**Contenido**

[**1.** **Introducción:** 2](#_Toc481173065)

[**2.** **Gestión de acceso:** 3](#_Toc481173066)

[**3.** **Gestión de usuario:** 4](#_Toc481173067)

[**4.** **Gestión de permisos:** 5](#_Toc481173068)

[**5.** **Gestión de grupos:** 6](#_Toc481173069)

[**6.** **Gestión de proyectos:** 8](#_Toc481173070)

[**7.** **Gestión de ejecución:** 10](#_Toc481173071)

[**8.** **Gestión de comunicación:** 11](#_Toc481173072)

# **Gestión de acceso:**

|  |  |  |
| --- | --- | --- |
| REF | Nombre | Descripción |
| **1** | **Gestión de acceso** | **Los usuarios deberán poder acceder al sistema.** |
| 1.1 | Autenticación | El usuario será autenticado mediante una identidad la cual contendrá:   * Email * Contraseña |
| 1.1.1 | Creación de identidades | El sistema dispondrá de la opción de crear identidades |
| 1.1.2 | Creación de identidad por parte del sistema | El sistema creara identidades, siguiendo las peticiones de usuarios que deseen entrar en el sistema. |
| 1.1.2.1 | Desactivación de la creación de identidades por parte del sistema | El administrador podrá desactivar la característica del **REQ 1.1.2** |
| 1.1.3 | Creación de identidades por parte del administrador | El administrador podrá crear identidades a los usuarios. |
| 1.2 | Sesiones de autenticación | El acceso del usuario será controlado y monitorizado, con el fin de preservar su seguridad |
| 1.2.1 | Desconexión activa | El sistema permitirá al usuario finalizar la sesión que tiene establecida |
| 1.2.2 | Desconexión pasiva | Pasado un tiempo, si no existe actividad por parte del usuario. El sistema eliminara la sesión referente a la identidad del usuario. |
| 1.3 | Información al usuario | Toda actividad de la gestión de acceso será informada al usuario, cuando realice la acción. |

# **Gestión de usuario:**

|  |  |  |
| --- | --- | --- |
| REF | Nombre | Descripción |
| **2** | **Gestión de usuarios** | **Toda identificación del sistema tendrá información del usuario detrás. Para facilitar su identificación a otros usuarios del sistema.** |
| 2.1 | Creación de usuarios | El usuario podrá rellenar sus datos personales para introducirlos en el sistema |
| 2.1.1 | Datos personales | El usuario podrá introducir los datos personales:   * Nombre * Apellidos * Ciudad, Provincia, País * Fecha de nacimiento * Bibliografía |
| 2.1.2 | Imagen de perfil | El usuario podrá asignar una imagen a su perfil |
| 2.1.3 | Creación de roles | El usuario poseerá un rol que le asignará funcionalidades. Pudiendo ser los roles:   * Usuario * Administrador |
| 2.1.3.1 | Creación de usuarios por el sistema | El sistema creara usuarios con el rol usuario. |
| 2.1.3.2 | Creación de administradores por el administrador | El administrador podrá crear usuarios con el rol administrador. |
| 2.2 | Modificación de usuarios | El usuario podrá modificar sus datos personales en el sistema |
| 2.2.1 | Datos personales | El usuario podrá introducir los datos personales |
| 2.2.2 | Imagen de perfil | El usuario podrá asignar una imagen a su perfil |
| 2.3 | Bloqueo de acceso a usuarios por parte del administrador | El administrador podrá bloquear el acceso a los usuarios. No pudiendo estos acceder al sistema. |

1. **Gestión de permisos:**

|  |  |  |
| --- | --- | --- |
| REF | Nombre | Descripción |
| **3** | **Gestión de permisos** | **Los permisos darán información sobre las acciones que puede realizar un usuario, sobre un proyecto o grupo.** |
| 3.1 | Disponibilidad de tipos de permisos | Existirán distintos tipos de permisos en función de su comportamiento: |
| 3.1.1 | Permisos de compartición | Permisos que actuaran sobre la compartición de proyectos en un grupo específico:   * Compartir proyectos * Remover proyectos propios * Remover proyectos ajenos |
| 3.1.2 | Permisos de propiedades de proyectos | Permisos que actuaran sobre la modificación de propiedades de proyectos en un grupo específico:   * Ejecución de proyectos * Modificar parámetros de entrada |
| 3.1.3 | Permisos sobre miembros | Permisos que actuaran sobre la integración o compartición de miembros a un grupo específico.   * Añadir miembro * Remover miembro |
| 3.1.4 | Permisos sobre creación de grupos | Permisos que actuaran sobre las creaciones de subgrupos de un grupo específico.   * Crear subgrupos (públicos) * Crear subgrupos privados |
| 3.2 | Creación de permisos | La aplicación dispondrá de la creación de permisos para modificar el comportamiento de los grupos. |
| 3.3 | Herencia de permisos | Los permisos heredados por el grupo padre son autoritarios. Siendo heredados por los permisos de todos los subgrupos hijos.  La autorización de permisos no concedidos por el grupo padre, no podrá ser realizada por el subgrupo hijo. |
| 3.4 | Modificación de permisos | Los permisos podrán ser modificados por el creador. |
| 3.4.1 | Modificación de permisos padre | La modificación de permisos de un grupo padre conllevará una modificación de todos los permisos de subgrupos hijos. |

# **Gestión de grupos:**

|  |  |  |
| --- | --- | --- |
| REF | Nombre | Descripción |
| **4** | **Gestión de grupos** | **Todo usuario podrá crear grupos en función de sus permisos e introducirlos en otros grupos.** |
| 4.1 | Creación de grupos | El sistema podrá crear un grupo dando los datos individuales del grupo. |
| 4.1.1 | Tipo de grupo | El grupo podrá ser de diferente tipo, modificando, la visibilidad:   * Publico * Privado * Principal |
| 4.1.1.1 | Tipo publico | Tipo de grupo que podrá ser visible por los miembros del grupo padre |
| 4.1.1.2 | Tipo privado | Tipo de grupo que solo podrá ser visto por sus miembros. |
| 4.1.1.3 | Tipo principal | Grupo raíz de una jerarquía de grupos.  Solo puede ser creado por el administrador. |
| 4.1.2 | Datos del grupo | Son datos que dan individualidad al grupo:   * Nombre * Descripción * Fecha de creación |
| 4.1.3 | Participantes | Agregación de usuarios como miembros del grupo. Estos participantes pueden ser agregados por el propietario del grupo o miembros que contengan permisos de agregación de miembros al grupo. |
| 4.1.4 | Proyectos | Proyectos que contendrá el grupo en cuestión. |
| 4.1.5 | Permisos | El grupo contendrá los permisos siguiendo los requisitos de los **REQ 3** |
| 4.2 | Modificación | El creador del grupo podrá modificar los datos referentes a la creación, salvo los del **REQ 4.1.1** y el nombre del grupo. |
| 4.3 | Eliminación | El usuario creador o el administrador podrán eliminar el grupo. |
| 4.3.1 | Eliminación por propagación | Cuando un grupo padre se elimine, todos sus hijos serán eliminados. Públicos o privado. |
| 4.4 | Compartición | El usuario creador o el usuario podrán invitar a formar parte del grupo a otros usuarios. |
| 4.4.1 | Compartición por propagación | El nuevo miembro del grupo, podrá visualizar todos los subgrupos públicos del grupo compartido. |
| 4.5 | Creación de subgrupos | Un usuario miembro de un grupo, si el grupo contiene los permisos de los **REQ 3.1.4** pertinentes, podrá crear subgrupos. |
| 4.6 | Grupo de visibilidad publica | El sistema proveerá un grupo donde todos los usuarios puedan visualizar proyectos de carácter público.  Sobre este grupo, no se podrán crear grupos, salvo los grupos principales creados por los administradores. |

# **Gestión de proyectos:**

|  |  |  |
| --- | --- | --- |
| REF | Nombre | Descripción |
| **5** | **Gestión de proyectos** | **Todo usuario podrá crear proyectos en el sistema e introducirlos en grupos. Siempre que disponga de permisos correctos.** |
| 5.1 | Creación de proyectos | Cualquier usuario existente en el sistema podrá crear un proyecto, incorporando información para su identificación y posterior ejecución. |
| 5.1.1 | Información básica del proyecto | Incluyendo información básica como:   * Nombre * Descripción * Fecha de creación |
| 5.1.2 | Tipo de proyecto | Información relacionada con la ejecución del proyecto. El sistema proveerá unos tipos diferentes, que serán elegidos por el usuario.   * Python * Octave * Java * ….. |
| 5.1.3 | Credenciales del repositorio | Para la obtención de los códigos de ejecución del proyecto será necesario la información de acceso a un repositorio de protocolo GIT. |
| 5.1.3.1 | URL del repositorio | Sitio web que contendrá el código actualizado para su ejecución. |
| 5.1.3.2 | Credenciales del repositorio | Usuario y contraseña, que será necesaria para el acceso a repositorios privados. |
| 5.1.4 | Descripciones de entrada y salida | Explicación detalla del comportamiento de los inputs y outputs del proyecto, con el fin de dar una información vital a los usuarios que van a utilizarlo. |
| 5.1.5 | Entrada de parámetros por defecto | El propietario del grupo, podrá introducir unos valores por defecto. Para la ejecución de su programa sin modificación de los inputs. |
| 5.2 | Modificación de proyectos | El usuario creador del grupo. Podrá modificar cualquier aparto salvo los requisitos de **REQ 5.1.2** y su nombre. |
| 5.3 | Integración en grupos | El usuario podrá integrar el proyecto en cualquier grupo que sea miembro, donde podrá ser visto y ejecutado por los miembros del grupo |
| 5.3.1 | Integración en grupo publico | El usuario podrá integrar el grupo en un espacio público donde podrá ser visto y ejecutado por cualquier usuario. |
| 5.4 | Eliminación de proyectos | El usuario creador del proyecto, podrá eliminar el proyecto en cualquier momento. Eliminándolo de los grupos compartidos. |

# **Gestión de ejecución:**

|  |  |  |
| --- | --- | --- |
| REF | Nombre | Descripción |
| **6** | **Gestión de ejecución** | **Todo usuario podrá ejecutar un proyecto, siempre que disponga de los permisos correctos.** |
| 6.1 | Introducción de parámetros de entrada | El usuario podrá introducir unos parámetros de entrada, para la ejecución de la salida.  La introducción de parámetros de entrada será condicionada por los permisos de los requisitos **REQ 3.1.2** |
| 6.1.1 | Verificación de los parámetros de entrada | El sistema realizara un análisis de los parámetros, para ver pueden ser ejecutables. |
| 6.2 | Ejecución de proyectos | El sistema ejecutara el proyecto, aportando información sobre el mismo. |
| 6.2.1 | Estado de la ejecución | El sistema tendrá monitorizado el estado. Pudiendo informar al usuario de los posibles estados de ejecución.   * Empezado * Arrancado * Finalizado con error * Finalizado con éxito |
| 6.2.2 | Tiempo de la ejecución | El sistema proporcionara al usuario el tiempo de ejecución. |
| 6.2.3 | Ejecuciones de diferentes proyectos | El sistema podrá ejecutar diversos proyectos:   * Python * Octave |
| 6.3 | Devolución de parámetros de salida | El sistema suministrará al usuario los resultados de las ejecuciones. |
| 6.4 | Visualización de ejecuciones | El usuario podrá ver los listados de las diferentes ejecuciones en función de los estados.   * Ejecuciones acabadas * Ejecuciones en marcha * Ejecuciones con error |
| 6.4.1 | Almacenamiento de ejecuciones | El sistema proveerá de un repositorio de ejecuciones, para recoger las respuestas en cualquier momento. |

# **Requisitos no funcionales:**

|  |  |  |
| --- | --- | --- |
| REF | Nombre | Descripción |
| **1** | **Gestión de comunicación** | **Toda comunicación del sistema deberá ser segura y personal.** |
| 1.1 | Comunicación cifrada | La comunicación entre usuario y cliente deberá estar cifrada para más seguridad. |
| 1.2 | Creación de protocolo de comunicación | La comunicación entre usuario y cliente deberá ser estructurada en forma de protocolo. |
| **2** | **Compatibilidad** | **El sistema deberá poder ejecutarse en diferentes dispositivos** |
| 2.1 | Aplicación web | La aplicación cliente deberá ser web y ejecutada en cualquier SO |
| 2.1.1 | Uso de HTML5 y CSS3 | La aplicación web deberá utilizar los estándares de desarrollo web |
| 2.1.2 | Compatibilidad con navegadores | La aplicación web tendrá que poder ejecutarse en todos los navegadores con soporte HTML5 y CSS3 |
| 2.2 | Repositorio web | El repositorio deberá ser implementar una arquitectura REST |
| 2.2.1 | Compatibilidad con SO | El repositorio podrá ser ejecutado en diferentes SO |
| 3 | Seguridad | La aplicación deberá proporcionar medidas de seguridad |
| 3.1 | Medidas contra acceso a áreas sin autorización | El sistema deberá proteger el acceso contra usuarios sin permiso para acceder a ciertas áreas privadas. |
| 3.2 | Medidas contra CORS | El sistema deberá proteger la peticiones asíncronas del repositorio contra ataques CORS |