UT7 PROYECTO ERASMUS+ GESTIÓN DE USUARIOS, PERFILES

Linda Kate Lovera Fernández

UT7. GESTIÓN DE USUARIOS Y PERMISOS ACTIVIDAD CASO REAL. GESTIÓN DE USUARIOS Y PERMISOS EN ERASMUS+

Análisis previo

El Proyecto Erasmus+ es un programa de la Unión Europea que promueve la movilidad y la cooperación entre instituciones de educación superior, medio en Europa. Uno de los componentes clave del programa es el intercambio de estudiantes, que permite a los estudiantes realizar prácticas de estudios en países europeos.

La base de datos del Proyecto Erasmus+ contiene información sobre los intercambios/movilidades de estos estudiantes, incluyendo los datos personales de los mismos, las instituciones participantes y los períodos de intercambio. Esta información es confidencial y solo debe ser utilizada para fines autorizados. También contiene datos personales respecto a los profesores participantes en el proyecto, así como los tutores e información de diversas pruebas y cursos de idiomas.

Esta política establece los principios y procedimientos para el acceso a la base de datos del Proyecto Erasmus+.

Principios

El acceso a la base de datos del Proyecto Erasmus+ se rige por los siguientes principios:

- **Legalidad:** El acceso a la base de datos debe cumplir con todas las leyes y regulaciones aplicables, incluyendo las leyes de protección de datos.
- **Legitimidad:** El acceso a la base de datos debe estar justificado por un propósito legítimo, como la gestión del programa Erasmus+, la investigación o la elaboración de estadísticas.
- **Necesidad:** El acceso a la base de datos debe limitarse a la información que es necesaria para el propósito legítimo.
- **Proporcionalidad:** El acceso a la base de datos debe ser proporcional al propósito legítimo.
- **Seguridad:** La base de datos debe estar protegida contra el acceso no autorizado, la *alteración*, la *divulgación* o la *destrucción*.

Procedimientos

Para acceder a la base de datos del Proyecto Erasmus+, se debe seguir el siguiente procedimiento:

1. **Solicitud de acceso:** El solicitante debe presentar una solicitud de acceso a la base de datos, en la que se especifique el propósito del acceso, la información que se necesita y las medidas de seguridad que se tomarán para proteger la información.
2. **Evaluación de la solicitud:** La solicitud de acceso será evaluada por el/la responsable del centro estudiantil en gestionar las movilidades de Erasmus+ correspondiente de dicho

centro en el que se encuentra el solicitante. Este responsable, verificará que la solicitud cumpla con los principios establecidos en esta política.

3. Concesión de acceso: Si la solicitud de acceso es aprobada, se proporcionará al solicitante acceso a la base de datos. El acceso estará sujeto a las condiciones establecidas en la política de acceso y a cualquier otra condición que se considere necesaria.

Excepciones

En algunos casos excepcionales, puede concederse acceso a la base de datos del Proyecto Erasmus+ sin necesidad de presentar una solicitud formal. Esto puede incluir, por ejemplo, el acceso a las autoridades policiales en el marco de una investigación criminal.

Revisión y actualización

Esta política de acceso será revisada y actualizada periódicamente para reflejar los cambios en la legislación, la normativa y las prácticas del Proyecto Erasmus+.

A considerar:

- La base de datos del Proyecto Erasmus+ contiene datos personales de los estudiantes y profesorado, por lo que es importante que se tomen todas las medidas necesarias para proteger la privacidad de los mismos.
- La base de datos del Proyecto Erasmus+ se utiliza para fines estadísticos, por lo que es importante que los datos se utilicen de forma responsable y que no se divulguen datos personales.
- El acceso a la base de datos del Proyecto Erasmus+ está sujeto a una tarifa. La tarifa se establecerá en función del volumen de datos a los que se accede y del uso que se haga de los datos.

- Política de usuarios (y roles).

Perfiles de usuarios para el Proyecto Erasmus+

1. Alumnos Aceptados:

- Descripción: Alumnos seleccionados mediante pruebas y entrevistas, para participar en un intercambio de prácticas estudiantiles dentro del programa Erasmus+.
- Funcionalidades:
    - Consultar información sobre su intercambio, como el destino, el centro destino de acogida, las fechas del programa y las becas disponibles.
    - Completar su expediente online, incluyendo datos personales, académicos y de salud.
    - Subir la documentación requerida para el intercambio.
    - Contactar con el tutor del programa Erasmus+ del centro de origen.
    - Acceder a foros y chats para conectarse con otros alumnos participantes.

2. Alumnos Asesores:

- Descripción: Ex-alumnos que participaron en el programa Erasmus+ y que ahora ofrecen apoyo y orientación a los nuevos alumnos seleccionados.
- Funcionalidades:
    - Responder a preguntas de los nuevos alumnos sobre el programa Erasmus+.
    - Compartir sus experiencias y consejos sobre el intercambio.
    - Ofrecer apoyo emocional y cultural a los nuevos alumnos.
    - Participar en eventos y talleres de orientación.

3. Profesores Tutores:

- Descripción: Profesores responsables de guiar y apoyar a los alumnos durante su intercambio Erasmus+.
- Funcionalidades:
    - Revisar y aprobar la documentación de los alumnos.
    - Ofrecer asesoramiento académico y personal a los alumnos.
    - Contactar con el tutor del centro empresarial/académico de acogida.
    - Evaluar el rendimiento académico del alumno durante el intercambio.
    - Validar la estancia del alumno en el país, ciudad de acogida.

4. Profesores Responsables:

- Descripción: Profesores encargados de la gestión general del programa Erasmus+ en el centro estudiantil.
- Funcionalidades:
    - Promocionar el programa Erasmus+ entre los alumnos.
    - Seleccionar a los alumnos participantes.
    - Gestionar las becas y ayudas económicas.
    - Coordinar las relaciones con las instituciones de acogida.
    - Supervisar el desarrollo del programa Erasmus+.
    - Dar de alta a los alumnos como usuarios en el OLS (Sistema Online de Gestión de Aprendizaje).

Consideraciones adicionales:

- El sistema debe permitir a cada perfil de usuario acceder únicamente a las funcionalidades y datos que sean relevantes para su rol.
- Es importante implementar medidas de seguridad para proteger la información personal de los usuarios.
- El sistema debe ser fácil de usar y accesible para todos los usuarios, independientemente de sus conocimientos informáticos.
- Se debe proporcionar formación y soporte técnico a los usuarios para que puedan utilizar el sistema de manera efectiva.

- Asignación de privilegios por perfil de usuario

A continuación, se presenta una tabla que resume los privilegios recomendados para cada perfil de usuario:

Perfil de usuario	Privilegios
Alumnos Aceptados	SELECT sobre sus datos personales, información del intercambio y documentación. UPDATE sobre sus datos personales. SELECT para varias tablas como USUARIOOLS, TESTOLS, PRUEBA_IDIOMAS, REALIZAPRUEBAIDIOMA
Alumnos Asesores	SELECT sobre la información de los alumnos asignados. INSERT y UPDATE sobre comentarios y recomendaciones para los alumnos, que podría añadirse a la tabla misma de alumnosasesoran.
Profesores Tutores	SELECT sobre la información de los alumnos asignados. SELECT, UPDATE sobre tabla tutor de sus mismos datos. UPDATE, INSERT, SELECT sobre la información del intercambio y la documentación de los alumnos. INSERT y UPDATE sobre las evaluaciones del rendimiento académico.
Profesores Responsables	SELECT, INSERT, UPDATE y DELETE sobre la información de los alumnos, intercambios, tutores y usuarios. GRANT para crear nuevos usuarios y asignar privilegios.
NOTA: se detalla más y se crean dichos perfiles en el archivo del script sql.	

Concesión de privilegios con comandos SQL

Los privilegios en MySQL se asignan utilizando el comando GRANT. La sintaxis básica del comando es la siguiente:

GRANT <privilegios> ON <objeto> TO <usuario>@<host>;

Donde:

- <privilegios> es una lista de los privilegios que se conceden, separados por comas.
- <objeto> es el objeto de la base de datos al que se conceden los privilegios, como una tabla o una base de datos completa.
- <usuario> es el nombre del usuario al que se conceden los privilegios.
- <host> es el host desde el que el usuario puede acceder a la base de datos.

Por ejemplo, para conceder a todos los alumnos aceptados el privilegio de SELECT sobre la tabla alumnos, se utilizaría el siguiente comando:

GRANT SELECT ON alumnos TO alumnos@localhost;

Nota:

- En el script de perfilesUsuarios_Privilegios se detallan los comandos utilizados para esto.
- Es importante utilizar el principio de mínimo privilegio, lo que significa que solo se deben conceder a cada usuario los privilegios que necesita para realizar su trabajo.

- Se deben utilizar contraseñas seguras y cambiarlas periódicamente.
- Se debe realizar una auditoría periódica de los privilegios para asegurarse de que no se han concedido privilegios innecesarios.

- Creación/modificación/borrado de cuentas de usuario.

Creación de cuentas de usuario

1. **Solicitud de creación de cuenta:** El usuario interesado deberá presentar una solicitud formal a su responsable directo (usuario prof. Responsable del proyecto), indicando su nombre completo, correo electrónico, perfil de usuario al que solicita pertenecer y una breve justificación del motivo por el que necesita acceso al sistema.
2. **Validación de la solicitud:** El responsable directo del usuario revisará la solicitud y verificará que la información sea correcta y que el usuario tenga una necesidad justificada para acceder al sistema.
3. **Creación de la cuenta:** Si la solicitud es validada, el responsable directo creará la cuenta de usuario en el sistema, asignándole un nombre de usuario, una contraseña segura y los privilegios correspondientes a su perfil de usuario.
4. **Entrega de credenciales:** Las credenciales de acceso (nombre de usuario y contraseña) serán entregadas al usuario de forma confidencial. El usuario deberá cambiar su contraseña por una nueva y segura en el primer acceso al sistema. Esto podría ocurrir a través de la recepción de un email confirmando dichos datos, y activación.

Modificación de cuentas de usuario

1. **Solicitud de modificación de cuenta:** El usuario que desee modificar su cuenta deberá presentar una solicitud formal a su responsable directo, indicando el cambio que desea realizar y la justificación correspondiente.
2. **Validación de la solicitud:** El responsable directo del usuario revisará la solicitud y verificará que la información sea correcta y que el usuario tenga una necesidad justificada para realizar la modificación.
3. **Modificación de la cuenta:** Si la solicitud es validada, el responsable directo modificará la cuenta de usuario en el sistema, según los cambios solicitados.
4. **Notificación al usuario:** El usuario será notificado por correo electrónico de la modificación realizada en su cuenta.

Borrado de cuentas de usuario

1. **Solicitud de borrado de cuenta:** El usuario que desee eliminar su cuenta deberá presentar una solicitud formal a su responsable directo, indicando el motivo por el que desea eliminar la cuenta.
2. **Validación de la solicitud:** El responsable directo del usuario revisará la solicitud y verificará que la información sea correcta y que el usuario tenga una necesidad justificada para eliminar la cuenta.
3. **Borrado de la cuenta:** Si la solicitud es validada, el responsable directo borrará la cuenta de usuario del sistema.

4. Notificación al usuario: El usuario será notificado por correo electrónico de la eliminación de su cuenta.

Caducidad de contraseñas

Las contraseñas de usuario caducarán cada 90 días. El usuario recibirá una notificación por correo electrónico 7 días antes de la fecha de caducidad, invitándolo a cambiar su contraseña. Si el usuario no cambia su contraseña antes de la fecha de caducidad, su cuenta será bloqueada. El usuario podrá desbloquear su cuenta siguiendo las instrucciones que se le enviarán por correo electrónico.

Seguridad de las contraseñas

Las contraseñas de usuario deben ser seguras y confidenciales. Se recomienda que las contraseñas tengan al menos 8 caracteres y que incluyan una combinación de letras mayúsculas, minúsculas, números y caracteres especiales (*-/%&$). De todas formas, se implementará un sistema de cifrado de contraseñas. En caso de no recordarlas, solicitar una recuperación de contraseñas, donde a través de un enlace al email usado para registro se pueda crear una nueva contraseña para dicho usuario.

Responsabilidades

- Responsables directos (prof. Responsables del proyecto): Son responsables de validar las solicitudes de creación, modificación y borrado de cuentas de usuario en su área de responsabilidad.
- Resto de usuarios: Son responsables de mantener la confidencialidad de sus credenciales de acceso y de cambiar su contraseña periódicamente.
- Administrador(es): El o los responsables del área de informática encargado de administrar la base de datos para el proyecto. Tendrá todas las responsabilidades inherentes al mismo sistema.

Auditoría

Se registrará una auditoría de todas las acciones realizadas en las cuentas de usuario, incluyendo la creación, modificación, borrado y cambios de contraseña. Esta auditoría estará disponible para su consulta por parte de los administradores del sistema.

- Revisión de permisos. Revisaremos periódicamente que los permisos concedidos a los usuarios son los adecuados.

El objetivo de este procedimiento es garantizar que los usuarios tengan únicamente los permisos que necesitan para realizar su trabajo y que no tengan acceso a información confidencial a la que no están autorizados.

Frecuencia de las revisiones

Se recomienda realizar una revisión de permisos o privilegios de usuario al menos una vez cada trimestralmente. Sin embargo, hay que tener en cuenta que cada vez que se añada nuevos usuarios porque bien hay un traslado de nuevos ingresos de alumnos, contratación profesor, habrá que añadir nueva revisión de los mismos, aprovechando las circunstancias. Lo mismo cada año que finalicé el proyecto, revisar nuevamente para saber si mantener los usuarios, darlos de baja o quizás pausarlos. Teniendo en cuenta que muchos profesores podrían continuar con el proyecto y los alumnos que quieran continuar de forma de asesores.

Responsabilidades

- Administradores del sistema: Son responsables de realizar las revisiones de permisos o privilegios de usuario.
- Responsables directos (profesores responsables del proyecto): Son responsables de colaborar con los administradores del sistema en la revisión de los permisos o privilegios de usuario de su área de responsabilidad.
- Resto de Usuarios: Son responsables de informar a su responsable directo si sus permisos o privilegios de usuario han cambiado o si ya no necesitan acceso a cierta información.

Procedimiento de revisión

1. Identificación de usuarios: Los administradores del sistema identificarán a todos los usuarios que tienen acceso al sistema de datos del Proyecto Erasmus+.
2. Recopilación de información: Los administradores del sistema recopilarán información sobre los permisos o privilegios actuales de cada usuario. Esta información incluirá el perfil de usuario, las tablas o vistas a las que tiene acceso y las acciones que puede realizar sobre los datos.
3. Análisis de necesidades: Los administradores del sistema analizarán las necesidades de cada usuario para determinar qué permisos o privilegios necesita para realizar su trabajo. Este análisis se realizará en colaboración con los responsables directos de los usuarios, es decir con los profesores responsables del proyecto.
4. Asignación de permisos o privilegios: Los administradores del sistema asignarán los permisos o privilegios adecuados a cada usuario en función de las necesidades identificadas en el análisis.
5. Documentación de cambios: Los administradores del sistema documentarán todos los cambios realizados en los permisos o privilegios de usuario.
6. Notificación a los usuarios: Los usuarios serán notificados por correo electrónico de los cambios realizados en sus permisos o privilegios.

Nota:

- Es importante utilizar el principio de **mínimo privilegio**, lo que significa que solo se deben conceder a cada usuario los permisos que necesita para realizar su trabajo.
- Se deben documentar todos los cambios realizados en los permisos o privilegios de usuario.

- Revocación de permisos y eliminación de cuentas.

En este apartado, se describe el procedimiento para la revocación de permisos y eliminación de cuentas.

Revocación de permisos

1. **Identificar las cuentas:** Los administradores del sistema identificarán las cuentas de usuario que ya no necesitan acceso a la base de datos. Esto incluirá las cuentas de los alumnos que han completado su participación en el proyecto Erasmus+, así como las cuentas de los profesores y tutores que ya no están involucrados en el programa.
2. **Revisión de permisos:** Los administradores del sistema revisarán los permisos de las cuentas identificadas y revocarán aquellos que ya no sean necesarios.
3. **Notificación a los usuarios:** Los usuarios afectados serán notificados por correo electrónico de la revocación de sus permisos.

Eliminación de cuentas

1. **Confirmación de eliminación:** Los administradores del sistema confirmarán con los responsables directos la eliminación de las cuentas identificadas.
2. **Eliminación de cuentas:** Los administradores del sistema eliminarán las cuentas de usuario del sistema de datos.
3. **Eliminación de datos:** Los administradores del sistema eliminarán los datos asociados a las cuentas eliminadas, al hacerlo tiene que ser de forma segura y confidencial. Documentando la revocación de dichos permisos y la eliminación de las cuentas.