documento CENTINELA

# introducción

# 1.1 NOMBRE DEL PROYECTO

CENTINELA

# 1.2 OBJETIVO GENERAL

Desarrollar una aplicación web que permita a los usuarios ingresar un dominio o IP pública y ejecutar escaneos automatizados para detectar posibles vulnerabilidades de seguridad, clasificarlas, y generar un informe visual y descargable.

# 1.3 PUBLICO OBJETIVO

* Profesionales y estudiantes del área de ciberseguridad.
* Empresas que deseen verificar la exposición y vulnerabilidad básica de sus servicios.
* Cualquier usuario que busque una evaluación automatizada.

# 1.4 alcance

Este proyecto contempla el desarrollo de una aplicación web llamada **Centinela/Golem**, orientada a realizar análisis de seguridad sobre dominios o IPs públicas.

La aplicación permitirá al usuario ingresar un dominio o dirección IP, y realizará de forma automática una serie de escaneos básicos y medios no intrusivos con el fin de identificar posibles vulnerabilidades de seguridad.

Los resultados serán procesados, clasificados y presentados visualmente mediante gráficos interactivos desarrollados en JavaScript, con un enfoque en legibilidad, claridad y estética.

## El sistema ejecutará escaneos como:

* Escaneo de puertos abiertos usando NMAP
* Verificación de headers HTTP potencialmente inseguros
* Validación del estado del certificado SSL
* Revisión de Información WHOIS
* Resolución DNS (cuando aplique)
* Generación de dorks para detectar archivos sensibles y contenido expuesto

## FUNCIONALIdades adicionales del sistema:

* Sistema de registro y autenticación de usuarios
* Generación de reporte descargable
* Envío de reporte por correo
* Historial de escaneos accesibles para usuarios registrados

## Tecnologías y arquitecturas

* Procesamiento asíncrono a través de Celery y Redis, permitiendo múltiples escaneos en segundo plano sin bloquear el servidor web.
* Backend desarrollado con Django.
* Frontend desarrollado con Django templates.
* Base de datos relacional MySQL para la persistencia de datos.
* Arquitectura modular con escáneres independientes y fácilmente integrables.
* Despliegue en contenedor Docker.

## Limite del alcance

El sistema **no incluirá pruebas ofensivas ni explotación activa de vulnerabilidades**. Se limitará exclusivamente a escaneos pasivos que no afecten la integridad de los sistemas analizados.

## Entregables del proyecto

* Código fuente funcional y documentado
* Módulos de escaneo independientes
* Interfaz web con visualización grafica de resultados
* Informe técnico completo y manual de usuario

# ESPECIFICACIÓN DE REQUERIMIENTOS

# 2.1 REQUERIMIENTOS FUNCIONALES (RF)

|  |  |
| --- | --- |
| CODIGO | REQUERIMIENTO |
| RF-01 | El sistema debe permitir al usuario registrarse y autenticarse en la plataforma. |
| RF-02 | |  | | --- | | El usuario podrá ingresar un dominio o una IP pública para iniciar un escaneo. |  |  | | --- | |  | |
| RF-03 | El sistema debe ejecutar múltiples escaneos: Nmap, WHOIS, Headers HTTP, Certificado SSL, DNS Resolver, Dorks. |
| RF-04 | El usuario podrá elegir qué escaneos desea realizar. |
| RF-04 | El usuario podrá visualizar el estado y progreso del escaneo en tiempo real. |
| RF-05 | Los resultados del escaneo deben ser presentados gráficamente y en texto. |
| RF-06 | El usuario podrá reintentar individualmente un escaneo si falla. |
| RF-07 | El usuario podrá generar un informe en formato PDF con los resultados de los escaneos que desee. |
| RF-08 | El usuario podrá descargar el informe generado. |
| RF-09 | El sistema debe permitir el envío del informe por correo electrónico. |
| RF-10 | El sistema debe guardar el historial de escaneos para cada usuario autenticado. |
| RF-11 | El usuario podrá consultar escaneos anteriores desde su cuenta. |
| RF-12 | El usuario podrá filtrar los resultados de los escaneos por riesgo, estado. |
| RF-13 | El usuario autenticado podrá cambiar sus datos desde su perfil. |
| RF-14 | El sistema debe permitir al usuario recuperar su contraseña mediante correo electrónico. |
| RF-15 | El administrador podrá visualizar todos los usuarios registrados. |
| RF-16 | El administrador podrá visualizar el historial de escaneo realizados por todos los usuarios. |
| RF-17 | El administrador podrá eliminar usuarios bajo ciertos criterios de seguridad. |
| RF-18 | El administrador podrá editar ciertos datos del perfil de un usuario (nombre, acceso) pero no su contraseña ni correo electrónico sin verificación previa. |

# 2.2 REQUERIMIENTOS NO FUNCIONALES (RNF)

|  |  |
| --- | --- |
| CODIGO | REQUERIMIENTO |
| RNF-01 | El sistema debe desarrollarse utilizando el framework Django y una base de datos MySQL. |
| RNF-02 | El sistema debe desplegarse en un contenedor Docker. |
| RNF-03 | Los escaneos deben ejecutarse en segundo plano mediante Celery y Redis para evitar bloquear el servidor principal. |
| RNF-04 | El escaneo completo no debe demorar más de 60 segundos en condiciones normales. |
| RNF-05 | La aplicación web debe ser responsiva y funcionar correctamente en dispositivos móviles y de escritorio. |
| RNF-06 | Las contraseñas deben almacenarse cifradas. |
| RNF-07 | El sistema debe garantizar la trazabilidad de los escaneos (fecha, hora, usuario, IP/dominio objetivo). |
| RNF-08 | Las visualizaciones deben generarse en menos de 1 segundo tras obtener los resultados. |
| RNF-09 | La creación y descarga del reporte debe tardar menos de 3 segundos. |
| RNF-10 | El sistema debe utilizar una arquitectura modular que permita agregar o quitar módulos de escaneo sin alterar los demás. |
| RNF-11 | El sistema debe ser capaz de enviar correos usando un servidor SMTP configurable. |
| RNF-12 | La aplicación debe estar documentada internamente (docstrings, README, manual de despliegue). |

# DISEÑO DEL SISTEMA

# 3.1 ARQUITECTURA GENERAL

El sistema desarrollado, denominado **Centinela**, se basa en una arquitectura **cliente–servidor** con separación clara entre las capas de presentación, lógica de negocio y persistencia.  
La solución implementa el patrón de diseño **MVC (Modelo–Vista–Controlador)**, siguiendo la estructura nativa del framework Django, lo que permite una adecuada separación de responsabilidades y facilita el mantenimiento y escalabilidad del proyecto.

## Componentes principales

|  |  |  |
| --- | --- | --- |
| Componente | Descripción | Tecnología |
| Frontend | Interfaz web responsiva para que el usuario ingrese datos (dominio o IP), configure módulos de escaneo y visualice resultados mediante gráficos y tablas. | DjangoTemplates, HTML5,CSS3,Tailwind, JavaScript,Chart.js |
| Backend | Procesa solicitudes, valida entradas, orquesta la ejecución de módulos de escaneo, y gestiona el estado de las tareas. | Django (Python) |
| Procesamiento asíncrono | Ejecuta escaneos pesados (Nmap, WHOIS, DNS, etc.) en segundo plano sin bloquear el servidor principal. | Celery + Redis |
| Base de datos | Almacena usuarios, historial de escaneos y resultados de módulos, asegurando trazabilidad. | MySQL |
| Infraestructura | Contenedores independientes para cada servicio, permitiendo portabilidad y despliegue sencillo. | Docker y Docker Compose |

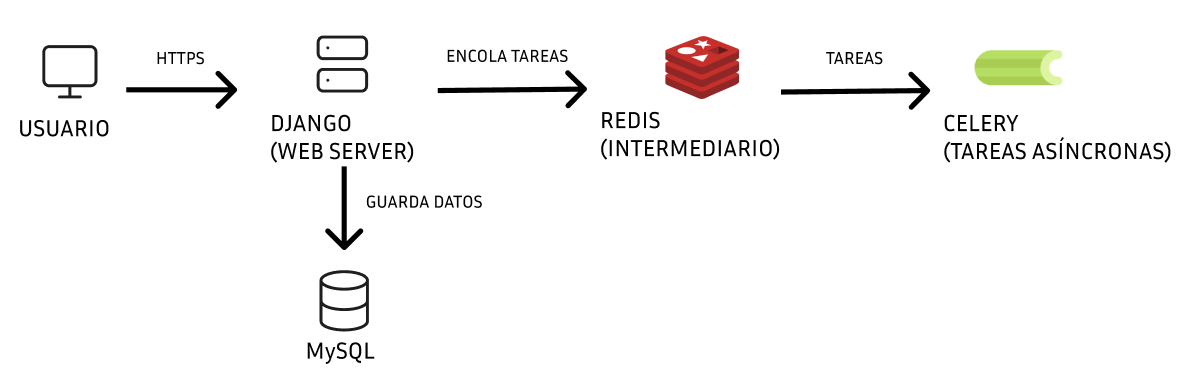
## Tecnologías seleccionadas y justificación

* **Django:** por su robustez, comunidad activa, patrón MTV(Model Template View), facilidad para crear aplicaciones modulares con autenticación integrada y ORM(Object-Relational Mapper).
* **Celery y Redis:** permiten ejecutar tareas en segundo plano, evitando bloqueos y mejorando la experiencia del usuario.
* **MySQL:** base de datos relacional confiable y ampliamente soportada.
* **Docker:** asegura portabilidad y replicabilidad del entorno.
* **Tailwind y Chart.js:** facilitan la creación de una interfaz moderna, responsiva, personalizable y visualmente atractiva.

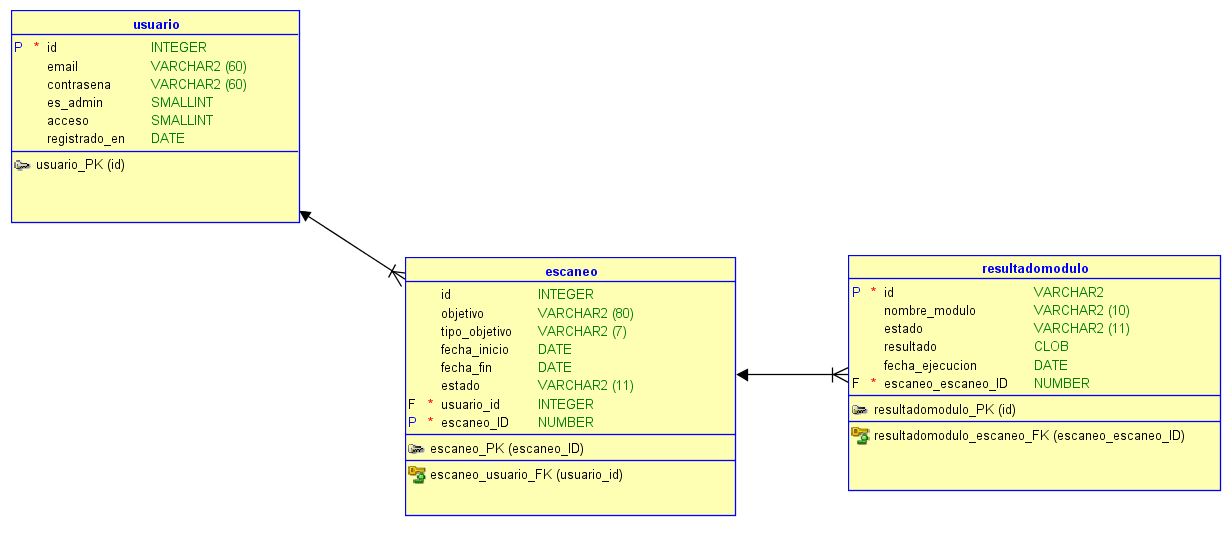
## Flujo de un escaneo

1. Usuario ingresa dominio o IP
2. Sistema registra escaneo y encola tareas para cada módulo seleccionado.
3. Workers Celery ejecutan módulos en paralelo (Nmap, WHOIS, etc.).
4. Resultados se guardan progresivamente en MySQL.
5. El frontend consulta el estado y muestra visualizaciones.
6. Usuario descarga un informe PDF o recibe el reporte por correo si así lo desea.

## Diagrama de ARQUITECTURA (Hecho con figma)

****

# 3.2 MODELO DE DATOS



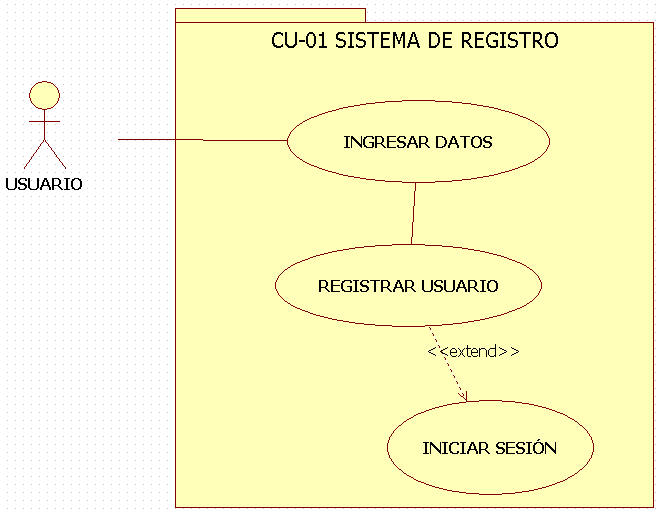
# 3.3 CASOS DE USO

## TABLA RESUMEN

|  |  |  |  |
| --- | --- | --- | --- |
| Código RF | Caso de uso (Nombre) | Actor principal | Descripción breve |
| CU-01 | Registrar usuario | Usuario | Permite al usuario crear una cuenta en el sistema |
| CU-02 | Iniciar sesión | Usuario | Permite al usuario iniciar sesión en la plataforma |
| CU-03 | Ejecutar escaneo | Usuario | Permite ingresar un dominio o IP como dato de entrada y ejecutar los escaneos seleccionados. |
| CU-04 | Ver resultados de escaneo | Usuario | Permite al usuario visualizar resultados en texto y gráficos. |
| CU-05 | Reintentar módulo fallido | Usuario | Permite relanzar un módulo específico que falló. |
| CU-06 | Generar informe PDF | Usuario | Permite crear un reporte PDF con los resultados elegidos. |
| CU-07 | Consultar historial de escaneos | Usuario | Permite al usuario ver escaneos previos desde su cuenta. |
| CU-08 | Editar datos de perfil | Usuario | Permite modificar datos personales desde su perfil. |
| CU-09 | Recuperar contraseña | Usuario | Permite restablecer contraseña vía correo electrónico. |
| CU-10 | Gestionar usuario | Administrador | Permite al administrador consultar, crear, editar y eliminar usuarios. |
| CU-11 | Consultar escaneos | Administrador | Permite al administrador consultar escaneos. |

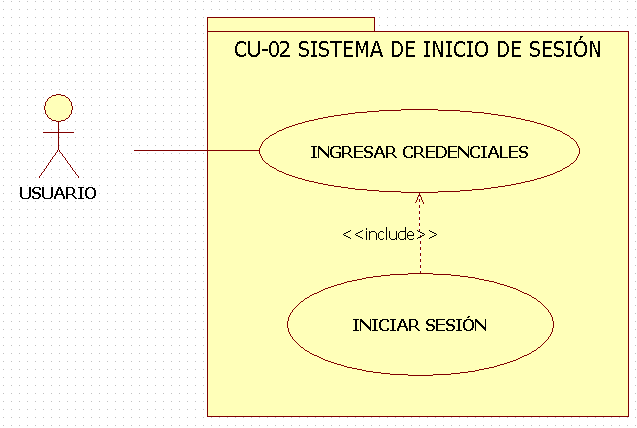
## CU-01 REGISTRar usuario

|  |  |
| --- | --- |
| Campo | Descripción |
| Nombre | Registrar usuario |
| Actor principal | Usuario |
| Descripción | Permite crear una cuenta proporcionando correo y contraseña entre otros datos. |
| Precondiciones | * No tener cuenta registrada. |
| Flujo principal | 1. El usuario accede al formulario de registro.  2. Ingresa datos (email, contraseña).  3. El sistema valida los datos.  4. Se crea la cuenta. |
| Flujo alternativo | * 3a. Datos inválidos. El sistema muestra error de validación y solicita corrección. * 3b. El correo ya existe. El sistema informa que el email ya está registrado. |
| Postcondiciones | * Se crea nueva cuenta de usuario. * El usuario puede iniciar sesión. |



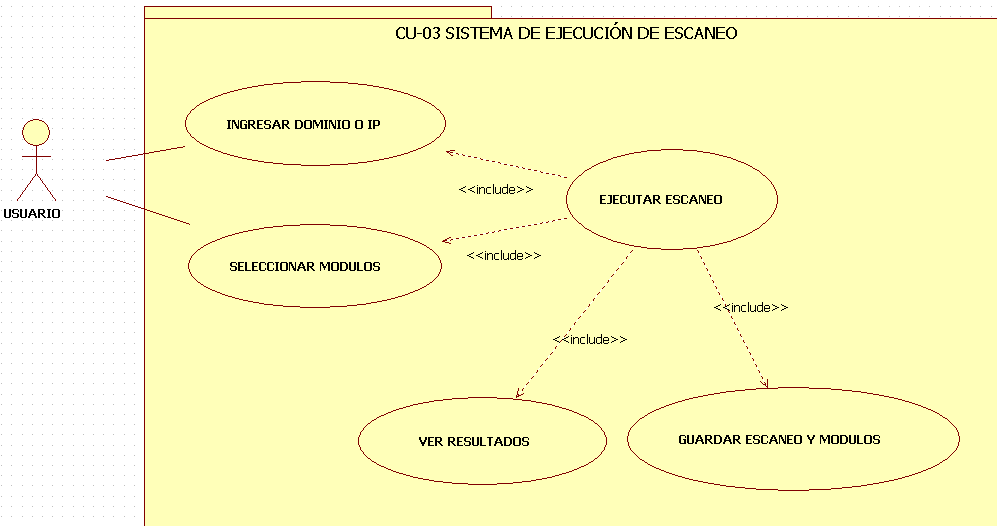
## CU-02 iniciar SESIÓN

|  |  |
| --- | --- |
| Campo | Descripción |
| Nombre | Iniciar sesión |
| Actor principal | Usuario |
| Descripción | Permite al usuario iniciar sesión con su correo y contraseña. |
| Precondiciones | * No tener sesión iniciada. * Estar registrado en el sistema. |
| Flujo principal | 1. El usuario accede al formulario de inicio de sesión.  2. Ingresa datos (email, contraseña).  3. El sistema valida los datos y realiza autenticación.  4. El usuario accede. |
| Flujo alternativo | * 3a. Datos inválidos. El sistema muestra error de validación y solicita corrección. * 3b. El correo no existe. El sistema informa que la cuenta no está registrada. * 3c. Contraseña incorrecta. El sistema informa que la contraseña no coincide con el email. * 3d. Acceso denegado. El sistema informado que el usuario no tiene acceso a la plataforma. |
| Postcondiciones | * Se crea una sesión activa para el usuario. |



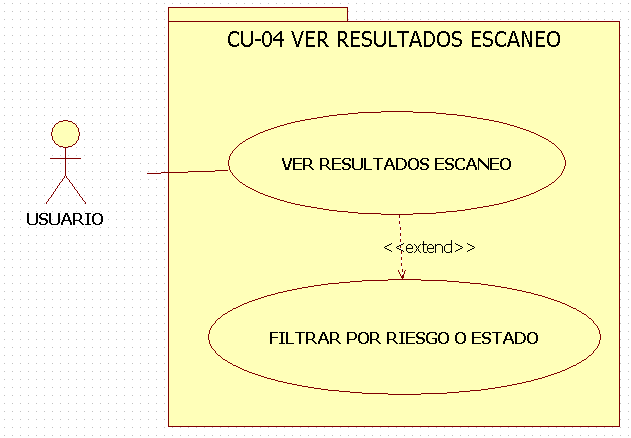
## CU-03 ejecutar escaneo

|  |  |
| --- | --- |
| Campo | Descripción |
| Nombre | Ejecutar escaneo |
| Actor principal | Usuario |
| Descripción | Permite ingresar un dominio o IP como dato de entrada y ejecutar los escaneos seleccionados. |
| Precondiciones | * Sistema disponible. * Usuario con sesión activa. * Sistema sin escaneos en proceso. |
| Flujo principal | 1. El usuario ingresa un dominio o IP como dato de entrada.  2. El usuario selecciona los módulos de escaneo que desee aplicar.  3. El usuario presionar botón de iniciar escaneo.  4. El sistema valida el dato de entrada.  5. El sistema ejecuta el escaneo y muestra progreso. |
| Flujo alternativo | * 4a. Datos inválidos. El sistema muestra error de validación y solicita corrección. * 4b. Módulo no disponible. El sistema informa que el módulo seleccionado presenta problemas y no está disponible. * 5a. Error durante ejecución del escaneo. El sistema informa que hubo un error durante la ejecución del escaneo. |
| Postcondiciones | * Se guarda el escaneo en la BDD. * Se guardan los resultados de cada módulo. * Se muestran los resultados de los escaneos con elementos visuales. |



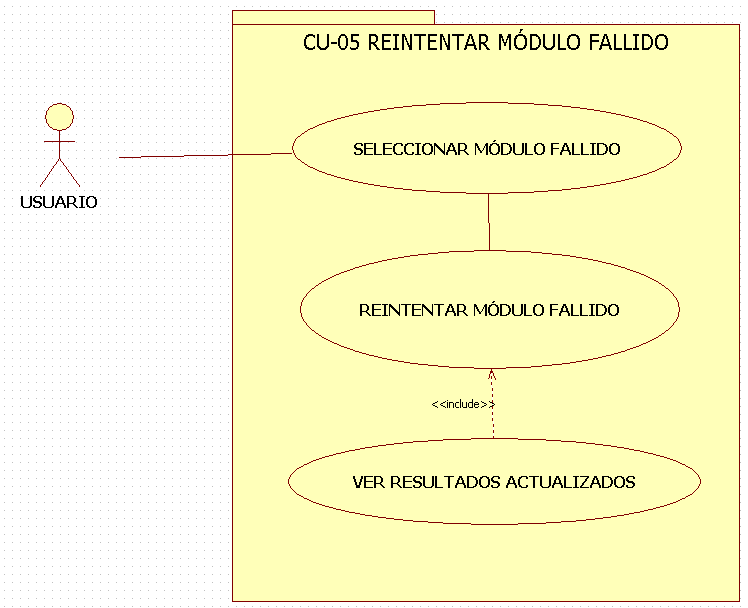
## Cu-04 ver resultados de escaneo

|  |  |
| --- | --- |
| Campo | Descripción |
| Nombre | Ver resultados de escaneo |
| Actor principal | Usuario |
| Descripción | Muestra resultados del escaneo en texto y gráficos. |
| Precondiciones | * Escaneo finalizado con al menos 1 módulo exitoso. * Usuario autenticado en el sistema. |
| Flujo principal | 1. El sistema detecta los módulos finalizados exitosamente.  2. El sistema procesa los resultados de los módulos y genera las visualizaciones correspondientes.  3. El usuario visualiza los resultados con la opción de filtrar por estado y riesgo. |
| Flujo alternativo | * 1a. Todos los módulos fallan. El sistema informa del error y ofrece reprocesar. * 2a. Error en generación de gráficos. El sistema muestra los resultados en otro formato. |
| Postcondiciones | * Los resultados se muestran correctamente al usuario. |



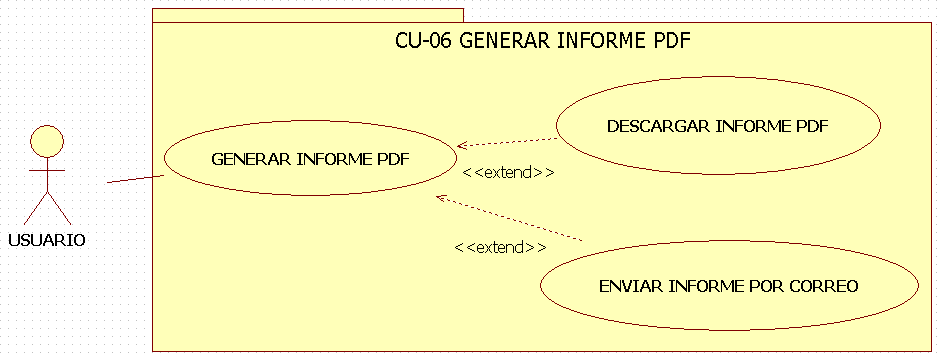
## CU-05 REINTENTAR MÓDULO FALLIDO

|  |  |
| --- | --- |
| Campo | Descripción |
| Nombre | Reintentar módulo fallido |
| Actor principal | Usuario |
| Descripción | Permite relanzar un módulo específico que falló. |
| Precondiciones | * Al menos 1 módulo debe tener estado: fallido. * Usuario autenticado en el sistema. |
| Flujo principal | 1. El sistema detecta los módulos que fallaron.  2. El sistema procesa el fallo de los módulos y ofrece la opción de reintentar módulo al usuario.  3. El usuario visualiza la opción y reintenta módulo.  4. El sistema relanza el módulo y espera resultados para mostrarlos al usuario. |
| Flujo alternativo | * 3a. La opción reintentar módulo no realiza la acción. El sistema informa al usuario que intente más tarde. |
| Postcondiciones | * Los resultados se muestran correctamente al usuario. * El módulo actualiza su estado. |



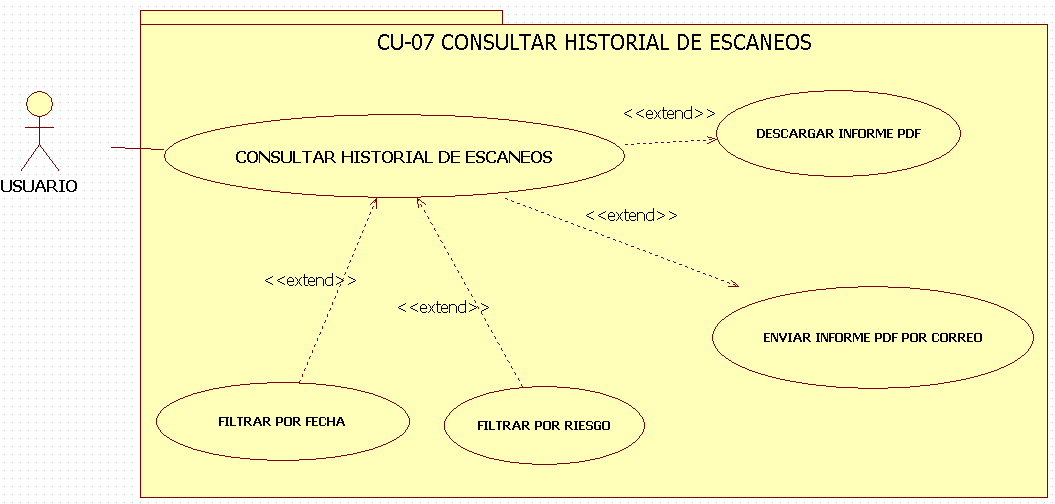
## CU-06 GENERAR INFORME PDF

|  |  |
| --- | --- |
| Campo | Descripción |
| Nombre | Generar informe PDF |
| Actor principal | Usuario |
| Descripción | Permite crear un reporte PDF con los resultados elegidos, y descargarlo o enviarlo por correo. |
| Precondiciones | * Al menos 1 módulo debe tener estado exitoso. * Usuario autenticado en el sistema. * Solo los módulos exitosos se pueden agregar al PDF. |
| Flujo principal | 1. El sistema finaliza el escaneo.  2. El sistema ofrece al usuario la opción de generar informe PDF.  3. El sistema despliega una vista con módulos exitosos disponibles a seleccionar.  3. El usuario selecciona qué módulos quiere agregar al informe.  4. El sistema ofrece la opción de descargar el informe y la opción de enviar el informe por correo a un destinatario.  5. El usuario selecciona su opción preferida. |
| Flujo alternativo | * 3a. Los módulos no se pueden seleccionar. El sistema informa al usuario que los módulos deben estar finalizados exitosamente para incluirlos en el informe. * 4a. El informe no se descarga. El sistema informa del problema al usuario y le pide reintentarlo más tarde. * 4b. El correo no llega al destinatario. El sistema informa al usuario que se cerciore de la correcta escritura de la dirección del correo. |
| Postcondiciones | * El usuario descarga el informe PDF en su dispositivo. * El informe PDF es recibido por el destinatario. * El informe PDF contiene los datos seleccionados por el usuario. |



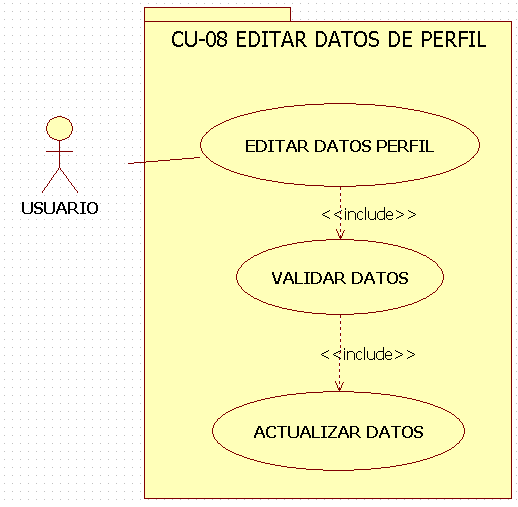
## CU-07 CONSULTAR HISTORIAL DE ESCANEOS

|  |  |
| --- | --- |
| Campo | Descripción |
| Nombre | Consultar historial de escaneos |
| Actor principal | Usuario |
| Descripción | Permite al usuario ver escaneos previos desde su cuenta. |
| Precondiciones | * Usuario autenticado en el sistema. |
| Flujo principal | 1. El usuario accede a la sección ‘historial de escaneos’.  2. El sistema muestra los escaneos realizados por el usuario.  3. El sistema ofrece filtrar los escaneos por fecha o por riesgo.  4. El sistema ofrece la opción de descargar informe PDF con módulos de escaneo específico y/o enviar informe PDF por correo. |
| Flujo alternativo | * 3a. El usuario no tiene escaneos realizados. El sistema informa al usuario que no tiene escaneos registrados. |
| Postcondiciones | * El usuario visualiza sus escaneos realizados. * El usuario descarga o envía por correo los escaneos que prefiera. |



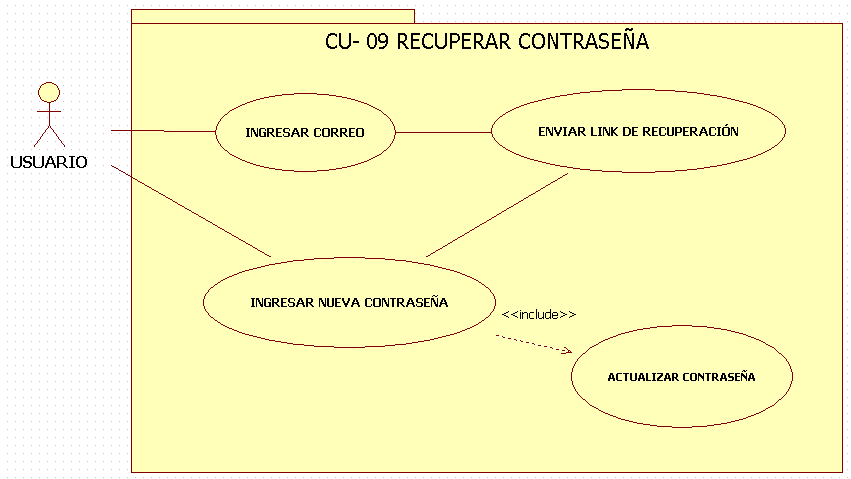
## CU-08 editar datos de perfil

|  |  |
| --- | --- |
| Campo | Descripción |
| Nombre | Editar datos de perfil |
| Actor principal | Usuario |
| Descripción | Permite modificar datos personales desde su perfil. |
| Precondiciones | * Usuario autenticado en el sistema. |
| Flujo principal | 1. El usuario accede a la sección ‘Mi perfil’.  2. El sistema muestra los datos personales en un formulario.  3. El usuario selecciona y edita los campos que desee.  4. El sistema valida los nuevos datos y los actualiza en la BDD. |
| Flujo alternativo | * 4a. El usuario ingresa datos no válidos. El sistema informa al usuario de los datos no válidos y solicita corrección. * 4b. Error durante la actualización de datos. El sistema revierte la actualización e informa al usuario que sus datos no han sido actualizados. |
| Postcondiciones | * El usuario visualiza sus datos personales actualizados. * Los datos del usuario han sido actualizados en la BDD. |



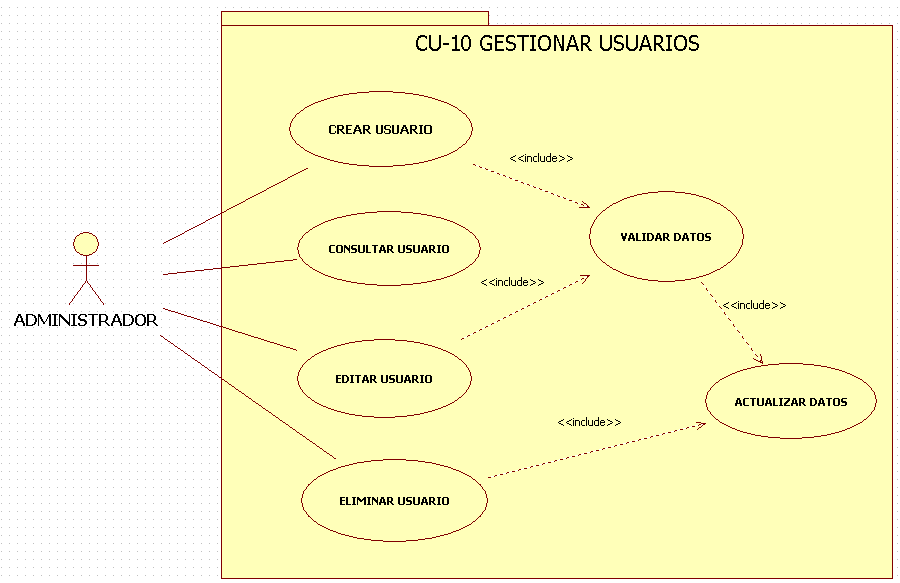
## CU- 09 RECUPERAR CONTRASEÑA

|  |  |
| --- | --- |
| Campo | Descripción |
| Nombre | Recuperar contraseña |
| Actor principal | Usuario |
| Descripción | Permite restablecer contraseña vía correo electrónico. |
| Precondiciones | * Usuario debe estar registrado en el sistema. |
| Flujo principal | 1. El usuario pincha la opción ‘¿Olvidaste tu contraseña?’.  2. El usuario ingresa su correo registrado.  3. El sistema valida la existencia en el sistema del correo ingresado.  4. El sistema envía email con instrucciones de recuperación.  5. El usuario ingresa su nueva contraseña.  6. El sistema valida y actualiza la nueva contraseña. |
| Flujo alternativo | * 3a. El correo no está registrado en el sistema. El sistema informa al usuario y solicita la correcta escritura del correo. * 4a. El sistema de correo no está disponible. El sistema informa al usuario y solicita intentarlo más tarde. * 6a. La contraseña no ha podido ser actualizada. Informa al usuario, revertir los cambios y solicita intentarlo más tarde. |
| Postcondiciones | * El usuario puede ingresar a su cuenta con la contraseña nueva. |



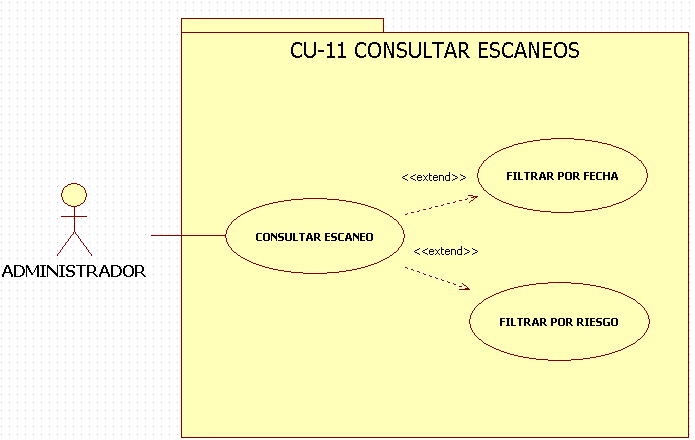
## CU-10 GESTIONAR USUARIOS

|  |  |
| --- | --- |
| Campo | Descripción |
| Nombre | Gestionar usuarios |
| Actor principal | Administrador |
| Descripción | Permite al administrador consultar, crear, editar y eliminar usuarios. |
| Precondiciones | * Administrador autenticado en el sistema. |
| Flujo principal | 1. El administrador ingresa a la sección ‘Usuarios’.  2. El administrador crea, consulta, edita o elimina un usuario.  3. El sistema valida los datos ingresados o solicita confirmación de acciones.  4. El sistema actualiza los datos en la BDD. |
| Flujo alternativo | * 2a. El sistema no tiene usuarios registrados. Informa al administrador con un mensaje. * 3a. Los datos no son válidos. Informa al administrador. Solicitar ingresar datos correctamente. * 4a. Error durante ejecución de actualización. Informar al administrador. Revertir cambios. |
| Postcondiciones | * Los datos son actualizados correctamente. |



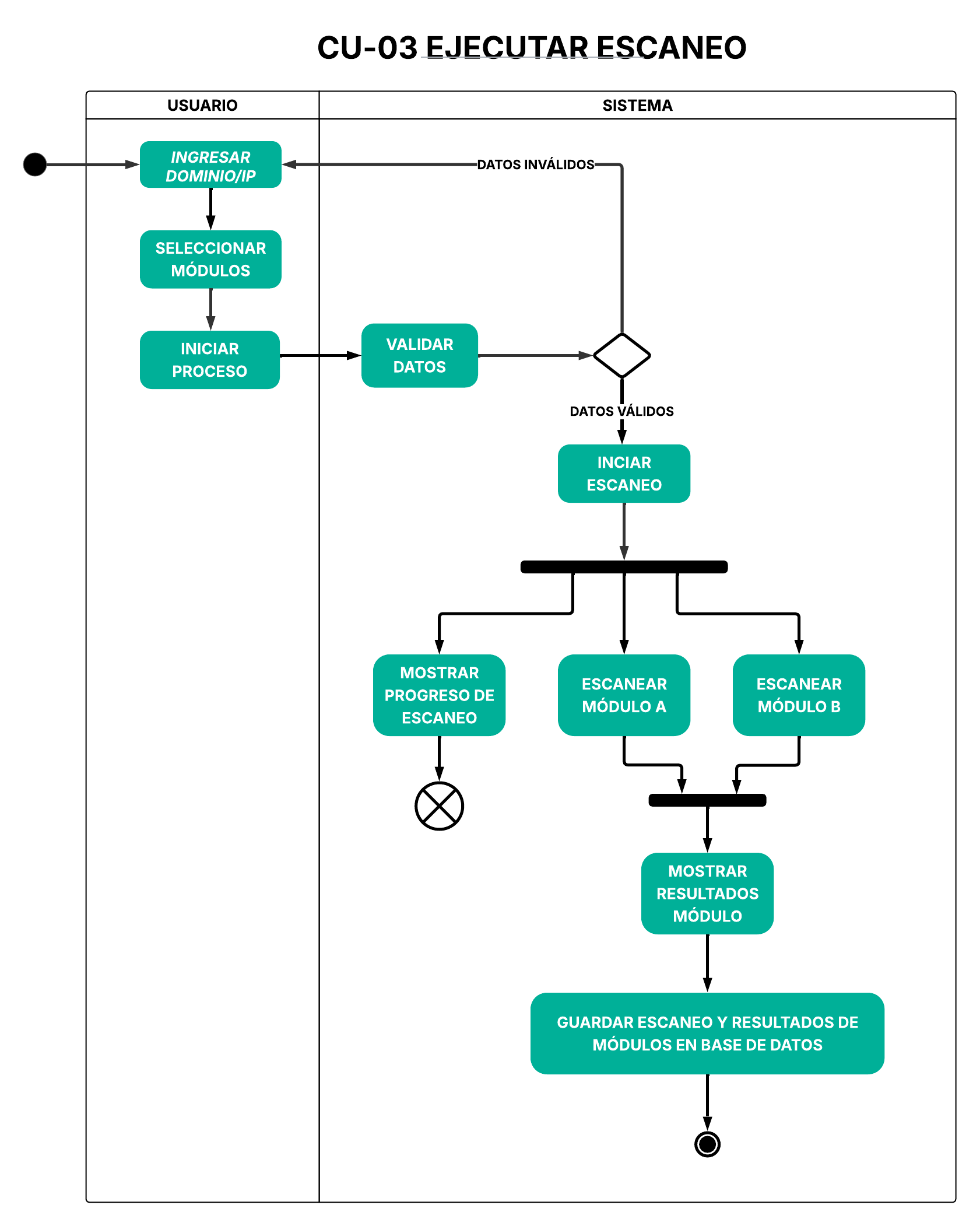
## CU-11 consultar ESCANEOS

|  |  |
| --- | --- |
| Campo | Descripción |
| Nombre | Consultar escaneos |
| Actor principal | Administrador |
| Descripción | Permite al administrador consultar escaneos. |
| Precondiciones | * Administrador autenticado en el sistema. |
| Flujo principal | 1. El administrador ingresa a la sección ‘Escaneos.  2. El administrador consulta un escaneo.  3. El sistema ofrece filtros por fecha y riesgo.  4. El administrador filtra los escaneos por fecha o riesgo.  5. El administrador ve los detalles de cada escaneo. |
| Flujo alternativo | * 2a. El sistema no tiene escaneos registrados. Informa al administrador con un mensaje. |
| Postcondiciones | * El administrador visualiza la información de escaneos solicitada |

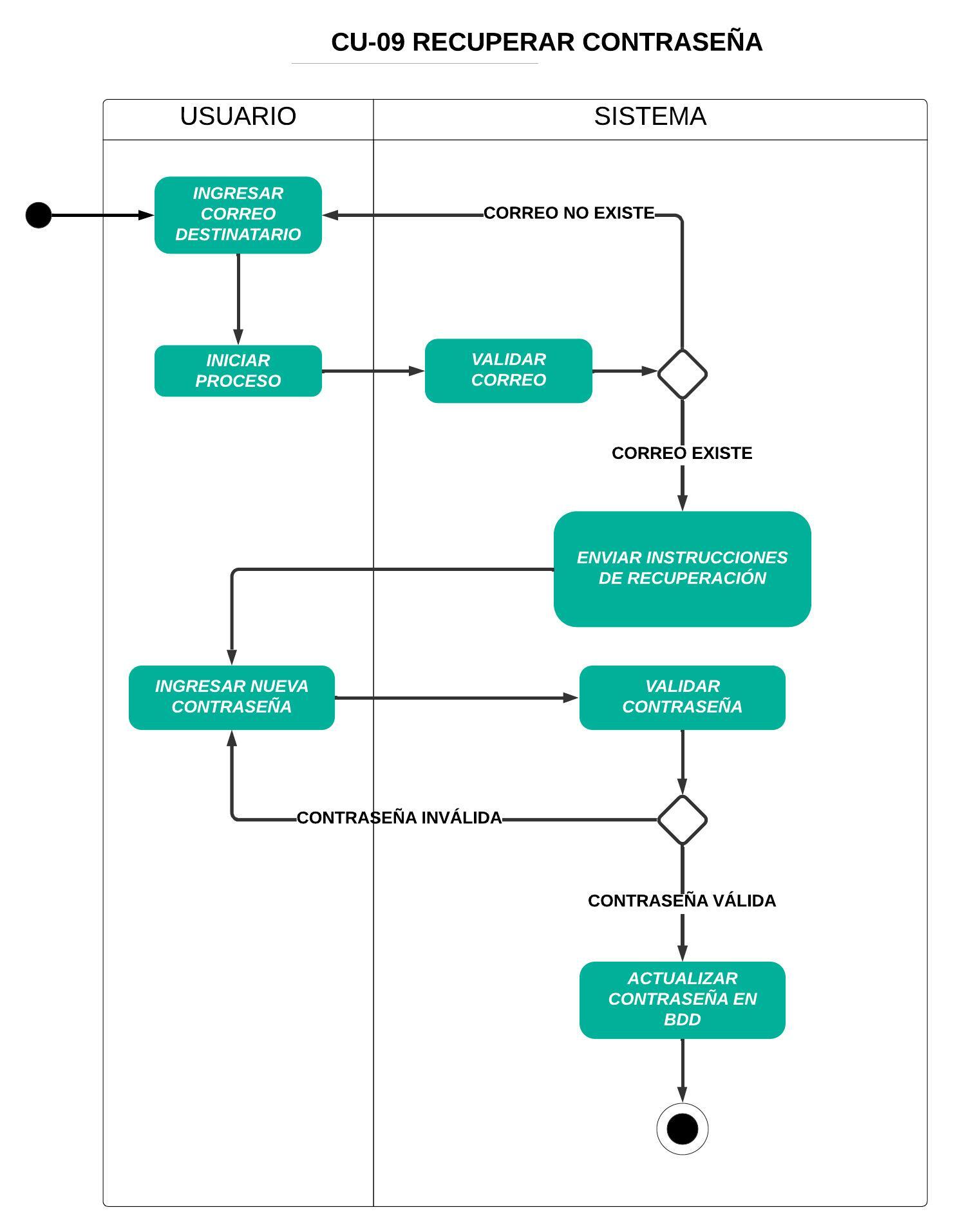


# 3.4 diagrama de actividades

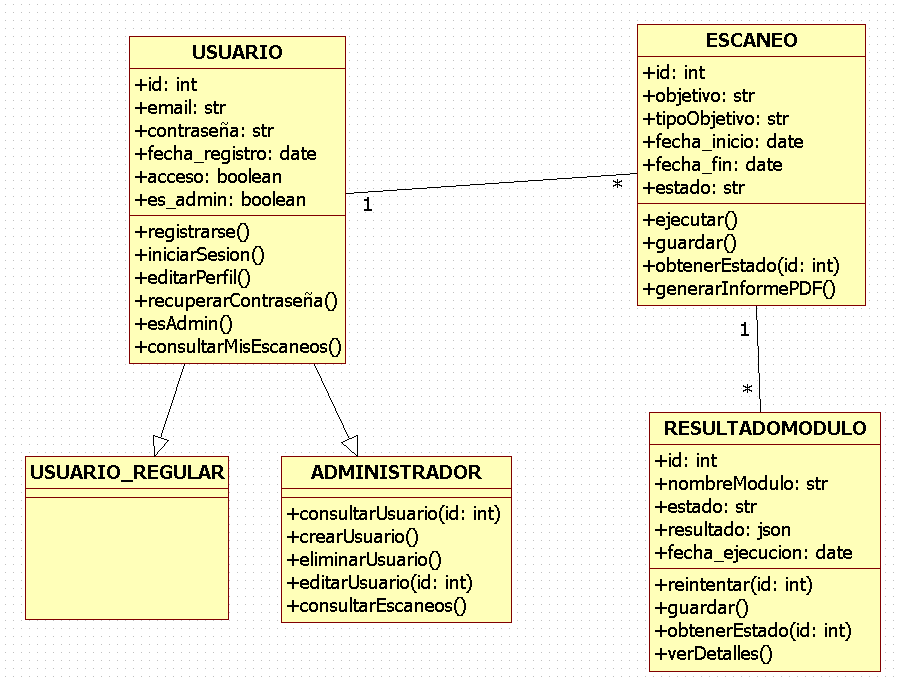
## CU-03 EJECUTAR ESCANEO



## CU-09 RECUPERAR CONTRASEÑA



# 3.5 diagrama de clases



# 3.6 diagrama de secuencia

## CU-03 EJECUTAR ESCANEO

