# 1.5.2. Seguridad en el acceso, almacenaje y recuperación de la información.

La transformación digital ha llevado a que tanto el alumnado como el profesorado, tenga acceso a una gran cantidad de información en línea. Esto les facilita el acceso a materiales de estudio y herramientas educativas. Sin embargo, el acceso a información digital también implica algunos riesgos. La gestión de la seguridad en el acceso digital y el almacenamiento de información en el ámbito educativo, resulta fundamental para garantizar la privacidad de los datos.

> Para **garantizar la seguridad digital**, se requiere la implementación de medidas de seguridad como el **uso de contraseñas seguras**, la **autenticación de usuarios**, la **validación de acceso** y la **actualización continua de sistemas operativos y aplicaciones** utilizadas.

Por otro lado, el **almacenamiento digital** de información es clave para la **organización de contenidos**, el **trabajo colaborativo** y para la realización de **copias de seguridad** que permitan evitar la pérdida de información en caso de fallos de dispositivos o ataques cibernéticos. Para ello, pueden utilizarse herramientas de **almacenamiento en la nube** tanto gratuitas como de pago. Estas herramientas permiten acceder a la información desde múltiples dispositivos y en diferentes ubicaciones, siempre y cuando se garantice la seguridad de acceso a ellos.

La **recuperación de la información** se refiere a la capacidad de **restaurar** los datos que se han perdido en los dispositivos digitales. Aunque los sistemas de almacenamiento en la nube son una herramienta muy útil, también conllevan riesgos de pérdida de datos. Para minimizar estos riesgos, se debe hacer una copia de seguridad de los materiales más valiosos y guardarlos tanto en **dispositivos físicos** como en servicios de **almacenamiento en línea.**

> La **gestión de la seguridad digital** es una tarea cada vez más importante en el ámbito educativo. La necesidad de garantizar el **acceso seguro a la información**, **proteger la privacidad** y **recuperar la información** son elementos fundamentales para lograr un entorno educativo tranquilo y eficiente en el uso de las nuevas tecnologías. Por ello, la

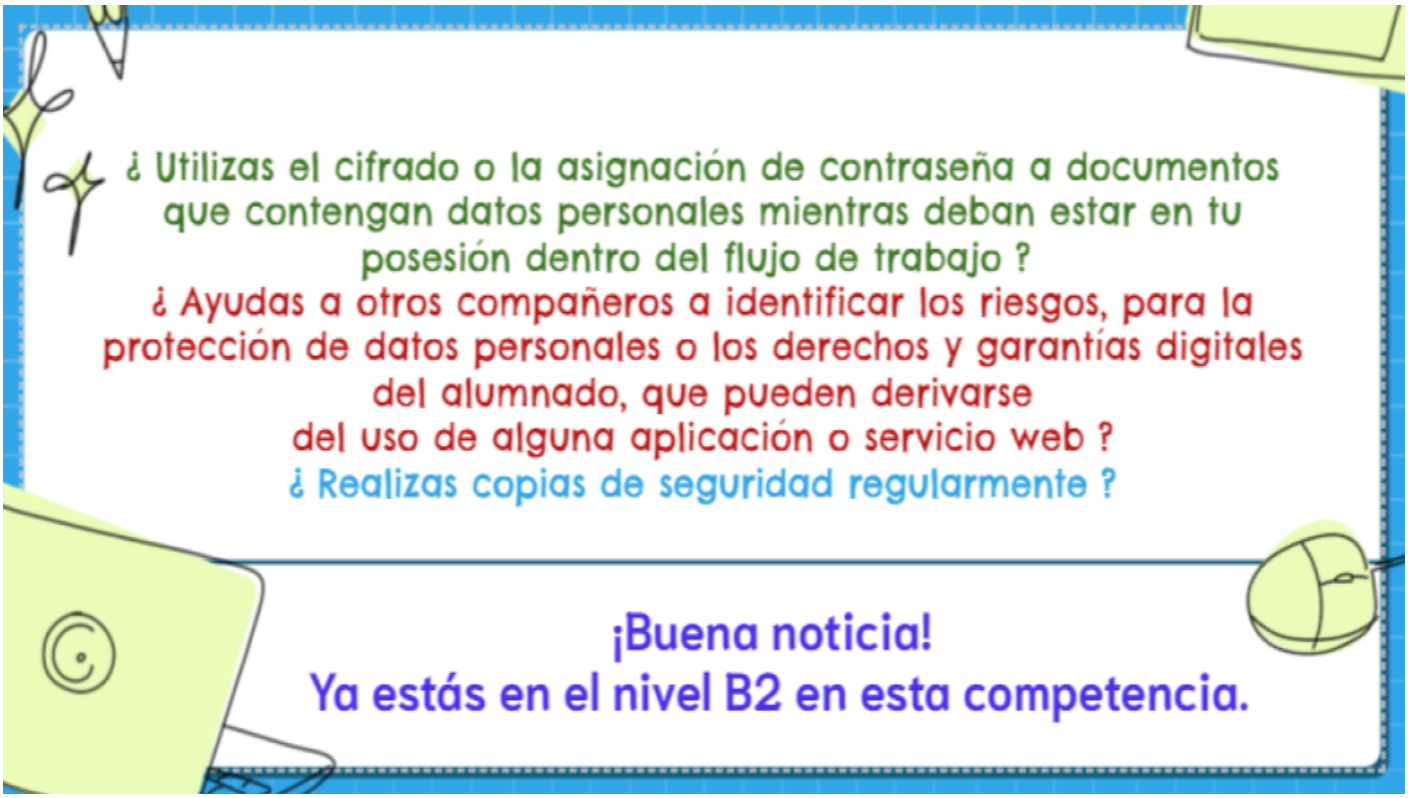
formación y la conciencia sobre estas cuestiones son cada vez más importantes en el ámbito de la educación.

| Medidas de seguridad pasiva | Medidas de seguridad activa |
| --- | --- |
| Las medidas de seguridad pasiva son aquellas que **se aplican de forma permanente** y están diseñadas para **minimizar el riesgo de acceso, almacenamiento y recuperación de información en la red**.<br>Algunas **medidas** de seguridad pasiva son:<br>• **Control de acceso**: limitar el acceso a la información sensible o confidencial a las personas autorizadas mediante la utilización de contraseñas, autenticación de dos factores, control de acceso físico, etc.<br>• **Encriptación**: utilizar sistemas de encriptación para proteger la información durante su almacenamiento y transmisión.<br>• **Copias de seguridad**: realizar copias de seguridad regulares para evitar la pérdida de datos en caso de algún accidente con ellos.<br>• **Firewall**: utilizar firewall para proteger la red de accesos no autorizados.<br>• **Actualización y parches**: mantener actualizado el software y aplicar parches de seguridad para evitar vulnerabilidades.<br>• **Monitoreo y detección**: monitorear la red para detectar y prevenir posible ataques cibernéticos.<br>• **Capacitación de usuarios**: concienciar y capacitar a los usuarios sobre las buenas prácticas de seguridad en la red para evitar incidentes. | Las medidas de seguridad activa son aquellas que **se aplican en tiempo real** y se utilizan para **detectar y responder rápidamente ante un incidente de seguridad en la red**.<br>Algunas **medidas** de seguridad activa son:<br>• **Software antivirus y malware**: utilizar un software específico que detecte y bloquee software malintencionado, virus y programas espía.<br>• **Firewall**: utilizar un firewall como medida no solo de seguridad pasiva sino también activa para controlar el tráfico de la red y evitar instrusiones.<br>• **Detección de intrusos (IDS/IPS)**: configurar sistemas de detección de intrusos y prevención de intrusiones que alerten en caso de una actividad sospechosa en la red.<br>• **Análisis de vulnerabilidades**: realizar análisis periódicos para detectar y corregir vulnerabilidades en la red.<br>• **Monitoreo de la actividad de los usuarios**: supervisar la actividad de los usuarios de la red para detectar comportamientos inusuales o sospechosos.<br>• **Configuración de políticas de seguridad**: establecer políticas y directrices de seguridad clara que ayuden a asegurar que todos los usuarios de la red cumplan con las normas establecidas.<br>• **Respuesta a incidentes**: tener un plan de respuesta de seguridad en caso de un incidente de seguridad en la red, para minimizar su impacto y recueprar la información perdida o dañada. |

Es necesario tomar conciencia de todas estas medidas y aplicar todas aquellas que estén a nuestro alcance:

- Utilizar el **almacenamiento** en la **nube** y también realizar copias de seguridad **físicas** de los documentos importantes.
- Establecer un **calendario** de realización de **copias** de **seguridad** periódico.
- Utilizar **contraseñas** de acceso para los documentos que contengan información sensible. En ocasiones, confiamos en que la información está contenida en una unidad a la que sólo tenemos acceso nosotros, pero cabe la posibilidad, incluso, de extraviarla.

- Instalación de **antivirus** y **actualización** del mismo.
- Uso de **herramientas** y **aplicaciones** seguras y **actualización** de las mismas.
- Evitar compartir documentos de la nube que contengan datos personales para cualquier usuario que tenga el enlace, sino utilizar la opción de **acceso restringido.**




Revision #12
Created 7 April 2023 00:58:13 by María Esther Arilla Luna
Updated 3 November 2023 12:11:41 by María Esther Arilla Luna