

Profundizar en ciberseguridad: apoyo a la privacidad y propiedad de los datos de los centros educativos

RESUMEN

30 June 2025

El problema y el contexto

A medida que los centros educativos neerlandeses aumentan su dependencia de las herramientas de aprendizaje digitales y de los servicios de tecnología educativa, la privacidad de los datos y la ciberseguridad se han convertido en preocupaciones fundamentales. Sin embargo, los centros educativos muchas veces carecen de los conocimientos, el tiempo o los procesos normalizados necesarios para gestionar estos riesgos de forma eficaz. El hecho de que el sistema educativo esté descentralizado, con consejos escolares que actúan de forma independiente, agrava el problema, pues genera una variabilidad en el nivel de madurez en seguridad digital entre las instituciones.

Ante esta situación, SIVON, con el apoyo de Kennisnet y el Ministerio de Educación neerlandés, puso en marcha una serie de medidas nacionales para reforzar la gobernanza de los datos y la ciberseguridad en la educación primaria y secundaria. Una de estas iniciativas, el proyecto Deep Dive, se puso en marcha para evaluar las prácticas de seguridad digital actuales y ayudar a los centros educativos a diseñar planes de mejora personalizados.

El proyecto Deep Dive

El proyecto Deep Dive, llevado a cabo por SIVON, evaluó el nivel de madurez en materia de seguridad de la información de 15 consejos escolares (que representan a 290 centros y 80 000 estudiantes), mediante un [marco de estándares](#) recientemente desarrollado que incluye 69 indicadores distribuidos en 15 ámbitos (por ejemplo, gestión de riesgos, política de seguridad o gestión de incidentes). Entre los pasos principales se incluyen los siguientes:

1. **Evaluación de referencia.** Auditores certificados pasaron dos días evaluando la infraestructura de privacidad de datos de cada consejo escolar y las calificaron en una escala de madurez del 1 al 4. Los centros obtuvieron unas puntuaciones que oscilaron entre 1,3 y 2,5, lo que indica que hay muchas diferencias entre ellos.
2. **Planes de mejora personalizados.** Se analizaron los resultados con las partes interesadas (directores escolares, personal de TIC, RRHH) y se ofrecieron recomendaciones adaptadas a cada situación. Los centros educativos recibieron resúmenes de los riesgos y se comprometieron a adoptar medidas específicas en función de sus necesidades y su nivel de madurez.
3. **Formación y desarrollo de capacidades.** Se animó a los centros educativos a formar al personal, definir las funciones en materia de seguridad digital, visualizar los entornos TIC y formular políticas para los protocolos relativos al correo electrónico y el almacenamiento de archivos.
4. **Ejemplo de caso: De Rank.** Este centro de educación primaria colaboró con SIVON para desarrollar un plan de acción sobre seguridad de datos, promover la formación en materia de TIC y mejorar el mapeo de la infraestructura digital y la asignación de responsabilidades.

Además del proyecto Deep Dive, SIVON y Kennisnet ofrecieron un **conjunto integral de servicios** para mejorar la seguridad digital en todo el centro educativo.

- **Compra a gran escala** de herramientas, servicios e infraestructuras de tecnología educativa a precios reducidos. Eso ayudó, por ejemplo, a negociar los precios: en un caso, se consiguió una reducción del 40 % en el precio de las pizarras interactivas.
- **Modelos de acuerdos de privacidad** para facilitar el cumplimiento legal.
- **Unidades de respuesta de emergencia** para incidentes de malware o ransomware.
- **Redes profesionales** como «Network IBP», que cuenta con 900 miembros, para compartir prácticas.
- **Servicios de análisis de riesgos** y directrices prácticas para aplicar políticas de ciberseguridad.

De forma paralela, **las negociaciones a escala nacional con los gigantes tecnológicos (como Google, Microsoft o Apple)** condujeron a logros importantes, como garantías sobre la propiedad de los datos y límites en el uso comercial de los datos. Estas negociaciones se basaron en las **evaluaciones de impacto sobre la protección de datos (EIPD)** que llevó a cabo SIVON.

Enseñanzas extraídas

- Las áreas de organización, gestión de riesgos y desarrollo de sistemas mostraron deficiencias constantes. Un problema común es que los centros educativos no cuentan con un plan de gestión de crisis ni con prácticas sólidas en materia de copias de seguridad de datos. Tampoco cuentan con descripciones de las tareas relacionadas con la seguridad de los datos. A primera vista, las necesidades más comunes de los centros educativos son aumentar el conocimiento en materia de seguridad de datos, centralizar la gestión de los proveedores de software como servicio y disponer de más directrices.
- Los centros educativos tienen un mayor nivel de madurez en la gestión de incidentes, ya que muchos consejos escolares externalizan sus procesos de protección de datos a proveedores de servicios profesionales.
- La mayoría de los centros no alcanzaron los niveles de referencia. Los centros educativos más pequeños, en particular, tuvieron dificultades debido a su capacidad limitada.
- Los centros educativos tienden a dar prioridad a la funcionalidad de las herramientas frente a las garantías de privacidad, como la forma en la que se almacenan o procesan los datos personales.
- Los centros solicitaron a SIVON un lenguaje más claro e indicadores más relevantes, en especial para aquellos que no desarrollan su propio software. También se sugirió que la gestión centralizada del riesgo de los proveedores era más factible que los esfuerzos a nivel de consejo escolar.

- Los eventos de creación de redes presenciales basados en la confianza pueden fomentar la transparencia de los centros con un nivel de madurez menor y favorecer el intercambio productivo de buenas prácticas.
- La muestra inicial se inclinó hacia los centros educativos que ya tenían interés en la seguridad digital o que ya trabajaban en ella. No obstante, al abarcar 290 centros educativos, este fue un piloto a gran escala e informativo para SIVON.

Mediante la combinación de marcos normativos, herramientas prácticas, negociaciones centralizadas y apoyo a nivel escolar, este modelo neerlandés muestra cómo los sistemas educativos pueden dar pasos importantes para proteger los datos escolares y llegar a acuerdos de compra más ventajosos para los centros.

Pese a que las evaluaciones iniciales mostraron un amplio margen de mejora, la orientación estructurada, el desarrollo de capacidades y el compromiso de las partes interesadas sentaron las bases para alcanzar la madurez en materia de seguridad digital a largo plazo. El objetivo final es que todos los centros cumplan los estándares para 2027, dentro de un marco legal que está elaborando el Ministerio de Educación. Esta historia sirve como modelo de coordinación a nivel nacional, de poder de negociación del sector público y de apoyo a la aplicación ascendente.



**Cofinanciado por
la Unión Europea**

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.