Entregable #1 - Proyecto

Facultad De Administración
Administración De Sistemas Informáticos

Ingeniería de Software I
Semestre 2024-2S

Docente:
Jose Albeiro Montes Gil

Estudiantes:
Santiago Blandón Forero
Laura Camila Herrera Murillo
Cristian Andrés Arenas Vargas

Universidad Nacional De Colombia - Sede Manizales

Documento de especificación de requerimientos.

ID: RF-001

Nombre del requerimiento: Registro y Almacenamiento de transacciones financieras.

Descripción: Registrar las transacciones que van a ser analizadas y posteriormente almacenarlas.

Requisito: El Usuario debe haber iniciado sesión.

Criterios de Aceptación:

- El usuario va poder registrar, almacenar mediante el ID de la transacción.
- El sistema deberá categorizar las transacciones en niveles de criticidad (BAJO, MEDIO, ALTO) .
- El sistema deberá mostrar un mensaje de confirmación para el registro y almacenamiento

Dependencias: Bases de datos, sistemas caché, API.

Prioridad: Alta

ID: RF-002

Nombre del requerimiento: Consulta de transacciones financieras.

Descripción: Consultar transacciones almacenadas en la base de datos .

Requisito: El Usuario debe haber iniciado sesión.

Criterios de Aceptación:

- El usuario va a consultar mediante el ID de la transacción.
- El sistema realizará la búsqueda en la base de datos.
- El sistema mostrará en una tabla los datos asociados a la transacción.

Dependencias: Bases de datos.

Prioridad: Media

ID: RF-003

Nombre del requerimiento: Implementación de Machine Learning.

Descripción: La adopción de esta metodología realizará los análisis correspondientes a las transacciones para detectar anomalías.

Requisito: El Sistema debe estar funcionando.

Criterios de Aceptación:

- Cada vez que se registre una transacción, el sistema ejecutará el respectivo análisis.
- Basado en Patrones de comportamiento inusuales, ejecutará una notificación para advertir al Analista de Seguridad.

Dependencias: API, Técnica Machine Learning.

Prioridad: Alta

ID: RF-004

Nombre del requerimiento: Implementación de Reportes .

Descripción: El sistema debe permitir generar reportes con métricas y estadísticas de las transacciones durante un periodo de tiempo.

Requisito: El analista debe haber iniciado sesión para acceder a esta información.

Criterios de Aceptación:

- El analista podrá consultar a un usuario en específico.
- El sistema deberá permitirle indicar el rango de tiempo que quiere analizar.
- El sistema deberá retornar un gráfico con todas las transacciones realizadas en ese periodo de tiempo en formato PDF.

Dependencias: Base de Datos.

Prioridad: Media.

ID: RF-005

Nombre del requerimiento: Inicio y cierre de sesión .

Descripción: El sistema debe tener una interfaz amigable y entendible que permita a los usuarios ingresar al sistema, de igual forma debe suceder con el cierre de sesión.

Requisito: El usuario deberá entrar al Sistema para poder realizar estas acciones.

Criterios de Aceptación:

- El usuario deberá ingresar al sistema.
- El usuario deberá iniciar sesión con su usuario y contraseña.
- El sistema verificará si estos datos son correctos, si son correctos deberá iniciar sesión. De lo contrario retorna un mensaje indicando que las credenciales son incorrectas.

Dependencias: Base de Datos, Sistema.

Prioridad: Alta.

ID: RF-006

Nombre del requerimiento: Recuperación de contraseña.

Descripción: El sistema deberá brindar la opción de recuperación de contraseña.

Requisito: El usuario debe entrar al sistema.

Criterios de Aceptación:

- El Usuario después de varios intentos fallidos tendrá la opción de recuperación de contraseña.
- El sistema lo enviará a una vista en donde va tener que responder unas preguntas personales para poder verificar que si es la persona correcta.
- El sistema le permitirá crear una nueva contraseña.
- El sistema le notificará que ya fue cambiada la contraseña correctamente.

Dependencias: Sistema, Servicios de envío de correo y SMS.

Prioridad: Baja.

ID: RF-007

Nombre del requerimiento: Manejo de Roles.

Descripción: Al registrar a los usuarios se les debe asignar un rol.

Requisito: Cada Usuario debe estar registrado con un rol.

Criterios de Aceptación:

- Según el rol que maneje el usuario será enviado a su interfaz correspondiente.

Dependencias: Permisos.

Prioridad: Media.

ID: RNF-001

Nombre del requerimiento: Encriptación de datos sensibles.

Descripción: Garantizar que los datos sensibles como la información personal, contraseñas, datos de transacciones sean encriptadas para así protegerlos de ataques.

Requisito: El sistema debe utilizar Bcrypt para la encriptación.

Criterios de Aceptación:

- El usuario ingresará los datos de transacciones y guardará.
- El sistema encriptará esos datos y posteriormente los guardará en la base de datos.

Dependencias: Base datos, Algoritmo de Encriptación.

Prioridad: Baja.

ID: RNF-002

Nombre del requerimiento: Autenticacion de Usuarios.

Descripción: Realizar autenticación al momento de que los usuarios inicien sesión.

Requisito: El sistema deberá utilizar tokens y realizar la autenticación mediante usuario y contraseña.

Criterios de Aceptación:

- El usuario ingresará sus credenciales (Usuario y Contraseña).
- El sistema genera un token si las credenciales son correctas.
- El sistema genera un mensaje si las credenciales son incorrectas.

Dependencias: Base datos, Middleware.

Prioridad: Baja.

ID: RNF-003

Nombre del requerimiento: Rendimiento del Sistema.

Descripción: El sistema debe poder analizar 50 transacciones por minuto.

Requisito: El sistema debe realizar el análisis en menos de 10 segundos para el 90%.

Criterios de Aceptación:

- El sistema debe realizar pruebas con las 50 transacciones.

Dependencias: Machine Learning.

Prioridad: Alta.

ID: RNF-004

Nombre del requerimiento: Disponibilidad del Sistema.

Descripción: El sistema debe estar funcionando el 99% de cada día, para no tener interrupciones en los procesos.

Requisito: El sistema debe tener sistemas de monitoreo para analizar las caídas del sistema y poder gestionar rápidamente una solución.

Criterios de Aceptación:

- Se deberá contar con 15 minutos para poder solucionar los problemas que ocurran para poder garantizar la buena disponibilidad.
- El sistema deberá tener mecanismos de respaldo para cuando se presenten estas fallas

Dependencias: Servidores, Servicio técnico.

Prioridad: Media.

ID: RNF-005

Nombre del requerimiento: Compatibilidad .

Descripción: El sistema debe funcionar en diferentes sistemas operativos.

Requisito: Sistema Multiplataforma .

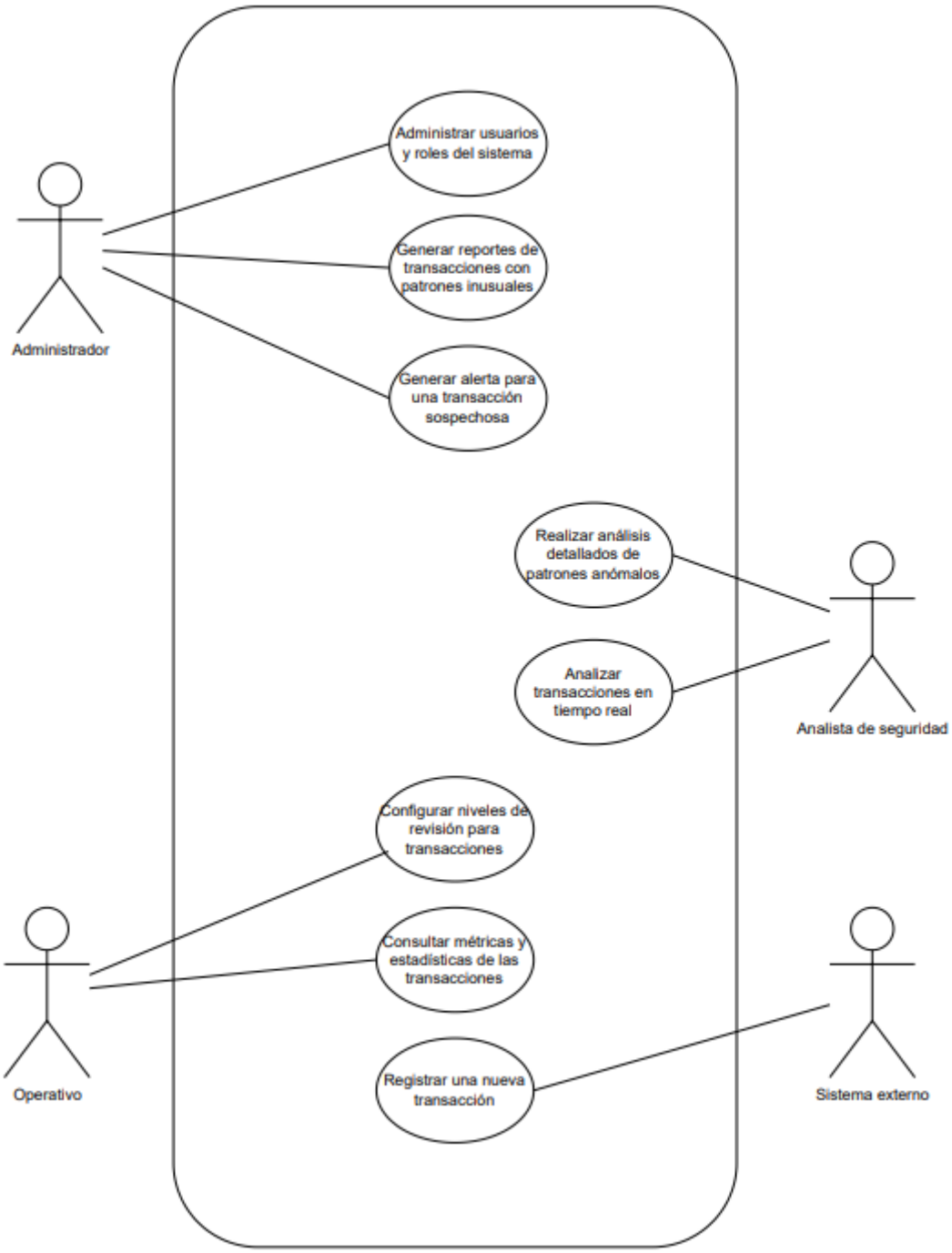
Criterios de Aceptación:

- El sistema debe poderse instalar en diferentes sistemas operativos sin ningún problema.
- Todas las funcionalidades deben ser accesibles y tener el mismo comportamiento en cada sistema operativo
- Se debe realizar una revisión periódica para verificar la compatibilidad con nuevas versiones de cada sistema operativo

Dependencias: Frameworks multiplataforma.

Prioridad: Media.

Diagrama de casos de uso



Descripción detallada de los casos de uso principales.

Caso de uso: Registrar una nueva transacción	
Actores	Cajero o sistema externo
Precondición	El usuario debe estar autenticado en el sistema, al igual que las cuentas de origen y destino.
Escenario	1. El usuario accede a la sección de registro de transacciones. 2. El usuario ingresa los datos de la transacción: monto, cuenta de origen, cuenta de destino, descripción. 3. El sistema valida que los datos ingresados son correctos. (Las cuentas existen, el monto es válido con sus respectivas validaciones como que la cuenta origen tiene dinero suficiente). 4. El sistema registra la transacción en la BD. 5. El sistema genera un ID único para la transacción. 6. El sistema muestra un mensaje confirmando que la transacción ha sido registrada exitosamente.
Postcondición	Se realiza la transacción de origen a destino, y aparece en el historial de transacciones estando disponible para futuras consultas o análisis.
Excepciones	- Si las cuentas no están registradas, el sistema muestra un mensaje de error indicando que no se puede realizar la transacción. - Si el monto ingresado excede el límite permitido por la cuenta origen, el sistema muestra un mensaje de advertencia.

Caso de uso: Analizar transacciones en tiempo real	
Actores	Analista de seguridad financiera, sistema de monitoreo de fraudes (microservicio),
Precondición	- Las transacciones deben estar registrándose en el sistema en tiempo real.
Escenario	1. El sistema recibe transacciones financieras en tiempo real desde diferentes fuentes (usuarios, sistemas externos como cajeros o pasarelas de pago). 2. Cada transacción es evaluada automáticamente mediante un modelo de machine learning 3. Si una transacción coincide con algún patrón sospechoso, el sistema la marca como "anómala". 4. El sistema genera una alerta que incluye detalles como el ID de la transacción, el tipo de irregularidad detectada y las cuentas involucradas. 5. El analista de seguridad recibe la alerta y revisa la transacción en otra interfaz del sistema. 6. Las transacciones analizadas quedan registradas con su estado (normal, sospechosa, validada, bloqueada) en el historial del

	sistema.
Postcondición	- Las transacciones sospechosas son registradas con su estado actualizado. - Se notifica al analista de seguridad o administrador sobre cualquier irregularidad detectada. - El sistema almacena un registro detallado para auditorías y análisis futuros.
Excepciones	Si se sobrepasa la capacidad de análisis del sistema, este prioriza las transacciones más críticas, dejando "en cola" las menos urgentes (puede ser con un criterio de cantidad de dinero que se va a transferir), y muestra una alerta al usuario operativo.

Caso de uso: Generar alerta para una transacción sospechosa	
Actores	Usuario administrador, sistema de monitoreo de fraudes (microservicio)
Precondición	La transacción debe haber sido registrada y evaluada.
Escenario	1. El sistema analiza una transacción por medio de un modelo de machine learning basado en patrones o reglas predefinidas. 2. Si la transacción cumple con alguno de los patrones definidos en el modelo, el sistema la marca como "sospechosa". 3. El sistema genera automáticamente una alerta que contiene: - ID único de la transacción. - Detalles relevantes (monto, cuentas involucradas, fecha y hora). - Descripción del criterio o patrón que la hizo sospechosa. 4. La alerta es enviada al usuario administrador en otra interfaz del sistema. 5. La alerta queda registrada en el sistema para su seguimiento y auditoría por el analista de seguridad.
Postcondición	- El analista de seguridad es notificado sobre la transacción sospechosa. - La alerta se almacena en el historial del sistema para futuras consultas o acciones.

Excepciones	-Si ocurre un fallo en la generación de la alerta, el sistema guarda la transacción sospechosa en un registro pendiente y notifica al usuario administrador para corregir el problema. - Si la transacción no puede ser evaluada adecuadamente por un error en el análisis hecho por machine learning, el sistema registra el evento y solicita revisión por parte del usuario administrador.

Caso de uso: Consultar métricas y estadísticas de las transacciones	
Actores	Usuario operativo
Precondición	El usuario operativo debe estar autenticado en el sistema y tener acceso autorizado para consultar métricas y estadísticas de las transacciones.
Escenario	1. El usuario operativo inicia sesión en la plataforma con sus credenciales. 2. El usuario operativo navega hasta la sección de métricas y estadísticas de transacciones. 3. El sistema muestra las opciones disponibles para consultar (por ejemplo, transacciones por fecha, por monto, transacciones sospechosas, etc.). 4. El usuario operativo selecciona el tipo de métrica o reporte que desea consultar (por ejemplo, transacciones realizadas en las últimas 24 horas, transacciones con montos inusuales, etc.). 5. El sistema genera y muestra las métricas o estadísticas solicitadas en formato de tablas, gráficos o resúmenes. 6. El usuario operativo puede visualizar los detalles de las transacciones o descargar el reporte si lo desea.
Postcondición	El usuario operativo obtiene el reporte con las métricas y estadísticas de las transacciones solicitadas, y tiene la opción de guardar o exportar los datos.
Excepciones	- Si el usuario operativo no tiene permisos suficientes para acceder a esa sección, el sistema muestra un mensaje de error indicando que no tiene acceso. - Si ocurre un error técnico al generar el reporte (por ejemplo, un problema de conexión o de datos), el sistema muestra un mensaje informando que no se pudo obtener la información y sugiere intentar más tarde. - Si no hay datos que coincidan con la consulta (por ejemplo, si no existen transacciones en el rango de fechas seleccionado), el sistema informa al usuario operativo que no se encontraron resultados.

Caso de uso: Generar reportes de transacciones con patrones inusuales	
Actores	Usuario administrador, sistema de monitoreo de fraudes (microservicio)

Precondición	El usuario administrador debe estar autenticado en el sistema y tener permisos de administrador para generar reportes de transacciones con patrones inusuales.
Escenario	1. El usuario administrador inicia sesión en la plataforma con sus credenciales. 2. El usuario administrador navega hasta la sección de reportes de transacciones. 3. El sistema presenta las opciones de reportes disponibles (por ejemplo, transacciones con montos inusuales, transacciones realizadas fuera del horario habitual, transacciones de ubicaciones sospechosas, etc.). 4. El usuario administrador selecciona el tipo de reporte que desea generar (por ejemplo, transacciones con montos anómalos). 5. El sistema aplica los algoritmos de detección de patrones inusuales sobre las transacciones registradas, basándose en los criterios definidos (por ejemplo, transacciones por encima de un monto específico, transacciones realizadas en horarios fuera de lo común, etc.). 6. El sistema genera el reporte con los resultados y lo presenta al usuario administrador en forma de una tabla o gráfico. 7. El usuario administrador puede visualizar los detalles de las transacciones con patrones inusuales o exportar el reporte para su análisis o archivado.
Postcondición	El reporte de transacciones con patrones inusuales es generado y mostrado al usuario administrador. El reporte puede ser descargado o guardado según lo desee el usuario.
Excepciones	- Si el usuario administrador no tiene permisos suficientes para generar este tipo de reportes, el sistema muestra un mensaje de error indicando que no tiene acceso. - Si el sistema no puede generar el reporte debido a un error técnico (por ejemplo, falla en la conexión con la base de datos), el sistema muestra un mensaje informando que no se pudo completar la operación y sugiere intentar más tarde. - Si no se encuentran transacciones que cumplan con los patrones inusuales especificados, el sistema muestra un mensaje indicando que no se encontraron resultados.

Caso de uso: Configurar los niveles de revisión para transacciones	
Actores	Usuario operativo
Precondición	El usuario operativo debe estar autenticado en el sistema y tener los permisos necesarios para configurar los niveles de revisión para las transacciones.

Escenario	1. El usuario operativo inicia sesión en la plataforma con sus credenciales. 2. El usuario accede a la sección de configuración de los niveles de revisión para transacciones. 3. El sistema muestra las opciones de configuración de niveles de revisión disponibles (por ejemplo, bajo, medio, alto, urgente). 4. El usuario selecciona un nivel de revisión para configurar. 5. El usuario define los criterios que determinarán cuándo una transacción será clasificada en ese nivel de revisión (por ejemplo, monto de la transacción, frecuencia de transacciones del mismo usuario, ubicación sospechosa, etc.). 6. El usuario guarda los cambios en la configuración. 7. El sistema actualiza la configuración de los niveles de revisión y confirma que la configuración se ha guardado correctamente.
Postcondición	Los niveles de revisión para las transacciones han sido configurados y guardados correctamente. Las transacciones futuras serán clasificadas de acuerdo con los nuevos criterios establecidos.
Excepciones	- Si el usuario no tiene permisos suficientes para realizar cambios en la configuración, el sistema muestra un mensaje de error indicando que no tiene acceso para modificar los niveles de revisión. - Si el sistema experimenta un error técnico (por ejemplo, fallos en la base de datos), el sistema informa que no se pudo guardar la configuración y sugiere intentar más tarde. - Si el usuario intenta configurar criterios de revisión sin ingresar valores válidos (por ejemplo, valores fuera de rango para el monto de la transacción), el sistema muestra un mensaje indicando que los datos ingresados son incorrectos.

Caso de uso: Realizar análisis detallados de patrones anómalos	
Actores	Usuario analista de seguridad
Precondición	- Las transacciones sospechosas deben estar previamente registradas y marcadas en el sistema. - El analista debe estar autenticado en el sistema con permisos para acceder al historial de transacciones y herramientas de análisis.

Escenario	1. El usuario analista de seguridad inicia sesión en la plataforma con sus credenciales. 2. El analista selecciona la sección de "Análisis de Patrones Anómalos" 3. El sistema muestra una lista de transacciones sospechosas agrupadas por criterios relevantes (por ejemplo: frecuencia, ubicación geográfica, tipo de irregularidad). 4. El analista selecciona un grupo de transacciones para analizar más a fondo. 5. El sistema presenta datos detallados, como: - Historial de transacciones del cliente. - Comparación con patrones de comportamiento normales. - Indicadores clave (por ejemplo, montos inusuales, horas de operación no comunes). - Visualizaciones como gráficos o mapas para identificar tendencias. 6. Basado en los datos, el analista puede: - Confirmar si las transacciones son fraudulentas. - Identificar nuevos patrones sospechosos que no estaban contemplados en las reglas actuales. - Marcar transacciones relacionadas para investigación adicional. 7. El analista registra sus hallazgos en el sistema y toma una de las siguientes acciones: - Solicitar ajustes a las reglas de detección. - Escalar el caso a otro equipo si el impacto es significativo. - Generar un reporte detallado para auditorías.
Postcondición	- Los hallazgos del analista quedan registrados en el sistema para futuras referencias. - Se identifica si las transacciones son legítimas, fraudulentas o requieren más investigación. - Las reglas o patrones del sistema pueden ser ajustados según sea necesario.
Excepciones	- El sistema alerta al analista sobre datos incompletos o errores en el registro de transacciones. - Si hay un error técnico en la generación de visualizaciones, el sistema ofrece alternativas, como exportar datos en tablas o gráficos básicos.

Caso de uso: Administrar usuarios y roles del sistema	
Actores	Usuario administrador
Precondición	El administrador debe estar autenticado con credenciales que le otorguen permisos de gestión de usuarios y roles.

Escenario	1. El administrador accede a la sección de "Gestión de usuarios y roles" en el sistema. 2. El sistema muestra una lista de usuarios existentes junto con sus roles actuales. 3. El administrador selecciona una de las siguientes opciones: - Crear un nuevo usuario. - Editar un usuario existente. - Eliminar un usuario. - Crear o modificar roles (Por ejemplo, permisos). 4. El sistema valida los cambios realizados por el administrador. 5. Los cambios se guardan en la base de datos y se reflejan en el sistema. 6. El sistema confirma mediante un mensaje en pantalla que la operación fue exitosa.
Postcondición	- Los datos actualizados del usuario o rol quedan reflejados en el sistema. - Los usuarios afectados tienen sus permisos ajustados según el cambio realizado.
Excepciones	- Si los datos están incompletos o inválidos al crear o editar un usuario, el sistema muestra un mensaje de error indicando los campos que deben corregirse. - Si se intenta eliminar un usuario crítico (por ejemplo, si hay un único usuario administrador), el sistema bloquea la operación y notifica que no se puede completar la acción. - Si hay un fallo en la conexión con la base de datos, el sistema muestra una alerta indicando que no se pudieron guardar los cambios y sugiere intentar más tarde. - Si al momento de asignar permisos a un rol se generan conflictos (por ejemplo, permisos duplicados), el sistema alerta al administrador.