Seguridad de la información y privacidad en los centros educativos holandeses

El uso de herramientas digitales para evaluar las tareas del alumnado requiere que docentes, directores escolares y responsables políticos se planteen el modo de garantizar un uso seguro y válido de los datos del alumnado.

Resumen

Kennisnet, organización financiada por el Ministerio de Educación, Cultura y Ciencia, ayuda a los centros educativos neerlandeses a sentar las bases de la seguridad de las TIC. Las herramientas digitales en la educación suscitan nuevas cuestiones en torno a la privacidad, la seguridad de la información, el intercambio y la propiedad de los datos sobre el aprendizaje. Para que docentes y estudiantes utilicen de manera eficaz las pruebas del aprendizaje, deben tener en cuenta estas cuestiones. Además, los responsables políticos deben establecer las condiciones adecuadas. Este estudio de caso describe el contexto neerlandés en relación con las cuestiones de privacidad y un plan de trabajo para establecer los acuerdos adecuados con los vendedores/proveedores en este ámbito.

Contexto

Los centros de educación secundaria de los Países Bajos tienen cierto grado de autonomía en el ámbito educativo. El alumnado de los dos últimos cursos tiene un plan de estudios más o menos «nacional» que contiene el 60 % de los planes de estudio (y que se examina de forma centralizada). El plan de estudios describe con detalle lo que deben saber y ser capaces de hacer. Sin embargo, la interpretación pedagógica depende siempre del profesorado, incluidas las estrategias de aprendizaje. En los Países Bajos hay un examen final centralizado solo para los dos últimos años de la educación secundaria.

Por otro lado, el plan de estudios de los cursos inferiores de educación secundaria ofrece a los centros educativos más libertad a la hora de tomar sus propias decisiones. La **Inspección de Educación**, un organismo vinculado al Gobierno pero con un estatus independiente, se encarga de la supervisión.

Las prácticas de evaluación formativa dependen del centro educativo y adoptan muchas formas. Se utilizan muchas herramientas digitales para adaptar la enseñanza y preparar la retroalimentación, desde herramientas de cuestionarios en el aula hasta sistemas muy amplios con rúbricas y sugerencias de seguimiento (algunas con la posibilidad generar retroalimentación automática).

Co-funded by the Erasmus+ Programme of the European Union

Muchos centros educativos utilizan herramientas digitales para la evaluación formativa porque pueden registrar información muy específica. El profesorado puede ver de forma rápida lo que se ha aprendido, el modo en que se ha puntuado y lo que le queda por hacer al alumnado. Además, el profesorado dispone de un «archivo»; por lo que siempre puede volver atrás y comprobar el modo en el que se hizo el trabajo anterior.

La evaluación y la digitalización están cada vez más unidas. Pero a medida que aumenta la atención hacia la evaluación formativa, también aumenta la atención de los responsables políticos a nivel nacional. Por lo tanto, es necesario cumplir ciertas condiciones previas en materia de privacidad y seguridad de la información, como se describirá en este documento en el contexto de los Países Bajos.

Un estudio piloto sobre la evaluación formativa

La escuela Leidsche Rijn (NL) comenzó un estudio piloto sobre evaluación formativa. Los estudiantes Fedor, Milan, Souraya y Emma dicen: «Ahora elijo yo mismo mis tareas y veo que los deberes también pueden ser útiles».

El estudio piloto comenzó en el tercer año, como parte del plan de estudios neerlandés para el alumnado del llamado nivel HAVO (educación secundaria superior). Todo el alumnado recibe información sobre las tareas que completa en clase. También puede elegir el modo de procesar el material, por ejemplo, mediante material visual o con el libro de texto. Además, el alumnado al completo habla con su mentor durante 15 minutos a la semana. Hablan del progreso del estudiante, pero también de cómo se siente.

Nelleke Veels, profesora de historia, explica que cada estudiante tiene la oportunidad de hacer un examen de prueba antes de completar el examen de calificación al final del bloque. «Como tenemos que cumplir las bases de transición de 3º a 4º, cada asignatura lleva a cabo 4 exámenes calificados por año. El examen de prueba y las tareas permiten al alumnado comprobar si ha aprendido la materia».

El caso

Desafíos

La educación depende cada vez más de las TIC. La cantidad de información, incluidos los datos personales, el comportamiento respecto al ordenador y los resultados de los exámenes (formales), que registran los distintos sistemas, aumenta cada día. Por ese motivo, es importante tener una buena administración de datos para no perder información vital sobre el aprendizaje.

Co-funded by the Erasmus+ Programme of the European Union

El uso de herramientas digitales es fácil de implementar, pero los centros educativos deben tener acuerdos claros con los proveedores/vendedores. Un reto importante es ponerse en contacto y establecer condiciones con los proveedores internacionales de productos «gratuitos». Para algunos centros educativos es incluso imposible o muy costoso llevarlo a cabo. La privacidad es un problema menor si el alumnado utiliza herramientas mediante una cuenta de invitado o en «modo incógnito» en el navegador (por ejemplo, Socrative, Kahoot!). Pero en el momento en que el alumnado debe iniciar sesión o introducir datos personales (como su nombre, fecha de nacimiento o lugar de residencia), los centros educativos deben ser conscientes de todo lo que ello implica. En el **siguiente artículo (en inglés)** se describe la complejidad del inicio de sesión en plataformas combinadas como Google, Microsoft o Apple.

Por lo tanto, trabajar con herramientas digitales en la evaluación formativa requiere buenos acuerdos, una gran concienciación (y conocimiento) de los posibles riesgos y una cultura profesional y de concienciación entre docentes, estudiantes, administradores escolares y responsables políticos. Todo el ecosistema es responsable de la *seguridad y la privacidad de la información* del alumnado.

Organizaciones neerlandesas responsabilizan a Google de los riesgos para la privacidad

En la educación, cada vez se almacenan e intercambian más datos (personales) de forma digital. Es importante que esto se haga de forma segura y responsable. Una investigación encomendada por la Universidad de Groningen (RUG) y la de Ámsterdam (HvA) revela que existen riesgos para la privacidad relacionados con el uso de Google G Suite. Los riesgos provienen de la recopilación de los llamados metadatos por parte de Google. Dos organizaciones (SURF y SIVON) apoyaron esta investigación y están en contacto con Google para asegurar que Google elimine estos riesgos para la privacidad.

Los riesgos para la privacidad han salido a la luz mediante las llamadas Evaluaciones del Impacto de la Protección de Datos (DPIA) a Google G Suite. Una DPIA permite conocer el modo en el que se recogen los datos, lo que se hace con ellos y los riesgos existentes. El Ministerio de Justicia y Seguridad ha exportado la DPIA a la versión para empresas, y la Universidad de Groningen y HvA han realizado una investigación sobre Google G Suite Education. También participan SIVON, Kennisnet, el Consejo del PO y el Consejo del VO (los consejos de la escuela primaria y secundaria, respectivamente).

Co-funded by the Erasmus+ Programme of the European Union

Seguridad de la información

La seguridad de la información implica mantener medidas coherentes para garantizar un flujo de información fiable. La información no debe modificarse (ya sea por fraude o por buenas intenciones) ni borrarse, sobre todo cuando se trata de datos importantes como los resultados de los exámenes (aprobado/suspendido) o las declaraciones de aprendizaje (bueno/malo).

La seguridad de la información se centra en los siguientes aspectos:

1. *Disponibilidad:* la medida en que los datos y/o las funcionalidades están disponibles en el momento adecuado. Si un centro educativo quiere que el alumnado utilice una herramienta concreta, por ejemplo, para un examen, la herramienta debe estar accesible en ese momento concreto. El alumnado debe poder conectarse, utilizar la herramienta y responder a las preguntas. Por ejemplo, el servidor y la herramienta deben ser capaces de gestionar la entrada simultánea de un gran número de estudiantes.
2. *Integridad:* el grado en el que los datos y/o funcionalidades son correctos y completos. Sería el caso, por ejemplo, de ajustar el resultado de un examen. Si los datos se modifican posteriormente, esto puede tener consecuencias importantes.
3. *Confidencialidad:* la medida en la que el acceso a los datos y a las funcionalidades está limitado a quienes estén autorizados a hacerlo. Por ejemplo, normalmente las familias no deberían tener acceso a los datos de otros estudiantes. Los centros educativos también deben considerar si el alumnado puede ver los resultados de los exámenes de los demás.

Si la seguridad de la información es insuficiente, puede provocar riesgos indeseables para el centro educativo, y eso puede suponer un perjuicio económico y un deterioro de la imagen.

Violación de la seguridad de la información en la escuela Stanislas

El ejemplo de la **escuela Stanislas** de Pijnacker ilustra un incidente que los centros educativos deberían evitar. La escuela recibió varios mensajes de estudiantes, familias y docentes sobre la presencia de imágenes o textos inapropiados durante las clases impartidas en la herramienta de conferencias en línea Zoom.

El **centro educativo decidió suspender inmediatamente el uso de Zoom**, después de que se mostraran imágenes pornográficas durante una clase en línea. El centro Stanislas cuenta con seis escuelas diferentes en esta región. «En la mayoría de los

Co-funded by the Erasmus+ Programme of the European Union

casos, parece que han sido personas ajenas al centro las que han mostrado las imágenes o los textos, y que han accedido de forma ilegal a la clase», comunicó el centro en una carta a las familias.

Privacidad

La privacidad hace referencia a los datos personales, que son cualquier información que pueda identificar directa o indirectamente a una persona física. El intercambio de datos personales debe estar regulado por las leyes y normativas vigentes. Por lo tanto, esto concierne de forma directa a los responsables políticos y a los dirigentes escolares.

Por ejemplo, el ***seguimiento de ojos*** es una tecnología que crea nuevas posibilidades en la educación. Se pueden identificar y mejorar los problemas de lectura y las estrategias de lectura mediante la retroalimentación y la personalización. Pero, al igual que el uso de datos biométricos o sanitarios, plantea nuevos problemas de privacidad.

El seguimiento de ojos y la evaluación formativa

El seguimiento de ojos se utiliza, entre otras cosas, para mejorar los sitios web (comerciales). Así, los diseñadores pueden ver con exactitud qué partes del sitio web miran los usuarios y durante cuánto tiempo. En su momento, los investigadores decidieron probarlo con fines educativos. Pero, ¿cuáles eran esos fines?

El seguimiento de ojos puede registrar hacia dónde mira el alumnado en la pantalla durante una tarea. Con estos datos, el profesorado, por ejemplo, puede ver el tipo de palabras que le cuesta leer. En **este vídeo** (en inglés) se explica el modo en el que el seguimiento de ojos puede ayudar a identificar las dificultades de lectura (por ejemplo, saltarse palabras) y apoyar al alumnado que las experimenta.

El profesorado también puede detectar si algunos elementos de una página distraen demasiado, es decir, si la mirada se desvía de determinados fragmentos del texto. Los diseñadores pueden utilizar esta información para ajustar y mejorar el material educativo digital.

Las nuevas tecnologías, como el seguimiento de ojos, las HoloLenses o la realidad virtual, suscitan nuevos interrogantes. Sin embargo, los responsables políticos también deben ser conscientes de que cualquier herramienta digital registra, procesa y comparte datos más sencillos, como el GPS, el comportamiento basado en los clics e incluso el historial de versiones de documentos del alumnado (por ejemplo, la hora a la que un estudiante completó una tarea). La palabra «tratamiento» incluye por ley la recogida, el

Co-funded by the Erasmus+ Programme of the European Union

registro, la organización, el almacenamiento, la actualización, la modificación, la recuperación, la consulta, la utilización, la divulgación mediante la transmisión, difusión o cualquier otra forma de puesta a disposición, la agregación, la vinculación, el blindaje, el borrado y la destrucción de los datos.

Comenzar con un análisis de riesgos

Los responsables políticos y los administradores de las TIC que se encargan de la privacidad en el centro educativo, deben pensar detenidamente en la razón por la que se utiliza una herramienta, en las personas que la utilizarán, en el objetivo de la misma y en la información que se registra. En el centro educativo se debe organizar de forma adecuada el uso de las herramientas digitales y determinar los proveedores específicos con los que se va a cooperar.

Esto también significa que un centro educativo debe informar de forma adecuada a las familias, formar al profesorado en el uso de las herramientas digitales y debatir con el alumnado los motivos por los que determinadas herramientas no son adecuadas. Al fin y al cabo, se trata del propio estudiante. Si él o ella no se sienten cómodos, esto se debería poder negociar. Es muy recomendable comenzar con un análisis de riesgos a la hora de organizar la seguridad y la privacidad de la información.

Privacidad de datos: análisis de riesgos en los centros educativos de Leiden

El 25 de mayo de 2018 entró en vigor la nueva ley de privacidad de datos (RGPD o AVG en holandés). Los 16 centros de primaria y 2 de secundaria de un consejo escolar de Leiden (llamado SCOL) también se pusieron a trabajar en ello. Melle Klamer, responsable de protección de datos (FG en holandés) en SCOL, y Frits Hekstroe, presidente del Consejo Ejecutivo de SCOL, hablan de su enfoque con un análisis de riesgos como punto de partida:

«Primero hicimos un análisis de riesgos y lo utilizamos como punto de partida para seguir trabajando en nuestra seguridad y privacidad de la información», dice Melle Kramer, responsable de protección de datos (FG) de SCOL.

«En un principio, habíamos creado un amplio grupo de trabajo para tratar este tema. Pronto llegamos a la conclusión de que era más eficaz trabajar con un grupo pequeño y decidido. Entonces empecé a trabajar con el secretario del consejo y un asesor de comunicación. Era un grupo ágil que pudo avanzar con rapidez en los puntos "rojos" del análisis de riesgos. Esos puntos se localizaban en tres áreas: política, tecnología y comportamiento.»

Co-funded by the Erasmus+ Programme of the European Union

El apoyo de la Comisión Europea en la elaboración de esta publicación no constituye una aprobación de su contenido, que refleja únicamente la opinión de los autores. La Comisión Europea no se hace responsable del uso que pueda hacerse de la información contenida en la misma.

Llegar a acuerdos con los proveedores en materia de privacidad

La organización **Schoolinfo**, que tiene como objetivo apoyar a los centros educativos en la digitalización, ha hecho un gran trabajo en los Países Bajos para **describir buenas herramientas** para los centros educativos y el profesorado que quieren iniciarse en las herramientas digitales.

Si el centro educativo utiliza este tipo de aplicaciones digitales, que incluyen datos personales del alumnado y del personal, se debe llegar a un acuerdo con el proveedor. El centro educativo debe asegurarse de que esta información se almacene de forma segura y de que no se utilice de forma indebida o se piratee. Por este motivo, **Kennisnet** ha desarrollado dos documentos que los centros educativos pueden utilizar para llegar a buenos acuerdos con los proveedores. Ambos documentos están disponibles a continuación para ayudar a los responsables políticos:

1. **Acuerdo de privacidad de recursos educativos digitales (3.0)**
2. **Modelo de acuerdo de procesamiento de datos (3.0)**

La nueva legislación sobre privacidad (RGPD) obliga a los centros educativos a registrar los acuerdos alcanzados con los proveedores en materia de seguridad y privacidad en el llamado acuerdo de procesamiento. Allí se recogen los acuerdos con los proveedores, también llamados responsables del tratamiento, sobre el tratamiento de los datos personales de la misma manera. Estos acuerdos han sido ampliamente probados desde el punto de vista legal, pero puede que haya que adaptarlos en el caso de otros países. Kennisnet también ha diseñado una **lista de proveedores** que han firmado el acuerdo de privacidad.

Hoja de ruta para contactar con los proveedores

Paso 1: ¿El proveedor ya está adscrito al acuerdo de privacidad?

Puede preguntárselo al proveedor o consultar la lista de proveedores adheridos existentes. Si el proveedor no está (todavía) adherido al acuerdo de privacidad, invítelo a hacerlo.

Paso 2: Solicitar el acuerdo de procesamiento al proveedor

Según el RGPD, el consejo escolar debe garantizar un acuerdo de procesamiento. Solicite una copia completa al proveedor. Según lo acordado, los centros educativos deben recibir un acuerdo de procesamiento de su proveedor en un plazo de 4 semanas desde la solicitud.

Paso 3: Comprobar el acuerdo de procesamiento

Co-funded by the Erasmus+ Programme of the European Union

El apoyo de la Comisión Europea en la elaboración de esta publicación no constituye una aprobación de su contenido, que refleja únicamente la opinión de los autores. La Comisión Europea no se hace responsable del uso que pueda hacerse de la información contenida en la misma.

Al recibir el contrato, las personas responsables del tratamiento tienen que comprobar que el contrato se haya cumplimentado de forma correcta y que el proveedor no haya adaptado el texto original.

Paso 4: Aceptar y devolver el acuerdo de procesamiento

¿Es correcto el acuerdo de procesamiento? Si es así, el consejo escolar puede firmarlo. La autoridad competente es la responsable en última instancia de la privacidad del alumnado y del personal.

Investigación: evaluar y cuestionar nuestra relación con la tecnología

La especialista en educación Keri Facer (2011) sugiere que tanto los educadores como el alumnado deben ser motivados a entender y cuestionar sus relaciones con la tecnología, y el modo en el que la información está siendo recopilada y filtrada en su nombre. Facer señala que «Cuando se aplica al filtrado de la información, como ocurre con los motores de búsqueda, no podemos simplemente pensar en nuestra interacción con estos sistemas como un proceso de "uso" de los mismos. Por el contrario, desempeñan un papel activo en la construcción y gestión de nuestras interacciones.» (p. 66).

La herramienta «appchecker»

Por último, en ocasiones el profesorado puede mostrarse demasiado entusiasta y apresurado a la hora de adoptar una nueva herramienta digital y no tener en cuenta los datos personales que esta procesa. Por ello, Kennisnet ha desarrollado una herramienta de autoevaluación denominada **appchecker** (disponible en inglés). La herramienta está concebida como un formulario/lista de comprobación en línea que pregunta al encuestado los puntos relacionados con la privacidad que debe tener en cuenta a la hora de seleccionar una herramienta digital (por ejemplo, «¿le pide la herramienta que rellene datos personales?», o «¿le pide que acceda a secciones de su teléfono u ordenador?»). También ofrece explicaciones sobre estas cuestiones. La herramienta tiene como objetivo, en última instancia, concienciar al profesorado y apoyar a los centros educativos a la hora de tratar la seguridad de la información.

Investigación: desarrollo de un marco ético para orientar la toma de decisiones sobre el uso de las tecnologías educativas

Olcott et al. (2014) se comprometieron con las escuelas de Cataluña para analizar las cuestiones éticas emergentes y opciones relativas al uso de las tecnologías digitales, con relevancia para otros contextos locales y nacionales. Desarrollaron un marco

Co-funded by the Erasmus+ Programme of the European Union

El apoyo de la Comisión Europea en la elaboración de esta publicación no constituye una aprobación de su contenido, que refleja únicamente la opinión de los autores. La Comisión Europea no se hace responsable del uso que pueda hacerse de la información contenida en la misma.

basado en el contexto ético continuo (CEC) para guiar la toma de decisiones sobre los posibles daños y/o beneficios de las diferentes tecnologías digitales para las personas y los grupos.

El marco establece cuatro principios que gobiernos, empresas, educadores, ciudadanos particulares y otros deben tener en cuenta:

- La formación en el uso responsable, seguro y ético de las tecnologías debe alcanzar a todos los miembros de la sociedad.
- La educación se basa en valores, y la educación se imparte en, con y desde los valores.
- Las tecnologías deben utilizarse de forma adecuada (con criterio y respeto), no solo utilizarlas y ya.
- El compromiso individual y colectivo determina el uso responsable y ejemplar de las tecnologías (por ejemplo, daños y/o beneficios individuales colectivos).

Los autores sugieren que es probable que sigan aumentando la complejidad y los posibles problemas éticos relacionados con el uso de las tecnologías digitales.

Conclusiones

Los centros educativos de los Países Bajos son cada vez más conscientes de la seguridad y la privacidad de la información. En consecuencia, los centros educativos tienen como objetivo manejar con cuidado los datos del alumnado y los resultados de los exámenes. La redacción de acuerdos de procesamiento es habitual. Sin embargo, el profesorado todavía puede buscar de forma independiente herramientas en Internet y utilizarlas en su enseñanza sin tomar precauciones.

Los instrumentos y las buenas prácticas presentados de los Países Bajos podrían adaptarse al contexto de otros países. A nivel escolar, también es importante mantener una buena cooperación entre el consejo escolar, un encargado de la privacidad (o el administrador de las TIC) y el profesorado.

El alumnado y las familias también deben implicarse en la concienciación, ya que son una parte crucial del ecosistema. El objetivo es que el alumnado se plantee preguntas críticas sobre el uso de una herramienta de evaluación digital en el aula. Aunque todavía haya camino que recorrer para alcanzar ese objetivo, en los Países Bajos ya se han dado los primeros pasos.

Co-funded by the Erasmus+ Programme of the European Union