**DOCUMENTACIÓN DEL SISTEMA DE INFORMACIÓN**

**CASO PRÁCTICO**

**SISTEMA DE INFORMACIÓN WEB, PARA EL CONTROL DE ASISTENCIA DE ESTUDIANTES DEL COLEGIO “DON BOSCO”**

Objetivo general:

* Desarrollar un sistema de información web, para el control de asistencia de estudiantes del colegio **“DON BOSCO”,** con la finalidad de efectuar un seguimiento académico respecto a informes generados para los padres de familia.

Objetivos específicos:

* Desarrollar el módulo de autenticación y gestión de usuarios, para permitir el acceso seguro y diferenciado de estudiantes, docentes y padres de familia al sistema, asegurando la protección de los datos personales.
* Implementar el módulo de registro de asistencia de los estudiantes, que permita a los docentes marcar la asistencia diaria y genere un historial de cada alumno para facilitar el seguimiento académico.
* Crear un módulo de notificaciones automáticas, para enviar informes de asistencia a los padres de familia a través de correos electrónicos o mensajes, con el fin de mantenerlos informados sobre el estado de asistencia de sus hijos.
* Desarrollar un módulo de generación de informes mediante un dashboard interactivo, con el objetivo de que el personal administrativo y los docentes puedan visualizar y analizar los datos de asistencia, identificando patrones y áreas de mejora.
* Implementar un sistema de reportes detallados de asistencia por períodos específicos, para generar informes personalizados que puedan ser utilizados en reuniones de padres de familia y consejos académicos.
* Integrar un módulo de gestión de datos históricos, que permita almacenar y recuperar información pasada sobre la asistencia de los estudiantes, facilitando la elaboración de estadísticas y el análisis a largo plazo.

**Base de Datos.**

Alumnos

Asistencias

Cursos

I. RECOLECCIÓN REQUISITOS O REQUERIMIENTOS DE USUARIOS

Ejemplo de requisitos para manejar roles de usuario en un sistema de gestión de contenido (CMS):

**1. Requisitos Funcionales**

**1.1. Gestión de Roles**

* **RF1.1.1:** El sistema debe permitir la creación de roles de usuario con nombres únicos.
* **RF1.1.2:** El sistema debe permitir la asignación de permisos específicos a cada rol de usuario, como acceso a módulos, creación, edición o eliminación de contenido.
* **RF1.1.3:** El sistema debe permitir la edición de roles existentes, incluyendo la modificación de su nombre y permisos asignados.
* **RF1.1.4:** El sistema debe permitir la eliminación de roles que no estén asociados a usuarios activos.

**1.2. Asignación de Roles a Usuarios**

* **RF1.2.1:** El sistema debe permitir la asignación de uno o más roles a cada usuario.
* **RF1.2.2:** El sistema debe permitir la reasignación de roles de usuario de forma manual por parte de un administrador.
* **RF1.2.3:** El sistema debe permitir la visualización de los roles asignados a cada usuario en su perfil.

**1.3. Control de Acceso**

* **RF1.3.1:** El sistema debe restringir el acceso a funcionalidades y datos basados en los roles asignados al usuario.
* **RF1.3.2:** El sistema debe mostrar un mensaje de error cuando un usuario intenta acceder a una función o módulo para el cual no tiene permisos.

**2. Requisitos No Funcionales**

**2.1. Seguridad**

* **RNF2.1.1:** El sistema debe garantizar que solo los usuarios con el rol de administrador puedan gestionar roles y permisos.
* **RNF2.1.2:** El sistema debe registrar en un log todas las acciones relacionadas con la creación, edición y eliminación de roles.

**2.2. Usabilidad**

* **RNF2.2.1:** La interfaz de gestión de roles debe ser intuitiva y permitir la búsqueda y filtrado de roles y usuarios de manera eficiente.
* **RNF2.2.2:** El sistema debe proporcionar mensajes claros y descriptivos en caso de error al asignar roles o gestionar permisos.

**2.3. Rendimiento**

* **RNF2.3.1:** El sistema debe poder manejar la gestión de roles y permisos para al menos 100,000 usuarios sin degradación significativa en el rendimiento.

**3. Requisitos de Integración**

* **RI3.1:** El sistema debe integrarse con el módulo de autenticación existente para aplicar los roles y permisos durante el proceso de inicio de sesión.
* **RI3.2:** El sistema debe ser capaz de sincronizar roles y permisos con aplicaciones externas a través de una API.

Este es un ejemplo general, y los requisitos pueden variar dependiendo de las necesidades específicas del proyecto o del entorno en el que se va a implementar el sistema.

II.Realizar la matriz Eisenhower

|  | Matriz de Eisenhower |  |
| --- | --- | --- |
|  | Urgente | No urgente |
| Importante | Creación de roles de usuario  La asignación de permisos específicos a cada rol de usuario  El sistema debe restringir el acceso a funcionalidades  El sistema debe mostrar un mensaje de error | Asignación de uno o más roles a cada usuario.  Reasignación de roles de usuario de forma manual por parte de un administrador.  El sistema debe registrar en un log todas las acciones  La interfaz de gestión de roles debe ser intuitiva y permitir la búsqueda y filtrado de roles El sistema debe poder manejar la gestión de roles y permisos para al menos 100,000 usuarios  El sistema debe integrarse con el módulo de autenticación existente para aplicar los roles |
| No importante | Permitir la edición de roles existentes  Permitir la eliminación de roles  Solo los usuarios con el rol de administrador puedan gestionar roles y permisos. | Permitir la visualización de los roles asignados a cada usuario en su perfil.  Proporcionar mensajes claros y descriptivos en caso de error al asignar roles o gestionar permisos. El sistema debe ser capaz de sincronizar roles y permisos con aplicaciones externas a través de una API |

**SEGUNDA PARTE DEL PROYECTO**

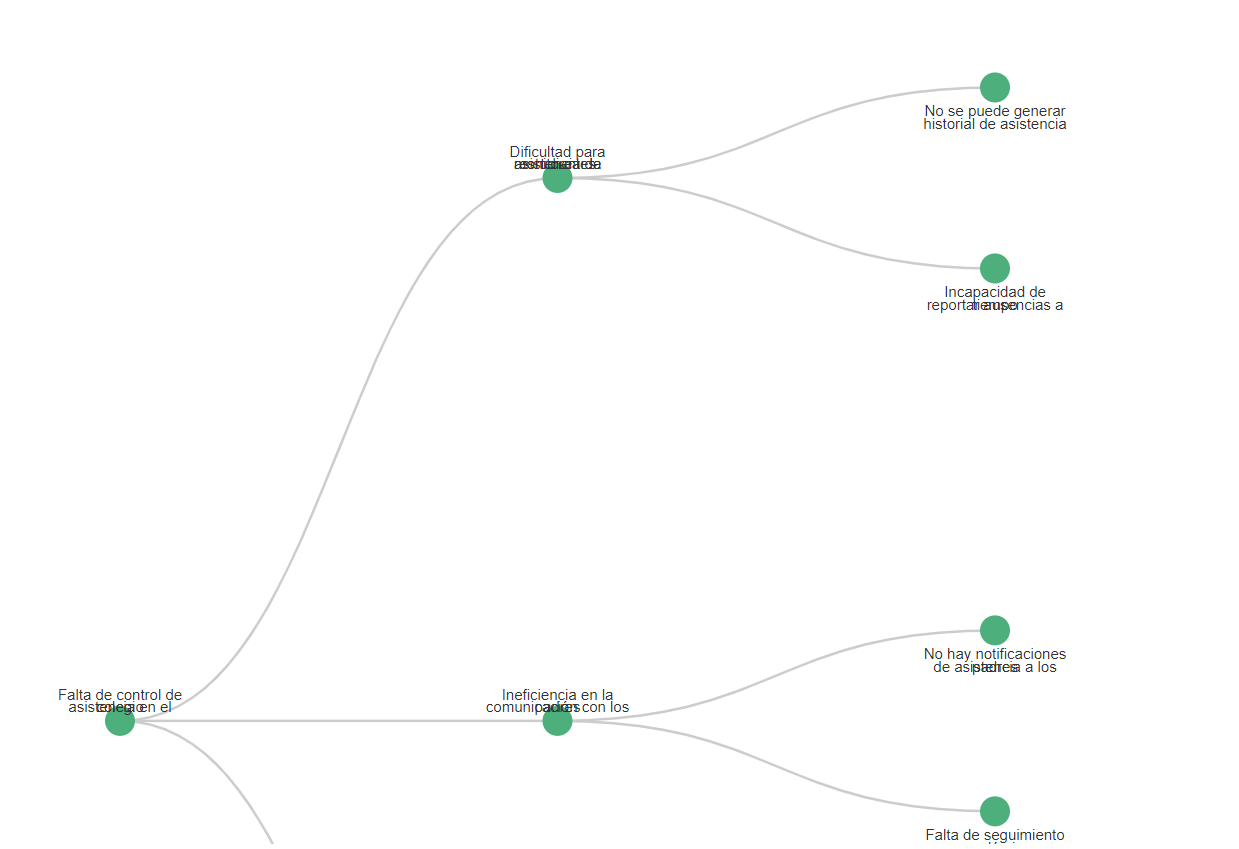
III. Objetivo general:

* Desarrollar un sistema de información web, para el control de asistencia de estudiantes del colegio **“DON BOSCO”,** con la finalidad de efectuar un seguimiento académico respecto a informes generados para los padres de familia.

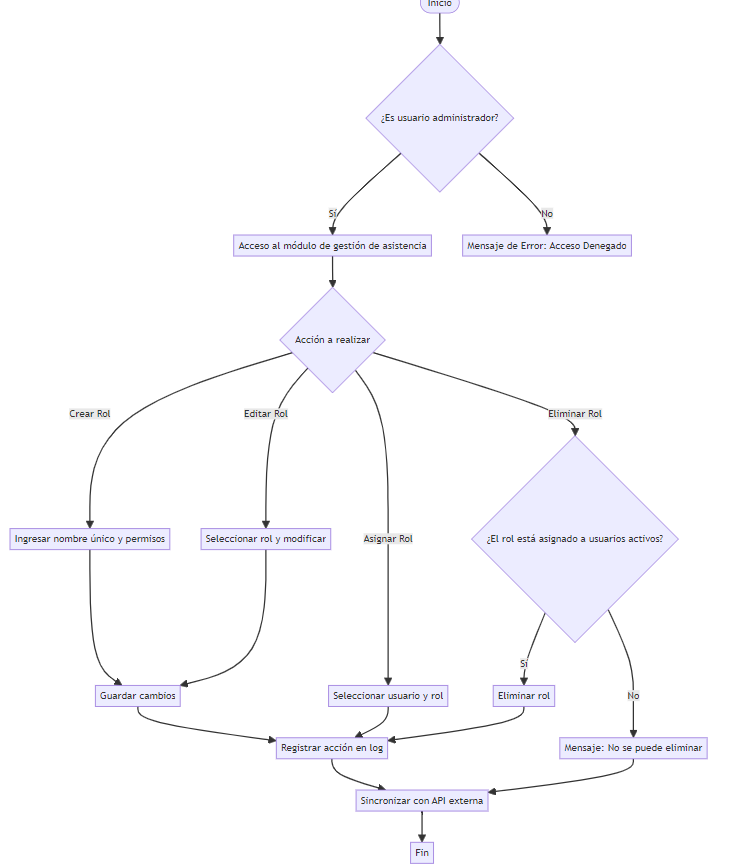
Objetivos específicos:

* Desarrollar el módulo de autenticación y gestión de usuarios, para permitir el acceso seguro y diferenciado de estudiantes, docentes y padres de familia al sistema, asegurando la protección de los datos personales.
* Implementar el módulo de registro de asistencia de los estudiantes, que permita a los docentes marcar la asistencia diaria y genere un historial de cada alumno para facilitar el seguimiento académico.
* Crear un módulo de notificaciones automáticas, para enviar informes de asistencia a los padres de familia a través de correos electrónicos o mensajes, con el fin de mantenerlos informados sobre el estado de asistencia de sus hijos.
* Desarrollar un módulo de generación de informes mediante un dashboard interactivo, con el objetivo de que el personal administrativo y los docentes puedan visualizar y analizar los datos de asistencia, identificando patrones y áreas de mejora.
* Implementar un sistema de reportes detallados de asistencia por períodos específicos, para generar informes personalizados que puedan ser utilizados en reuniones de padres de familia y consejos académicos.
* Integrar un módulo de gestión de datos históricos, que permita almacenar y recuperar información pasada sobre la asistencia de los estudiantes, facilitando la elaboración de estadísticas y el análisis a largo plazo.

IV. Realizar el árbol de problemas y objetivos



V. Realizar un diagrama de flujo



VI. Realizar las historias de Usuarios

|  |
| --- |
| HU1: El sistema debe permitir la creación de roles de usuario con nombres únicos |
| Como: Administrador  Quiero: Crear un rol de Usuario  Para: Poder acceder al espacio de administrador |
| Condiciones:   * Los nombres de Usuario deben ser únicos |

|  |
| --- |
| HU2: El sistema debe permitir la asignación de permisos específicos a cada rol de usuario, como acceso a módulos, creación, edición o eliminación |
| Como: Administrador  Quiero: Asignar permisos específicos a cada rol de usuario  Para: Poder acceder a módulos de creación, edición o eliminación de contenido |
| Condiciones:   * Los permisos deben ser específicos a cada rol de usuario |

|  |
| --- |
| HU3: El sistema debe restringir el acceso a funcionalidades y datos basados en los roles asignados al usuario |
| Como: Administrador  Quiero: Restringir el acceso a funcionalidades y datos basados en los roles asignados a los usuarios  Para: Asegurar que cada usuario solo pueda acceder a las funcionalidades y datos que están autorizados según su rol |
| Condiciones:   * Los usuarios deben ver solo las opciones y datos que están permitidos para su rol. |

|  |
| --- |
| HU4: El sistema debe mostrar un mensaje de error cuando un usuario intenta acceder a una función o módulo para el cual no tiene permisos |
| Como: Administrador  Quiero: Que el sistema muestre un mensaje de error cuando un usuario intenta acceder a una función o módulo para el cual no tiene permisos  Para: Asegurar que los usuarios reciben una notificación clara sobre la falta de permisos y evitar intentos de acceso no autorizado |
| Condiciones:   * Mostrar un mensaje de error claro y específico cuando un usuario sin permisos intente acceder a una función o módulo restringido |

|  |
| --- |
| HU5: El sistema debe permitir la edición de roles existentes, incluyendo la modificación de su nombre y permisos asignados |
| Como: Administrador  Quiero: Editar roles existentes, incluyendo la modificación de su nombre y permisos asignados  Para: Ajustar los roles según las necesidades de la organización y garantizar que los permisos estén actualizados |
| Condiciones:   * Sólo los administradores pueden editar los roles |

|  |
| --- |
| HU6: El sistema debe permitir la eliminación de roles que no estén asociados a usuarios activos |
| Como: Administrador  Quiero: Eliminar roles que no estén asociados a usuarios activos  Para: Eliminar roles obsoletos o no utilizados |
| Condiciones:   * Eliminar roles solo si no están asociados a ningún usuario activo |

|  |
| --- |
| HU7: El sistema debe garantizar que solo los usuarios con el rol de administrador puedan gestionar roles y permisos |
| Como: Administrador  Quiero: Garantizar que solo los usuarios con el rol de administrador puedan gestionar roles y permisos  Para: Asegurar que la gestión de roles y permisos esté restringida a usuarios con autoridad adecuada |
| Condiciones:   * Solo los usuarios con el rol de administrador puedan acceder a las funciones de gestión de roles y permisos |

|  |
| --- |
| HU8: El sistema debe permitir la asignación de uno o más roles a cada usuario |
| Como: Administrador  Quiero: Asignar uno o más roles a cada usuario  Para: Permitir una gestión flexible de permisos y accesos |
| Condiciones:   * Las asignaciones deben estar protegidas por mecanismos de autenticación y autorización adecuados |

|  |
| --- |
| HU9: El sistema debe permitir la reasignación de roles de usuario de forma manual por parte de un administrador |
| Como: Administrador  Quiero: Reasignar roles de usuario de forma manual  Para: Ajustar los permisos y accesos de los usuarios según cambien sus responsabilidades o necesidades en la organización |
| Condiciones:   * Solo un administrador puede reasignar roles |

|  |
| --- |
| HU10: El sistema debe registrar en un log todas las acciones relacionadas con la creación, edición y eliminación de roles |
| Como: Administrador  Quiero: Registrar en un log todas las acciones relacionadas con la creación, edición y eliminación de roles  Para: Tener un historial detallado de cambios en los roles para fines de auditoría, seguridad y resolución de problemas |
| Condiciones:   * Los registros se almacenarán en un log seguro y accesible solo por personal autorizado |

|  |
| --- |
| HU11: La interfaz de gestión de roles debe ser intuitiva y permitir la búsqueda y filtrado de roles y usuarios de manera eficiente |
| Como: Administrador  Quiero: Que la interfaz de gestión de roles sea intuitiva y permita la búsqueda y filtrado de roles y usuarios de manera eficiente  Para: Facilitar la administración y configuración de roles y usuarios |
| Condiciones:   * La interfaz de gestión de roles debe ser intuitiva |

|  |
| --- |
| HU12: El sistema debe poder manejar la gestión de roles y permisos para al menos 100,000 usuarios sin degradación significativa en el rendimiento |
| Como: Administrador  Quiero: Que el sistema maneje la gestión de roles y permisos para al menos 100,000 usuarios sin degradación significativa en el rendimiento  Para: Asegurar que el sistema se mantenga eficiente y rápido incluso con una gran cantidad de usuarios |
| Condiciones:   * No experimentar una degradación significativa en el rendimiento |

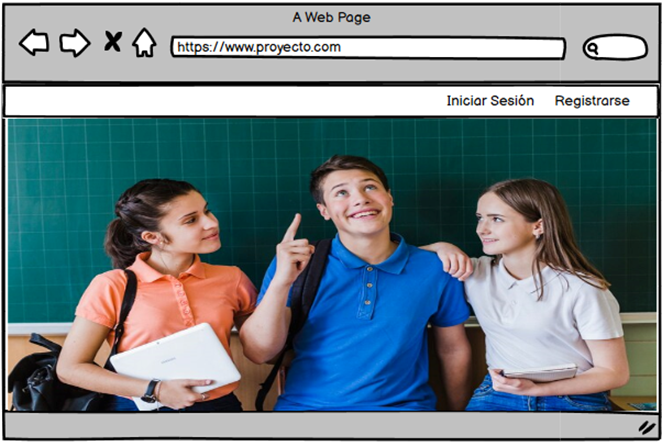
|  |
| --- |
| HU13: El sistema debe integrarse con el módulo de autenticación existente para aplicar los roles y permisos durante el proceso de inicio de sesión |
| Como: Administrador  Quiero: Que el sistema se integre con el módulo de autenticación existente para aplicar los roles y permisos durante el proceso de inicio de sesión  Para: Asegurar que los roles y permisos asignados a los usuarios se apliquen correctamente en el momento del inicio de sesión |
| Condiciones:   * Debe registrarse para luego iniciar sesión |

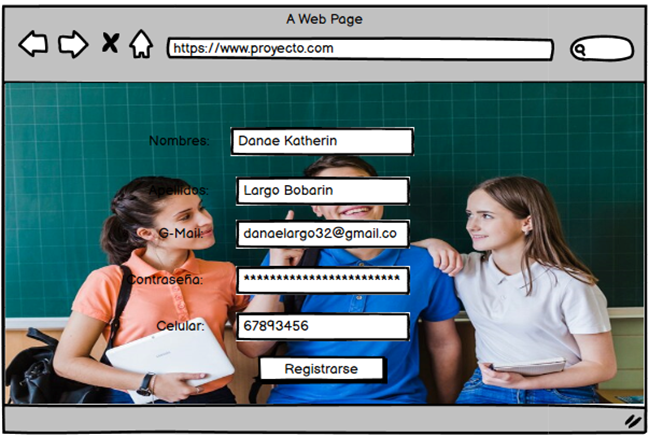
|  |
| --- |
| HU14: El sistema debe permitir la visualización de los roles asignados a cada usuario en su perfil |
| Como: Administrador  Quiero: Que el sistema permita la visualización de los roles asignados a cada usuario en su perfil  Para: Facilitar la revisión y gestión de roles |
| Condiciones:   * Mostrar claramente los roles asignados a cada usuario en su perfil |

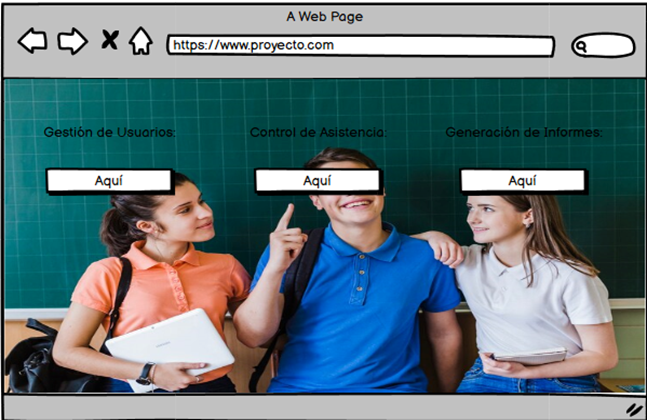
|  |
| --- |
| HU15: El sistema debe proporcionar mensajes claros y descriptivos en caso de error al asignar roles o gestionar permisos |
| Como: Administrador  Quiero: Que el sistema proporcione mensajes claros y descriptivos en caso de error al asignar roles o gestionar permisos  Para: Facilitar la identificación y resolución de problemas |
| Condiciones:   * Mostrar mensajes de error claros y descriptivos si ocurre un problema al asignar roles o gestionar permisos |

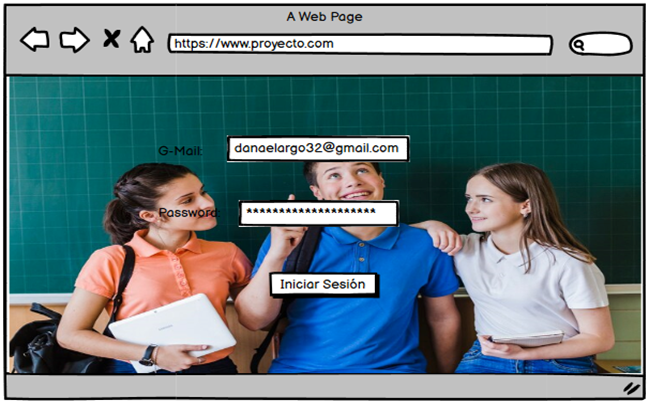
|  |
| --- |
| HU16: El sistema debe ser capaz de sincronizar roles y permisos con aplicaciones externas a través de una API |
| Como: Administrador  Quiero: Que el sistema sea capaz de sincronizar roles y permisos con aplicaciones externas a través de una API  Para: Mantener la coherencia y actualización de roles y permisos en múltiples sistemas y aplicaciones |
| Condiciones:   * Proporcionar una API para la sincronización de roles y permisos con aplicaciones externas |

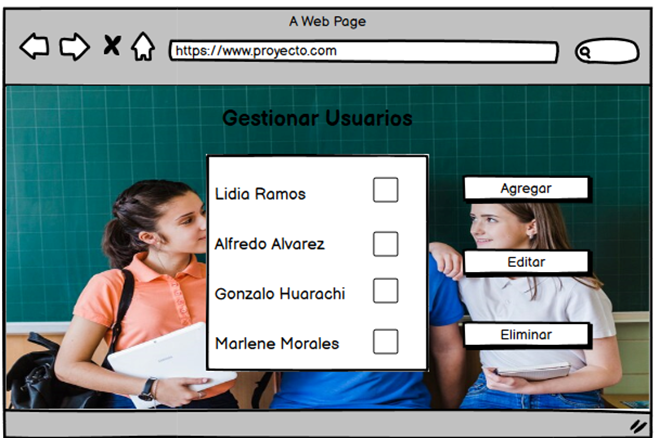
VII. Con los requisitos recolectados, se desea trabajar con un conjunto de interfaces adecuadas a cada usuario, puede elaborarlo en Figma o Balsamiq Mockups











**TERCERA PARTE DEL PROYECTO**

**Casos de uso**