Medidas para evitar la fuga de información

Para terminar trataremos de dar respuesta al indicador abajo indicado, mediante unas pequeñas pautas:

> *2.2.B2.2. Utiliza medidas de seguridad para evitar la pérdida de información en situaciones de edición compartida de contenidos educativos digitales,*

1. **Copias de seguridad regulares:**

Las copias de seguridad son una medida esencial para evitar la pérdida de información en situaciones de edición compartida de contenidos educativos digitales. Deben realizase con cierta regularidad y almacenarlas en un lugar seguro. De esta forma, si se produce una pérdida de información debido a un fallo del sistema o un error humano, es posible recuperar los datos a partir de las copias de seguridad.

> *Ejemplo*: Un grupo de estudiantes está trabajando en un proyecto de investigación y han creado una presentación para compartir sus hallazgos. Cada vez que realizan cambios importantes en la presentación, crean una copia de seguridad de la versión anterior y la almacenan en un disco duro externo. De esta manera, si ocurre un error en el servidor de la plataforma en línea o si alguien elimina accidentalmente una parte de la presentación, pueden restaurar la información desde la última copia de seguridad realizada.

2. **Autenticación de usuarios:**

La autenticación de usuarios es una medida de seguridad importante para garantizar que solo los usuarios autorizados tengan acceso a los contenidos educativos digitales compartidos. La autenticación se realiza mediante un nombre de usuario y una contraseña segura. Los usuarios deben asegurarse de que su contraseña sea fuerte y no compartirla con otros.

Copyright 2026

> *Ejemplo*: Un profesor ha creado una carpeta compartida en línea para que los estudiantes puedan subir sus trabajos. Cada estudiante tiene una cuenta de usuario y una contraseña única. El profesor ha asegurado la carpeta compartida con una contraseña adicional, que solo él conoce. De esta forma, solo los estudiantes y el profesor autorizados pueden acceder a la carpeta y ver los trabajos.

3. Control de versiones

El control de versiones es una medida de seguridad que registra todas las ediciones realizadas en un contenido educativo digital y permite a los usuarios volver a versiones anteriores si se produce una pérdida de información. Los sistemas de control de versiones se utilizan comúnmente en el desarrollo de software y también son útiles para los contenidos educativos digitales.

> *Ejemplo*: Un grupo de estudiantes está trabajando en un proyecto de investigación en una plataforma en línea. La plataforma tiene un sistema de control de versiones que registra todas las ediciones realizadas en el proyecto. Si alguien elimina accidentalmente parte del proyecto, los estudiantes pueden volver a una versión anterior y recuperar la información perdida.

4. **Restricción de permisos**

La restricción de permisos es una medida de seguridad importante para evitar la eliminación accidental de información. Los usuarios solo deben tener los permisos necesarios para realizar sus tareas y no más. Si un usuario tiene demasiados permisos, puede eliminar información importante por error.

> *Ejemplo*: Un profesor ha creado un documento compartido en línea para que los estudiantes puedan colaborar en una tarea. Los estudiantes solo tienen permiso para editar partes específicas del documento y no pueden eliminar o modificar otras secciones importantes. De esta forma, se evita que los estudiantes eliminen información importante por error.

5. **Protección de datos**

La protección de datos es una medida de seguridad crítica para cualquier contenido educativo digital. Los contenidos educativos digitales deben protegerse mediante el uso de medidas de

Copyright 2026

seguridad adecuadas, como la encriptación de datos y el uso de firewalls y antivirus. Esto ayuda a evitar la pérdida de información a causa de ciberataques o malware.

> Ejemplo: Un grupo de estudiantes está trabajando en un proyecto y necesitan compartir información confidencial, como números de identificación personal y datos de contacto. Para proteger esta información, los estudiantes utilizan una plataforma de mensajería en línea que utiliza encriptación de extremo a extremo. De esta forma, solo los estudiantes autorizados pueden descifrar los mensajes y acceder a la información confidencial.

Revision #1
Created 2025-01-30 23:07:15 CET by Vladi
Updated 2025-01-30 23:07:15 CET by Vladi

Copyright 2026