**UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS**

UNIVERSIDAD DEL PERÚ, DECANA DE AMÉRICA



**SGI – Documento de Pruebas de Validación del Software**

**Curso:** Gestión de Configuración de Software

**Integrantes (Grupo N° 5):**

* Balarezo Ramos, Luis Jesús
* Durand Caracuzma, Marlon Milko
* Del Aguila Febres, Brayan Tadeo
* Balceda Delgado, Mariana Alejandra
* Canecillas Contreras, Juan Mariano
* Soller Barnechea, Carlos Javier
* Huarhua Piñas, Edson Sebastian
* Justiniano Quispe, Diego André

**Índice**

[**Introducción** 3](#_Toc136434916)

[**Objetivo de las Pruebas** 3](#_Toc136434917)

[**Estrategia de las Pruebas** 3](#_Toc136434918)

[**Caso de Pruebas por Caso de Uso** 4](#_Toc136434919)

[**Criterio de Pruebas** 5](#_Toc136434920)

[**Acercamiento de las Pruebas** 28](#_Toc136434921)

# **Introducción**

Este documento identificará las características que serán probadas mediante el diseño y sus pruebas asociadas, identificará los procedimientos para ejecutar las pruebas definidas y especificará casos de prueba específicos para las funcionalidades del Sistema de Gestión de Incidencias.

# **Objetivo de las Pruebas**

El objetivo de este documento es ampliar el plan de pruebas y proporcionar la información específica requerida para realizar las pruebas. Al proporcionar detalles e información, reducimos la probabilidad de pasar por alto elementos, mejorando la cobertura y calidad de las pruebas.

# **Estrategia de las Pruebas**

En el marco del proyecto de desarrollo del Sistema de Gestión de Incidencias, se llevarán a cabo varios tipos de pruebas con el objetivo de garantizar la calidad y funcionalidad del sistema. A continuación, se detallan los diferentes tipos de pruebas que se realizarán:

**Pruebas del sistema**

Las pruebas del sistema se llevarán a cabo para validar los flujos completos del sistema y evaluar si cumple con los requisitos y comportamiento especificados. Estas pruebas implicarán la ejecución exhaustiva de diferentes escenarios y casos de uso, verificando la correcta funcionalidad del sistema en aspectos clave como el registro de incidencias, asignación de incidencias a miembros del equipo, resolución de incidencias, comunicación con los usuarios y generación de informes. El objetivo es asegurar que todas las funcionalidades del sistema estén implementadas de manera adecuada y se comporten según lo esperado.

**Pruebas exploratorias**

Dado que no se cuenta con documentación detallada por parte del proveedor del sistema de gestión de incidencias, se llevarán a cabo pruebas exploratorias para comprender y documentar el comportamiento real de la aplicación. Estas pruebas consistirán en investigar y experimentar con la aplicación para descubrir su funcionalidad, flujos de trabajo y posibles problemas. El enfoque estará en explorar cómo los diferentes usuarios interactúan con el sistema, cómo se gestionan las incidencias y cómo se generan los informes. El objetivo es identificar cualquier brecha en la documentación existente y obtener un mejor entendimiento del sistema.

**Pruebas de aceptación**

Las pruebas de aceptación se realizarán para evaluar si el sistema cumple con los requisitos de gestión de incidencias y si está listo para su implementación. Estas pruebas se basarán en los criterios de aceptación previamente definidos y validarán que el sistema se ajuste a las necesidades del usuario y a las expectativas establecidas. Los escenarios de prueba se centrarán en la funcionalidad principal del sistema, incluyendo la correcta creación y seguimiento de incidencias, la asignación adecuada de responsabilidades, la generación de informes y la comunicación efectiva con los usuarios.

**Pruebas de humo**

Se realizarán pruebas de humo, las cuales consisten en un conjunto breve y enfocado de tareas para validar la estabilidad y capacidad de prueba del sistema. Estas pruebas se ejecutarán de manera rápida para verificar si las principales funcionalidades del sistema están funcionando correctamente y si no existen errores graves que impidan su uso. El objetivo es identificar cualquier problema importante que pueda surgir antes de realizar pruebas más exhaustivas.

**Pruebas de regresión**

Una vez que todas las características del sistema hayan sido validadas y comprendidas por completo, se definirá un conjunto de pruebas de regresión. Estas pruebas se llevarán a cabo para garantizar que lo desarrollado y probado anteriormente siga funcionando como se espera. Se ejecutarán casos de prueba específicos para verificar que los cambios o correcciones realizados en el sistema no

# **Caso de Pruebas por Caso de Uso**

**Requerimiento 1: Creación de Cuenta**

**[ID] Nombre:** [TC0001] Creación de Cuenta

**Resumen:** Este caso de prueba validará el proceso de creación de cuenta en el sistema.

**Caso de uso a probar:** El usuario puede crear una nueva cuenta.

**Usuarios:** Todos los usuarios.

**Precondiciones:** Ninguna.

**Pasos:**

1. El usuario accede a la página de registro.
2. El usuario ingresa la información requerida, como nombre, correo electrónico y contraseña.
3. El usuario acepta los términos y condiciones.
4. El usuario envía el formulario de registro.
5. El sistema verifica la unicidad del correo electrónico y la fortaleza de la contraseña.
6. El sistema crea una nueva cuenta con la información proporcionada.
7. El sistema genera un identificador único para la nueva cuenta.
8. El sistema envía un correo electrónico de confirmación al usuario.
9. El usuario accede al correo electrónico y hace clic en el enlace de confirmación.
10. El sistema verifica la confirmación y activa la cuenta.

**Resultado esperado:**

* El usuario es redirigido a una página de confirmación después de enviar el formulario de registro.
* El usuario recibe un correo electrónico de confirmación con un enlace para activar la cuenta.
* Al hacer clic en el enlace de confirmación se activa la cuenta.

**Postcondiciones:** La cuenta del usuario se crea y activa correctamente en el sistema.

**[ID] Nombre:** [TC0002] Registro sin proporcionar información básica requerida

**Resumen:** Este caso de prueba verificará el comportamiento del sistema cuando el usuario intenta registrarse sin proporcionar la información básica requerida.

**Caso de uso a probar:** El usuario no puede registrar una cuenta sin completar la información requerida.

**Usuarios:** Todos los usuarios.

**Precondiciones:** Ninguna.

**Pasos:**

1. El usuario accede a la página de registro.
2. El usuario deja en blanco uno o más campos de información básica requerida, como nombre, correo electrónico o contraseña.
3. El usuario intenta enviar el formulario de registro.

**Resultado esperado:**

* El sistema muestra un mensaje de error indicando que la información básica es obligatoria y solicita al usuario completar los campos faltantes.
* No se crea ninguna cuenta en el sistema.
* El usuario permanece en la página de registro y puede completar la información faltante.

**Postcondiciones:**

* No se crea ninguna cuenta en el sistema debido a la falta de información básica requerida.
* El usuario puede completar los campos faltantes y volver a intentar el registro.

# **Criterio de Pruebas**

• Una prueba se considerará fallida si no se logra el resultado esperado o la salida esperada.

• Se completará un informe de error (bug report) para cada falla y se enviará al equipo de desarrollo para su corrección. Este informe de error debe tener la prioridad y gravedad validadas por el equipo de producto.

• Después de que el equipo de desarrollo complete la corrección de un error, se volverá a probar, siguiendo el Ciclo de Vida del Error definido.

• Todos los defectos o errores deben ser reproducibles y reportados correctamente para evitar tiempos de corrección prolongados.

**[ID] Nombre:** [TC0003] Registro con una contraseña no segura

**Resumen:** Este caso de prueba verificará el comportamiento del sistema cuando el usuario intenta registrarse con una contraseña que no cumple con los requisitos de seguridad.

**Caso de uso a probar:** El usuario no puede registrar una cuenta con una contraseña no segura.

**Usuarios:** Todos los usuarios.

**Precondiciones:** Ninguna.

**Pasos:**

1. El usuario accede a la página de registro.
2. El usuario proporciona la información básica requerida, como nombre, correo electrónico y contraseña.
3. El usuario ingresa una contraseña que no cumple con los requisitos de seguridad (por ejemplo, una contraseña demasiado corta o que no contiene caracteres especiales).
4. El usuario intenta enviar el formulario de registro.

**Resultado esperado:**

* El sistema muestra un mensaje de error indicando que la contraseña no cumple con los requisitos de seguridad y solicita al usuario ingresar una contraseña más segura.
* No se crea ninguna cuenta en el sistema.
* El usuario permanece en la página de registro y puede ingresar una contraseña que cumpla con los requisitos de seguridad.

**Postcondiciones:**

* No se crea ninguna cuenta en el sistema debido a que la contraseña proporcionada no cumple con los requisitos de seguridad.
* El usuario puede ingresar una contraseña más segura y volver a intentar el registro.

**Requerimiento 2: Gestión de Roles**

**[ID] Nombre**: [TC0004] Asignación exitosa de roles y permisos a los usuarios

**Resumen:** Este caso de prueba verificará que el sistema pueda asignar correctamente roles y permisos a los usuarios.

**Caso de uso a probar:** Asignación de roles y permisos a los usuarios.

**Usuarios:** Administradores del sistema.

**Precondiciones:**

El administrador ha iniciado sesión en el sistema.

Existen roles y permisos definidos en el sistema.

**Pasos:**

1. El administrador accede al panel de control del sistema.
2. El administrador selecciona la opción "Gestión de Roles".
3. El sistema muestra una lista de roles disponibles junto con una descripción de cada uno.
4. El administrador selecciona un usuario al cual asignar un rol.
5. El sistema muestra una lista de roles disponibles para asignar al usuario seleccionado.
6. El administrador selecciona el rol adecuado que define los permisos necesarios para el usuario.
7. El administrador confirma la asignación del rol y permisos.
8. El sistema guarda la asignación de rol y permisos y muestra un mensaje de confirmación.
9. El administrador verifica que el usuario tenga el rol y permisos asignados correctamente en su perfil.

**Resultado esperado:**

* El sistema asigna correctamente el rol y permisos al usuario seleccionado.
* El usuario ahora tiene los permisos definidos por el rol asignado.
* El administrador recibe una confirmación visual de que la asignación se realizó correctamente.

**Postcondiciones:**

* El usuario cuenta con el rol y permisos asignados, lo que le permite acceder a las funcionalidades correspondientes según su rol.
* El sistema guarda correctamente la asignación de rol y permisos en la base de datos.

**[ID] Nombre:** [TC0005] Asignación de roles incorrectos Resumen: Este caso de prueba verificará que el sistema no permita la asignación de roles incorrectos a los usuarios.

**Caso de uso a probar:** Asignación de roles a los usuarios.

**Usuarios:** Administradores del sistema.

**Precondiciones:**

El administrador ha iniciado sesión en el sistema.

Existen roles definidos en el sistema.

**Pasos:**

1. El administrador accede al panel de control del sistema.
2. El administrador selecciona la opción "Gestión de Roles".
3. El sistema muestra una lista de roles disponibles junto con una descripción de cada uno.
4. El administrador selecciona un usuario al cual asignar un rol.
5. El sistema muestra una lista de roles disponibles para asignar al usuario seleccionado.
6. El administrador selecciona un rol incorrecto que no corresponde a las responsabilidades del usuario.
7. El administrador confirma la asignación del rol incorrecto.
8. El sistema intenta guardar la asignación de rol y permisos.
9. El sistema muestra un mensaje de error indicando que la asignación no se pudo realizar debido a un rol incorrecto.

**Resultado esperado:**

* El sistema no permite la asignación de roles incorrectos a los usuarios.
* Se muestra un mensaje de error indicando que la asignación no se pudo realizar debido a un rol incorrecto.
* El usuario no adquiere el rol incorrecto en su perfil.

**Postcondiciones:**

* El usuario no cuenta con el rol incorrecto asignado.
* El sistema no guarda la asignación de rol incorrecto en la base de datos.

**[ID] Nombre:** [TC0006] Acceso a recursos protegidos según los roles asignados

**Resumen:** Este caso de prueba verificará que los usuarios tengan acceso correcto a los recursos protegidos de acuerdo a los roles asignados en el sistema.

**Caso de uso a probar:** Acceso a recursos protegidos.

**Usuarios:** Usuarios con roles asignados.

**Precondiciones:**

* Los usuarios han iniciado sesión en el sistema.
* Se han asignado roles a los usuarios en el sistema.

**Pasos:**

1. El usuario inicia sesión en el sistema.
2. El sistema autentica al usuario y muestra la página principal.
3. El usuario intenta acceder a un recurso protegido que requiere un rol específico.
4. El sistema verifica el rol del usuario y su acceso a ese recurso.
5. Si el usuario tiene el rol correcto para acceder al recurso:
   1. El sistema muestra el recurso protegido.
   2. El usuario puede interactuar y realizar acciones permitidas en el recurso.
6. Si el usuario no tiene el rol correcto para acceder al recurso:
   1. El sistema muestra un mensaje de error indicando que el usuario no tiene permisos suficientes para acceder al recurso.
   2. El usuario no puede acceder ni interactuar con el recurso protegido.

**Resultado esperado:**

* El sistema permite el acceso a los recursos protegidos solo a los usuarios con los roles asignados correspondientes.
* Si un usuario tiene el rol correcto, puede acceder y realizar acciones permitidas en el recurso protegido.
* Si un usuario no tiene el rol correcto, se muestra un mensaje de error y no puede acceder ni interactuar con el recurso protegido.

**Postcondiciones:**

* El usuario tiene acceso adecuado a los recursos protegidos según los roles asignados.
* El sistema registra correctamente los intentos de acceso a recursos protegidos por parte de los usuarios y su resultado.

**Requerimiento 3: Autenticación De Usuario**

**[ID] Nombre:** [TC0007] Autenticación exitosa de un usuario válido

**Resumen:** Este caso de prueba verificará que un usuario válido pueda autenticarse correctamente en el sistema.

**Caso de uso a probar:** Autenticación de usuario.

**Usuarios:** Usuarios registrados en el sistema.

**Precondiciones:**

* El usuario ha proporcionado correctamente su nombre de usuario y contraseña durante el registro.
* El usuario ha accedido a la página de inicio de sesión del sistema.

**Pasos:**

1. El usuario accede a la página de inicio de sesión del sistema.
2. El sistema presenta un formulario de inicio de sesión que solicita el nombre de usuario y la contraseña del usuario.
3. El usuario ingresa su nombre de usuario y contraseña correctos en los campos correspondientes del formulario de inicio de sesión.
4. El usuario hace clic en el botón de inicio de sesión.
5. El sistema verifica la información de inicio de sesión ingresada por el usuario.
6. Si la información de inicio de sesión es correcta:
   1. El sistema autentica al usuario.
   2. El sistema redirige al usuario a la página de inicio del sistema de gestión de incidencias.
   3. El usuario tiene acceso a las funcionalidades y recursos permitidos para su rol.
7. Si la información de inicio de sesión es incorrecta:
   1. El sistema muestra un mensaje de error indicando que la información de inicio de sesión es incorrecta.
   2. El usuario no puede acceder al sistema y se le solicita que vuelva a ingresar la información de inicio de sesión.

**Resultado esperado:**

* El sistema autentica correctamente a los usuarios válidos que proporcionan la información de inicio de sesión correcta.
* Los usuarios autenticados tienen acceso adecuado a las funcionalidades y recursos permitidos para su rol.
* Si la información de inicio de sesión es incorrecta, el sistema muestra un mensaje de error y no permite el acceso al sistema.

**Postcondiciones:**

* El usuario ha iniciado sesión correctamente en el sistema.
* El usuario tiene acceso adecuado a las funcionalidades y recursos permitidos para su rol.
* El sistema registra correctamente los intentos de inicio de sesión y su resultado.

**[ID] Nombre:** [TC0008] Autenticación con usuario incorrecto

**Resumen:** Este caso de prueba verificará que un usuario con credenciales incorrectas no pueda autenticarse en el sistema.

**Caso de uso a probar:** Autenticación de usuario.

**Usuarios:** Usuarios registrados en el sistema.

**Precondiciones:**

* El usuario ha proporcionado correctamente su nombre de usuario y contraseña durante el registro.
* El usuario ha accedido a la página de inicio de sesión del sistema.

**Pasos:**

1. El usuario accede a la página de inicio de sesión del sistema.
2. El sistema presenta un formulario de inicio de sesión que solicita el nombre de usuario y la contraseña del usuario.
3. El usuario ingresa un nombre de usuario incorrecto o no registrado en el campo correspondiente del formulario de inicio de sesión.
4. El usuario ingresa una contraseña incorrecta en el campo correspondiente del formulario de inicio de sesión.
5. El usuario hace clic en el botón de inicio de sesión.
6. El sistema verifica la información de inicio de sesión ingresada por el usuario.
7. Si la información de inicio de sesión es incorrecta o el usuario no está registrado:
   1. El sistema muestra un mensaje de error indicando que la información de inicio de sesión es incorrecta.
   2. El usuario no puede acceder al sistema y se le solicita que vuelva a ingresar la información de inicio de sesión.

**Resultado esperado:**

* Si el nombre de usuario no está registrado en el sistema, el sistema muestra un mensaje de error indicando que la información de inicio de sesión es incorrecta.
* Si el nombre de usuario está registrado pero la contraseña no coincide, el sistema muestra un mensaje de error indicando que la información de inicio de sesión es incorrecta.
* El usuario no puede acceder al sistema y se le solicita que vuelva a ingresar la información de inicio de sesión.

**Postcondiciones:**

* El usuario no ha podido autenticarse en el sistema.
* El usuario no tiene acceso a las funcionalidades y recursos del sistema.
* El sistema registra correctamente los intentos de inicio de sesión fallidos.

**[ID] Nombre:** [TC0009] Autenticación con contraseña incorrecta

**Resumen:** Este caso de prueba verificará que un usuario con una contraseña incorrecta no pueda autenticarse en el sistema.

**Caso de uso a probar:** Autenticación de usuario.

**Usuarios:** Usuarios registrados en el sistema.

**Precondiciones:**

* El usuario ha proporcionado correctamente su nombre de usuario y contraseña durante el registro.
* El usuario ha accedido a la página de inicio de sesión del sistema.

**Pasos:**

1. El usuario accede a la página de inicio de sesión del sistema.
2. El sistema presenta un formulario de inicio de sesión que solicita el nombre de usuario y la contraseña del usuario.
3. El usuario ingresa su nombre de usuario válido en el campo correspondiente del formulario de inicio de sesión.
4. El usuario ingresa una contraseña incorrecta en el campo correspondiente del formulario de inicio de sesión.
5. El usuario hace clic en el botón de inicio de sesión.
6. El sistema verifica la información de inicio de sesión ingresada por el usuario.
7. Si la contraseña ingresada no coincide con la contraseña registrada para el usuario:
   1. El sistema muestra un mensaje de error indicando que la información de inicio de sesión es incorrecta.
   2. El usuario no puede acceder al sistema y se le solicita que vuelva a ingresar la información de inicio de sesión.

**Resultado esperado:**

* Si la contraseña ingresada no coincide con la contraseña registrada para el usuario, el sistema muestra un mensaje de error indicando que la información de inicio de sesión es incorrecta.
* El usuario no puede acceder al sistema y se le solicita que vuelva a ingresar la información de inicio de sesión.

**Postcondiciones:**

* El usuario no ha podido autenticarse en el sistema.
* El usuario no tiene acceso a las funcionalidades y recursos del sistema.
* El sistema registra correctamente los intentos de inicio de sesión fallidos.

**Requerimiento 4: Registro de Incidencias**

**[ID] Nombre**: [TC0010] Registro exitoso de una incidencia con información relevante

**Resumen:** Este caso de prueba verificará que se pueda realizar el registro exitoso de una incidencia con información relevante en el sistema.

**Caso de uso a probar:** Registro de incidencias.

**Usuarios:** Usuarios del sistema.

**Precondiciones:**

El usuario ha accedido al sistema y ha iniciado sesión correctamente.

**Pasos:**

1. El usuario accede a la opción de registro de incidencias a través de la interfaz principal.
2. El usuario selecciona la opción para crear un nuevo registro de incidencia.
3. El usuario proporciona la siguiente información relevante:
4. Descripción detallada del problema.
5. Fecha y hora de ocurrencia de la incidencia.
6. Usuarios afectados por la incidencia.
7. Cualquier información adicional relevante.
8. Una vez completada la información, el usuario envía el registro de la incidencia para su procesamiento.
9. El sistema registra la incidencia con la información proporcionada.
10. El sistema muestra un mensaje de confirmación indicando que la incidencia se ha registrado exitosamente.

**Resultado esperado:**

* El sistema registra correctamente la incidencia en el sistema, almacenando todos los datos relevantes proporcionados por el usuario.
* El usuario recibe un mensaje de confirmación indicando que la incidencia se ha registrado exitosamente.

**Postcondiciones:**

* La incidencia se ha registrado en el sistema y está disponible para su posterior seguimiento y resolución.
* El usuario puede visualizar la incidencia registrada en su historial de incidencias o en la lista general de incidencias del sistema.

**[ID] Nombre:** [TC0011] Registro de una incidencia sin especificar la categoría

**Resumen**: Este caso de prueba verificará que no sea posible registrar una incidencia sin especificar la categoría en el sistema.

**Caso de uso a probar:** Registro de incidencias.

**Usuarios:** Usuarios del sistema.

**Precondiciones:**

El usuario ha accedido al sistema y ha iniciado sesión correctamente.

**Pasos:**

1. El usuario accede a la opción de registro de incidencias a través de la interfaz principal.
2. El usuario selecciona la opción para crear un nuevo registro de incidencia.
3. El usuario proporciona la siguiente información relevante:
4. Descripción detallada del problema.
5. Fecha y hora de ocurrencia de la incidencia.
6. Usuarios afectados por la incidencia.
7. Cualquier información adicional relevante.
8. El usuario omite seleccionar una categoría para la incidencia.
9. Una vez completada la información, el usuario intenta enviar el registro de la incidencia para su procesamiento.

**Resultado esperado:**

* El sistema muestra un mensaje de error indicando que la categoría de la incidencia no ha sido especificada.
* El usuario no puede completar el registro de la incidencia hasta que seleccione una categoría válida.

**Postcondiciones:**

* No se registra una incidencia sin especificar la categoría en el sistema.
* El usuario debe seleccionar una categoría válida antes de poder enviar el registro de la incidencia.

**[ID] Nombre:** [TC0012] Registro de una incidencia sin proporcionar información adicional

**Resumen:** Este caso de prueba verificará que no sea posible registrar una incidencia sin proporcionar información adicional en el sistema.

**Caso de uso a probar:** Registro de incidencias.

**Usuarios:** Usuarios del sistema.

**Precondiciones:**

El usuario ha accedido al sistema y ha iniciado sesión correctamente.

**Pasos:**

1. El usuario accede a la opción de registro de incidencias a través de la interfaz principal.
2. El usuario selecciona la opción para crear un nuevo registro de incidencia.
3. El usuario proporciona la siguiente información relevante:
4. Descripción detallada del problema.
5. Fecha y hora de ocurrencia de la incidencia.
6. Usuarios afectados por la incidencia.
7. El usuario omite proporcionar información adicional sobre la incidencia.
8. Una vez completada la información, el usuario intenta enviar el registro de la incidencia para su procesamiento.

**Resultado esperado:**

* El sistema muestra un mensaje de error indicando que se debe proporcionar información adicional sobre la incidencia.
* El usuario no puede completar el registro de la incidencia hasta que proporcione información adicional válida.

**Postcondiciones:**

* No se registra una incidencia sin proporcionar información adicional en el sistema.
* El usuario debe proporcionar información adicional válida antes de poder enviar el registro de la incidencia.

**Requerimiento 5: Asignación de Incidencias**

**[ID] Nombre:** [TC0013] Asignación exitosa de una incidencia a otro agente según su rol

**Resumen**: Este caso de prueba verificará que sea posible asignar correctamente una incidencia a otro agente del sistema según su rol asignado.

**Caso de uso a probar:** Asignación de incidencias.

**Usuarios:** Administrador del sistema, miembros del equipo.

**Precondiciones:**

* El administrador del sistema ha accedido al panel de control del sistema y ha seleccionado la opción de "Gestión de Roles".
* Existen agentes del equipo con roles asignados en el sistema.

**Pasos:**

1. El administrador del sistema accede al sistema de gestión de incidencias.
2. El administrador selecciona la opción para registrar una nueva incidencia.
3. El administrador completa la información requerida de la incidencia, como la descripción del problema, la fecha y hora de ocurrencia, y los usuarios afectados.
4. El administrador procede a asignar la incidencia a otro agente según su rol asignado.
5. El administrador selecciona el agente adecuado en función de su rol que le permita manejar y resolver incidencias.
6. El administrador guarda la asignación de la incidencia y muestra un mensaje de confirmación.

**Resultado esperado:**

* La incidencia se asigna correctamente al agente seleccionado según su rol asignado.
* El agente asignado puede ver la incidencia en su lista de tareas pendientes.
* El sistema registra correctamente la asignación de la incidencia.

**Postcondiciones:**

* La incidencia ha sido asignada correctamente a otro agente según su rol asignado.
* El agente asignado puede acceder a la incidencia y tomar las acciones necesarias para resolverla.

**[ID] Nombre:** [TC0014] Intento de asignación de una incidencia a un agente no autorizado

**Resumen:** Este caso de prueba verificará que no sea posible asignar una incidencia a un agente no autorizado en el sistema.

**Caso de uso a probar**: Asignación de incidencias.

**Usuarios:** Administrador del sistema, miembros del equipo.

**Precondiciones:**

* El administrador del sistema ha accedido al panel de control del sistema y ha seleccionado la opción de "Gestión de Roles".
* Existen agentes del equipo con roles asignados en el sistema.

Pasos:

1. El administrador del sistema accede al sistema de gestión de incidencias.
2. El administrador selecciona la opción para registrar una nueva incidencia.
3. El administrador completa la información requerida de la incidencia, como la descripción del problema, la fecha y hora de ocurrencia, y los usuarios afectados.
4. El administrador intenta asignar la incidencia a un agente no autorizado en el sistema.
5. El administrador selecciona un agente que no posee el rol adecuado para manejar y resolver incidencias.
6. El administrador intenta guardar la asignación de la incidencia.

**Resultado esperado:**

* El sistema no permite la asignación de la incidencia al agente no autorizado.
* Se muestra un mensaje de error indicando que la asignación no es válida debido al rol del agente seleccionado.
* La incidencia permanece sin asignar y no aparece en la lista de tareas pendientes del agente no autorizado.

**Postcondiciones:**

* La incidencia no se ha asignado al agente no autorizado.
* El sistema registra correctamente que se ha intentado asignar la incidencia a un agente no autorizado.

**[ID] Nombre:** [TC0015] Verificación de la correcta asignación de incidencias

**Resumen:** Este caso de prueba tiene como objetivo verificar que las incidencias se asignen correctamente a los agentes correspondientes en el sistema de gestión de incidencias.

**Caso de uso a probar:** Asignación de incidencias.

**Usuarios:** Administrador del sistema, miembros del equipo.

**Precondiciones:**

* El administrador del sistema ha accedido al panel de control del sistema y ha seleccionado la opción de "Gestión de Roles".
* Existen agentes del equipo con roles asignados en el sistema.
* Hay incidencias registradas y disponibles para asignar.

**Pasos:**

1. El administrador del sistema accede al sistema de gestión de incidencias.
2. El administrador selecciona una incidencia disponible para asignar.
3. El administrador elige un agente apropiado para la resolución de la incidencia.
4. El administrador asigna la incidencia al agente seleccionado.
5. El administrador verifica que la incidencia se haya asignado correctamente al agente.

**Resultado esperado:**

* La incidencia se asigna correctamente al agente seleccionado.
* El sistema actualiza el estado de la incidencia para reflejar que está asignada al agente correspondiente.
* El agente asignado puede ver la incidencia en su lista de tareas pendientes.
* El agente puede acceder a la incidencia, actualizar su estado y resolverla según sea necesario.

**Postcondiciones:**

* La incidencia está correctamente asignada al agente designado.
* El sistema registra la asignación de la incidencia para su seguimiento y control.
* El agente asignado puede trabajar en la resolución de la incidencia de acuerdo con su rol y permisos asignados.

**Requerimiento 6: Priorización de Incidencias**

**[ID] Nombre:** [TC0016] Priorización exitosa de incidencias según su gravedad y tiempos de respuesta

**Resumen:** Este caso de prueba tiene como objetivo verificar que las incidencias se prioricen correctamente en el sistema de gestión de incidencias, de acuerdo con su gravedad y los tiempos de respuesta establecidos.

**Caso de uso a probar:** Priorización de incidencias.

**Usuarios:** Equipo de soporte técnico, administrador del sistema.

**Precondiciones:**

* Existen incidencias registradas en el sistema de gestión de incidencias.
* Se han establecido criterios de priorización basados en la gravedad y los tiempos de respuesta.
* El equipo de soporte técnico y el administrador del sistema tienen acceso al sistema.

**Pasos:**

1. El equipo de soporte técnico accede al sistema de gestión de incidencias.
2. El equipo revisa las incidencias registradas y las clasifica según su gravedad y los tiempos de respuesta establecidos.
3. El equipo asigna a cada incidencia un nivel de prioridad correspondiente.
4. El equipo verifica que las incidencias se hayan priorizado correctamente de acuerdo con los criterios establecidos.
5. El equipo actualiza el estado de las incidencias para reflejar su prioridad asignada.

**Resultado esperado:**

* Las incidencias se priorizan correctamente según su gravedad y los tiempos de respuesta establecidos.
* Las incidencias de mayor gravedad y con tiempos de respuesta más cortos se asignan a niveles de prioridad más altos.
* Las incidencias de menor gravedad y con tiempos de respuesta más largos se asignan a niveles de prioridad más bajos.
* El sistema actualiza el estado de las incidencias para reflejar su nivel de prioridad asignado.

**Postcondiciones:**

* Las incidencias se encuentran correctamente priorizadas en el sistema de gestión de incidencias.
* El equipo de soporte técnico puede trabajar en la resolución de las incidencias de acuerdo con su nivel de prioridad.
* El administrador del sistema puede realizar un seguimiento y control de las incidencias prioritarias.

**[ID] Nombre:** [TC0017] Intento de priorización de una incidencia por parte de un usuario no autorizado

**Resumen:** Este caso de prueba tiene como objetivo verificar que el sistema de gestión de incidencias impida que un usuario no autorizado intente priorizar una incidencia.

**Caso de uso a probar:** Priorización de incidencias.

**Usuarios:** Usuario no autorizado.

**Precondiciones:**

* Existe al menos una incidencia registrada en el sistema de gestión de incidencias.
* El usuario no autorizado tiene acceso al sistema, pero no tiene permisos para priorizar incidencias.

**Pasos:**

1. El usuario no autorizado accede al sistema de gestión de incidencias.
2. El usuario intenta seleccionar una incidencia y asignarle un nivel de prioridad.
3. El sistema verifica los permisos del usuario y detecta que no tiene autorización para priorizar incidencias.
4. El sistema muestra un mensaje de error indicando que el usuario no tiene los permisos necesarios para realizar la priorización.

**Resultado esperado:**

* El sistema impide que el usuario no autorizado intente priorizar una incidencia.
* Se muestra un mensaje de error indicando la falta de permisos para realizar la acción de priorización.

**Postcondiciones:**

* El estado de la incidencia no se modifica.
* El usuario no autorizado no puede realizar la priorización de incidencias.
* El sistema mantiene la integridad de los permisos y restricciones de acceso.

**[ID] Nombre:** [TC0018] Verificación de la correcta priorización de incidencias

**Resumen:** Este caso de prueba tiene como objetivo verificar que el sistema de gestión de incidencias priorice correctamente las incidencias según su gravedad y los tiempos de respuesta establecidos.

**Caso de uso a probar:** Priorización de incidencias.

**Usuarios:** Equipo de soporte técnico.

**Precondiciones:**

* Existen incidencias registradas en el sistema de gestión de incidencias.
* Se han asignado niveles de gravedad y tiempos de respuesta a las incidencias.

**Pasos:**

1. El equipo de soporte técnico accede al sistema de gestión de incidencias.
2. El equipo revisa la lista de incidencias y selecciona una incidencia específica.
3. El equipo analiza la gravedad de la incidencia y los tiempos de respuesta establecidos.
4. El equipo asigna el nivel de prioridad correspondiente a la incidencia según la gravedad y los tiempos de respuesta.
5. El equipo guarda los cambios realizados en la priorización de la incidencia.

**Resultado esperado:**

* El sistema actualiza correctamente el nivel de prioridad de la incidencia de acuerdo con la gravedad y los tiempos de respuesta establecidos.
* La priorización de la incidencia se refleja correctamente en el sistema.
* El equipo de soporte técnico puede verificar que la incidencia ha sido priorizada correctamente.

**Postcondiciones:**

* El estado de la incidencia se actualiza con el nivel de prioridad asignado.
* El sistema mantiene la integridad de la priorización de incidencias.
* El equipo de soporte técnico puede continuar con el proceso de resolución de la incidencia según su prioridad asignada.

# **Acercamiento de las Pruebas**

**Pruebas Exploratorias:** Las Pruebas Exploratorias fueron utilizadas para sumergirse en la aplicación sin restricciones predefinidas, permitiendo un enfoque más intuitivo y basado en la experiencia del tester. Durante estas pruebas, se realizaron diversas acciones y se exploraron diferentes flujos de trabajo, buscando descubrir funcionalidades ocultas, casos límite y posibles problemas de usabilidad.

**Herramientas Utilizadas:** Durante el proceso de pruebas, se emplearon herramientas libres para facilitar el desarrollo de scripts y la creación de tablas de decisiones:

**Scripts de Pruebas:** Se utilizó Selenium WebDriver, una herramienta de automatización de pruebas, para crear scripts que permitieron registrar y reproducir acciones realizadas en la aplicación. Estos scripts automatizados se ejecutaron repetidamente para detectar posibles regresiones y asegurar la estabilidad del sistema.

**Tablas de Decisiones:** Para estructurar y organizar las pruebas, se emplearon hojas de cálculo como Microsoft Excel. En estas tablas de decisiones, se definieron variables y condiciones relevantes, así como los resultados esperados para cada combinación de valores. Esto permitió garantizar una cobertura exhaustiva de los diferentes escenarios posibles durante las pruebas.