Plan de estudios sobre protección de datos

Universidad de Educación de Friburgo

Enero 2025

Lucie Brzáková, Deborah Krzyzowski, con Bernd Remmele, y Zlatko Valentic

Co-funded by the European Union

Financiado por la Unión Europea. Sin embargo, los puntos de vista y opiniones expresados son únicamente los del autor o autores y no reflejan necesariamente los de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser consideradas responsables de ellos.

Tabla de contenidos

1. Introducción

Las tecnologías digitales impregnan todos los aspectos de nuestra vida privada y pública, y la capitalización de la información personal en línea hizo que la privacidad fuera un bien valioso para las empresas, el gobierno y las personas[1]. En consecuencia, la protección de los datos personales con principios de minimización de datos y medidas de protección de datos es la preocupación crucial.

DataPro es un proyecto dentro del programa Erasmus Plus de la Unión Europea y reconoce la necesidad de cultivar la comprensión de los ciudadanos jóvenes sobre el valor de sus datos, sus derechos de privacidad y las medidas para la protección de datos. En los tres años de duración del proyecto, los socios transdisciplinarios desarrollarán herramientas de aprendizaje sobre protección de datos para los estudiantes. Este plan de estudios profundizará en las tres áreas mencionadas de uso y protección de datos, y otorga a los profesores y socios una visión de los conceptos operacionalizados en las herramientas educativas.

El objetivo más amplio del proyecto DataPro es, por lo tanto, apoyar a los profesores con un marco educativo integral que ayude a los estudiantes a convertirse en agentes digitales activos y autónomos. Concientizar a los estudiantes sobre el valor de sus datos como un bien y el valor de su propia privacidad para la democracia son las intenciones subyacentes detrás de la enseñanza de los métodos de protección de datos. Al educar a los estudiantes sobre la naturaleza multifacética del uso de datos y la importancia crítica de proteger la información personal, DataPro busca cultivar una ciudadanía bien informada y equipada para defender y defender sus derechos sobre los datos.

Este plan de estudios establece objetivos de aprendizaje específicos. Estos objetivos deben alcanzarse con una serie de competencias que mejoren la comprensión de los estudiantes sobre las complejidades de la protección de datos y el reconocimiento de la privacidad como una cuestión de derechos humanos. A través de un enfoque estructurado que involucra la recopilación, adaptación y desarrollo de herramientas de aprendizaje innovadoras, DataPro quiere integrar el

[1] Véase "capitalismo de vigilancia" en Zuboff, S. (2018) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power - Zuboff, Shoshana*. Disponible en: http://archive.org/details/zuboff-shoshana.-the-age-of-surveillance-capitalism.-2019 (Consultado: 10 de enero de 2025).

conocimiento teórico y la comprensión práctica. Esta iniciativa no solo se centra en la difusión de estos recursos entre las escuelas y los actores educativos, sino que también hace hincapié en la integración de las preocupaciones y comentarios de los estudiantes y los docentes. Otra ventaja de las herramientas de aprendizaje es que animan a los estudiantes a convertirse en agentes digitales. En ese rol, estarían equipados para identificar y protegerse de las amenazas digitales. Por ejemplo, la falsa influencia a través de la desinformación digital o los ataques coordinados a los datos mediante tácticas de ingeniería social. El plan de estudios también tiene en cuenta los obstáculos de aprendizaje previamente investigados, como el efecto desensibilizante del uso cotidiano de Internet en la privacidad en línea[2]. Sobre la base de la versión actual en inglés del plan de estudios, los programas de estudio se traducirán para los grupos destinatarios de los respectivos países.

Al integrar este plan de estudios en los entornos educativos, imaginamos nutrir a una generación que no solo sea consciente de la importancia de la protección de datos, sino que también esté capacitada para implementar las mejores prácticas. Se espera que este conocimiento fundamental fomente las actitudes sociales de los estudiantes hacia la protección de datos y los derechos de privacidad para el desarrollo de ciudadanos digitales informados y responsables.

2. Competencias en foco dentro de DataPro

El currículo de protección de datos informa a los profesores y socios sobre los conocimientos esenciales que los jóvenes ciudadanos necesitan para navegar por las complejidades de la protección de datos. La cuestión central del proyecto son las competencias que los estudiantes necesitan para abordar de forma segura los retos digitales. Los jóvenes crecen en un entorno en el que los datos juegan un papel central, ya sea a través de las redes sociales, el aprendizaje en línea o la comunicación digital. Sin embargo, muchos no son conscientes de los riesgos y derechos asociados al uso de las tecnologías digitales. El proyecto DataPro tiene como objetivo desarrollar herramientas de aprendizaje lúdicas y creativas para que los estudiantes desarrollen mecanismos para la gestión segura de sus datos.

Como se ha presentado en el capítulo anterior, las áreas de competencia previstas se basan en el

[2] Krzyzowski, D. (2024) *Informe sobre el análisis cuantitativo de los datos de las encuestas*. Friburgo: Universidad de Educación de Friburgo, p. 21-23.

conocimiento de los datos como un bien; que abarca los mecanismos de procesamiento de datos, la capitalización de la información personal en línea, los sistemas de recomendación algorítmica y las inferencias del comportamiento en línea, por nombrar algunos. En la siguiente sección, el currículo presenta un esquema integral que establece las implicaciones de los datos como un bien en contexto para los individuos y la sociedad. Dado que los datos son el bien en cuestión, el esquema también incluye competencias relevantes que los estudiantes deben adquirir para proteger con éxito sus datos en línea.

El currículo se orienta en el marco DigComp[3], mientras que en su desarrollo se implementaron varios ciclos de retroalimentación con profesionales de la educación. Se obtuvo el asesoramiento de los miembros del consorcio, expertos en protección de datos y, especialmente, de los docentes. De este modo, se garantizará la idoneidad de las herramientas educativas para el grupo destinatario, que son los estudiantes de secundaria.

El punto de partida del plan de estudios es arrojar luz sobre el oscurecido valor económico de los datos personales. A partir de esta premisa crucial, se subraya la importancia del derecho a la privacidad para las democracias sanas y la protección de datos para la autonomía individual de los ciudadanos de dichas sociedades. El plan de estudios integra tres áreas temáticas nombradas para garantizar que los estudiantes adquieran las habilidades para proteger su privacidad y actuar de manera responsable en el espacio digital. La dinámica interrelacionada entre estos temas de protección de datos se explicará en la Sección 4., con la ayuda de la visualización en una Matriz de Competencias (*Figura 1*).

3. Descripción de las competencias

Las competencias de DataPro se estructuran a lo largo de tres áreas temáticas que cubren diferentes implicaciones de los datos digitales:

1. **Los datos como bien**: el 'qué' del proyecto. El objeto de la protección son los datos personales en línea que los proveedores de servicios en línea y las plataformas en línea comercializan y manejan como un bien intercambiable.

[3] Centro Científico de la UE y Comisión Europea (2022) *DigComp Framework*. Disponible en: https://joint-research-centre.ec.europa.eu/scientific-activities-z/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/digcomp-framework_en.

2. **La privacidad como derecho humano**: el "por qué" del proyecto. La importancia social de proteger el bien en cuestión debido al papel vital que desempeña la privacidad individual para el ejercicio de los derechos fundamentales en las democracias.

3. **Protección de datos**: el 'cómo' del proyecto. Después de la sensibilización orientada al usuario sobre los temas antes mencionados de capitalización de datos y privacidad en línea, se pueden introducir medidas prácticas para que los estudiantes protejan sus datos. Estas medidas son medios para una mayor autonomía en línea y autoeficacia en el ejercicio de los derechos.

En la próxima sección se tratan las competencias específicas necesarias para navegar por estos grupos de temas interrelacionados.

3.1 Los datos como bien

"Los datos como bien" es la premisa que subyace a la acuciante importancia de la educación en materia de protección de datos. La privacidad ha sido un punto de debate político desde que los gobiernos y la prensa documentaron la información sobre sus ciudadanos[4], sin embargo, la publicidad algorítmica y la recolección de datos para seguros convirtieron a los datos en una moneda intercambiable por servicios en línea gratuitos. DataPro busca explicar dichos mecanismos de la industria de datos para alentar a los estudiantes a beneficiarse del valor de sus datos. El reconocimiento del valor económico de los datos es posible cuando los estudiantes adquieren las siguientes competencias:

Competencias Grupo A.	Medidas prácticas
A.1 **Convertir datos en un activo**	***Tratar los datos como una moneda en línea*** Comprenda el valor de sus datos personales, al igual que cómo valoran el dinero. Esto incluye reconocer cuándo y qué datos son procesados por los servicios en línea, comprender cómo se pueden monetizar los datos personales, conocer los riesgos de la

[4] Para el desarrollo histórico del discurso sobre el derecho a la privacidad, véase Warren, S.D. y Brandeis, L.D. (1890) 'The Right to Privacy', *Harvard Law Review*, 4(5), pp. 193-220. Disponible en: https://doi.org/10.2307/1321160.

	explotación de los datos personales y tomar decisiones informadas sobre el intercambio de sus datos. ***Concienciación sobre la monetización*** Conozca las principales formas en que las empresas ganan dinero con los datos personales y agregados, por ejemplo, a través de plataformas publicitarias y mejorando la publicidad dirigida (incluidos los anuncios políticos). Tenga en cuenta que muchos servicios de comunicación gratuitos (como las redes sociales) y contenido en línea se pagan con publicidad o venta de datos de usuarios. Este modelo económico se basa en la monetización de los datos personales.
A.2 **Distinguir los riesgos de seguridad del intercambio de datos**	***Uso compartido público*** Comprenda que cualquier cosa que se comparta públicamente en línea (por ejemplo, imágenes, videos, sonidos) se puede usar para entrenar sistemas de IA, lo que puede incluir funciones de seguimiento no deseadas. Tenga cuidado con el alcance de su intercambio de datos públicos. ***Práctica de minimización de datos*** Cuestionar regularmente la necesidad de conservar y compartir datos personales. Adopte prácticas como proporcionar solo información esencial y usar direcciones de correo electrónico o números de teléfono desechables cuando corresponda. ***Medidas de seguridad*** Esté atento a los ataques comunes de ingeniería social (phishing) a través de varios canales de comunicación para evitar la adquisición fraudulenta de activos (digitales).
A.3	***Evaluación crítica***

Evalúe las intenciones detrás de la monetización de datos	Pregunte regularmente quién está detrás de la información que se encuentra en Internet, especialmente en las redes sociales. Identifique quién podría tener interés en crear cámaras de eco (burbujas). ***Conciencia de calidad*** Comprenda que la desinformación puede ser muy convincente, especialmente con el uso de tecnologías avanzadas como la IA, que puede crear visualizaciones sofisticadas. Cuestiona siempre la calidad y la fuente de la información.
A.4 **Conciencia del control del comportamiento**	***Conocimiento del mecanismo*** Ten en cuenta que muchas plataformas digitales utilizan tácticas psicológicas como el empujón, la gamificación y la manipulación para influir en el comportamiento de los usuarios. Reconozca estas tácticas para evitar ser influenciado indebidamente. Reconocer que los patrones de uso y los dispositivos conectados pueden utilizarse para optimizar los servicios en línea y la publicidad dirigida. Esto implica realizar un seguimiento del comportamiento del usuario para ofrecer contenido personalizado. ***Medidas de control*** Aprenda estrategias para controlar y limitar el alcance del seguimiento del comportamiento, como ajustar la configuración de privacidad y usar tecnologías que mejoren la privacidad. Desarrolle estrategias para disminuir estas influencias, como establecer límites personales en el uso y evaluar críticamente el contenido que se consume.

3.2 La privacidad como derecho humano

Desde una perspectiva educativa general, la dimensión de la "privacidad como derecho humano" enfatiza la importancia de la vida privada y la autodeterminación informativa tanto para los

individuos como para las democracias. La *Declaración Universal de Derechos Humanos* protege la "intimidad, la familia, el domicilio o la correspondencia" de toda persona contra cualquier tipo de "injerencia arbitraria".[5] Como ejemplo negativo, estos derechos se ven gravemente vulnerados por el uso ilegítimo de software espía por parte de los gobiernos, como lo confirmó el caso de *Pegasus*[6]. La privacidad como derecho humano ayuda a los estudiantes a contextualizar su propia privacidad en línea dentro de su vida como miembros de una democracia (europea). El estatus especial de la privacidad y una vida privada protegida de la interferencia estatal y corporativa también deben concientizar sobre el valor de la autonomía individual para toda la sociedad. Por lo tanto, la privacidad es un pilar fundamental para otros valores de la democracia, como la libertad de expresión y la autodeterminación informativa. Sólo en ausencia de control, ya sea por parte del gobierno, las instituciones o los poderes del sector privado, los individuos pueden formarse opiniones autónomas y expresarlas en un discurso democrático. Por lo tanto, la privacidad puede conceptualizarse como la ausencia de conocimiento registrable sobre el individuo, un estado en el que pueden experimentar la oscuridad de sí mismos por parte de los funcionarios y las autoridades[7].

Competencias Grupo B.	**Medidas prácticas**
B.1 **Comprender el alcance de la libertad**	***Reconociendo la libertad*** Reconozca la importancia de la privacidad para su libertad. Al proteger su privacidad, salvaguarda su capacidad de expresar opiniones libremente y vivir sin interferencias innecesarias. Tenga en cuenta que cuando otros pueden observar o controlar su comportamiento, su libertad personal puede estar en riesgo.

[5] Véase el artículo 12 de la Declaración Universal de Derechos Humanos de *las Naciones Unidas (1948).* Organización de las Naciones Unidas. Disponible en: https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[6] Asamblea General de las Naciones Unidas (2022) *El derecho a la privacidad en la era digital*. Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos* A/HRC/51/17. Consejo de Derechos Humanos, pág. 2. Disponible en: https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf.

[7] Compárese con la conceptualización de la privacidad como oscuridad en Selinger, E. y Hartzog, W. (2016) 'Obscurity and Privacy', *Spaces for the Future: A Companion to Philosophy of Technology* [Preprint]. Disponible en: https://scholarship.law.bu.edu/faculty_scholarship/3099.

B.2 **Entender la autodeterminación**	***Control de datos*** Recuerde que tiene derecho a controlar qué datos sobre usted se recopilan, procesan y utilizan. Ejercer este derecho te ayuda a mantener tu autonomía personal y a mantenerte a cargo de tu identidad digital. ***Protección de automatización*** Tenga en cuenta 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. ***Prevención de uso indebido*** La protección de los datos personales ayuda a protegerse contra la vigilancia no deseada, el robo de identidad, la discriminación y otras formas de uso indebido de los datos personales. Esté atento a los ataques comunes de ingeniería social (phishing) a través de varios canales de comunicación para evitar la adquisición fraudulenta de activos (digitales).
B.3 **Conocimiento sobre los derechos de privacidad (GDPR)**	***Derechos de datos y necesidad de consentimiento*** Conozca sus derechos frente a las empresas que utilizan sus datos, incluido el derecho a acceder a los datos que tenemos sobre usted, rectificar inexactitudes, borrar datos (derecho al olvido) y presentar quejas ante las autoridades. Comprenda que las empresas generalmente necesitan obtener su consentimiento para manejar sus datos personales. Evaluar periódicamente si es necesario dar dicho consentimiento. ***Evaluación del consentimiento***

	Evalúe con frecuencia la necesidad de dar su consentimiento para el uso de datos para garantizar que su información personal no sea explotada innecesariamente.
B.4 **Concienciación sobre 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 los derechos de privacidad y datos de los demás y abogar por prácticas de datos responsables.
B.5 **Evalúe los riesgos para la privacidad individual**	***Niveles de riesgo*** Comprenda que existen diferentes niveles de riesgo de privacidad asociados con diferentes prácticas de datos. Algunos procesos de datos, en particular los que involucran IA, conllevan mayores riesgos. ***Riesgos de la IA*** Tenga 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 confidencial.
B.6 **Evaluación del potencial de Internet**	***Reconocer la dualidad de Internet*** Hay que tener en cuenta 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 **Revisar las Políticas de Privacidad**	***Evaluación de políticas*** Desarrollar la capacidad de revisar y juzgar críticamente las políticas de privacidad de las aplicaciones y los servicios. Esto incluye comprender qué datos se recopilan, cómo se utilizan y los derechos que tiene con respecto a sus datos.

3.3 Medidas de protección de datos

"Protección de datos" es el objetivo general de aprendizaje del plan de estudios. Esta dimensión se basa en la comprensión de los grupos temáticos 1: Los datos como un bien y 2: La privacidad como un derecho humano. Competencias dentro del clúster 3. Consulte las medidas prácticas de protección de datos y seguridad cibernética que las personas pueden tomar en el día a día.

Competencias Grupo C.	Medidas prácticas
C.1 **Gestión de identidades**	***Conocimiento del uso*** Preguntar regularmente cómo y dónde usar y compartir información de identificación personal de forma segura. Comprenda los riesgos asociados con el intercambio de datos personales. ***Medidas de anonimato*** Utilice medidas para ocultar su identidad en línea, como VPN, herramientas de comunicación encriptadas y navegadores centrados en la privacidad.
C.2 **Garantizar la seguridad de los datos**	***Medidas de seguridad*** Emplee prácticas de seguridad estándar, como el uso de diferentes contraseñas seguras para diferentes servicios en línea, la habilitación de la autenticación multifactor, el uso de bloqueos biométricos, la realización de actualizaciones periódicas de software y la instalación de software de protección. ***Identificación segura*** Aprenda a proteger su identificación electrónica a través de métodos como contraseñas seguras y únicas y autenticación de dos factores.
C.3 **Examinar la capacidad de seguimiento en línea**	***Gestión de seguimiento*** Implementar medidas para limitar y administrar el seguimiento de sus actividades en Internet, incluido el uso de extensiones de navegador que bloquean los rastreadores y las cookies. ***Controles de comunicación*** Conozca y use medidas para dejar de recibir mensajes o correos electrónicos no deseados, como filtros de spam y reglas de correo electrónico.

C.4 **Validación de la información**	***Comprobación de la fuente*** Esté preparado para consultar múltiples fuentes para verificar la información. Esto ayuda a reconocer y comprender diferentes puntos de vista o sesgos detrás de fuentes particulares de información y datos. ***Reconocimiento de sesgos*** Aprenda a identificar posibles sesgos en la información, entendiendo que cada fuente de datos puede tener un sesgo inherente basado en su origen o propósito.
C.5 **Protección mutua de datos**	***Consideración del uso compartido de datos*** Preguntar regularmente si se está compartiendo información de identificación personal de otros y si podría usarse indebidamente. ***Conciencia legal*** Tenga en cuenta que compartir información sobre otras personas puede tener graves consecuencias legales. Solicite siempre el consentimiento antes de compartir los datos personales de otra persona.

4. Relaciones entre competencias

Las competencias necesarias para el uso autodeterminado y responsable de los servicios en línea se pueden clasificar en los tres grupos temáticos presentados. Los clústeres están conectados de forma interdependiente. *Los datos como bien* y *la privacidad como derecho humano* se superponen a la hora de sopesar el interés (legítimo) de las empresas basadas en datos frente a la privacidad de cada uno. El plan de estudios aborda el equilibrio entre los intereses corporativos en la utilización de datos y los derechos individuales a la privacidad. Esto ayudará a los alumnos a comprender las implicaciones más amplias de la economía de datos, como las asimetrías de información y los desequilibrios de poder entre la sociedad, las empresas y el Estado[8].

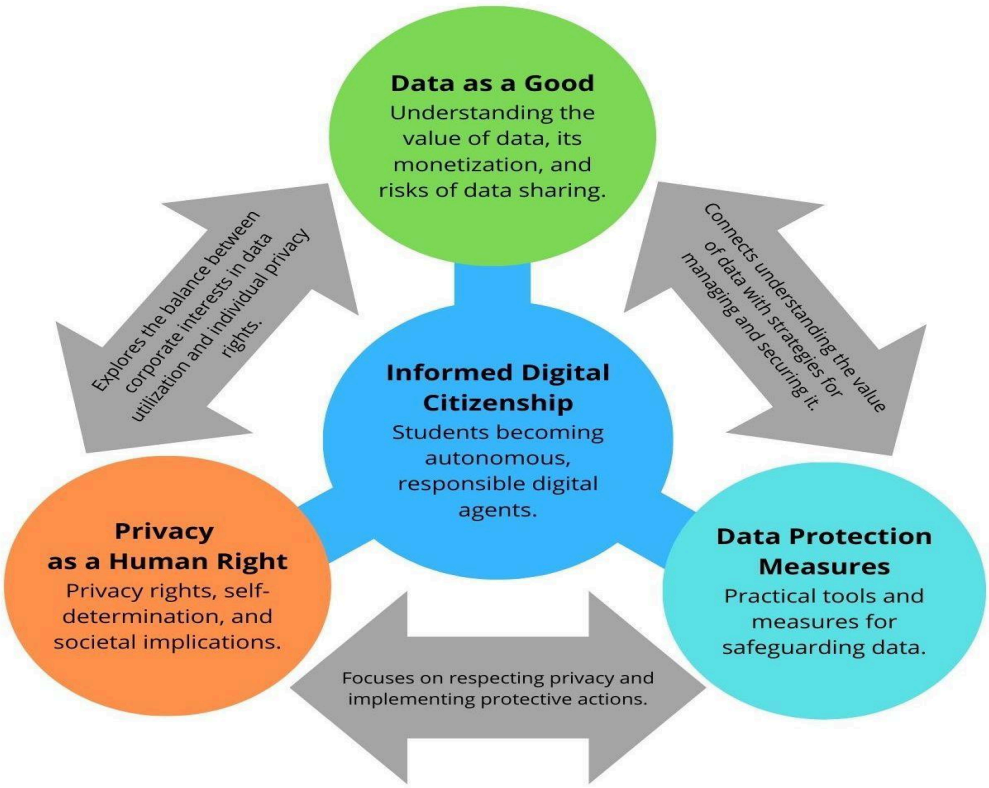
[8] Véase, por ejemplo, van de Waerdt, P.J. (2020) «Information asymmetries: recognizing the limits of the GDPR on the data-driven market», *Computer Law & Security Review*, 38, p. 105436. Disponible en: https://doi.org/10.1016/j.clsr.2020.105436.

Las medidas de protección de datos y la *privacidad como derecho humano se* superponen en la pragmática de cómo proteger los datos individuales teniendo en cuenta los derechos de privacidad de los demás. Esto significa que el plan de estudios no solo prevé enseñar a las personas cómo proteger sus propios datos, sino que también inculca el respeto por la privacidad de los datos de los demás. La práctica mutua del cuidado de los datos personales conceptualiza la privacidad como un bien interdependiente en las democracias y no como una simple preferencia personal. El reconocimiento de la interdependencia ayuda a los estudiantes a comprender que no cuidar su propia privacidad también conduce a una erosión del derecho a la privacidad en la sociedad en general, y que mantener la privacidad en línea para ellos mismos y para los demás fortalece la democracia.

La tautología se completa con la relación entre *las Medidas de Protección de Datos* y *los Datos como Bien*. Estas dimensiones se superponen en la pragmática de cómo utilizar los propios datos a la luz de las asimetrías de información. Esta intersección se centra en las habilidades prácticas necesarias para gestionar y aprovechar los datos personales de forma responsable y eficaz en diversos contextos.

Las dinámicas y dependencias entre las dimensiones de la educación en protección de datos se visualizan en la siguiente Matriz de Competencias (*Figura 1*).. El currículo no discrimina en importancia de las competencias de una dimensión sobre las competencias de otra dimensión. Todas las competencias y su interacción con otras competencias se consideran igualmente fundamentales para la autoeficacia y la libertad de los individuos en una sociedad de la información. Estas habilidades esenciales, y la comprensión subyacente de las tres dimensiones de la protección de datos, se consideran necesarias para que las personas naveguen por el mundo interconectado digitalmente de manera efectiva y responsable.

Figura 1: **Matriz de competencias.** El diagrama muestra los tres grupos de temas ("Los datos como bien", "La privacidad como derecho humano" y "Medidas de protección de datos") que forman un triángulo. En el centro se encuentra el objetivo general, "Ciudadanía Digital Informada", conectada a todas las dimensiones para significar su integración y confianza en su interacción.



5. Resultados de aprendizaje más amplios

Entre el objetivo general de educar a los estudiantes para que tomen decisiones informadas como ciudadanos digitales, un resultado de aprendizaje indirecto debería ser el reconocimiento del comportamiento malévolo en línea. Esto puede incluir ataques de seguridad cibernética como phishing o ransomware. Además, los ataques a la libertad y el discurso democráticos pueden ser más difíciles de distinguir en forma de campañas de desinformación. Tales cuestiones no son un tema central del currículo, sin embargo, se ven como ventajas subordinadas al dominio de las competencias DataPro. Por lo tanto, saber cómo las plataformas en línea se benefician de la atención de sus usuarios, tanto positiva como negativa, presupone la conciencia de los *datos como un bien*. Este tipo de conocimientos podría ayudar a los estudiantes a examinar críticamente los encabezados sensacionalistas y la información manipulada, equipándolos con herramientas para identificar y abordar la información errónea en línea. Por lo tanto, conectar las competencias del grupo A: *Los datos como bien*, al grupo B: *La privacidad como derecho humano* , fomenta la conciencia democrática y la resiliencia frente a ataques como la desinformación.

Conocer los mecanismos del comercio de datos e implementar la práctica de minimización de datos ayuda a los estudiantes a protegerse del control del comportamiento. Los mecanismos de control del comportamiento son omnipresentes en las plataformas en línea, por ejemplo, en la publicidad algorítmica y los algoritmos que buscan capitalizar la atención mediante el aumento del tiempo de pantalla en el servicio. La interdependencia entre el grupo A: *Datos como bien* y el grupo C: *Medidas de protección de datos* está apoyando la autonomía y la autodeterminación de los estudiantes en línea.

En lo que respecta a la ciberseguridad, se cruzan el grupo B: *La privacidad como derecho humano*, y el grupo C: *Medidas de protección de datos*. Establecer la interconexión entre el valor de la privacidad en línea y las medidas prácticas para protegerla ayuda a los estudiantes a crear resistencia a las prácticas engañosas. Ejemplos negativos de la falta de privacidad en línea serían la explotación de la información personal por parte de, por ejemplo, Estados autoritativos o delincuencia organizada. Fortalecer a los estudiantes contra el engaño significa comprender los riesgos de privacidad y las formas prácticas de mantener su privacidad en línea con la ayuda de las competencias del grupo C.

6. Conclusión para los educadores

Para transmitir a los alumnos una conciencia crítica de las tecnologías digitales, fomentando su uso beneficioso y eficaz, es crucial enseñar las competencias de los grupos A, B y C. Sobre la base del marco DigComp[9], los siguientes puntos clave del plan de estudios serán puntos de orientación para los educadores:

Protección de dispositivos y contenidos digitales:

- Eduque a los alumnos sobre cómo proteger los dispositivos digitales de amenazas como el malware y los daños físicos, utilizando software antivirus, actualizaciones periódicas y contraseñas seguras.
- Enseñe a los alumnos a identificar y responder a amenazas como el phishing, el ransomware, el robo de identidad y el ciberacoso.

Comprensión de las medidas de seguridad y protección:

- Instruya sobre hábitos de navegación seguros, autenticación de dos factores y uso de redes seguras como VPN.
- Enfatice la importancia de proteger los datos personales, comprender qué compartir en línea y administrar contraseñas seguras y únicas.

Protección de los datos personales y la privacidad:

- Resalte la importancia de evitar compartir información confidencial en sitios web inseguros y comprender las políticas de privacidad de los servicios digitales.
- Enseñe cómo establecer la configuración de privacidad en las redes sociales y otras plataformas.

Uso seguro e intercambio de información personal:

[9] Centro Científico de la UE y Comisión Europea (2022) *DigComp Framework*. Disponible en: https://joint-research-centre.ec.europa.eu/scientific-activities-z/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/digcomp-framework_en.

- Eduque sobre cómo compartir información personal de forma segura, cifrar datos confidenciales y reconocer el daño potencial del uso inadecuado de datos.

Entendiendo las Políticas de Privacidad:

- Explique la importancia de las políticas de privacidad en los servicios digitales y enseñe a los alumnos a leerlas y entenderlas para tomar decisiones informadas.

Evitar riesgos para la salud:

- Instruir sobre la mitigación de los riesgos para la salud derivados del uso prolongado de dispositivos digitales, como la fatiga visual, la mala postura y los impactos en la salud mental.

Protección contra los peligros digitales:

- Educar sobre cómo identificar, evitar y denunciar el ciberacoso, los depredadores en línea y otros comportamientos dañinos.

Promover el bienestar social y la inclusión:

- Destacar los aspectos positivos de las tecnologías digitales en el fomento de las conexiones sociales y las prácticas inclusivas.

Conciencia de Impacto Ambiental:

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

Monitoreo y Salvaguarda del Bienestar:

- Monitorear activamente las actividades en línea para garantizar el bienestar e intervenir cuando sea necesario para prevenir comportamientos dañinos.

Esté preparado para tomar medidas inmediatas contra las amenazas al bienestar de los alumnos, como el ciberacoso.

Permita 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.