

DataPro

Curriculum

sobre protección de datos

Bernd Remmele, Zlatko Valentic

Universidad de Educación de Friburgo

Friburgo 2024

Índice

Introducción	3
1. Preámbulo	5
2. Descripción de competencias	6
A. ¿Cómo proteger mis datos privados (y mi confianza en la información)?	7
Contra la desinformación:	7
Validación de la información:	8
Contra el control del comportamiento:	8
Gestión de identidades:	8
Protección de los demás:	8
Autoprotección:	9
Minimización de datos:	9
Contra el engaño:	9
B. ¿Qué hace que la protección de datos sea un derecho humano?	10
Privacidad es Libertad:	10
Privacidad - Autodeterminación:	10
El poder de la privacidad:	10
Respeto de los derechos humanos:	11
Riesgos para la privacidad de los datos:	11
Inclusión en Internet:	11
Políticas de privacidad:	11
C. ¿Qué hace que los datos sean valiosos (económicamente)?	12
El comportamiento como identificador:	12
Datos comerciales:	12
Ganar dinero con los datos:	12
3. Conclusión para los educadores	13

Introducción

En una era en la que las tecnologías digitales impregnan todos los aspectos de nuestras vidas, la salvaguarda de los datos personales emerge como una preocupación crucial. DataPro, una iniciativa educativa pionera en el marco del programa Erasmus Plus de la Unión Europea, reconoce la necesidad imperiosa de fomentar una comprensión profunda de la protección de datos como derecho humano fundamental entre las generaciones más jóvenes. Este plan de estudios está diseñado para abordar el intrincado panorama del uso y la protección de datos, con el objetivo de dotar a los estudiantes de los conocimientos y las herramientas necesarias para desenvolverse en este complejo campo.

Nuestra sociedad está cada vez más impulsada por los datos, con enormes cantidades de información que se procesan a diario y que afectan a la privacidad individual y a la seguridad colectiva. Con este telón de fondo, el proyecto DataPro ofrece un amplio marco educativo para ilustrar a los jóvenes sobre la importancia de la privacidad de los datos y las consideraciones éticas que conlleva. Al educar a los estudiantes sobre la naturaleza polifacética del uso de los datos y la importancia crítica de proteger la información personal, DataPro pretende cultivar una ciudadanía bien informada y preparada para defender y defender sus derechos sobre los datos.

El plan de estudios establece una serie de objetivos y metas específicos destinados a mejorar la comprensión de los estudiantes de las complejidades de la protección de datos y su reconocimiento como una cuestión vital de derechos humanos. A través de un enfoque estructurado que implica la recopilación, adaptación y desarrollo de herramientas de aprendizaje innovadoras, DataPro quiere integrar el conocimiento teórico y la comprensión práctica. Esta iniciativa no sólo se centra en la difusión de estos recursos entre las escuelas y las partes interesadas en la educación, sino que también hace hincapié en la participación activa de estudiantes y profesores en un proceso de aprendizaje dinámico.

El impacto previsto de DataPro es profundo. Mediante la integración de este plan de estudios en los centros educativos, prevemos formar una generación que no sólo sea consciente de la importancia de la protección de datos, sino que también esté capacitada para aplicar las mejores prácticas. Se espera que este conocimiento básico fomente medidas de privacidad mejoradas e influya en actitudes sociales más amplias hacia la protección de datos y los derechos de privacidad en nuestro mundo cada vez más digital.

Plan de estudios sobre protección de datos

A través de su metodología estructurada y sus esfuerzos de colaboración bajo los auspicios del programa Erasmus Plus, DataPro se compromete a lograr estos resultados, contribuyendo así significativamente al desarrollo de ciudadanos digitales informados y responsables. Este plan de estudios sirve de faro para la innovación educativa, guiando a los jóvenes hacia un futuro en el que sean capaces y confíen en la protección de sus datos en una era digital interconectada.

1. Preámbulo

El plan de estudios sobre protección de datos, que forma parte del proyecto DataPro del programa Erasmus Plus de la Unión Europea, tiene por objeto dotar a los jóvenes de los conocimientos y aptitudes esenciales para comprender y desenvolverse en las complejidades de la protección de datos. El plan de estudios se basa en una matriz de competencias exhaustiva, dividida en ámbitos educativos pertinentes. Las siguientes secciones ofrecen una visión detallada de la estructura del plan de estudios.

En el mundo digital actual, proteger los datos personales es de vital importancia. Los jóvenes crecen en un entorno en el que los datos desempeñan un papel central, ya sea a través de las redes sociales, el aprendizaje en línea o la comunicación digital. Sin embargo, muchos desconocen los riesgos y derechos asociados al uso de las tecnologías digitales. El proyecto DataPro pretende desarrollar una solución educativa integral que permita a los estudiantes gestionar sus datos de forma competente y segura.

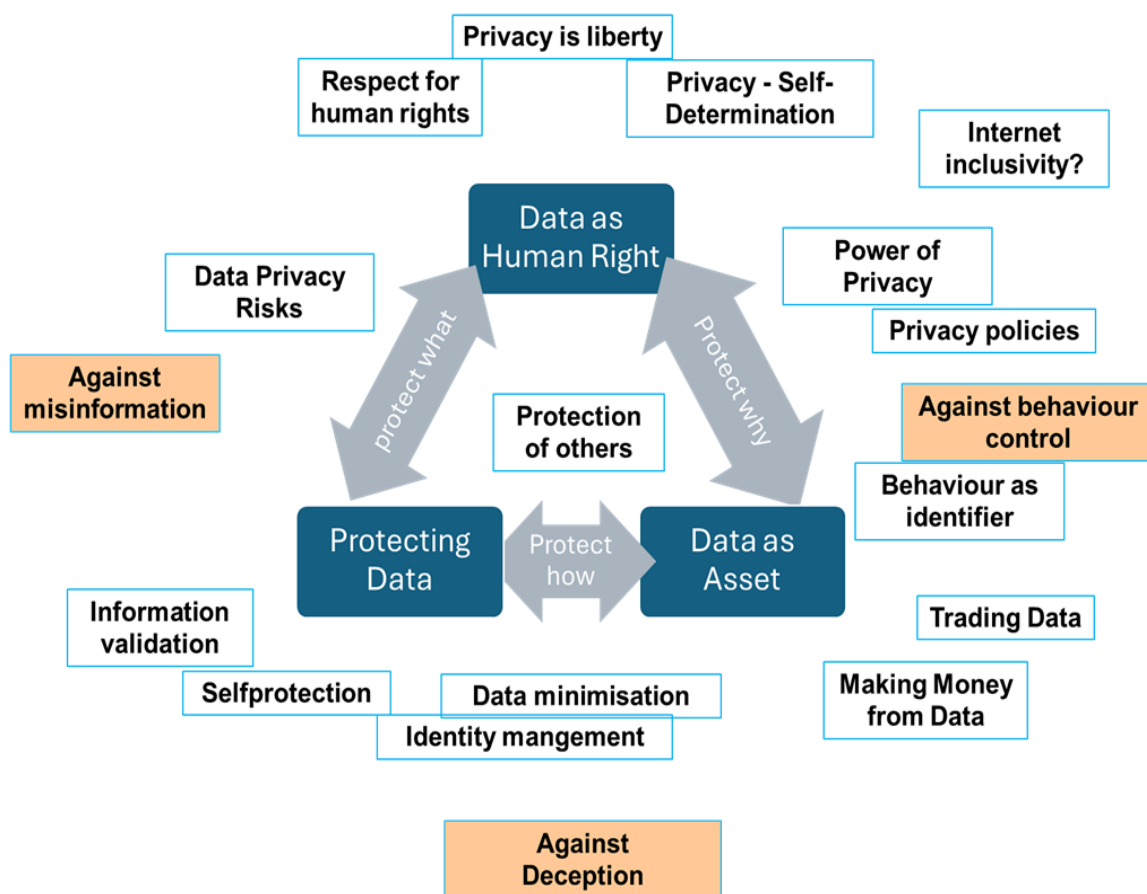
El plan de estudios refleja campos temáticos, cada uno de los cuales abarca competencias específicas y tiene en cuenta los obstáculos al aprendizaje previamente investigados. Basándose en el plan de estudios, se adaptarán los programas específicos de cada país para cada grupo destinatario. Los prototipos de formación del WP3 se basarán en los fundamentos teóricos de los resultados del WP2.

Aunque el plan de estudios se basa en gran medida en el marco DigComp¹, su desarrollo selectivo incluyó varios ciclos de retroalimentación con miembros del consorcio y expertos en protección de datos, lo que garantiza que sea exhaustivo y práctico. Transmite, por un lado, que la protección de datos es tanto un derecho individual como una práctica que incluye riesgos para terceros y, por otro, que los datos tienen un valor económico a menudo oculto. El plan de estudios DataPro integra estas dimensiones para garantizar que los estudiantes adquieran las competencias necesarias para proteger su privacidad y actuar de forma responsable en el espacio digital.

¹ https://joint-research-centre.ec.europa.eu/digcomp/digcomp-framework_en

2. Descripción de la competencia

En la siguiente sección, se describe el plan de estudios utilizando el gráfico proporcionado, que sirve como representación visual de la matriz de competencias. El plan de estudios DataPro está estructurado en tres campos que se solapan: **Protección de Datos**, **Privacidad como Derecho** y **Datos como Bien**. Refleja los requisitos de un miembro activo, autónomo y responsable de una sociedad de mercado democrática e impulsada por los datos y la información.



El plan de estudios se centra en tres temas interrelacionados:

- Proteger los datos" es la parte más obvia, ya que se refiere a los aspectos prácticos de la protección de datos y la ciberseguridad, tal y como se entiende en muchas directrices.
- Los datos como derecho humano", desde la perspectiva de la educación general, se refiere a la importancia de la autodeterminación informativa como derecho humano.

Plan de estudios sobre protección de datos

- Los datos como activo" adopta una postura económica para explicar, por un lado, cómo funciona la industria de los datos y, por otro, cómo los particulares pueden beneficiarse del valor de sus datos.

Así pues, en general, las competencias pueden aclararse respondiendo a las tres preguntas siguientes: A. ¿Cómo puedo proteger mis datos privados (y mi confianza en la información)? B. ¿Qué hace que la protección de datos sea un derecho humano? C. ¿Qué hace que los datos sean valiosos (económicamente)?

Los tres focos no son dimensiones separadas, sino que se solapan en gran medida. La protección de datos y la privacidad como derecho se solapan en la pragmática de cómo proteger "qué" y la consideración de los derechos de privacidad de los demás. Esto significa que el plan de estudios no sólo enseña a las personas cómo proteger sus propios datos, sino que también inculca el respeto por la privacidad de los datos de los demás.

La privacidad como derecho y los datos como bien se solapan a la hora de sopesar el interés (legítimo) de las empresas que manejan datos frente a la propia privacidad. El plan de estudios aborda el equilibrio entre los intereses de las empresas en la utilización de los datos y los derechos individuales a la intimidad, ayudando a los alumnos a comprender las implicaciones más amplias de la economía de los datos.

La protección de datos y los datos como bien se solapan en la pragmática de cómo utilizar los propios datos. Este campo se centra en las habilidades prácticas necesarias para gestionar y aprovechar los datos personales de forma responsable y eficaz en diversos contextos.

El plan de estudios DataPro no tiene niveles de competencia porque la lista de competencias proporcionadas se considera fundamental para una sociedad de la información. Estas habilidades y conocimientos esenciales se consideran necesarios para que las personas funcionen de forma eficaz y responsable en un mundo interconectado digitalmente.

Se destacan específicamente las competencias para reconocer y manejar comportamientos malintencionados en Internet.

A. ¿Cómo proteger mis datos privados (y mi confianza en la información)?

Para proteger sus datos privados y mantener la confianza en la información, tenga en cuenta los siguientes objetivos de aprendizaje, que se centran en capacitar a los estudiantes para navegar por el mundo digital de forma más segura y responsable.

A.1 Gestión de identidades:

- a) *Identificación segura*: Aprenda a proteger su identificación electrónica mediante métodos como contraseñas fuertes y únicas y autenticación de dos factores.
- b) *Conciencia de uso*: Cuestionarse periódicamente cómo y dónde utilizar y compartir información personal identificable de forma segura. Comprender los riesgos asociados a compartir datos personales.
- c) *Medidas de anonimato*: Utiliza medidas para ocultar tu identidad en Internet, como VPN, herramientas de comunicación encriptadas y navegadores centrados en la privacidad.

A.2 Autoprotección:

- a) *Controles de comunicación*: Conocer y utilizar medidas para dejar de recibir mensajes o correos electrónicos no deseados, como filtros de spam y reglas de correo electrónico.
- b) *Gestión del seguimiento*: Aplique medidas para limitar y gestionar el seguimiento de sus actividades en Internet, incluido el uso de extensiones del navegador que bloqueen los rastreadores y las cookies.
- c) *Medidas de seguridad*: Emplea prácticas de seguridad estándar, como utilizar diferentes contraseñas seguras para distintos servicios online, habilitar la autenticación multifactor, utilizar cerraduras biométricas, realizar actualizaciones periódicas de software e instalar software de protección.

A.3 Contra la desinformación:

- a) *Evaluación crítica*: Pregúntese regularmente quién está detrás de la información que se encuentra en Internet, especialmente en las redes sociales. Identifique quién puede tener interés en difundir noticias falsas, como los bots sociales, los propagadores de discursos de odio o los que crean cámaras de eco (burbujas).

Plan de estudios sobre protección de datos

- b) *Conciencia de calidad*: Comprenda que la desinformación puede ser muy convincente, especialmente con el uso de tecnologías avanzadas como la IA, que puede crear sofisticadas visualizaciones. Cuestiona siempre la calidad y la fuente de la información.

A.4 Validación de la información:

- a) *Comprobación de fuentes*: Hay que estar preparado para consultar varias fuentes para verificar la información. Esto ayuda a reconocer y comprender los diferentes puntos de vista o sesgos que subyacen a determinadas fuentes de información y datos.
- b) *Reconocimiento de sesgos*: Aprender a identificar posibles sesgos en la información, entendiendo que cada fuente de datos puede tener un sesgo inherente basado en su origen o propósito.

A.5 Protección de terceros:

- a) *Consideraciones sobre el intercambio de datos*: Cuestionarse periódicamente si se está compartiendo información personal identificable de otras personas y si podría utilizarse indebidamente.
- b) *Conciencia legal*: Ten en cuenta que compartir información sobre otras personas puede tener graves consecuencias legales. Pide siempre tu consentimiento antes de compartir los datos personales de otra persona.

A.6 Minimización de datos:

- *Cuestionamiento de la necesidad*: Cuestionarse periódicamente la necesidad de conservar y compartir datos personales. Adopte prácticas como proporcionar únicamente la información esencial y utilizar direcciones de correo electrónico o números de teléfono desechables cuando proceda.

A.6 Contra el engaño:

- *Medidas de seguridad*: Estar al tanto de los ataques comunes de ingeniería social (phishing) a través de diversos canales de comunicación para evitar la adquisición fraudulenta de activos (digitales).

B. ¿Qué hace que la protección de datos sea un derecho humano?

En relación con la protección de datos como derecho humano, considere los siguientes objetivos de aprendizaje, que se centran en la comprensión por parte de los alumnos de la protección de datos y sus implicaciones:

B.1 Privacidad es Libertad:

- *Libertad fundamental:* La privacidad es esencial para la libertad, ya que permite a los individuos expresar sus opiniones libremente y vivir sin interferencias indebidas. Si otros pueden observar o controlar el comportamiento, la libertad personal se ve comprometida.

B.2 Privacidad - Autodeterminación:

- a) *Control de los datos:* Toda persona tiene derecho a decidir qué datos sobre ella se recogen, procesan y utilizan. Este derecho de autodeterminación es crucial para mantener la autonomía personal.
- b) *Protección automatizada:* Sepa que la protección de datos incluye el derecho a no ser sometido a procesos de toma de decisiones totalmente automatizados que puedan afectar significativamente a las personas.
- c) *Prevención del uso indebido:* La protección de los datos personales ayuda a evitar la vigilancia no deseada, el robo de identidad, la discriminación y otras formas de uso indebido de los datos personales.

B.3 Poder de privacidad:

- a) *Derechos sobre los datos:* Conozca sus derechos frente a las empresas que utilizan sus datos, incluido el derecho a acceder a los datos que tienen sobre usted, rectificar las inexactitudes, borrar los datos (Derecho al Olvido) y presentar reclamaciones ante las autoridades.
- b) *Necesidad de consentimiento:* Comprenda que, por lo general, las empresas necesitan obtener su consentimiento para tratar sus datos personales. Evalúe periódicamente si es necesario dar dicho consentimiento.
- c) *Evaluación del consentimiento:* Evalúa con frecuencia la necesidad de dar el consentimiento para el uso de datos con el fin de garantizar que tu información personal no se explote innecesariamente.

Plan de estudios sobre protección de datos

B.4 Respeto de los derechos humanos:

- *Responsabilidad digital:* Sé consciente de tu responsabilidad de salvaguardar la dignidad humana, la libertad, la democracia y la igualdad mientras actúas en internet. Esto implica respetar la privacidad y los derechos de datos de los demás y abogar por prácticas de datos responsables.

B.5 Riesgos para la privacidad de los datos:

- a) *Niveles de riesgo:* Comprenda que existen distintos niveles de riesgo para la privacidad asociados a las diferentes prácticas de datos. Algunos procesos de datos, en particular los que implican IA, conllevan mayores riesgos.
- b) *Riesgos de la IA:* Ten en cuenta que los procesos y servicios basados en IA pueden plantear diferentes niveles de riesgo para la privacidad, a menudo debido a su capacidad para procesar grandes cantidades de datos e inferir información sensible.

B.6 Inclusión en Internet:

- *Conciencia de la dualidad de Internet:* Hay que ser consciente de que Internet crea nuevas oportunidades de participación en la sociedad para los grupos vulnerables, pero también puede contribuir al aislamiento de quienes no lo utilizan.

B.7 Políticas de privacidad:

- *Evaluación de políticas:* Desarrollar la capacidad de revisar y juzgar de forma crítica las políticas de privacidad de aplicaciones y servicios. Esto incluye comprender qué datos se recopilan, cómo se utilizan y los derechos que tienes en relación con tus datos.

C. ¿Qué hace que los datos sean valiosos (económicamente)?

Dado que los datos tienen un importante valor económico que afecta también a los estudiantes, considere los siguientes objetivos de aprendizaje, que se centran más bien en una comprensión económica general:

C.1 Ganar dinero con los datos:

- a) *Modelos de ingresos*: Conozca las principales formas que tienen las empresas de ganar dinero con los datos personales y agregados, como a través de plataformas publicitarias y mejorando la publicidad dirigida (incluidos los anuncios políticos).
- b) *Economía de los servicios*: Reconocer que la mayoría de los servicios gratuitos de Internet son prestados por empresas con ánimo de lucro, que a menudo monetizan los datos de los usuarios para generar ingresos.

C.2 El comportamiento como identificador:

- a) *Uso de datos*: Reconocer que los patrones de uso y los dispositivos conectados pueden utilizarse para optimizar los servicios en línea y la publicidad dirigida. Esto implica rastrear el comportamiento del usuario para ofrecer contenidos personalizados.
- b) *Estrategias de control*: Aprenda estrategias para controlar y limitar el alcance del seguimiento del comportamiento, como ajustar la configuración de privacidad y utilizar tecnologías que mejoren la privacidad.

C.3 Contra el control del comportamiento:

- a) *Conciencia de los mecanismos*: Sé consciente de que muchas plataformas digitales utilizan tácticas psicológicas como el nudging, la gamificación y la manipulación para influir en el comportamiento de los usuarios. Reconoce estas tácticas para evitar que te influyan indebidamente.
- b) *Medidas de control*: Desarrollar estrategias para disminuir estas influencias, como establecer límites personales de uso y evaluar críticamente los contenidos que se consumen.

Plan de estudios sobre protección de datos

C.4 Datos comerciales:

- a) *Conciencia de monetización:* Ten en cuenta que muchos servicios de comunicación gratuitos (como las redes sociales) y contenidos en línea se pagan con publicidad o con la venta de datos de los usuarios. Este modelo económico se basa en la monetización de los datos personales.
- b) *Compartir públicamente:* Comprenda que todo lo que se comparta públicamente en línea (por ejemplo, imágenes, vídeos, sonidos) puede utilizarse para entrenar sistemas de IA, que pueden incluir funciones de rastreo no deseadas. Ten cuidado con el alcance de los datos que compartes públicamente.

3. Conclusión para los educadores y sus competencias

Para transmitir a los alumnos una conciencia crítica de las tecnologías digitales, fomentando su uso beneficioso y eficaz, son cruciales las siguientes competencias basadas en el Marco DigiCompEdu² :

Protección de dispositivos y contenidos digitales:

- Enseñe a los alumnos a proteger los dispositivos digitales de amenazas como los programas maliciosos y los daños físicos, utilizando programas antivirus, actualizaciones periódicas y contraseñas seguras.
- Enseñar a los alumnos a identificar y responder a amenazas como el phishing, el ransomware, el robo de identidad y el ciberacoso.

Comprender las medidas de seguridad y protección:

- Instruya sobre hábitos de navegación seguros, autenticación de dos factores y uso de redes seguras como las VPN.
- Haga hincapié en la importancia de proteger los datos personales, saber qué compartir en línea y gestionar contraseñas seguras y únicas.

Protección de datos personales y privacidad:

- Destacar la importancia de evitar compartir información sensible en sitios web inseguros y de conocer las políticas de privacidad de los servicios digitales.
- Enseñar a configurar la privacidad en las redes sociales y otras plataformas.

Uso seguro e intercambio de información personal:

- Educar en el intercambio seguro de información personal, la encriptación de datos confidenciales y el reconocimiento de los daños potenciales derivados del uso inadecuado de los datos.

Entender las políticas de privacidad:

² Marco de competencias digitales para educadores (fuente: https://joint-research-centre.ec.europa.eu/digcompedu_en)

Plan de estudios sobre protección de datos

- Explicar la importancia de las políticas de privacidad en los servicios digitales y enseñar a los alumnos a leerlas y comprenderlas para tomar decisiones con conocimiento de causa.

Evitar riesgos para la salud:

- Dar instrucciones para mitigar los riesgos para la salud derivados del uso prolongado de dispositivos digitales, como la fatiga visual, las malas posturas y los efectos sobre la salud mental.

Protegerse contra los peligros digitales:

- Educar para identificar, evitar y denunciar el ciberacoso, los depredadores en línea y otros comportamientos nocivos.

Promover el bienestar social y la inclusión:

- Destacar los aspectos positivos de las tecnologías digitales para fomentar las conexiones sociales y las prácticas integradoras.

Concienciación sobre el impacto ambiental:

- Enseñar las implicaciones medioambientales de las tecnologías digitales, incluidos los residuos electrónicos y el consumo de energía.

Supervisión y salvaguardia del bienestar:

- Supervisar activamente las actividades en línea para garantizar el bienestar e intervenir cuando sea necesario para evitar comportamientos nocivos.
- Estar preparado para tomar medidas inmediatas contra las amenazas al bienestar de los alumnos, como el ciberacoso.

Permitir que los alumnos valoren sus datos como si fueran dinero

Un aspecto importante que no se aborda en el Marco basado en DigiCompEdu, es decir, en las actividades actuales, es el valor de los datos como activo. Por lo tanto, nos gustaría añadir **Valoración de los datos como activo**.

Se debe enseñar a los alumnos a comprender el valor de sus datos personales, de forma similar a como valoran el dinero. Esto incluye reconocer la importancia de proteger sus

Plan de estudios sobre protección de datos

datos, comprender cómo pueden monetizarse o explotarse y tomar decisiones informadas sobre cómo compartir sus datos.