DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Análisis y Diseño se Software

Integrantes: Zaith Manango, Simoné Medina, Oswaldo Tipán, Fernando Sandoval

NRC: 27835

Ing. Jenny Ruiz

Fecha: 18/12/2025

Requisitos priorizados

Con el fin de asegurar una implementación eficiente y alineada con los objetivos del negocio, se llevó a cabo un proceso de priorización de requisitos que permitiera identificar aquellos con mayor impacto en el funcionamiento del sistema. Dicha priorización fue necesaria para enfocar los esfuerzos iniciales de desarrollo en los requisitos críticos, reduciendo riesgos y garantizando la continuidad operativa desde las primeras fases del proyecto. Para ello, se adoptó un enfoque cuantitativo basado en criterios reconocidos en la Ingeniería de Requisitos, considerando aspectos como el valor aportado al negocio, el riesgo asociado a su no implementación, las dependencias entre requisitos y el esfuerzo requerido para su desarrollo.

Requisito	Valor	Riesgo	Dependencia	Esfuerzo	Total	Prioridad
RF1 – Registro de Cuenta de Cliente	5	5	5	3	18	Alta
RF1.1 – Gestión de Cuentas de Asistente	5	4	4	3	16	Alta
RF1.2 – Inicio de Sesión Multirol	5	5	4	4	18	Alta
RF1.3 – Recuperación de Contraseña	4	5	4	3	16	Alta
RF1.4 – Notificación de resultado al cliente	4	4	3	2	13	Media
RF1.5 – Cierre Seguro de Sesión	4	4	4	3	15	Media–Alta

A partir de este análisis, se aplicó una matriz de valor, riesgo y dependencia que permitió clasificar los requisitos de manera objetiva. Como resultado, el requisito RF-1 fue identificado como un “cuello de botella” dentro del sistema, por lo que se determinó su implementación prioritaria. En contraste, los requisitos relacionados con reportes, notificaciones y gestión de crédito fueron programados para fases posteriores, al no afectar directamente el núcleo funcional del sistema en sus primeras etapas.

RF-1: Gestionar Acceso Sistema

Actor(es): Cliente, Asistente, Gerente

Descripción: El sistema deberá receptar los datos necesarios para gestionar el acceso de los actores según su rol. Como entrada, se considerará el ingreso de información básica como nombre completo, correo electrónico, contraseña y tipo de usuario, permitiendo al cliente registrarse por primera vez y al gerente registrar un nuevo asistente. El gerente contará con acceso previamente autorizado por el sistema, por lo que no necesita crear una cuenta. Los tres actores podrán iniciar sesión según su rol, validando las credenciales correspondientes. En caso de olvido de contraseña, el sistema deberá ofrecer la opción de recuperación mediante verificación por correo electrónico, donde se enviará un código de verificación numérico de seis dígitos al correo registrado del usuario. Este código, permitirá validar la identidad del actor antes de restablecer la contraseña. Como salida, el sistema permitirá el acceso únicamente si las credenciales son válidas, redireccionando a cada actor a su entorno correspondiente dentro del sistema, garantizando seguridad, trazabilidad y control individualizado de accesos.

Nombre del Requerimiento	RF-1.1-RegistrarCliente
Requerimientos del Sistema Asociados	RNF-01: Seguridad de acceso al sistema: Para encriptar contraseñas y garantizar autenticación segura.
	RNF-03: Facilidad de uso e interfaz amigable: Ya que el sistema debe guiar al usuario con formularios claros, validaciones visuales y mensajes comprensibles. RNF-04: Respaldo de datos: Porque los datos registrados deben conservarse de forma segura y recuperable. RNF-09: Registro y monitoreo del sistema: Para dejar trazabilidad del registro de nuevos clientes y cualquier fallo en el proceso.
Descripción	El sistema deberá recibir credenciales del cliente, registrarlo y almacenarlas en una base de datos. El sistema deberá validar que el correo no esté previamente registrado, verificar el formato de los datos e insertar la cuenta en la base de datos. El sistema deberá mostrar una confirmación de registro exitoso y habilitar el inicio de sesión para el nuevo cliente ya registrado.
Actor	Cliente
Precondición	El cliente no debe estar previamente registrado en el sistema y debe tener acceso al formulario de registro.
Secuencia normal	Acción
1	El actor accede a registrar cliente
2	El sistema muestra los datos requeridos: nombre completo en formato de (nombre y apellido), correo, contraseña, y confirmar contraseña, para mejorar la experiencia del usuario y evitar errores en el colocamiento de la contraseña, se debe colocar iconos con visualizar la contraseña escrita, tanto en contraseña como en confirmar contraseña y el sistema considera por defecto el rol cliente.
3	El actor ingresa los datos específicos del punto 2.
4	**El sistema deberá validar los siguientes datos**
4.1	Nombre no vacío, solo letras y espacios (3–50 caracteres).
4.2	El campo correo electrónico también es verificado para asegurar que no esté vacío, que tenga un formato válido (por ejemplo: usuario@dominio.com) usando una expresión regular adecuada, y que no se encuentre registrado previamente en la base de datos.
4.3	La contraseña es validada para que no esté vacía, tenga una longitud mínima de 8 caracteres y contenga al menos una letra mayúscula, una minúscula, un número y un carácter especial como @, # o $.
5	El sistema registra al nuevo usuario.
6	Se envía una confirmación al correo electrónico del actor (esto cuando ya tenga funcionalidad).
Secuencia alterna	Acción

1	**Campos obligatorios incompletos**
1.1	El actor deja uno o más campos obligatorios vacíos.
1.2	El sistema resalta los campos incompletos y muestra un mensaje: “Por favor complete todos los campos obligatorios.”
1.3	El actor puede corregir la información y continuar con el registro.
1.4	Vuelve al paso 3 del flujo principal.
Contraseña débil	Acción
2	**Contraseña débil**
2.1	El sistema detecta que la contraseña no cumple con los requisitos mínimos (mínimo 8 caracteres, al menos un número, una mayúscula) y mostrará un mensaje diciendo que tiene que hacer con ejemplos incluidos.
2.2	La contraseña no es segura. Asegúrese de que tenga al menos 8 caracteres, incluya una letra mayúscula, una minúscula, un número y un carácter especial (@, #, $...).
2.3	El actor introduce una nueva contraseña.
2.4	Vuelve al paso 4 del flujo principal.
Postcondición	El cliente podrá iniciar sesión utilizando sus nuevas credenciales.
Excepciones	Acción
1	**Correo electrónico ya registrado**
1.1	El sistema detecta que el correo electrónico ingresado ya está en uso en la base de datos.
1.2	El sistema muestra el mensaje: “El correo ingresado ya está en uso. Intente con otro o recupere su cuenta.”
1.3	El actor puede corregir el dato y volver a intentarlo.
1.4	El flujo continúa desde el paso 3 del flujo principal.
Comentarios	Se recomienda aplicar validaciones estrictas de seguridad para contraseñas (como longitud mínima, uso de mayúsculas, minúsculas, números y caracteres especiales), y se sugiere incluir la confirmación de correo electrónico como una medida adicional de seguridad. Si bien esta confirmación ya está contemplada en el flujo normal, debe evaluarse e implementarse.

Nombre del Requerimiento	RF-1.2- RegistrarNuevoAsistente

Requerimientos del Sistema Asociados	RNF-01: Seguridad de acceso al sistema: Porque debe garantizarse que solo usuarios autorizados (como el gerente) puedan registrar nuevos asistentes. RNF-03: Facilidad de uso e interfaz amigable: Para que el registro sea intuitivo y los errores de ingreso puedan corregirse fácilmente. RNF-04: Respaldo de datos: Los datos del nuevo asistente deben almacenarse de forma segura y recuperable ante fallos.
	RNF-09: Registro y monitoreo del sistema: Para dejar trazabilidad de la acción realizada, incluyendo fecha, hora y usuario que registró al asistente.
Descripción	El sistema deberá permitir al gerente registrar nuevos asistentes mediante el ingreso manual de información personal y de acceso, la cual se toma a partir de la nómina física gestionada internamente por la empresa. Para ello, el sistema mostrará un formulario exclusivo para el gerente que incluirá campos obligatorios como nombre completo, número de identificación, correo electrónico, y una contraseña temporal. El sistema validará que todos los campos estén completos, que los datos cumplan con el formato requerido (por ejemplo, correo válido y longitud mínima de contraseña) y que el correo electrónico no esté previamente registrado. Una vez verificados los datos, el sistema registrará al nuevo asistente y enviará automáticamente un correo de confirmación con instrucciones para su primer inicio de sesión.
Actor	Gerente
Precondición	El gerente debe haber iniciado sesión previamente.
Secuencia normal	Acción
1	El actor accede al módulo "Registrar nuevo asistente".
2	El sistema presenta datos con campos requeridos: nombre, correo electrónico y contraseña inicial.
3	El gerente ingresa los datos del nuevo asistente.
4	El sistema valida los siguientes datos:
4.1	El campo Nombre completo debe ingresarse en formato libre con nombres y apellidos separados por espacios (por ejemplo: “Juan Pérez” o “María del Carmen Torres”), sin abreviaturas, sin números ni caracteres especiales. Debe contener únicamente letras, incluyendo tildes, permitir espacios intermedios y tener una longitud total entre 3 y 50 caracteres. No se aceptan campos vacíos ni secuencias de caracteres no alfabéticos.
4.2	Correo: debe tener formato válido y no estar registrado.
4.3	Contraseña inicial: mínimo 8 caracteres, al menos una mayúscula, una minúscula, un número y un símbolo.
5	El sistema registra al asistente y lo asocia al gerente correspondiente.

Secuencia alterna	Acción
1	Campos vacíos o mal formateados:
1.1	El sistema detecta errores en uno o más campos.
1.2	El sistema muestra el mensaje: "Complete todos los campos requeridos con el formato correcto."
1.3	El gerente corrige los campos.
1.4	Vuelve al paso 3
2	Correo ya registrado:
2.1	El sistema verifica que el correo ya existe.
2.2	Muestra: "El correo ingresado ya está registrado. Intente con otro."
2.3	El gerente introduce un nuevo correo.
2.4	Vuelve al paso 3
Postcondición	El asistente quedará registrado y podrá iniciar sesión al activar su cuenta desde el correo.
Excepciones	Acción
1	Fallo en el servidor o conexión:
1.1	El sistema no puede registrar al asistente por un error técnico.
1.2	Se muestra: "Error en el registro. Intente nuevamente más tarde."
1.3	El sistema registra el error para revisión técnica.
Comentarios	Solo el gerente puede acceder a esta funcionalidad. Se recomienda forzar cambio de contraseña al primer inicio.

Nombre del Requerimiento	RF-1.3-IniciarSesion
Requerimientos del Sistema Asociados	RNF-01: Seguridad de acceso al sistema: Asegurar que solo usuarios con credenciales válidas puedan ingresar. RNF-02: Disponibilidad del sistema: El sistema debe estar disponible para permitir el inicio de sesión en cualquier momento. RNF-03: Facilidad de uso e interfaz amigable: El proceso de autenticación debe ser claro y fácil de utilizar. RNF-09: Registro y monitoreo del sistema: El sistema debe registrar cada intento de inicio de sesión exitoso o fallido para efectos de trazabilidad y seguridad.

Descripción	El sistema deberá permitir el inicio de sesión automáticamente según las credenciales y rol del actor. Al ingresar el correo y contraseña, el sistema deberá validar la existencia del usuario, la exactitud de la contraseña, y redirigirlo a su respectiva interfaz (cliente, asistente o gerente). Acceso concedido y redirección automática al entorno del usuario según rol.
Actor	Cliente, Asistente, Gerente
Precondición	El usuario debe estar previamente registrado en el sistema.
Secuencia normal	Acción
1	El usuario accede al formulario de inicio de sesión.
2	Ingresa su correo electrónico y contraseña.
3	El sistema valida los datos:
3.1	El correo debe existir en la base de datos.
3.2	La contraseña debe coincidir con la almacenada (encriptada con bcrypt).
4	El sistema identifica el rol del usuario (cliente, asistente o gerente).
5	Se redirige automáticamente al entorno correspondiente.
Secuencia alterna	Acción
1	Contraseña incorrecta:
1.1	El sistema detecta un error en la contraseña.
1.2	Muestra mensaje: "Credenciales incorrectas. Intente nuevamente."
1.3	El usuario reintenta.
2	Usuario no registrado:
2.1	El sistema no encuentra el correo en la base de datos.
2.2	Muestra mensaje: "Usuario no encontrado. Regístrese primero."
3	Formato de correo inválido:
3.1	El sistema detecta que el correo electrónico ingresado no cumple con el formato esperado (por ejemplo, falta el símbolo “@” o el dominio).
3.2	El sistema muestra el mensaje: “El correo ingresado no tiene un formato válido. Verifique e intente nuevamente.”
3.3	El usuario corrige el correo y vuelve a intentarlo.
Postcondición	El usuario queda autenticado en su sesión correspondiente
Excepciones	Acción
1	Si las credenciales no son válidas, se muestra un mensaje de error.
2	Si el usuario olvidó su contraseña, puede iniciar el flujo extendido “Recuperar Contraseña”.

Comentarios	Este caso se extiende con “Recuperar Contraseña” cuando el usuario lo solicita.

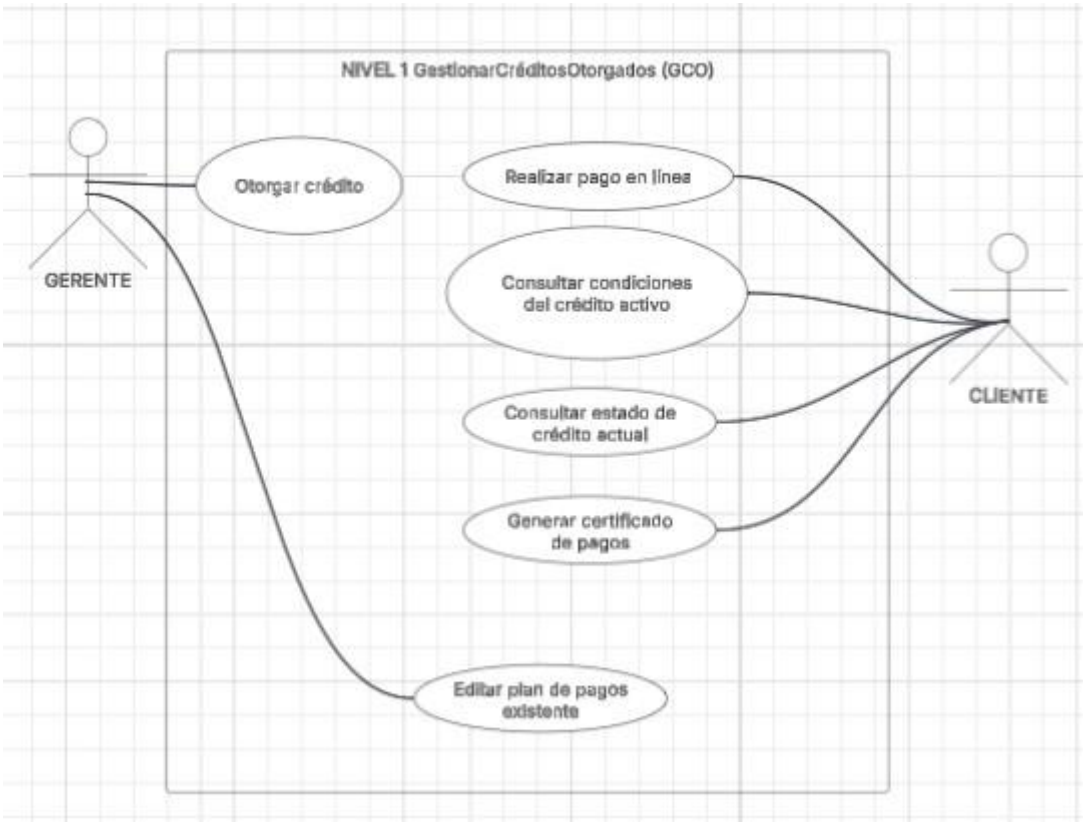
Nombre del Requerimiento	RF-1.4-Recuperar Contraseña
Requerimientos del Sistema Asociados	RNF-01: Seguridad de acceso al sistema: Validar la identidad del usuario antes de permitir el restablecimiento de la contraseña.
	RNF-04: Integridad del sistema: Asegurar que el proceso de recuperación no comprometa los datos del usuario ni del sistema. RNF-09: Registro y monitoreo del sistema: Registrar cada solicitud y restablecimiento de contraseña para fines de auditoría. RNF-10: Disponibilidad y soporte: El mecanismo de recuperación debe estar disponible en todo momento y ser confiable para el usuario.
Descripción	El usuario solicita recuperar el acceso al sistema proporcionando su correo electrónico registrado para eso se dirigirá al apartado de ¿olvidaste tu contraseña?. El sistema verifica que el correo exista en la base de datos y, si es válido, genera un código numérico temporal o un enlace de recuperación único, ambos con un tiempo de expiración (por ejemplo, 10 minutos). Este código o enlace se envía al correo del usuario y está vinculado a una solicitud cifrada. Al acceder mediante el enlace o ingresar el código, el usuario podrá definir una nueva contraseña. En el caso de los asistentes registrados por el gerente, que reciben una contraseña predefinida, este proceso también les permitirá cambiarla por una personalizada en su primer ingreso. Una vez validado el código o enlace, el sistema actualiza la contraseña en la base de datos y el usuario podrá iniciar sesión con sus nuevas credenciales.
Precondición	El usuario debe tener un correo previamente registrado en el sistema.
Secuencia normal	Acción
1	El usuario selecciona la opción “¿Olvidaste tu contraseña?”.
2	Ingresa su correo registrado.
3	El sistema verifica la existencia del correo.
4	Envía un código o enlace de recuperación al correo electronico.
5	El usuario establece una nueva contraseña.
Postcondición	El usuario puede autenticarse nuevamente con la nueva contraseña.
Excepciones	Acción
1	Si el correo no existe, se notifica que no hay cuenta asociada.
2	Si el código expira o es incorrecto, se bloquea temporalmente el intento. El código dura activo un máximo de 10 minutos.

Comentarios	El proceso debe implementar medidas de seguridad como expiración de enlaces y validación de identidad. Todo esto se valida por correo electrónico.
Nombre del Requerimiento	RF-1.5- CerrarSesion
Requerimientos del Sistema Asociados	RNF-01: Seguridad de acceso al sistema: Asegurar que, al cerrar sesión, se terminen correctamente todas las sesiones activas del usuario. RNF-04: Integridad del sistema: Evitar accesos no autorizados después del cierre de sesión eliminando tokens o sesiones abiertas. RNF-09: Registro y monitoreo del sistema: Registrar la hora y usuario que cerró sesión para fines de trazabilidad. RNF-10: Disponibilidad y soporte: Garantizar que la funcionalidad esté disponible en cualquier momento del uso del sistema.
Descripción	El sistema deberá permitir a cualquier usuario autenticado cerrar su sesión de manera segura y redirigirlo a la pantalla de inicio de sesión. El sistema invalidará la sesión activa del usuario y eliminará los tokens de autenticación en uso. Si la sesión ya estaba expirada, simplemente lo redirigirá al inicio sin mostrar errores. El sistema cerrará correctamente la sesión del usuario y lo enviará a la pantalla de inicio de sesión.
Actor	Cliente, Asistente, Gerente
Precondición	El usuario debe haber iniciado sesión correctamente y encontrarse en una vista del sistema.
Secuencia normal	Acción
1	El usuario hace clic en el botón "Cerrar sesión" desde cualquier pantalla con sesión activa.
2	El sistema invalida la sesión activa, eliminando los tokens de acceso (en memoria y/o cookies).
3	El sistema redirige automáticamente al usuario a la pantalla de inicio de sesión.
4	El caso de uso finaliza correctamente.
Secuencia alterna	Acción
1	Sesión ya expirada
1.1	El usuario intenta cerrar sesión, pero la sesión ya ha expirado por inactividad.
1.2	El sistema detecta la sesión inactiva y redirige automáticamente al inicio de sesión.
1.3	El sistema no muestra errores y finaliza el flujo.
Postcondición	El usuario se encuentra fuera del sistema y debe volver a autenticarse para acceder a cualquier funcionalidad restringida.
Excepciones	Acción

1	Botón o evento de cierre de sesión no responde:
1.1	El sistema no responde al evento por problemas en el cliente (navegador).
1.2	Se recomienda mostrar un mensaje alternativo: “Parece que no se pudo cerrar sesión. Recargue la página o intente nuevamente.”
1.3	No se compromete la seguridad del sistema, ya que no hay acceso sin sesión activa.
Comentarios	La opción de cerrar sesión debe estar disponible en todas las vistas internas del sistema. No se requiere confirmación adicional para cerrar sesión, salvo que existan cambios sin guardar. Si se utilizan tokens en el backend, deben invalidarse correctamente al cerrar sesión para garantizar la seguridad.

Nombre del Requerimiento	RF-1.6-AccederDashboard
Requerimientos del Sistema Asociados	RNF-02: Disponibilidad del sistema RNF-03: Facilidad de uso e interfaz amigable RNF-09: Registro y monitoreo del sistema
Descripción	El sistema deberá presentar a cada actor (Cliente, Asistente o Gerente) una página de resumen (“Dashboard”) con la información y accesos rápidos correspondientes a su rol, inmediatamente después de iniciar sesión correctamente.
Actor	Cliente, Asistente, Gerente
Precondición	El usuario debe haber iniciado sesión exitosamente (CU-ElGranito-003).
Secuencia normal	Acción
1	El sistema identifica el rol del usuario autenticado.
2	El sistema redirige al usuario a su Dashboard particular

2.1	ClienteDashboard para Clientes.
2.2	AssistantDashboard para Asistentes
2.3	ManagerDashboard para Gerentes.
3	El sistema carga y muestra widgets con datos resumidos
3.1	Clientes: estado de créditos, últimos pagos
3.2	Asistentes: tareas pendientes, solicitudes de consulta.
3.3	Gerentes: reportes rápidos, riesgos de morosidad.
4	El usuario interactúa con los accesos rápidos del Dashboard (por ejemplo, “Realizar Pago”, “Generar Reporte”).
Postcondición	El actor dispone de una vista inicial con acceso a las funcionalidades clave del sistema.
Excepciones	Acción
1	Si la sesión ha expirado, el sistema redirige al inicio de sesión.
Comentarios	El Dashboard debe ser responsive y ofrecer enlaces directos a los casos de uso principales según el rol.


NIVEL 1 GestionarCréditosOtorgados (GCO)
GERENTE
Otorgar crédito
Realizar pago en línea
Consultar condiciones del crédito activo
Consultar estado de crédito actual
Generar certificado de pagos
Editar plan de pagos existente
CLIENTE