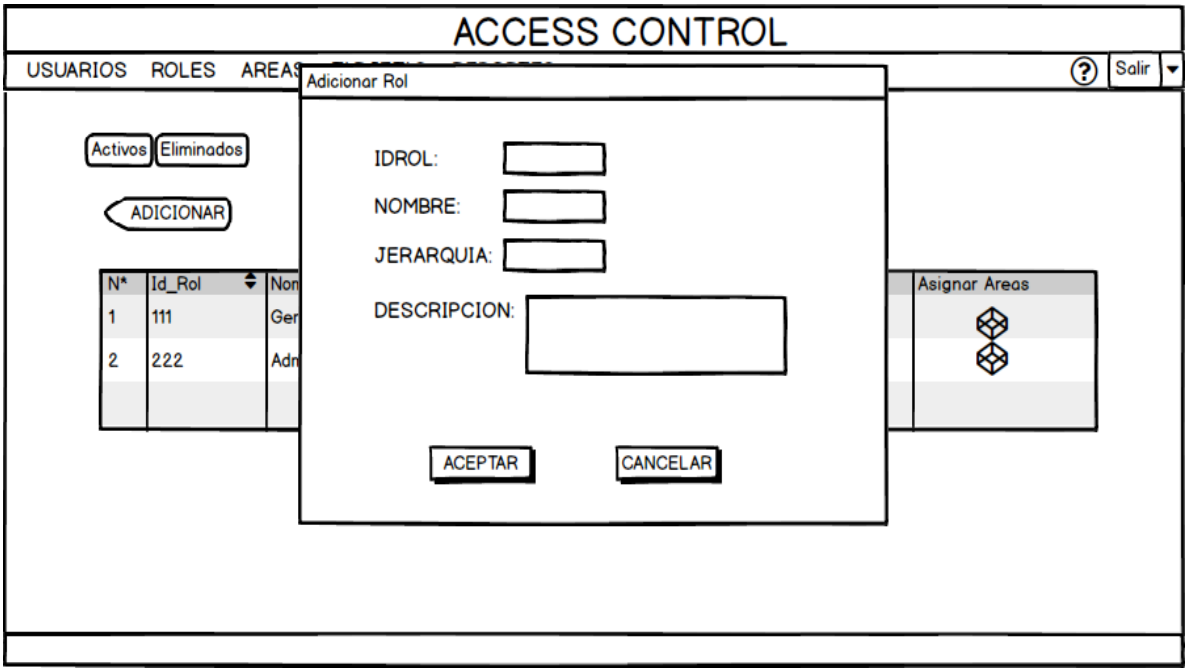
Pantalla Asignar Tarjeta: En esta pantalla solo el Administrador podrá asignar una tarjeta a un usuario.



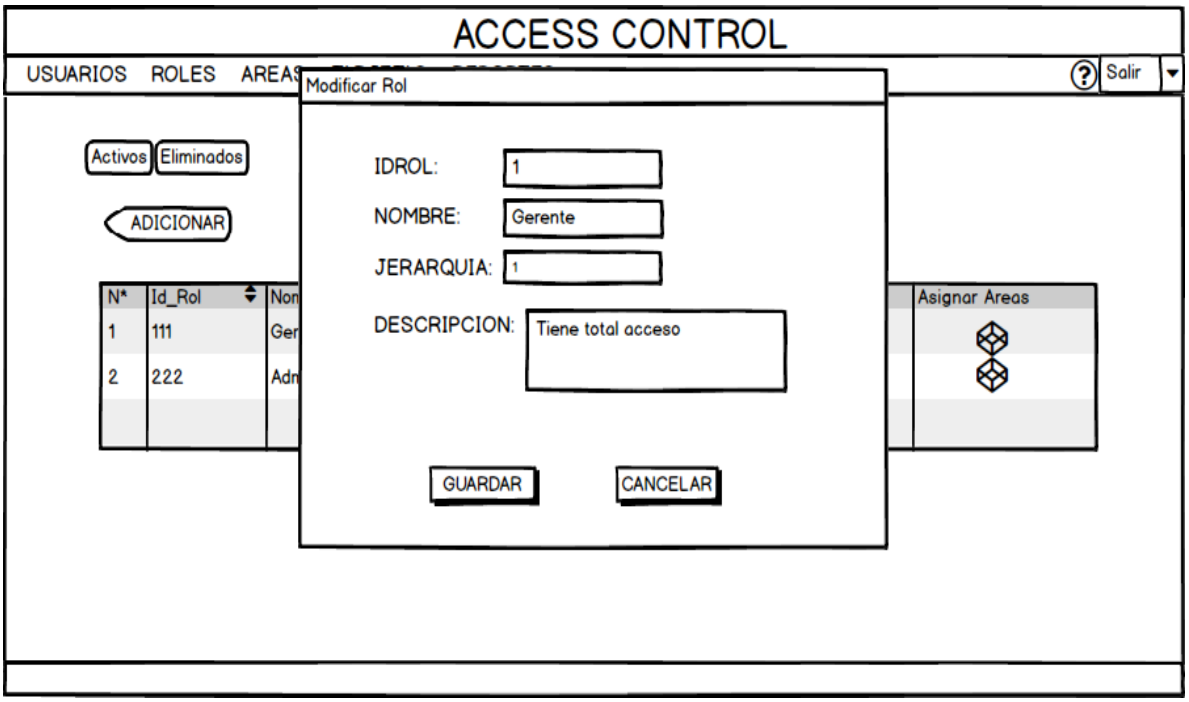
Pantalla Roles: En esta pantalla se nos presentan las diferentes opciones que nos ofrece la Gestión de Roles como: Adicionar, Modificar, Eliminar y Asignar Áreas.



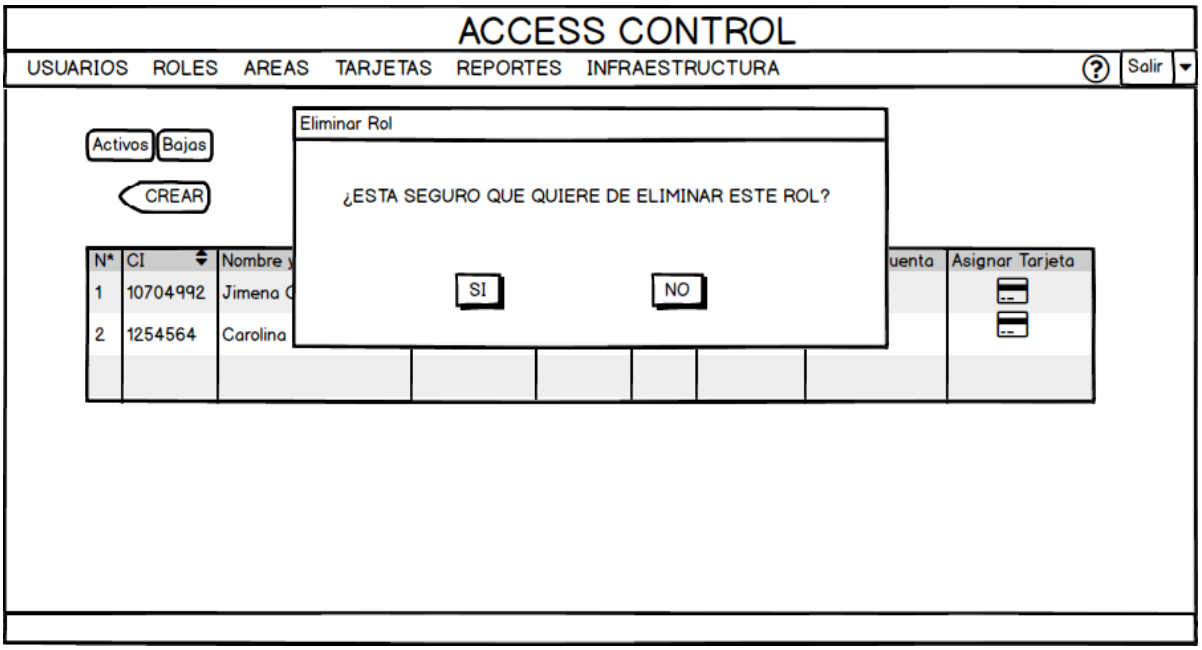
Pantalla Adicionar Rol: En esta pantalla podemos adicionar un nuevo rol al Sistema.



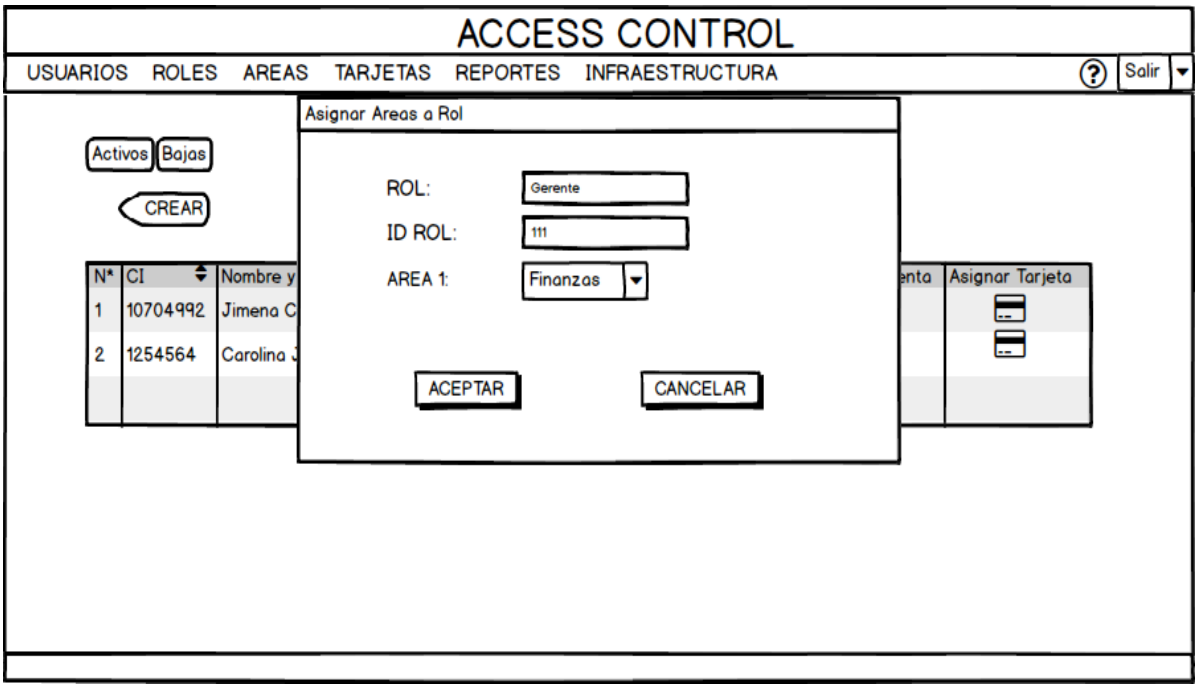
Pantalla Modificar Rol. En esta pantalla el Administrador podrá modificar cualquier dato de un rol ya registrado en el Sistema.



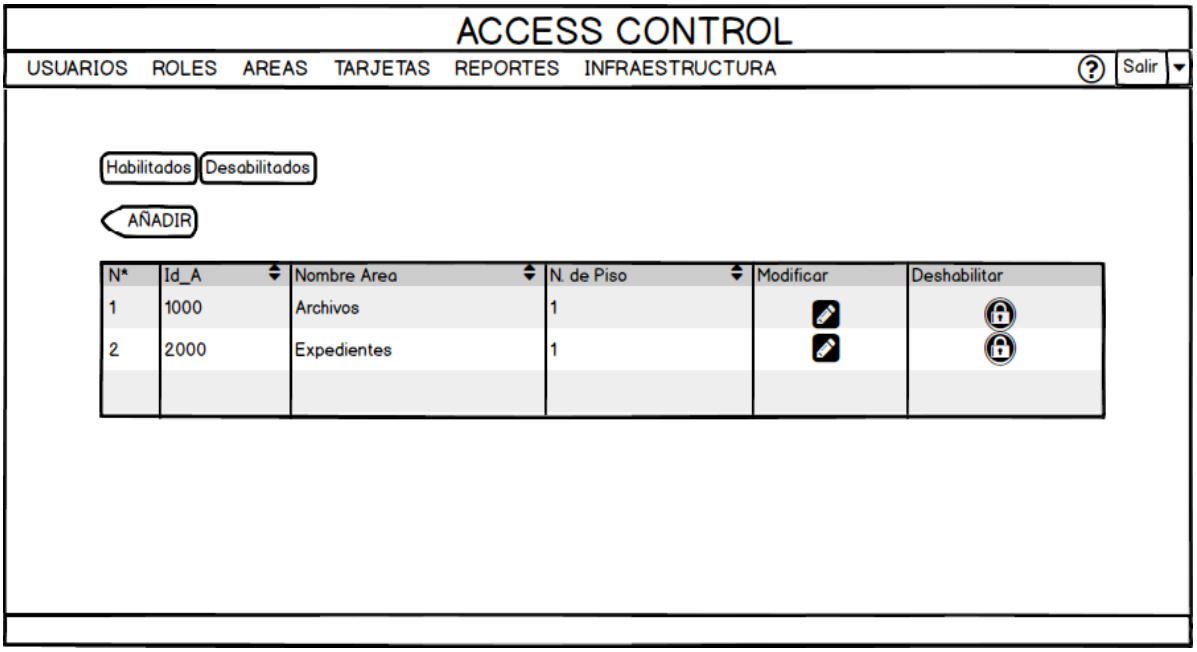
Pantalla Eliminar Rol: En esta pantalla el Administrador podrá eliminar físicamente del Sistema a un Rol.



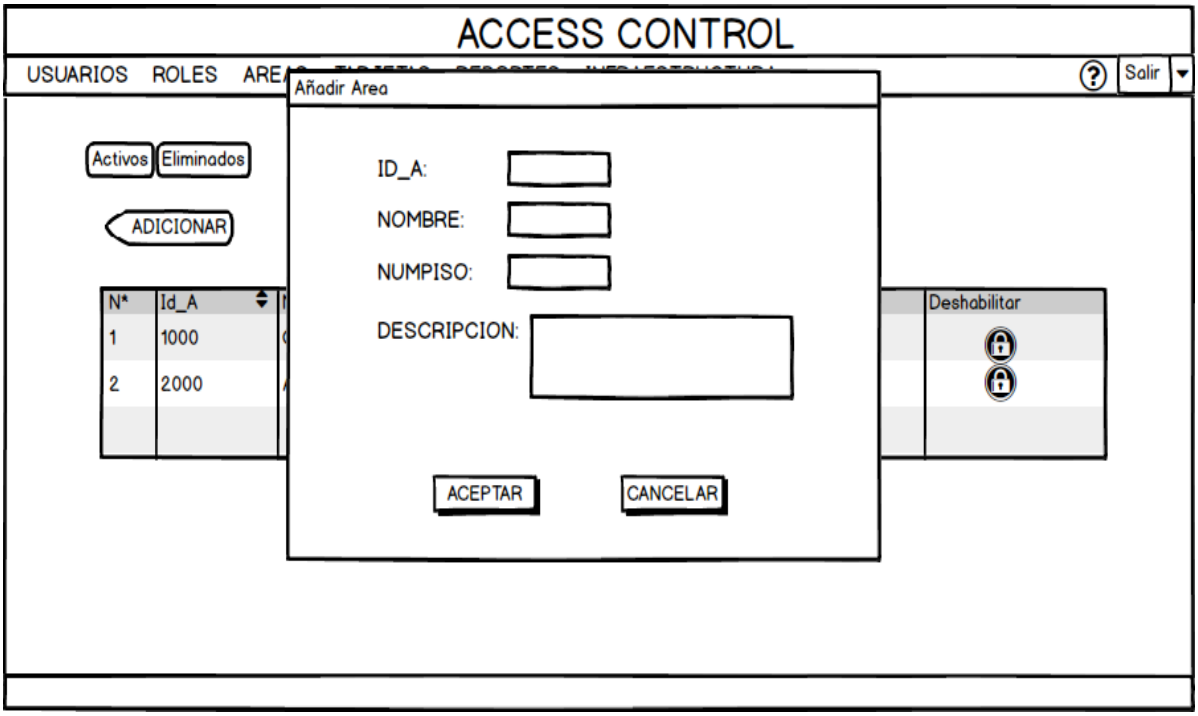
Pantalla Asignar Áreas a Rol: En esta pantalla el administrador podrá asignar determinadas áreas a un rol.



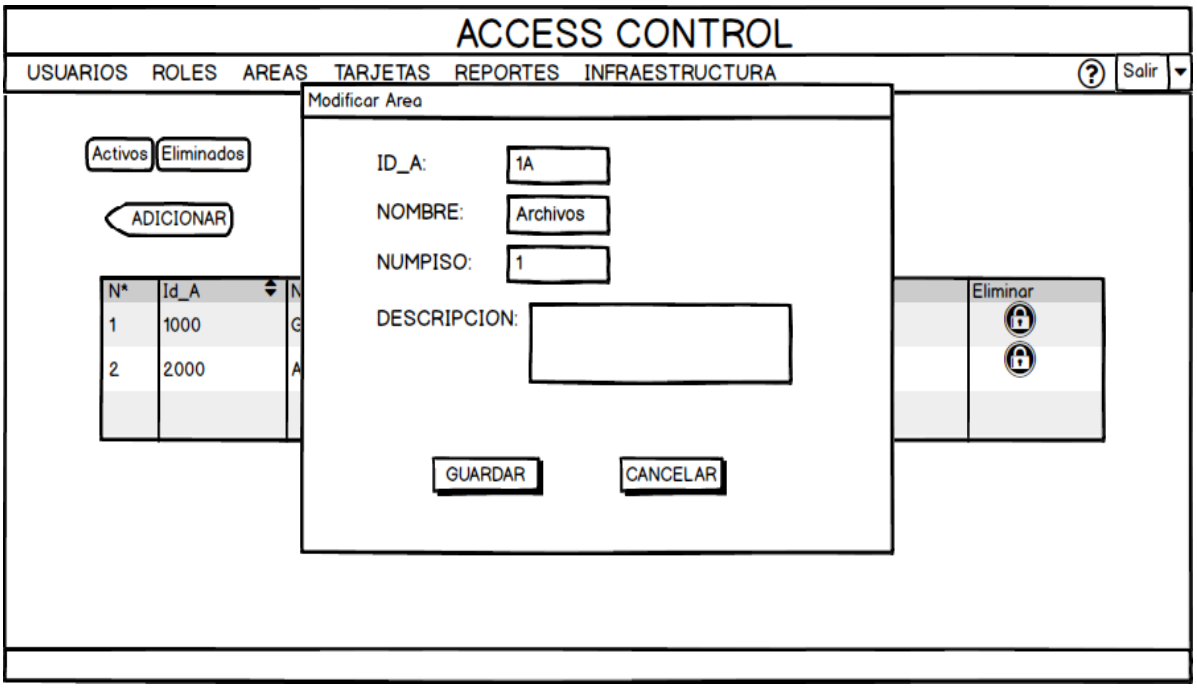
Pantalla Áreas: En esta pantalla se nos presentan las diferentes opciones que nos ofrece la Gestión de Áreas como: Añadir, Modificar y Deshabilitar.



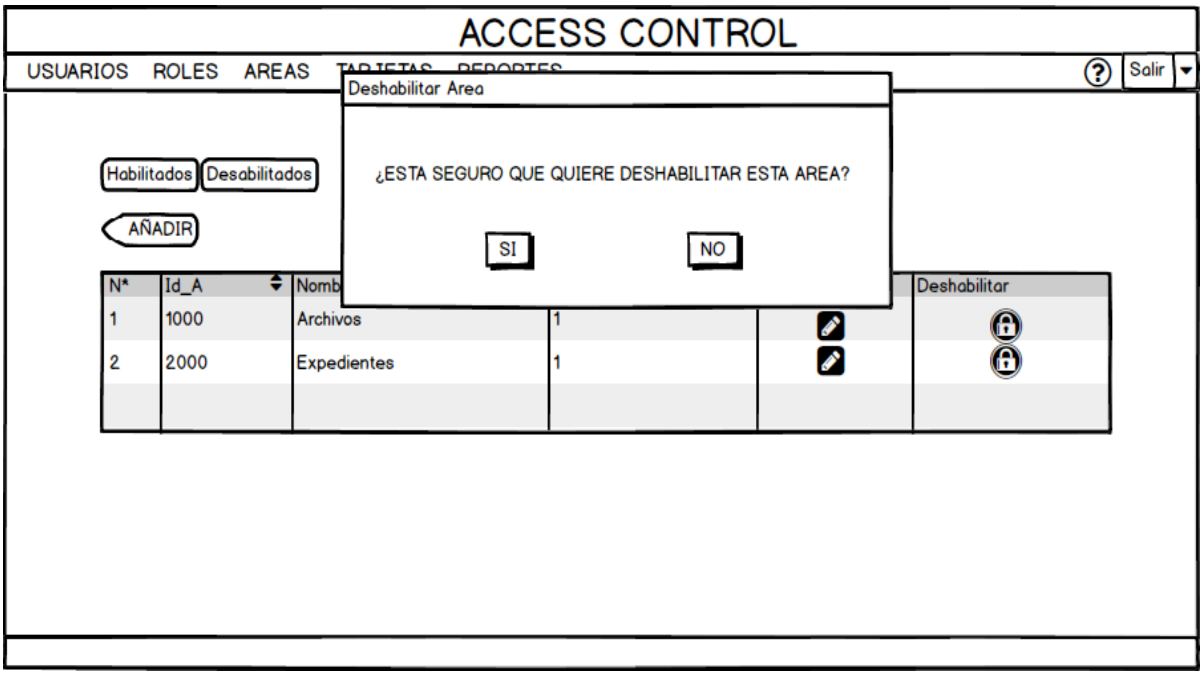
Pantalla Añadir Área: En esta pantalla podemos añadir una nueva área al Sistema.



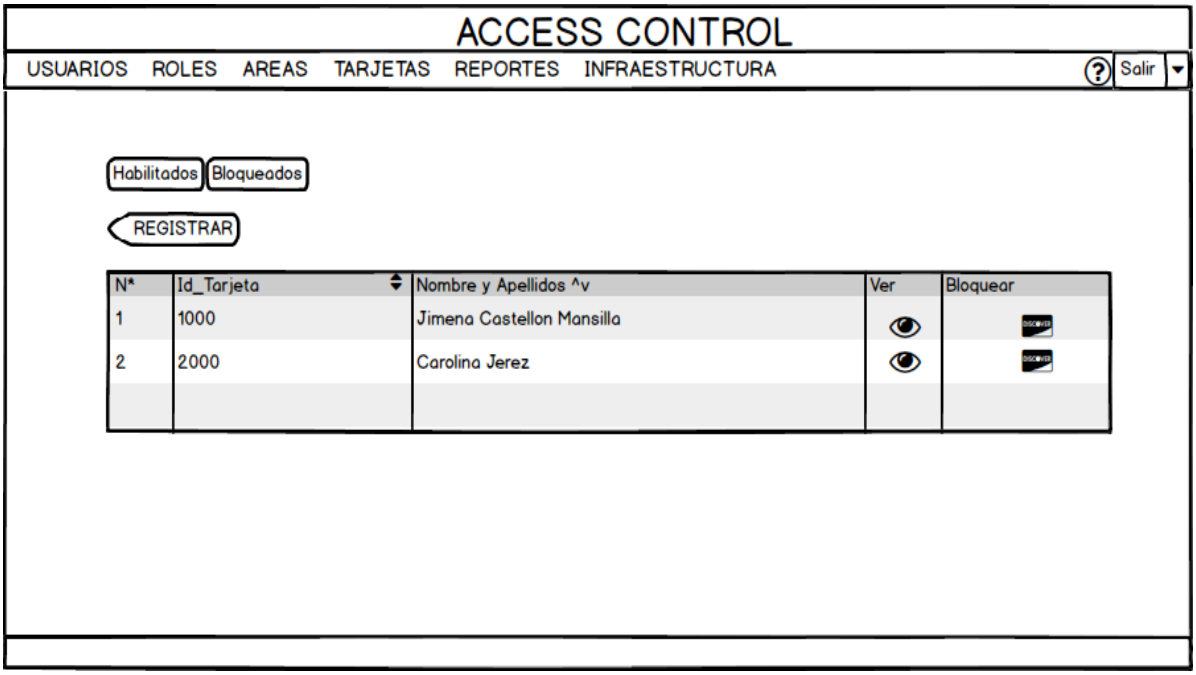
Pantalla Modificar Área: En esta pantalla se podrá modificar cualquier dato de un área ya registrada en el Sistema.



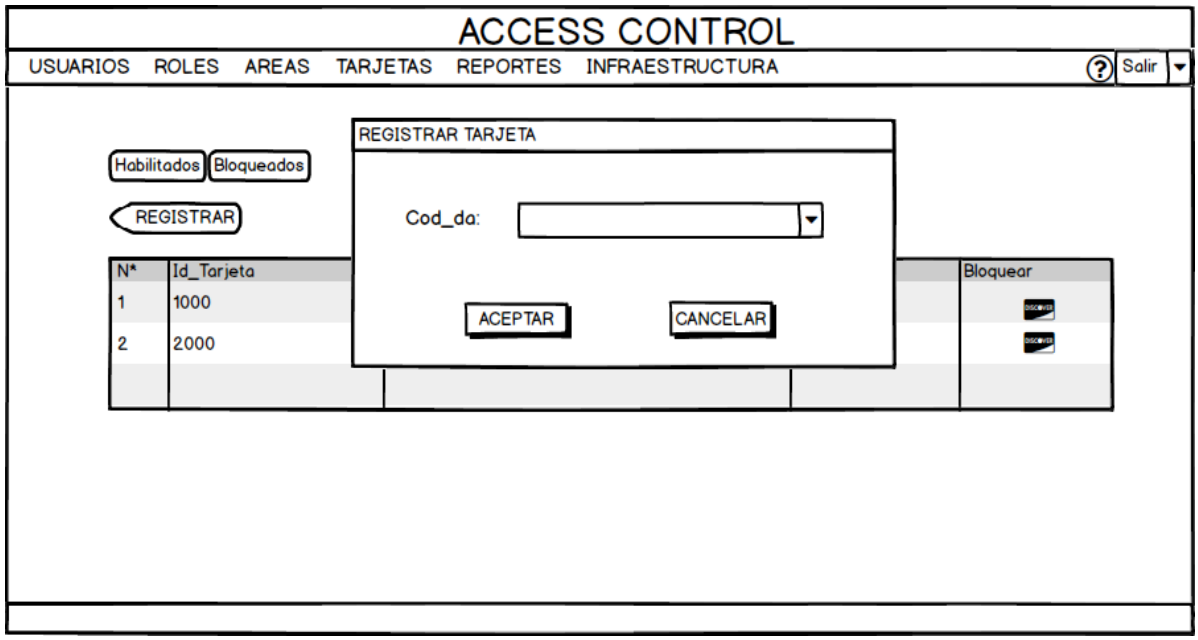
Pantalla Deshabilitar Área: En esta pantalla se podrá deshabilitar un área ya registrada en el Sistema; es decir, cambiar su estado a falso.



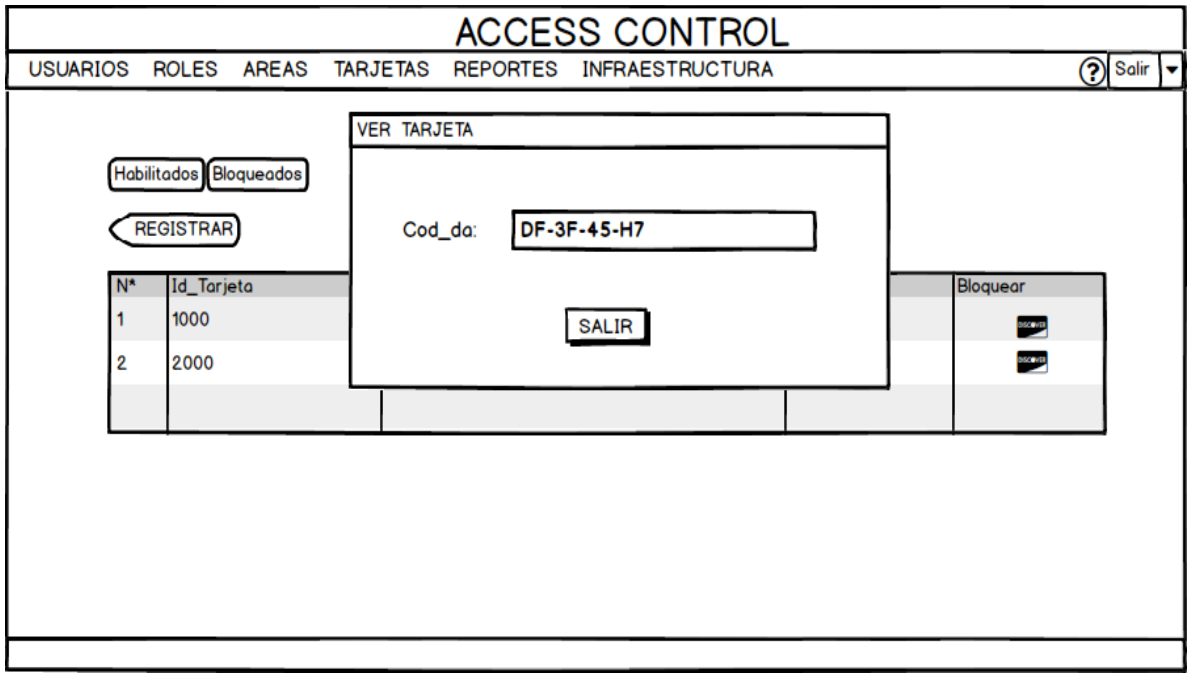
Pantalla Tarjetas: En esta pantalla se nos presentan las diferentes opciones que nos ofrece la Gestión de Tarjetas como: Registrar, Ver y Bloquear.



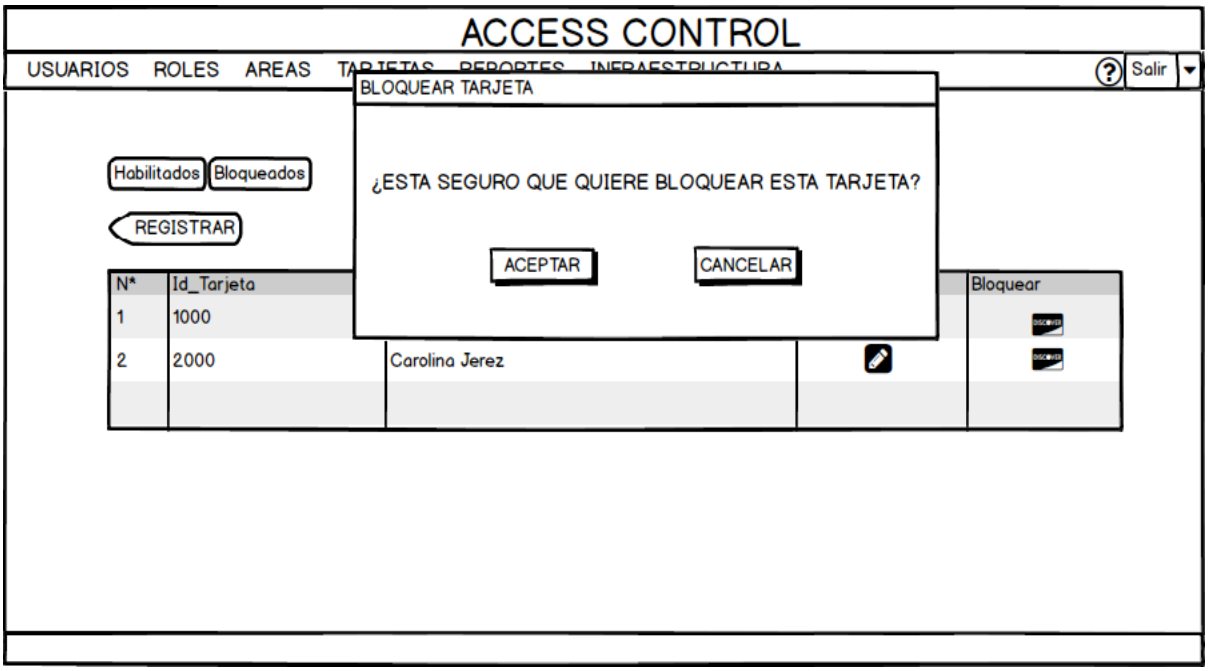
Pantalla Registrar Tarjeta: En esta Pantalla se puede registrar una tarjeta en el Sistema.



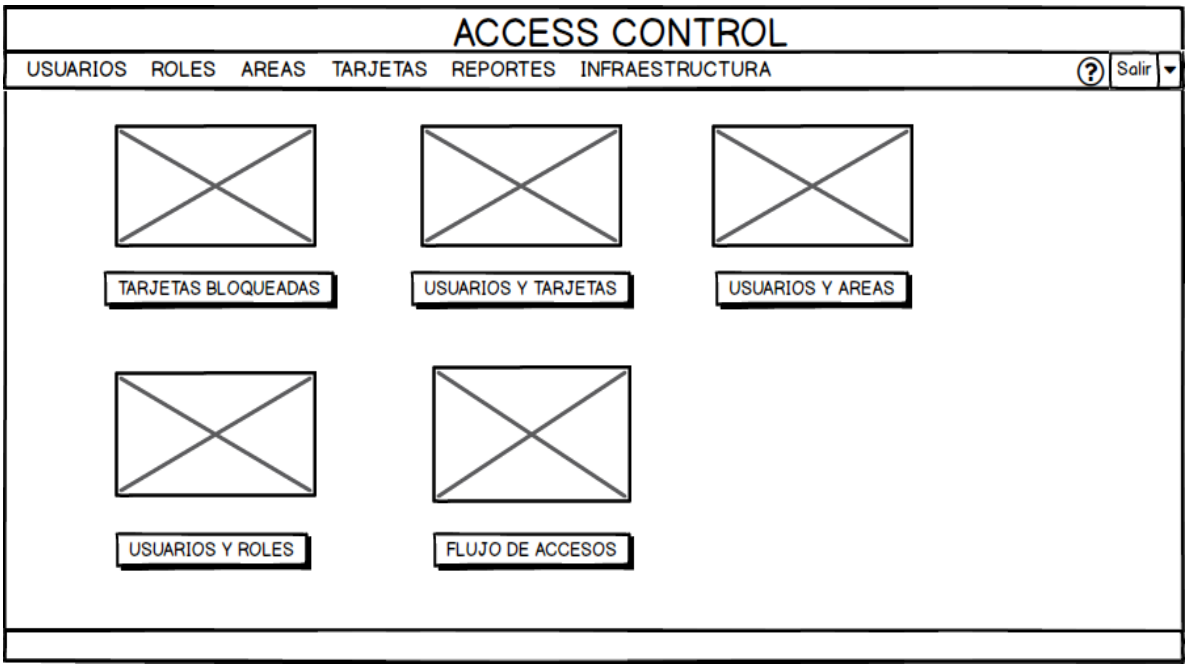
Pantalla Ver Tarjeta: En esta pantalla se podrá ver todos los datos de una tarjeta registrada en el Sistema.



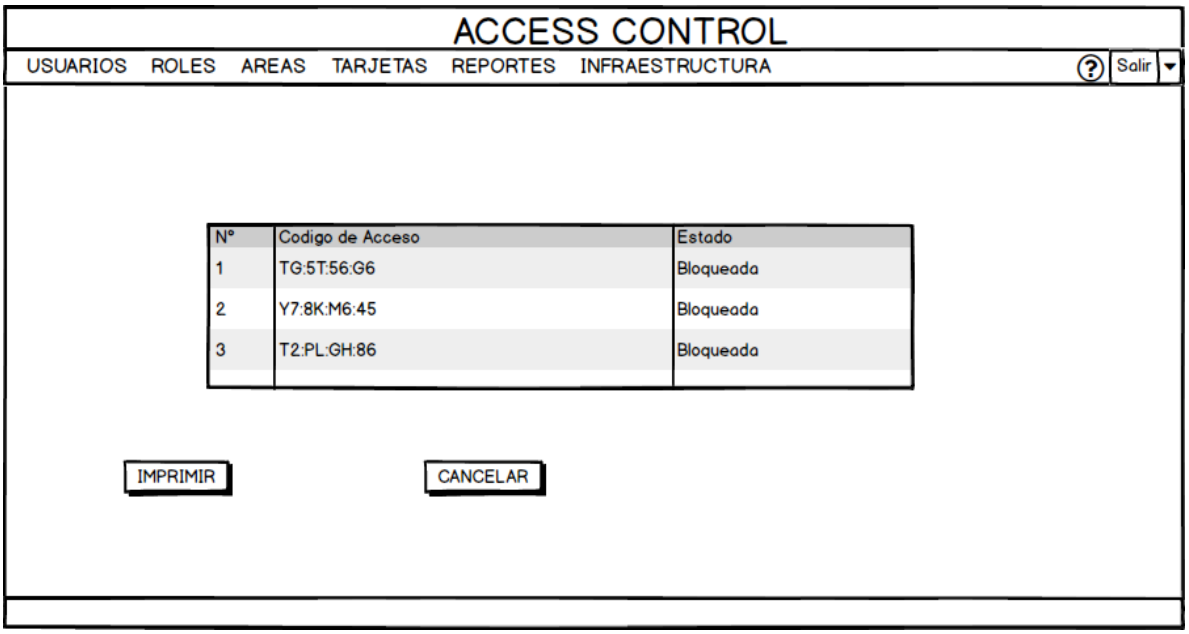
Pantalla Bloquear Tarjeta: En esta pantalla se podrá realizar la confirmación para poder bloquear una tarjeta del Sistema.



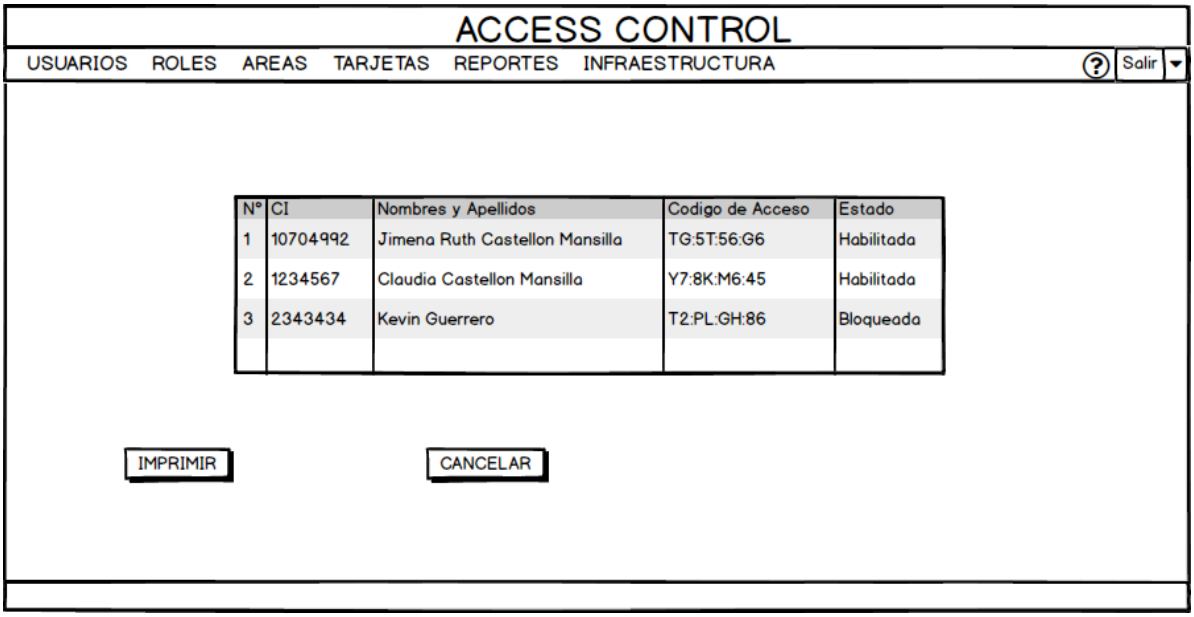
Pantalla Reportes: En esta pantalla podemos observar las opciones que nos da la Gestión de Reportes como: Reporte Tarjetas Bloqueadas, Usuarios Tarjetas, Flujo de Accesos.



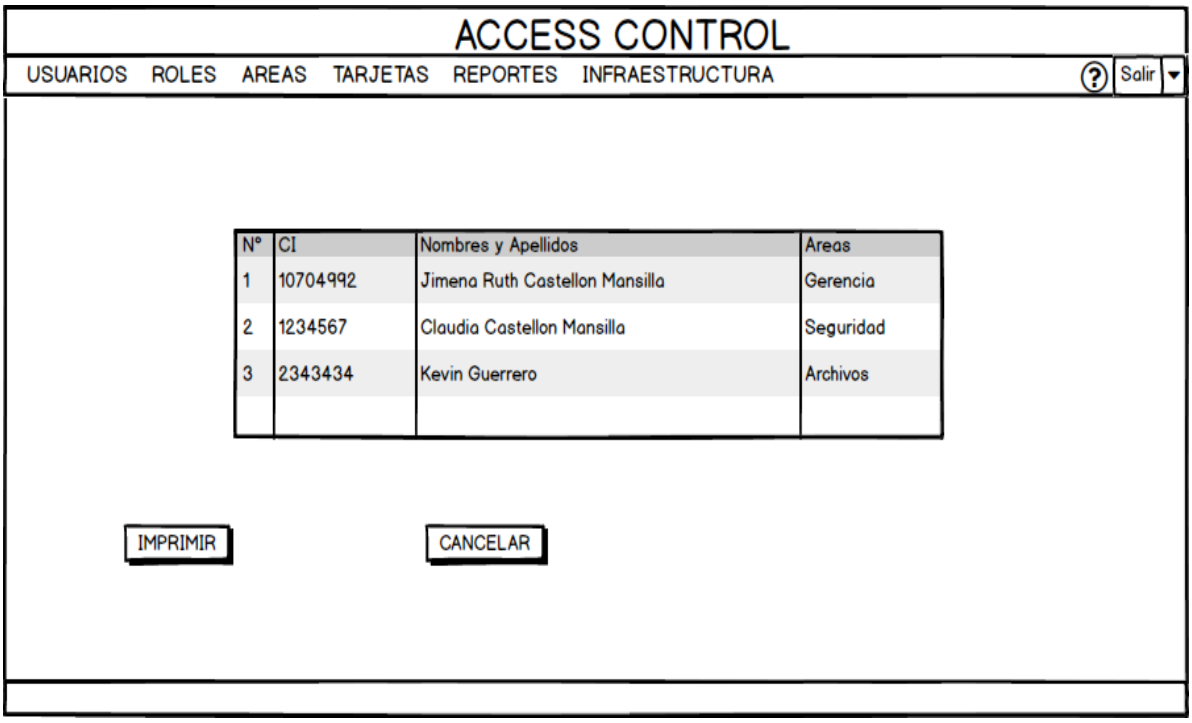
Pantalla Reporte Tarjetas Bloqueadas: En esta pantalla podremos obtener un reporte de todas las tarjetas que han sido bloqueadas por el Sistema y a que usuario le pertenecen.



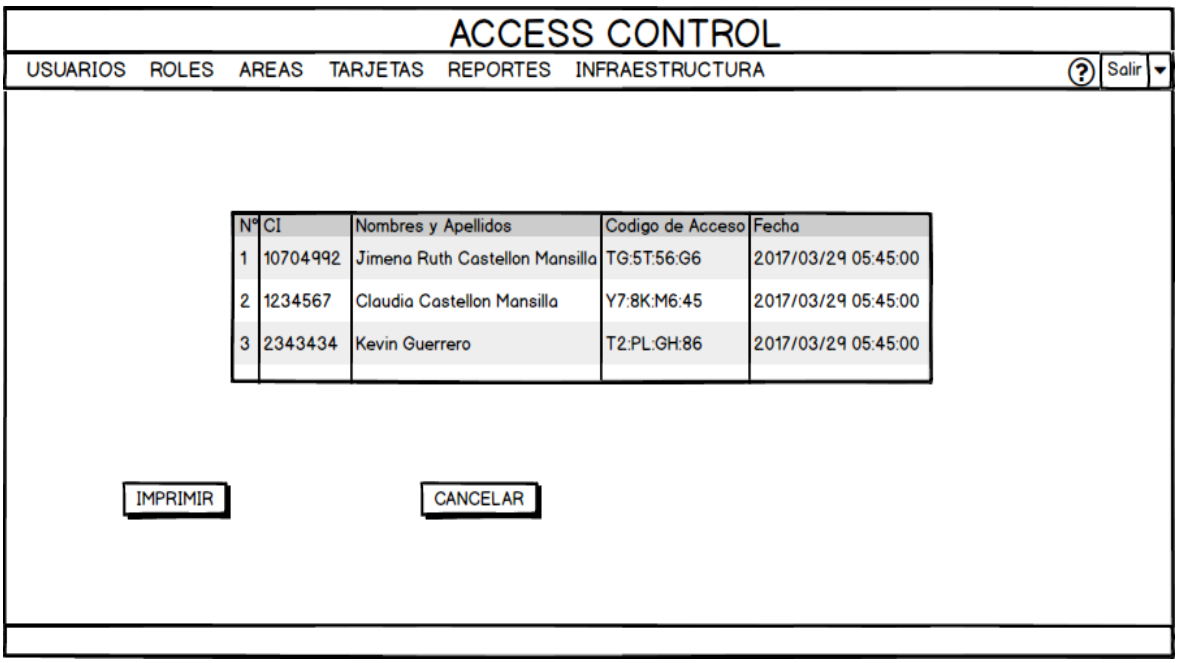
Pantalla Reporte Usuarios y Tarjetas: En esta pantalla podremos obtener un reporte de los usuarios y todas las tarjetas que se le fueron debidamente asignadas por el Sistema.



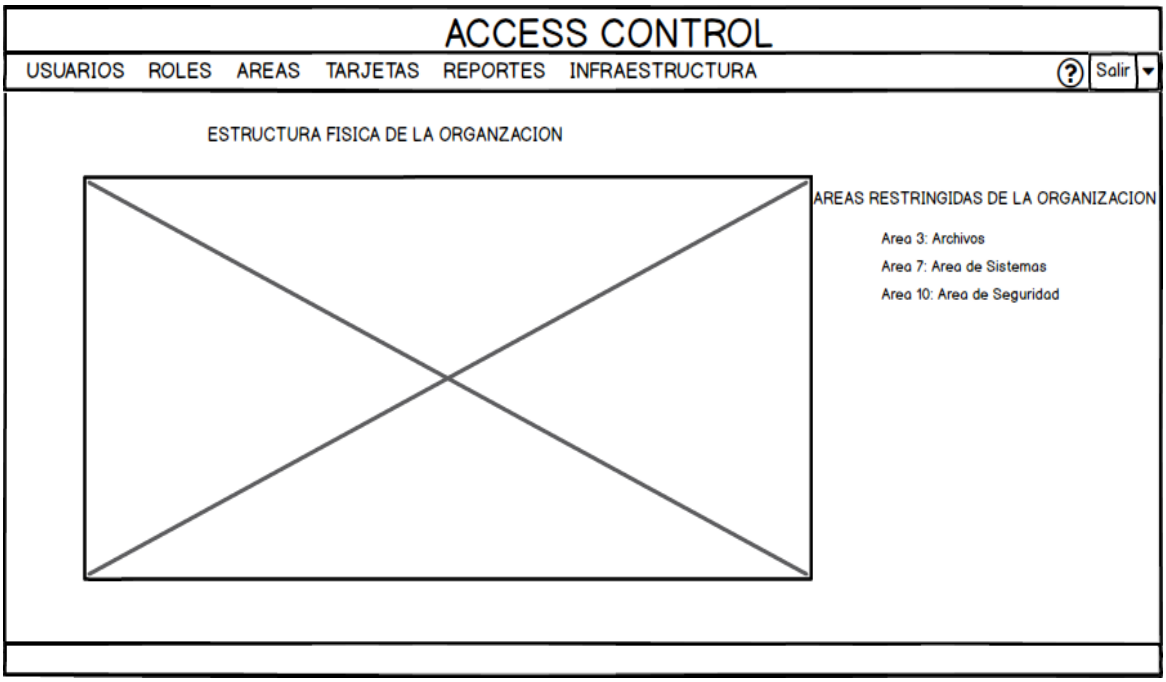
Pantalla Reporte Usuarios Áreas: En esta pantalla podemos ver detalladamente los usuarios y sus debidamente asignadas áreas según su rol en el sistema.



Pantalla Reporte Flujo de Datos: En esta pantalla se podrá ver detalladamente el usuario y las fechas y horas en las que paso por el lector la tarjeta asignada al usuario.



Pantalla Infraestructura: En esta pantalla se podrá ver un poco más detalladamente cómo son las distintas áreas restringidas de la Organización.



16. MODELO DE DIAGRAMA DE COMPONENTES

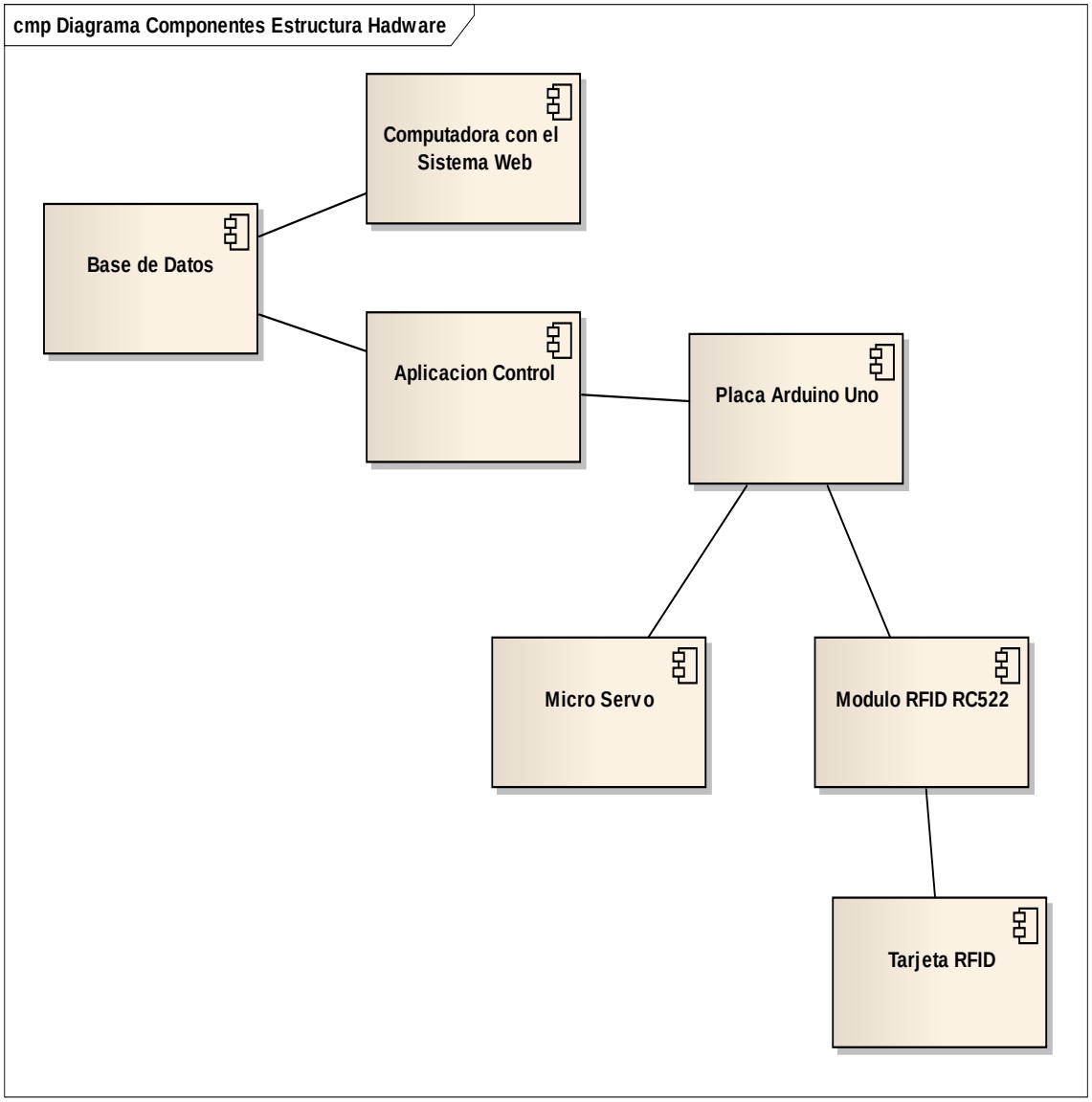


Diagrama de Componentes: Menú Principal

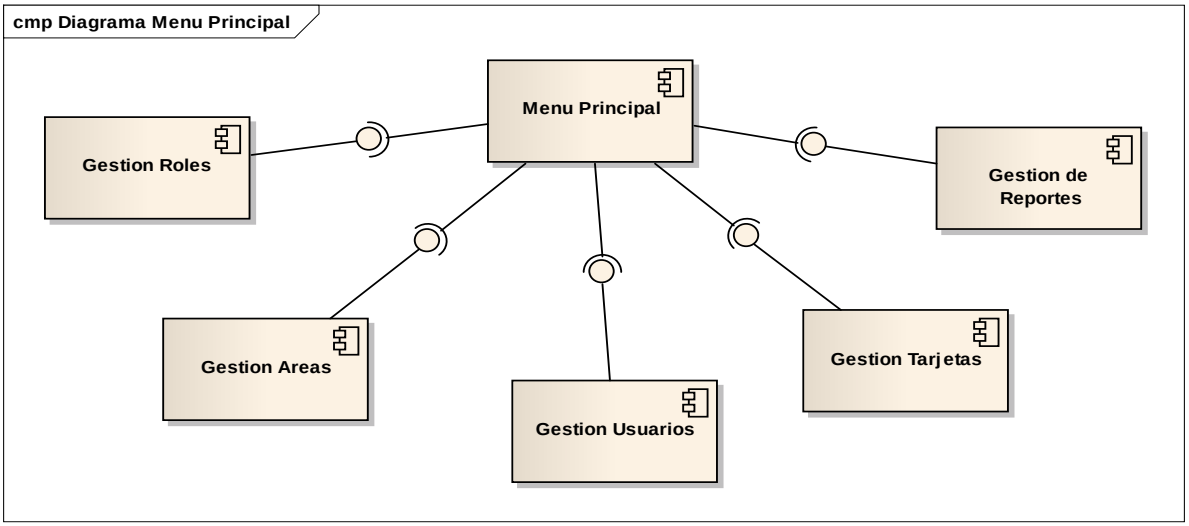


Diagrama de Componentes: Ingreso al Sistema

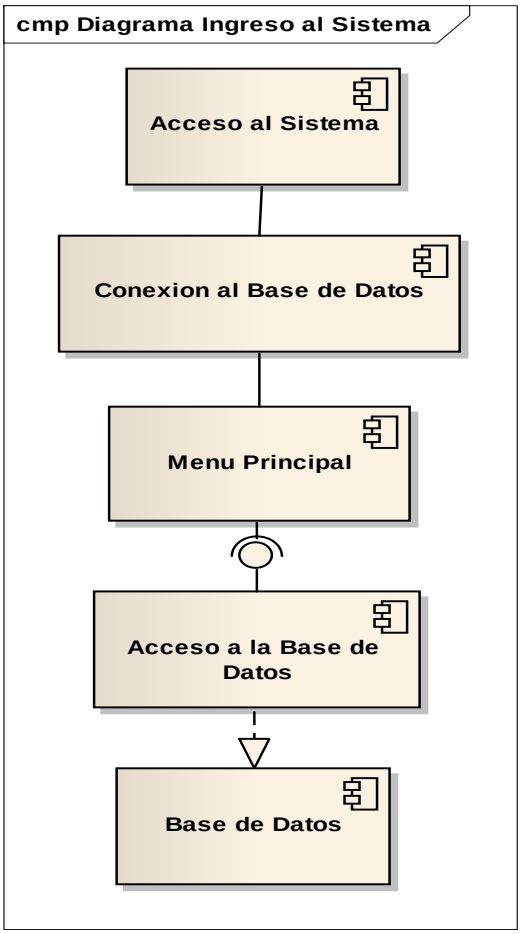


Diagrama de Componentes:

Gestión de Usuarios

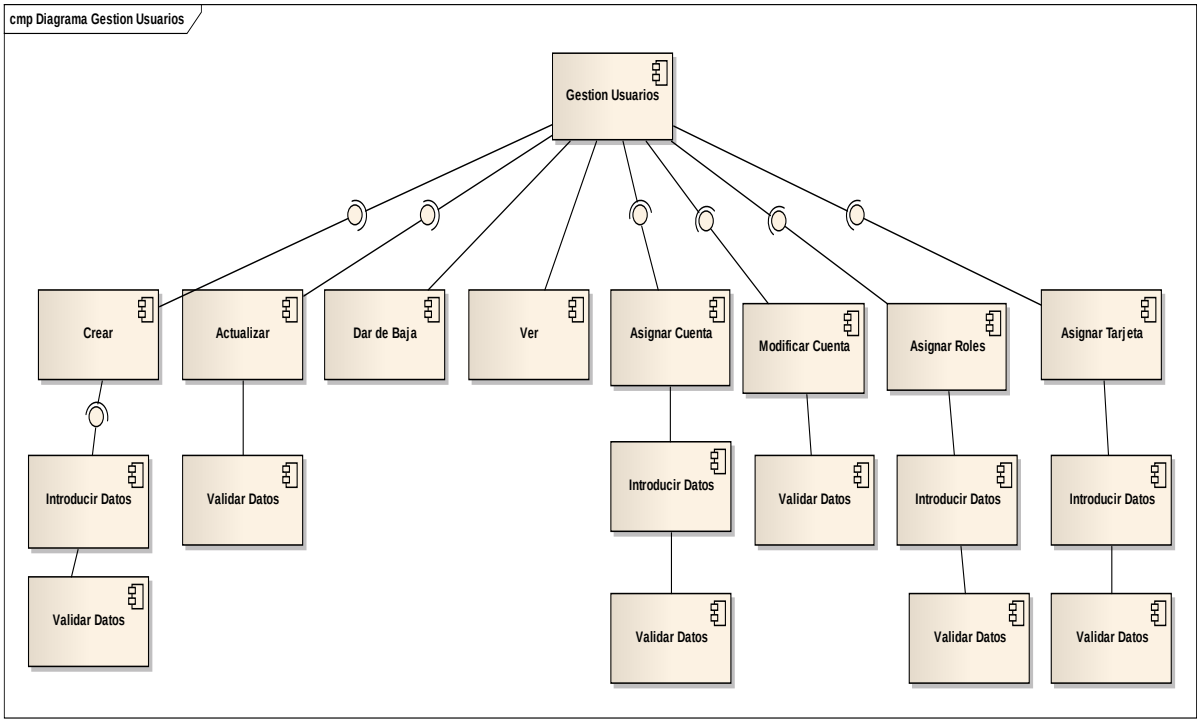


Diagrama de Componentes: Gestión Roles

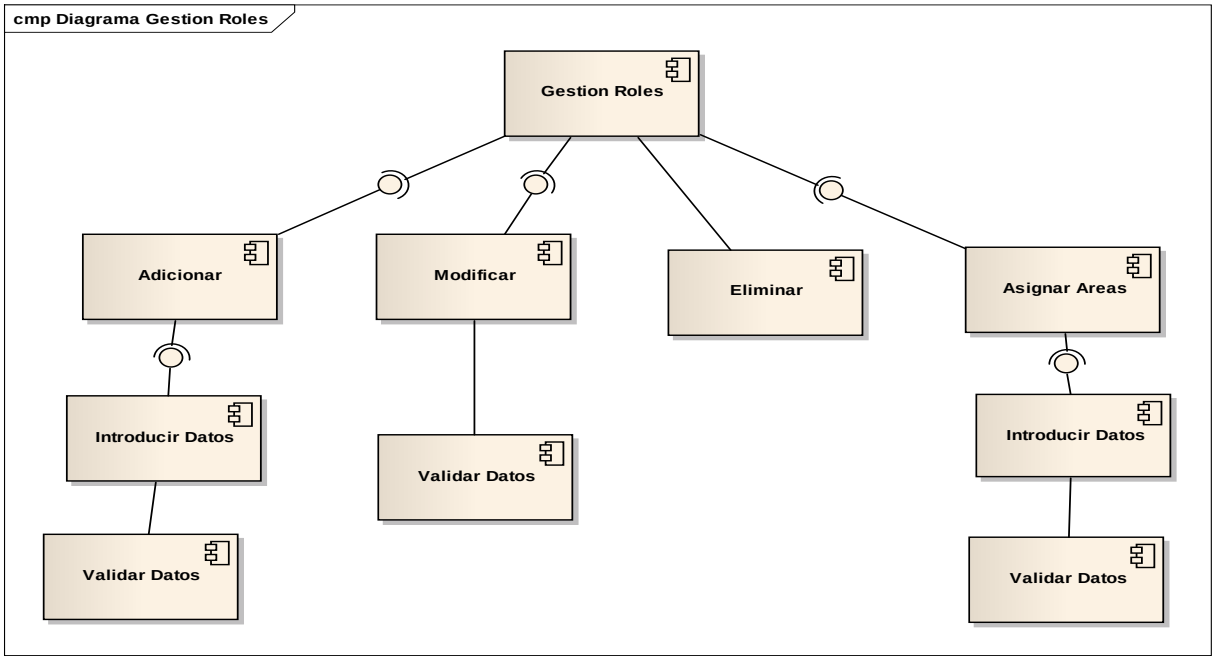


Diagrama de Componentes: Gestión Áreas

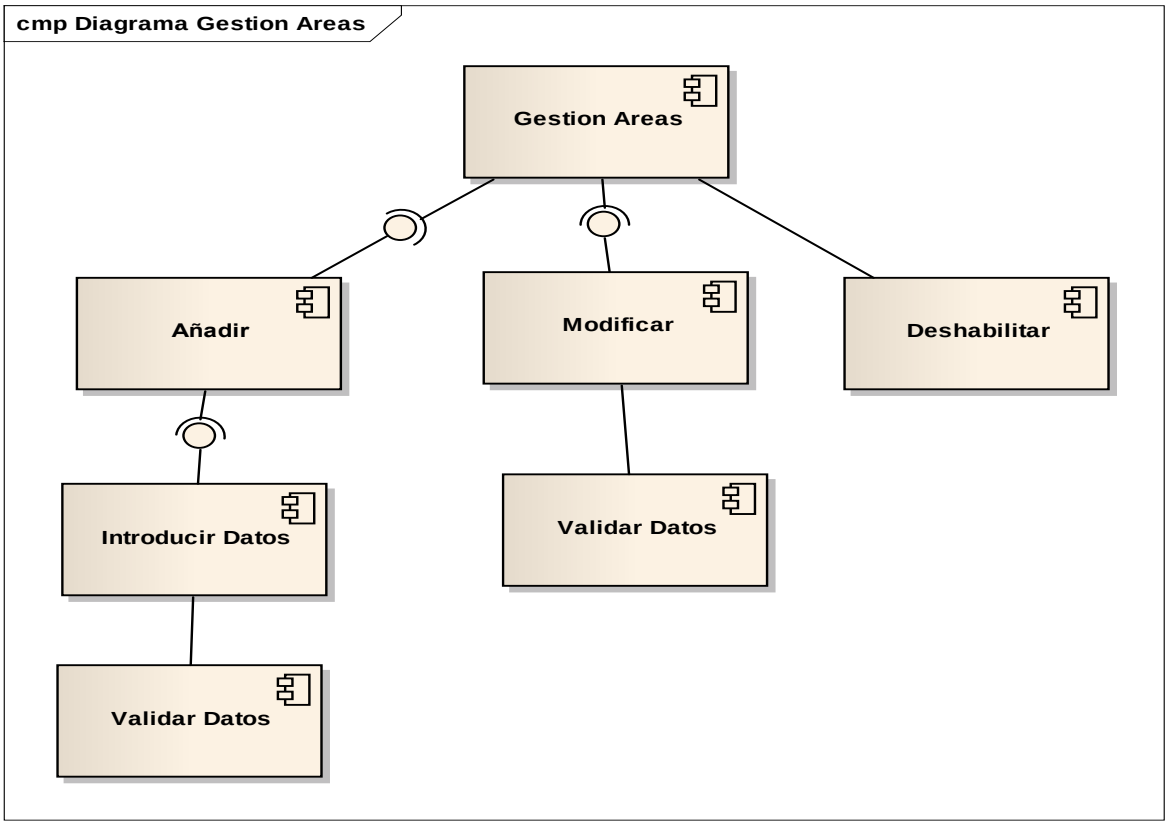
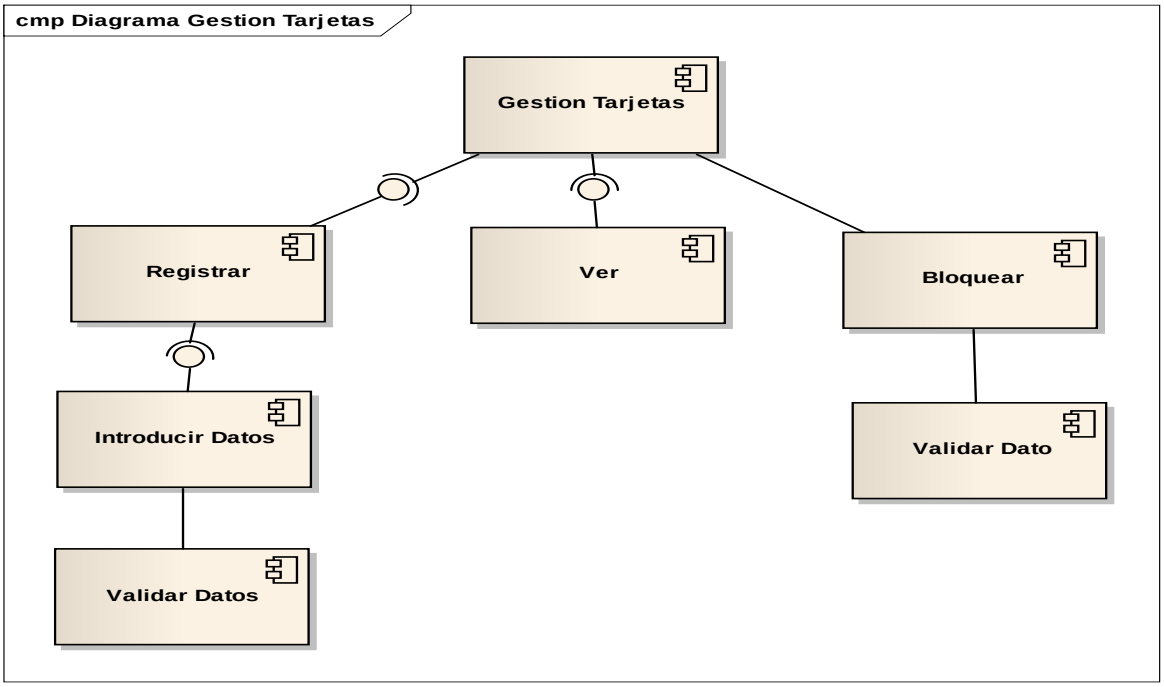


Diagrama de Componentes: Gestión Tarjetas



PRUEBAS DE CAJA NEGRA

INICIO SESION

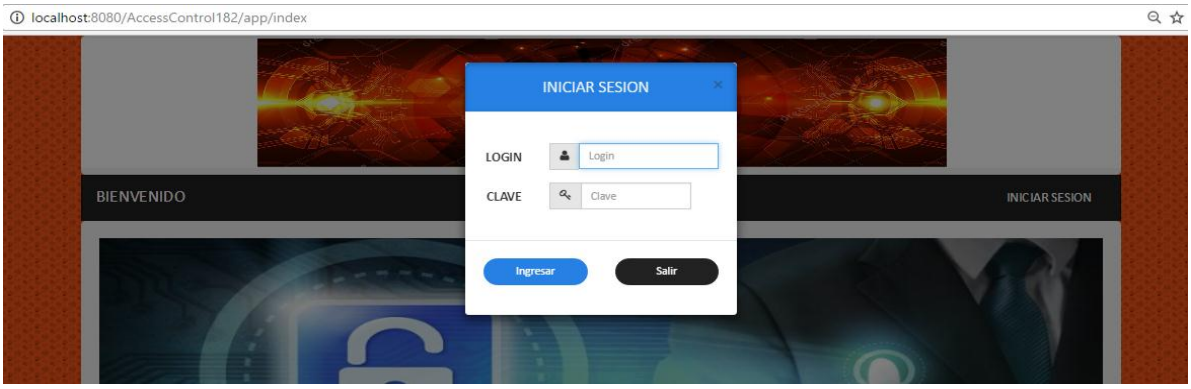


TABLA DE EQUIVALENCIA

Condición de entrada	Tipo	Clase de Equivalencia Válida	Clase de Equivalencia no Válida
Login	Valor Especifico	1: Valores entre caracteres y números de máximo 20 dígitos	2: Espacio en blanco 3: Solo valores numéricos negativos
Clave	Valor Especifico	4: Valores entre caracteres y números de máximo 20 dígitos	5: Espacio en blanco 6: Valores que sobre pasen los 20 dígitos

CASOS DE PRUEBA

Nº	Clase de Equivalencia	Propósito del caso	Dato de prueba	Mensaje
1	Valores entre caracteres y números de máximo 20 dígitos	Valor ingresado es correcto	JimenaCas2794	
2	Espacio en blanco	Valor ingresado	“ ”	Error: Dato incorrecto
3	Solo valores numéricos negativos	Valor ingresado	-854711226	Error: Dato incorrecto
4	Valores entre caracteres y números de	Valor ingresado es correcto	Familia12345	

	máximo 20 dígitos			
5	Espacio en blanco	Valor ingresado	“ ”	Error: Dato incorrecto
6	Valores que sobre pasen los 20 dígitos	Valor ingresado	Gsdygyigsyigdgysgdygdg sddsbdsbdbhggg	Error: Dato incorrecto

MODULO USUARIOS

Crear Usuario

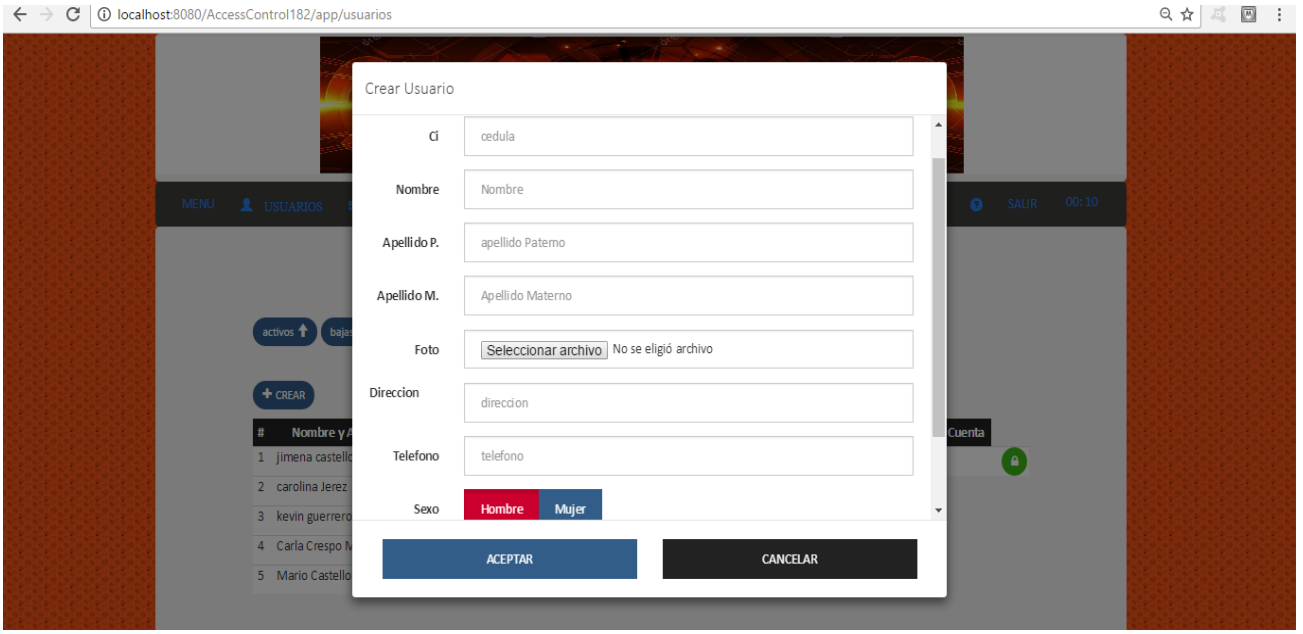


TABLA DE EQUIVALENCIA

Condición de entrada	Tipo	Clase de Equivalencia Válida	Clase de Equivalencia no Válida
CI	Valor Especifico	1: Valor numérico de 8 dígitos más un carácter	2: Espacio en blanco 3: Solo valores numéricos negativos
Nombre	Valor Especifico	4: Cadena de caracteres (alfanuméricos) de 20 posiciones	5: Valor numérico 6: Espacio en blanco
Apellido P	Valor Especifico	7: Cadena de caracteres	8: Valor numérico 9: Cadena de Caracteres

		(alfanuméricos) de 20 posiciones	de más de 20 posiciones.
Apellido M	Valor Especifico	10: Cadena de caracteres (alfanuméricos) de 20 posiciones	11: Valor numérico 12: Cadena de Caracteres de más de 20 posiciones.
Dirección	Valor Especifico	13: Cadena de caracteres (alfanuméricos) de 30 posiciones	14: Valor numérico 15: Espacio en blanco
Teléfono	Numérico	16: Valor numérico de 8 dígitos	17: Cadena de caracteres (alfanuméricos) 18: Valor numérico mayor a 8 dígitos
Sexo	Conjunto	19: Valor de un solo carácter.	20:Espacion en blanco

CASOS DE PRUEBA

Nº	**Clase de Equivalencia**	**Propósito del caso**	**Dato de prueba**	**Mensaje**
1	Valor numérico de 8 dígitos más un carácter	Valor ingresado es correcto	10661124J	
2	Espacio en blanco	Valor ingresado	“ ”	Error: Dato incorrecto
3	Solo valores numéricos negativos	Valor ingresado	-58741126	Error: Dato incorrecto
4	Cadena de caracteres (alfanuméricos) de 20 posiciones	Valor ingresado es correcto	Fernando	
5	Valor numérico	Valor ingresado	484848770111	Error: Dato incorrecto
6	Espacio en blanco	Valor ingresado	“ ”	Error: Dato incorrecto
7	Cadena de caracteres (alfanuméricos) de 20 posiciones	Valor ingresado es correcto	De la huerta	
8	Valor numérico	Valor ingresado	1154887752	Error: Dato incorrecto

9	Cadena de Caracteres de más de 20 posiciones.	Valor ingresado	Ahsuhduhdahhdsaiuh asdhdahdhshshahdhd	Error: Dato incorrecto
10	Cadena de caracteres (alfanuméricos) de 20 posiciones	Valor ingresado es correcto	gutierrez	
11	Valor numérico	Valor ingresado	1548777722	Error: Dato incorrecto
12	Cadena de Caracteres de más de 20 posiciones.	Valor ingresado	Ahsgygydagygdgaydg adsuuhduhahhhhuhu	Error: Dato incorrecto
13	Cadena de caracteres (alfanuméricos) de 30 posiciones	Valor ingresado es correcto	Calle Madrid entre Ballivian y ramón rojas	
14	Valor numérico	Valor ingresado	587874846454448	Error: Dato incorrecto
15	Espacio en blanco	Valor ingresado	“ ”	Error: Dato incorrecto
16	Valor numérico de 8 dígitos	Valor ingresado es correcto	78895422	
17	Cadena de caracteres (alfanuméricos)	Valor ingresado	uhasuhusdhshhasu	Error: Dato incorrecto
18	Valor numérico mayor a 8 dígitos	Valor ingresado	755898552	Error: Dato incorrecto
19	Valor de un solo carácter.	Valor ingresado	F	
20	Espacio en blanco	Valor ingresado	“ ”	Error: Dato incorrecto

Asignar Roles

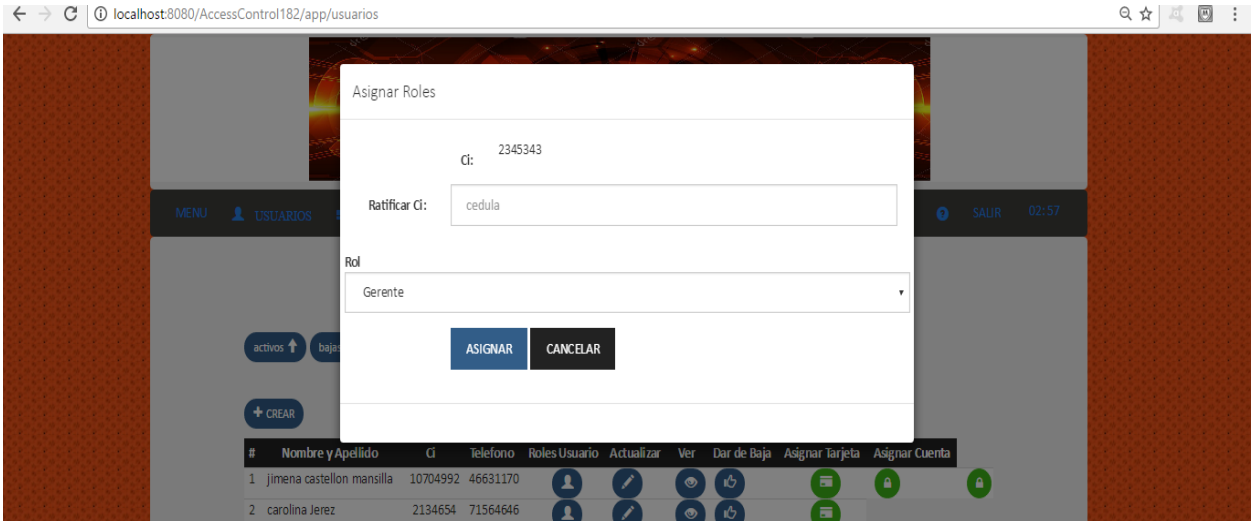


TABLA DE EQUIVALENCIA

Condición de entrada	**Tipo**	**Clase de Equivalencia Válida**	**Clase de Equivalencia no Válida**
Ci	Valor Especifico	1:Valor numérico de máximo 8 dígitos	2: Cadena de caracteres (alfanuméricos) 3:Numeros Negativos
Rol	Miembro de un Conjunto	4: Cadena de caracteres (alfanuméricos) de 5 posiciones	5: Valor numérico

CASOS DE PRUEBA

Nº	**Clase de Equivalencia**	**Propósito del caso**	**Dato de prueba**	**Mensaje**
1	Valor numérico de máximo 8 dígitos	Valor ingresado es correcto	8547997	
2	Cadena de caracteres (alfanuméricos)	Valor ingresado	fdhhyhthccz	Error: Dato incorrecto
3	Números Negativos	Valor ingresado	-85744159	Error: Dato incorrecto
4	Cadena de caracteres (alfanuméricos) de 5 posiciones	Valor ingresado es correcto	Gerente	
5	Valor Numérico	Valor	25588774411558	Error: Dato

		ingresado		incorrecto

Asignar Cuenta

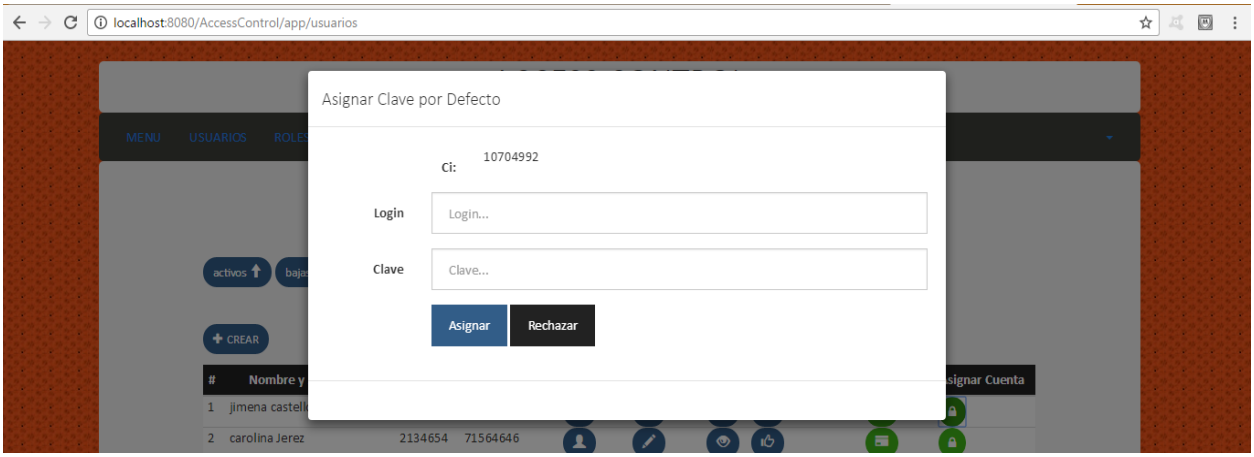


TABLA DE EQUIVALENCIA

Condición de entrada	**Tipo**	**Clase de Equivalencia Válida**	**Clase de Equivalencia no Válida**
Ci	Valor Especifico	1:Valor numérico de máximo 8 dígitos	2Espacio en blanco 3:Numeros Negativos
Login	Valor Especifico	4: Valores entre caracteres y números de máximo 20 dígitos	5: Espacio en blanco 6: Solo valores numéricos negativos
Clave	Valor Especifico	7: Valores entre caracteres y números de máximo 20 dígitos	8: Espacio en blanco 9: Valores que sobre pasen los 20 dígitos

CASOS DE PRUEBA

Nº	**Clase de Equivalencia**	**Propósito del caso**	**Dato de prueba**	**Mensaje**
1	Valor numérico de máximo 8 dígitos	Valor ingresado es correcto	10661124J	
2	Espacio en Blanco	Valor ingresado es correcto	“ ”	Error: Dato incorrecto

3	Números Negativos	Valor ingresado es correcto	-546546564	Error: Dato incorrecto
4	Valores entre caracteres y números de máximo 20 dígitos	Valor ingresado es correcto	JimenaCas2794	
5	Espacio en blanco	Valor ingresado	“ ”	Error: Dato incorrecto
6	Solo valores numéricos negativos	Valor ingresado	-854711226	Error: Dato incorrecto
7	Valores entre caracteres y números de máximo 20 dígitos	Valor ingresado es correcto	Familia12345	
8	Espacio en blanco	Valor ingresado	“ ”	Error: Dato incorrecto
9	Valores que sobre pasen los 20 dígitos	Valor ingresado	Gsdygyigsyigdgysgdygdgsddsbdsbdbhggg	Error: Dato incorrecto

Asignar Tarjeta

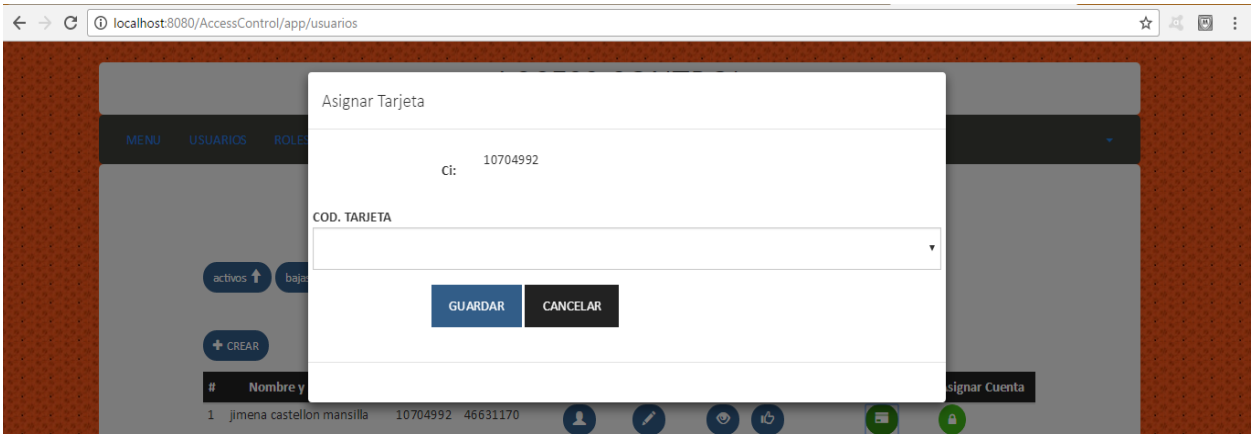


TABLA DE EQUIVALENCIA

Condición de	Tipo	Clase de	Clase de Equivalencia

entrada		Equivalencia Válida	no Válida
Ci	Valor Especifico	1:Valor numérico de máximo 8 dígitos	2: Cadena de caracteres (alfanuméricos) 3:Numeros Negativos
Tarjeta	Miembro de un Conjunto	4: Cadena de caracteres (alfanuméricos) de 20 posiciones	5: Sin Selecionar

CASOS DE PRUEBA

Nº	Clase de Equivalencia	Propósito del caso	Dato de prueba	Mensaje
1	Valor numérico de máximo 8 dígitos	Valor ingresado es correcto	8547997	
2	Cadena de caracteres (alfanuméricos)	Valor ingresado	fdhhyhthccz	Error: Dato incorrecto
3	Números Negativos	Valor ingresado	-85744159	Error: Dato incorrecto
4	Cadena de caracteres (alfanuméricos) de 5 posiciones	Valor ingresado es correcto	FR:56:H7:0K	
5	Sin Seleccionar	Valor ingresado		Error: Dato incorrecto

MODULO ROLES

Adicionar Rol

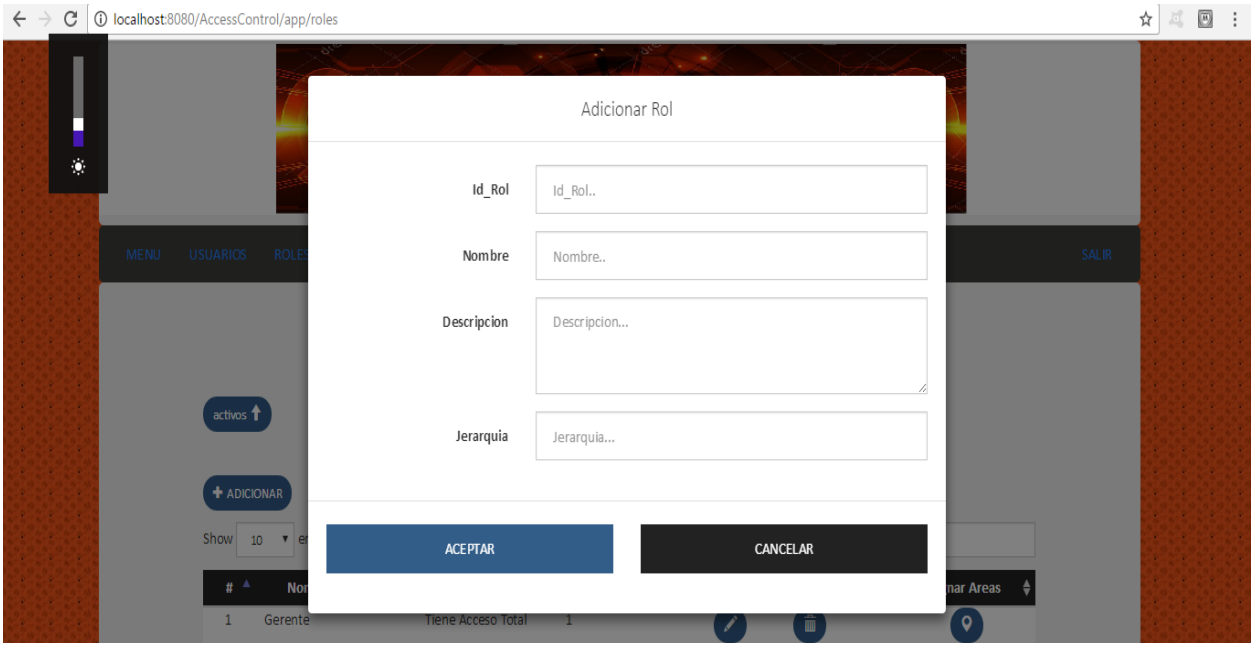


TABLA DE EQUIVALENCIA

Condición de entrada	Tipo	Clase de Equivalencia Válida	Clase de Equivalencia no Válida
ID_Rol	Numérico	1: Valor numérico de máximo 4 dígitos	2: Cadena de caracteres (alfanuméricos) 3: Números Negativos
Nombre	Valor Especifico	4: Cadena de caracteres (alfanuméricos) de 15 posiciones	5: Valor numérico 6: Espacio en blanco
Descripción	Valor Especifico	7: Cadena de caracteres (alfanuméricos) de 30 posiciones	8: Cadena de Caracteres de más de 30 posiciones. 9: Copia de imagen
Jerarquía	Numérico Especifico	10: Valor numérico de un solo digito	11: Números Negativos 12: Espacio en blanco

CASOS DE PRUEBA

Nº	Clase de Equivalencia	Propósito del caso	Dato de prueba	Mensaje
1	Valor numérico de máximo 4 dígitos	Valor ingresado es correcto	154	
2	Cadena de caracteres (alfanuméricos)	Valor ingresado	agdgyagdyiiss	Error: Dato incorrecto
3	Números Negativos	Valor ingresado	-48751148	Error: Dato incorrecto
4	Cadena de caracteres (alfanuméricos) de 15 posiciones	Valor ingresado es correcto	Secretaria	
5	Valor Numérico	Valor ingresado	5588744112545	Error: Dato incorrecto
6	Espacio en blanco	Valor ingresado	“ ”	Error: Dato incorrecto
7	Cadena de caracteres (alfanuméricos) de 30 posiciones	Valor ingresado es correcto	Encargado de gestionar los archivos de la organización	
8	Cadena de Caracteres de más de 30 posiciones.	Valor ingresado	Uahdhahdhuagdguggagg Ahhuhhdhasodho	Error: Dato incorrecto
9	Copia de imagen	Valor ingresado	#@##@###	Error: Dato incorrecto
10	Valor numérico de un solo digito	Valor ingresado es correcto	1	
11	Números Negativos	Valor ingresado	-4887551221	Error: Dato incorrecto
12	Espacio en blanco	Valor ingresado	“ ”	Error: Dato incorrecto

MODULO AREAS

Añadir Área

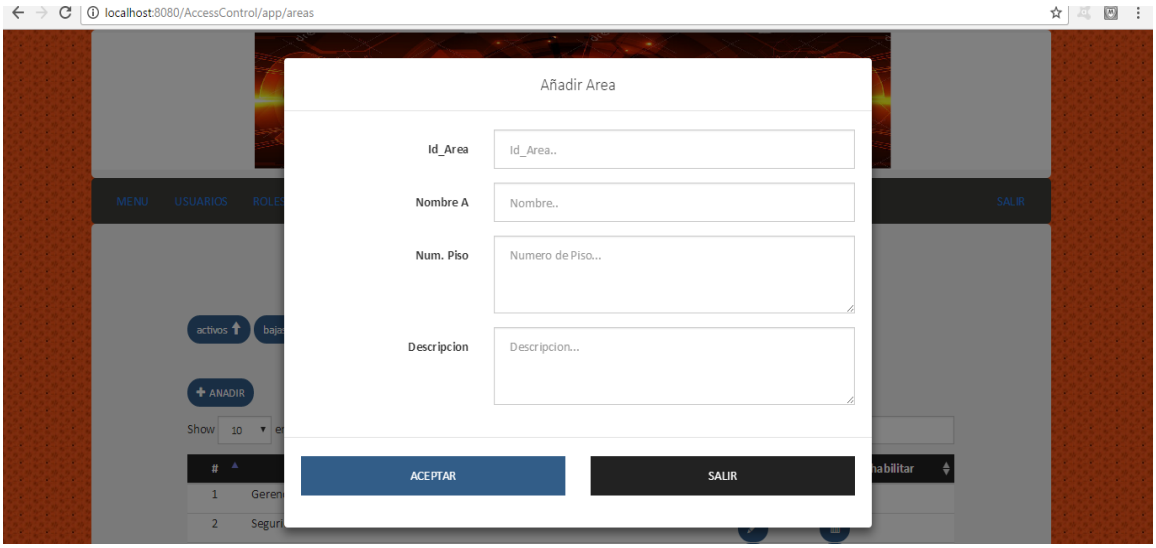


TABLA DE EQUIVALENCIA

Condición de entrada	Tipo	Clase de Equivalencia Válida	Clase de Equivalencia no Válida
ID_Area	Valor	1:Valor numérico de máximo 8 dígitos	2: Cadena de caracteres (alfanuméricos) 3:Numeros Negativos
Nombre_A	Conjunto	4: Cadena de caracteres (alfanuméricos) de 5 posiciones	5: Valor numérico 6: Espacio en blanco
Núm. Piso	Valor	7: Valor numérico de máximo 2 dígitos	8: Cadena de caracteres (alfanuméricos) 9: Valores Negativos
Descripción	Conjunto	10: Cadena de caracteres (alfanuméricos) de 30 posiciones	11: Cadena de Caracteres de más de 30 posiciones. 12: Copia de imagen

CASOS DE PRUEBA

Nº	Clase de Equivalencia	Propósito del caso	Dato de prueba	Mensaje
1	Valor numérico de máximo 8 dígitos	Valor ingresado es correcto	8547997	
2	Cadena de caracteres (alfanuméricos)	Valor ingresado	fdhhyhthccz	Error: Dato incorrecto
3	Números Negativos	Valor ingresado	-85744159	Error: Dato incorrecto
4	Cadena de caracteres (alfanuméricos) de 5 posiciones	Valor ingresado es correcto	jacob	
5	Valor Numérico	Valor ingresado	25588774411558	Error: Dato incorrecto
6	Espacio en blanco	Valor ingresado	“ ”	Error: Dato incorrecto
7	Valor numérico de máximo 2 dígitos	Valor ingresado es correcto	2	
8	Cadena de caracteres (alfanuméricos)	Valor ingresado	asdggaydgyg	Error: Dato incorrecto
9	Valores Negativos	Valor ingresado	-487759	Error: Dato incorrecto
10	Cadena de caracteres (alfanuméricos) de 30 posiciones	Valor ingresado es correcto	Ambiente solo designado solo para archivos	
11	Cadena de Caracteres de más de 30 posiciones.	Valor ingresado	Asdbhbhbabdhabhhuhdusndshdushudhushudh	Error: Dato incorrecto
12	Copia de imagen	Valor ingresado	#@##@###	Error: Dato incorrecto

MODULO TARJETAS

Registrar Tarjeta

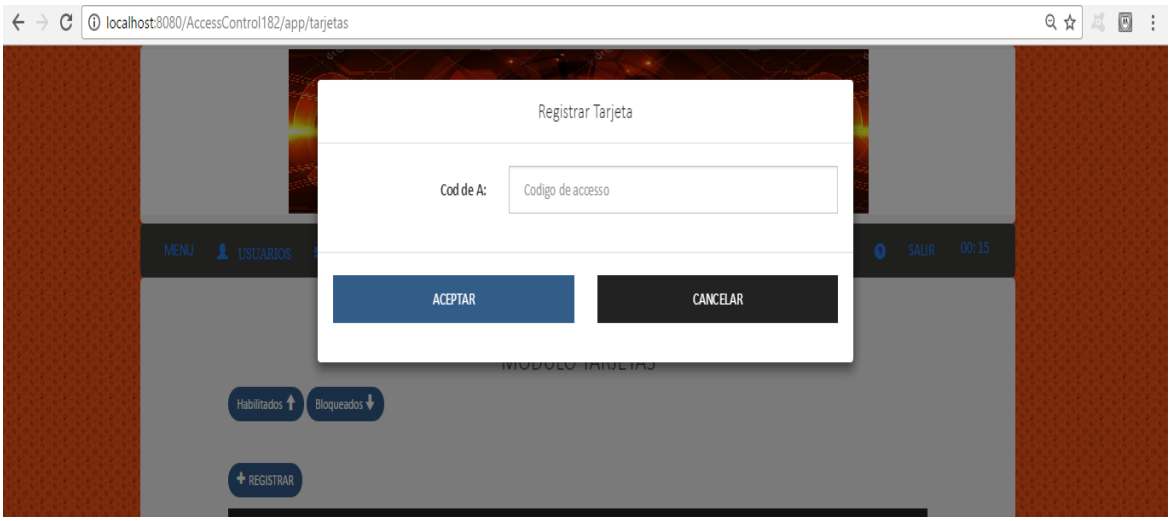


TABLA DE EQUIVALENCIA

Condición de entrada	Tipo	Clase de Equivalencia Válida	Clase de Equivalencia no Válida
Cod_da	Valor Especifico	1:Valor Alfanumérico de máximo 20 dígitos	2: Valor Numérico 3:Espacio en Blanco

CASOS DE PRUEBA

Nº	Clase de Equivalencia	Propósito del caso	Dato de prueba	Mensaje
1	Valor Alfanumérico de máximo 20 dígitos	Valor ingresado es correcto	F5:GH:J7:56	
2	Valor Numérico	Valor ingresado	244545345	Error: Dato incorrecto
3	Espacio en Blanco	Valor ingresado	“ “	Error: Dato incorrecto

TALLER DE SOCIALIZACION

Índice

II.3.1 Introducción

II.3.2 Objetivo General del Taller de Socialización

II.3.3 Objetivos Específicos

II.3.4 Justificación

II.3.5 Desarrollo de Socialización

II.3.6 Medios de Verificación Anexos del Componentes

INFORME TALLER DE SOCIALIZACION DE PROYECTO:

CONTROL DE ACCESOS DE PERSONAL A AREAS RESTRINGIDAS DE UNA ORGANIZACIÓN MEJORADO ATRAVES DE LAS TIC

I. INTRODUCCION

En la actualidad la existencia de PYMES y MYPES ha crecido de sobre manera en Bolivia ya que este tipo de emprendimientos nacieron de gente con pocos recursos para invertir en crear grandes empresas, pero con grandes ideas de productos.

De acuerdo a un diagnóstico sobre la situación empresarial, 9 de cada 10 empresas son consideradas de la Pequeña y Micro Empresa (Pymes), responsables del 50 por ciento de la economía nacional; sin embargo, el 80% muere antes de cumplir su primer año.

Ahora según estudios referenciales se llegó a la conclusión que el 87% de las pequeñas y medianas empresas (pymes) en Bolivia está en la necesidad y la búsqueda de tecnología que las ayude a crecer y mejorar sus gestiones en el mercado, ya sea en el comercio, industria o servicios, pero solo el 30% de las mismas la adquiere. Asimismo, según este estudio, el 31% de estas empresas utilizan tecnología, en el marco de cuatro situaciones que se busca solucionar: Las que están satisfechas con la solución actual (15%); las que buscan mejorar (45%); las que tienen problemas con la solución actual y buscan sistemas globales (37%); y las que utilizan sistemas globalizados (3%).

II. OBJETIVO GENERAL DEL TALLER DE SOCIALIZACION

El taller de socialización del Proyecto de grado tendrá como objetivo

Socializar y promocionar dos componentes principales que forman parte del Proyecto "Control de Acceso de Personal a Áreas Restringidas de una Organización", para que la sociedad en general pueda conocer el uso de las Tics en esta área.

III. OBJETIVOS ESPECIFICOS

1.- Dar a conocer un modelo de normas, restricciones y procedimientos que puede ser adaptado para cualquier tipo de Empresa u Organización.

2.- Dar a conocer parte del Sistema Informático que está siendo desarrollado el cual está siendo orientado a la Seguridad de los ambientes de una Organización a la cual puede ser adaptado fácilmente.

3.- Promocionar la tecnología innovadora que se está utilizando en Proyecto como es la tecnología RFID (identificación de radio frecuencia)

4.- Impulsar a la juventud emprendedora a hacer el uso de este tipo de sistema informático de seguridad en sus PYMES (Micro Empresas).

5.- Dar a conocer una tecnología eficiente y económica que se utilizara en el proyecto que se está socializando.

IV.- JUSTIFICACION

En la actualidad es poco el porcentaje de Pymes que tiene la posibilidad de poder adquirir la tecnología que necesitan para mejorar su Empresa ya que su economía no abastece para realizar este tipo de inversiones. En muchos casos se ven imposibilitados de poder hasta invertir en la seguridad de sus instalaciones lo cual es un aspecto muy importante puesto que es dichas instalaciones es donde se realizan todas las actividades comerciales o de servicio a la que se dedica dicha Pyme. Es bueno resaltar que es de gran importancia mantener un control del acceso del personal a distintas áreas que podrían ser consideradas como restringidas o dicho de otra manera a aquellas áreas donde solo puede ingresar personal autorizado.

Es por eso que al realizar esta socialización se presenta una alternativa más alcanzable económicamente para las Pymes en cuanto al tipo de tecnología que se utilizara en este proyecto es tecnología que se encuentra vigente además de ser eficiente para cumplir lo que requiere el cliente, utilizando tecnología moderna y economizando recursos al mismo tiempo.

V.- DESARROLLO DE SOCIALIZACION

El taller de Socialización del Proyecto Sistema de Control de Accesos de Personal a Áreas Restringidas en una Organización se basó en el siguiente programa en ejecución:

Fecha	**Tema**	**Tiempo de desarrollo**	**Preguntas**	**Tiempo de participación**
5/02/2016	**Conceptos centrales del Tema Seguridad Informática e introducción al Perfil del Proyecto**	**De 15:00 pm a 15:45pm**	**10 minutos**	
5/02/201	**Socialización de árbol de**	**De 16:00 pm a**	**10 minutos**	

6	**problemas**	**16:45pm**		
5//02/2016	**Retroalimentación de los objetivos específicos, alcances, descripción y fundamentación del proyecto.**	**De 17:00 pm a 17:45pm**	**10 minutos**	
5/02/2016	**Refrigerio**	**De 18:00 pm a 18:20 pm**		
5/02/2016	**Mesas de trabajo por grupos con temas a tratar: Seguridad de guardias, control de accesos a ciertas áreas, la aceptación de la nueva tecnología de seguridad en distintas Empresas u Organizaciones.**	**De 18:20pm a 19:20 pm**	**15 minutos**	
	Interacción de los asistentes con uno de los componentes del proyecto: El Sistema Informático que se está desarrollando	**De 19:20pm a 19:50**	**10min**	
	Mesas redonda general para compartir experiencias	**De 19:50 a 20:30**	**TOTAL**	**5:30 Hrs.**

En la primera parte se desarrolló una serie de conceptos básicos que permitan entender los temas centrales del proyecto como el control de accesos y su relación con la seguridad en una Empresa. Además de la importancia de la seguridad tanto física como lógica en la base de datos de un sistema.

En la segunda parte se desarrolló la presentación del perfil del proyecto realizando la socialización del árbol de problemas y posteriormente la retroalimentación de los objetivos especificación, gracias al árbol de objetivos existente en el perfil del proyecto, los alcances, la descripción y fundamentación del proyecto

En la tercera parte se formó mesas de trabajo por grupos de 6 miembros para que puedan tocar temas relacionados con el proyecto como Seguridad física de guardias en una Empresa u Organización, formas de controlar el acceso de solo personal autorizado a ciertas áreas, La aceptación en inversión de las Empresas en seguridad a través de las nuevas Tecnologías. ¿Cuán dispuestas estas distintas Empresas u Organizaciones a invertir en seguridad? Fue una de las cuestiones más utilizadas.

Finalmente, en la cuarta parte se comenzó dando paso a que los asistentes interactuaran con cierta parte del Sistema Informático que está siendo desarrollado para el proyecto.

Esto se hizo con la intención de que la interfaz del Sistema Informático llamase bastante la atención de los asistentes.

Nombre de la organización donde se realizó la replica	**Total de número de alumnos asistentes**	**N° de hombres**	**N° de mujeres**
	25	**12**	**13**

Cabe resaltar que la participación de los asistentes fue muy activa ya que la se notó un interés positivo hacia el tema del proyecto que se estaba socializando con un importante rol de preguntas y cuestionamientos además de cierta curiosidad de parte de los asistentes, cumpliendo de esta manera con los objetivos de la actividad.

VI. ANEXOS

MESAS REDONDAS

Los asistentes al Taller tuvieron la oportunidad de interactuar un poco con parte del sistema en desarrollo.

MODELO DE CERTIFICADOS OTORGADOS EN EL TALLER DE SOCIALIZACION

CAPITULO III
CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

- El proyecto "Sistema de Control de acceso de personal a áreas restringidas de una Organización" tiene como objetivo general: Mejorar el control seguro y eficiente del Personal a áreas restringidas de una Organización mediante la utilización de nuevas TIC, a costos accesibles en el corto plazo.

- Como resultado de la mejora del control de acceso que se hizo he concluido que la utilización de la tecnología Arduino en conjunto con el Modulo lector RC522 o lector de tarjetas RFID (radio frecuencia) resulta económicamente más accesible a comparación de tecnología actuales como los lectores de huellas digitales o los biométricos faciales que actualmente también son utilizados en sistemas de control de accesos, pero económicamente de alto costo.

- El lenguaje de programación que utiliza la Placa Arduino es relativamente fácil de aprender y aplicar ya que este lenguaje es similar al lenguaje JAVA en cuanto a sintaxis y lógica que se aplica.

- La tecnología RFID tiene como ventaja fundamental con respecto a otras es que no necesita contacto visual directo para transmitir los datos; como ocurre en la transmisión de infrarrojos.

- También pude concluir que la metodología RUP es la más adecuada para poder documentar este proyecto ya que las etapas y los diagramas que se utilizan en la misma pueden identificar de manera correcta el funcionamiento que tendrá el Sistema Informático que es parte del Proyecto.

- La elaboración del modelo genérico de normas de ingreso a infraestructuras restringidas no fue muy fácil de elaborar puesto que la mayoría de instituciones no cuenta con un documento donde se especifiquen puntos como los necesarios para el manejo adecuado de las áreas restringidas de las mismas.

- La realización del Taller de Socialización fue muy positiva para el Proyecto ya que permitió que se diera a conocer a más personas entre ellas jóvenes emprendedores y algunos dueños de PYMES las tecnologías usadas en el sistema de control como son Arduino y el Modulo RFID (Identificación de Radio Frecuencia).

RECOMENDACIONES:

- Se recomienda que el modelo genérico de normas y restricciones presentado en este proyecto sea correctamente adecuado por cada una de las Organizaciones que decidan implementar este proyecto de Control de Accesos.

- Se recomienda ampliar los conocimientos sobre la tecnología Arduino, RFID y sobre todo sobre la conexión de lectores en cada área para poder implementar este proyecto a una Organización de manera que este proyecto sea implementado de forma eficiente puesto que en el proyecto actual solo se presentará un prototipo de conexión.

- Es necesario para un buen uso del Sistema y su explotación los usuarios encargados del su manejo que en este caso serían el Gerente y el Administrador tengan conocimientos básicos de computación.

- Se recomienda implementar este proyecto de Control de Accesos a empresas PYMES por el presupuesto y tecnología avanzada que se presenta lo cual beneficiara muchos a las mismas.