MEMORIA DESCRIPTIVA

Premio a la formación, educación y concienciación en protección de datos personales

Modalidad: CIUDADANÍA

Entidad solicitante: Asociación Aragón Privacidad

Proyecto: Escuela de Privacidad

1. Introducción y objeto de la candidatura

La presente memoria se presenta a la categoría Premio a la formación, educación y concienciación en protección de datos personales – Modalidad Ciudadanía, con el objeto de poner en valor el proyecto Escuela de Privacidad, impulsado por la Asociación Aragón Privacidad como una iniciativa estructural, permanente y orientada al interés general, destinada a promover el conocimiento y el ejercicio efectivo del derecho fundamental a la protección de datos personales en la sociedad.

La protección de datos personales constituye hoy uno de los derechos fundamentales con mayor impacto directo en la vida cotidiana de la ciudadanía. El uso generalizado de tecnologías digitales, redes sociales, aplicaciones móviles, servicios en línea e inteligencia artificial ha multiplicado las situaciones en las que las personas comparten información personal, muchas veces sin plena conciencia de los riesgos asociados ni de los derechos que les asisten.

La Escuela de Privacidad se concibe desde un enfoque transversal, integrando educación, prevención y concienciación en distintos ámbitos sociales, educativos y comunitarios, y adaptándose a la diversidad de públicos y contextos en los que se ejercen los derechos digitales.

Pese a la existencia de un marco normativo sólido y garantista, persiste una brecha significativa entre el reconocimiento jurídico del derecho a la protección de datos y su comprensión y ejercicio real por parte de la ciudadanía. Esta brecha no es esencialmente normativa, sino educativa, comunicativa y cultural, y se manifiesta en el desconocimiento de los riesgos digitales, en la dificultad para identificar situaciones de abuso o uso indebido de datos personales y en la escasa utilización de los derechos reconocidos por la normativa.

Esta realidad afecta de forma especialmente intensa a determinados colectivos, como menores, personas mayores, personas con discapacidad y otros grupos en situación de vulnerabilidad, que se encuentran más expuestos a fraudes, estafas, violencia digital o pérdida de control sobre su información personal.

La Escuela de Privacidad nace como respuesta directa a esta necesidad social, con la convicción de que la educación y la concienciación constituyen las herramientas más eficaces para garantizar una protección real y efectiva de los datos personales. El proyecto se concibe como un programa permanente de formación, educación y concienciación, que traslada la protección de datos al terreno de lo cotidiano, utilizando un lenguaje claro, accesible y no técnico, y adaptando los contenidos a los distintos contextos educativos y sociales.

A través de acciones formativas presenciales, recursos didácticos propios, campañas de sensibilización y colaboración con instituciones públicas, entidades sociales y medios de comunicación, la Escuela de Privacidad persigue empoderar a la ciudadanía, fomentar hábitos digitales responsables, prevenir situaciones de riesgo y favorecer el ejercicio informado y consciente de los derechos digitales.

La presente candidatura tiene como finalidad poner de manifiesto el carácter estructural, continuado y socialmente útil de la Escuela de Privacidad, así como su plena adecuación a los objetivos del Premio de la Agencia Española de Protección de Datos en su modalidad de Ciudadanía, al promover una cultura de la privacidad basada en el conocimiento, la prevención y la protección efectiva de los derechos fundamentales.

2. Entidad promotora y vocación social

La Asociación Aragón Privacidad es una entidad sin ánimo de lucro que agrupa a más de 40 profesionales del ámbito de la protección de datos personales y la privacidad que desarrollan su actividad en la Comunidad Autónoma de Aragón. Desde su constitución, la asociación se orienta de manera clara al interés general y al servicio público, entendiendo la protección de datos no solo como una obligación normativa, sino como un derecho fundamental que debe ser conocido, comprendido y ejercido por la ciudadanía.

La asociación nace con la voluntad de actuar como puente entre el ámbito especializado de la protección de datos y la sociedad, contribuyendo a trasladar el conocimiento técnico y jurídico a un lenguaje comprensible y útil para las personas en su vida cotidiana. En este sentido, Aragón Privacidad asume como uno de sus ejes estratégicos la difusión de la cultura de la privacidad y la promoción de buenas prácticas en el uso de la información personal, desde una perspectiva preventiva, educativa y social.

Desde sus inicios, la entidad ha impulsado una colaboración activa con la AEPD, administraciones públicas, entidades sociales, centros educativos y otros agentes del entorno institucional y comunitario, con el objetivo de integrar la protección de datos en ámbitos diversos como la educación, los servicios sociales, la igualdad, la juventud o la innovación tecnológica. Esta forma de actuación responde a la convicción de que la protección de datos no puede quedar restringida a entornos técnicos o profesionales, sino que debe formar parte del debate público y de la educación cívica.

La Escuela de Privacidad materializa de forma concreta esta vocación social de Aragón Privacidad. Concebida como un instrumento estable y permanente, la Escuela actúa como eje vertebrador de las acciones de formación, educación y concienciación dirigidas a la ciudadanía, permitiendo acercar el derecho fundamental a la protección de datos de manera comprensible, práctica y accesible a personas de distintos perfiles y edades.

A través de este proyecto, la Asociación Aragón Privacidad refuerza su compromiso con la educación en derechos digitales, la prevención de riesgos en el entorno digital y la construcción de una cultura de privacidad compartida, contribuyendo de forma activa a la protección efectiva de la dignidad, la intimidad y la libertad de las personas en la sociedad digital.

3. Fundamentación y necesidad del proyecto

La generalización del uso de tecnologías digitales, redes sociales, servicios en línea, dispositivos conectados e inteligencia artificial ha transformado de manera profunda la forma en que las personas se relacionan, se informan, trabajan y participan en la vida social. En este contexto, la generación y el tratamiento de datos personales se han convertido en una constante de la vida cotidiana, incrementando de forma exponencial la exposición de la ciudadanía a riesgos que afectan directamente a su intimidad, identidad digital, dignidad y autonomía personal.

Si bien el marco normativo en materia de protección de datos personales es sólido y garantista, la experiencia cotidiana pone de manifiesto que la mera existencia de normas no garantiza, por sí sola, una protección efectiva de los derechos. En la práctica, una parte significativa de la ciudadanía desconoce aspectos esenciales como:

- qué información personal genera en su interacción diaria con tecnologías y servicios digitales;
- cómo y con qué finalidad se utilizan sus datos personales;
- qué riesgos existen en el entorno digital, tanto en términos de fraude como de exposición indebida o pérdida de control sobre la información personal;
- qué decisiones informadas puede adoptar para proteger sus datos y ejercer sus derechos.

Esta brecha entre el reconocimiento jurídico del derecho fundamental a la protección de datos y su comprensión y ejercicio real no tiene un origen estrictamente normativo, sino educativo, comunicativo y cultural. Se traduce en una baja percepción del riesgo, en la normalización de prácticas invasivas de la privacidad y en una utilización limitada de los derechos reconocidos por la normativa.

La situación descrita afecta de manera especialmente intensa a colectivos vulnerables, como menores, personas mayores y personas con discapacidad, que presentan mayores dificultades para identificar situaciones de riesgo, comprender las implicaciones del tratamiento de datos personales o adoptar medidas de autoprotección en el entorno digital. En estos colectivos, la falta de información y formación adecuada puede derivar en situaciones de abuso, fraude, violencia digital o exclusión.

La Escuela de Privacidad surge como respuesta directa a esta realidad social, desde la convicción de que la educación en privacidad constituye la herramienta más eficaz para la protección real de los derechos fundamentales. El proyecto adopta un enfoque preventivo, educativo y social, orientado a anticipar riesgos, reforzar la capacidad de decisión de las personas y fomentar hábitos digitales responsables.

Desde esta perspectiva, la Escuela de Privacidad no se limita a transmitir conocimientos teóricos, sino que persigue dotar a la ciudadanía de criterios prácticos para desenvolverse de forma segura y consciente en el entorno digital, contribuyendo a que la protección de datos deje de percibirse como una cuestión técnica o lejana y pase a formar parte de la educación cívica y de la vida cotidiana.

4. Objetivos del proyecto

4.1. Objetivo general

Promover el conocimiento, la comprensión y el ejercicio efectivo del derecho fundamental a la protección de datos personales mediante acciones estructuradas de formación, educación y concienciación dirigidas a la ciudadanía, con el fin de favorecer una cultura de privacidad basada en la prevención, el empoderamiento y el uso responsable de la información personal en la vida cotidiana.

4.2. Objetivos específicos

Con el fin de alcanzar el objetivo general señalado, la Escuela de Privacidad persigue los siguientes objetivos específicos:

- Fomentar una cultura de la privacidad asentada en el conocimiento de los derechos digitales y en la adopción de hábitos responsables en el uso de tecnologías y servicios digitales.
- Traducir la normativa de protección de datos a un lenguaje claro, comprensible y accesible, facilitando su comprensión por parte de la ciudadanía con independencia de su nivel de formación o experiencia tecnológica.
- Facilitar recursos educativos y didácticos accesibles, adaptados a distintos públicos y contextos sociales, que permitan reforzar el aprendizaje autónomo y la concienciación continuada.
- Prevenir situaciones de fraude, abuso y violencia digital, promoviendo la identificación temprana de riesgos y la adopción de medidas de autoprotección en el entorno digital.
- Capacitar a formadores, educadores y agentes sociales como figuras clave para la transmisión del conocimiento, actuando como multiplicadores del mensaje educativo y preventivo en sus respectivos ámbitos de actuación.
- Priorizar la atención a colectivos especialmente vulnerables, como menores, personas mayores y personas con discapacidad, adaptando contenidos y metodologías a sus necesidades específicas.

5. Público destinatario

La Escuela de Privacidad dirige sus actuaciones a la ciudadanía en sentido amplio, partiendo de un enfoque inclusivo y transversal que entiende la protección de datos personales como un derecho fundamental que afecta a todas las personas en su vida cotidiana, con independencia de su edad, formación o nivel de competencia digital.

Dentro de este marco general, el proyecto presta una atención prioritaria a determinados colectivos, por su mayor exposición a riesgos digitales o por su papel estratégico en la transmisión del conocimiento:

- Menores y jóvenes, en contextos educativos y sociales, como colectivo especialmente expuesto al uso intensivo de redes sociales, aplicaciones y servicios digitales. Las actuaciones dirigidas a este público se centran en el uso responsable de la tecnología, el respeto a la intimidad propia y ajena, el consentimiento digital y la prevención de situaciones de abuso o violencia en entornos digitales.
- Personas mayores, especialmente en relación con estafas, fraudes digitales y usos indebidos de datos personales. En este colectivo, la Escuela de Privacidad orienta sus acciones a reforzar la autonomía digital, facilitar la comprensión de riesgos reales y promover decisiones informadas en el uso de dispositivos y servicios digitales.
- Personas con discapacidad, incorporando criterios de accesibilidad, claridad comunicativa y adaptación metodológica. Las actuaciones dirigidas a este colectivo buscan prevenir situaciones de abuso o exclusión digital y reforzar la capacidad de autoprotección y ejercicio de derechos en el entorno digital.
- Formadores, educadores y agentes sociales, considerados figuras clave para la transmisión del conocimiento y la concienciación en materia de privacidad. La capacitación de este colectivo permite amplificar el impacto del proyecto, actuando como multiplicadores del mensaje educativo y preventivo en distintos ámbitos sociales y educativos.
- Ciudadanía en general, interesada en comprender y ejercer sus derechos digitales, a través de acciones de sensibilización, recursos educativos y espacios de educación ciudadana accesibles.

Este enfoque permite a la Escuela de Privacidad adaptar contenidos, formatos y metodologías a las características de cada colectivo, garantizando una intervención educativa eficaz y socialmente relevante, orientada al ejercicio real del derecho fundamental a la protección de datos personales.

6. Metodología educativa

La metodología de la Escuela de Privacidad se fundamenta en un enfoque pedagógico, preventivo y centrado en la persona, común a todas las actuaciones desarrolladas en el marco del proyecto. Este enfoque parte de la convicción de que la educación en protección de datos debe ser comprensible, cercana y aplicable a la vida cotidiana para resultar verdaderamente eficaz.

Con carácter general, la metodología aplicada se apoya en los siguientes principios:

- Lenguaje claro y no técnico, evitando el uso de terminología jurídica o tecnológica compleja y traduciendo los conceptos esenciales de la protección de datos a expresiones accesibles para todos los públicos.
- Uso de ejemplos extraídos de la vida cotidiana, que permiten a las personas participantes identificar situaciones reales de riesgo y comprender de forma práctica cómo se generan y utilizan los datos personales en su día a día.
- Enfoque preventivo y no sancionador, orientado a anticipar riesgos, fomentar la reflexión y promover decisiones informadas, sin recurrir a discursos alarmistas ni punitivos.
- Participación activa de las personas asistentes, favoreciendo el diálogo, la formulación de preguntas y el intercambio de experiencias, como elementos clave del proceso de aprendizaje.
- Adaptación al contexto social y cultural de cada colectivo, ajustando contenidos, ritmo, ejemplos y dinámicas a las características específicas de menores, personas mayores, personas con discapacidad, formadores u otros grupos destinatarios.

Este enfoque metodológico favorece la creación de un clima de confianza, facilita la comprensión real de los riesgos digitales y contribuye a la interiorización de hábitos responsables en el uso de tecnologías y servicios digitales. De este modo, la Escuela de Privacidad no se limita a transmitir información, sino que promueve un aprendizaje significativo y duradero orientado al ejercicio efectivo del derecho fundamental a la protección de datos personales.

La metodología adoptada permite una intervención transversal, aplicable a distintos públicos, entornos y canales, garantizando la coherencia del mensaje educativo y su adaptación a la realidad social de cada colectivo.

7. Líneas de actuación

La Escuela de Privacidad articula su actividad a través de un conjunto coherente y complementario de líneas de actuación, concebidas como un sistema integrado de formación, educación y concienciación ciudadana en protección de datos personales. Estas líneas combinan formación presencial, recursos educativos propios, educación ciudadana a través de medios de comunicación y campañas de sensibilización, en colaboración con administraciones públicas y entidades sociales.

Las líneas de actuación de la Escuela de Privacidad se conciben de forma transversal, permitiendo que los contenidos, enfoques y mensajes educativos se refuercen mutuamente a través de distintos canales y contextos de intervención.

Todas las actuaciones comparten un enfoque pedagógico común, basado en la prevención, la accesibilidad y la orientación al ejercicio efectivo de los derechos digitales en la vida cotidiana.

7.1. Formación presencial y talleres educativos

La Escuela de Privacidad desarrolla acciones formativas presenciales adaptadas a distintos públicos y contextos sociales, diseñadas con objetivos claros, contenidos estructurados y metodología participativa. Estas actuaciones permiten una intervención directa y cercana, facilitando la comprensión práctica de la protección de datos personales.

Entre las principales líneas de formación destacan:

- Talleres dirigidos a menores y jóvenes, centrados en el uso responsable de redes sociales y aplicaciones digitales, la publicación de imágenes, el rastro digital, el consentimiento y el respeto a la intimidad propia y ajena. Estas acciones fomentan una conciencia temprana sobre la privacidad y la responsabilidad digital.
- Acciones formativas dirigidas a personas mayores, orientadas a la prevención de estafas y fraudes digitales, la suplantación de identidad y el uso seguro de dispositivos y servicios digitales. El objetivo es reforzar la autonomía digital y la capacidad de identificación de riesgos reales.
- Formación específica para personas con discapacidad, incorporando criterios de accesibilidad, claridad comunicativa y adaptación metodológica, con el fin de prevenir situaciones de abuso o exclusión digital y reforzar el ejercicio autónomo de derechos.
- Sesiones de sensibilización dirigidas a formadores, educadores y agentes sociales, concebidas para capacitar a figuras clave como multiplicadores del mensaje educativo y preventivo en sus respectivos ámbitos de actuación.

Estas acciones permiten trasladar la protección de datos al ámbito cotidiano de las personas, reforzando su capacidad de tomar decisiones informadas y responsables en el entorno digital.

7.2. Programas de prevención de la violencia digital

La Escuela de Privacidad integra la protección de datos personales y la privacidad como elementos esenciales en la prevención de la violencia digital, entendiendo que muchas situaciones de acoso, control o abuso tienen su origen en el uso indebido de información personal.

En colaboración con administraciones públicas, se han desarrollado programas formativos específicos que abordan, entre otras, las siguientes cuestiones:

- privacidad y consentimiento en entornos digitales;
- control y acoso a través de dispositivos y redes sociales;
- difusión no consentida de imágenes y contenidos íntimos;
- suplantación de identidad;
- configuración segura de móviles, aplicaciones y redes sociales;
- identificación de situaciones de riesgo y conocimiento de recursos de ayuda.

Estas actuaciones se han materializado, entre otras, en dos sesiones educativas dirigidas a más de 200 escolares en el marco de la Semana de la Prevención de la Violencia promovida por el Ayuntamiento de Zaragoza, así como en el marco de la misma, una sesión específica de sensibilización para 100 formadores, orientada a reforzar su capacidad de intervención educativa y preventiva, acompañando a Policía Nacional, Guardia Civil y Pantallas Amigas.

7.3. Recursos educativos y materiales didácticos propios

La Escuela de Privacidad desarrolla materiales educativos propios, concebidos como herramientas de apoyo a la formación presencial y a la concienciación autónoma de la ciudadanía. Estos recursos permiten ampliar el alcance de las actuaciones y garantizar la continuidad del mensaje educativo.

Entre ellos destaca la Guía práctica de privacidad para personas mayores, elaborada en lenguaje claro y directo, que aborda de forma comprensible los principales riesgos digitales y ofrece pautas concretas de actuación para la protección de los datos personales en situaciones cotidianas.

Asimismo, se han elaborado materiales dirigidos a menores y adolescentes que trabajan la privacidad, el consentimiento y la capacidad de decir no desde un enfoque pedagógico, respetuoso y adaptado a su realidad social y digital.

7.4. Educación ciudadana a través de medios de comunicación

La Escuela de Privacidad utiliza los medios de comunicación como espacios estables de educación social, entendiendo su capacidad para llegar a amplios sectores de la ciudadanía y normalizar la cultura de la privacidad en el espacio público.

En este sentido, la sección semanal en COPE Más Zaragoza constituye un programa continuado de alfabetización ciudadana en privacidad, que aborda de forma progresiva y didáctica cuestiones relacionadas con la protección de datos en la vida diaria.

Asimismo, la colaboración con Heraldo Escolar permite trasladar la cultura de la privacidad al ámbito educativo y familiar, reforzando la educación en derechos digitales desde edades tempranas y contribuyendo a la sensibilización de alumnado, familias y profesorado.

7.5. Campañas de sensibilización y efemérides

La Escuela de Privacidad impulsa campañas de sensibilización dirigidas a la ciudadanía, concebidas para reforzar la visibilidad social de la protección de datos como derecho fundamental.

Entre estas actuaciones destaca la celebración y difusión del Día Europeo de la Protección de Datos (28 de enero), mediante mensajes claros y accesibles orientados a fomentar la reflexión ciudadana sobre la importancia de la privacidad, la libertad y la protección de la información personal en el entorno digital.

8. Impacto educativo y social

La actividad desarrollada por la Escuela de Privacidad ha generado un impacto educativo y social significativo, sostenido en el tiempo y verificable, tanto por el volumen de personas alcanzadas como por la diversidad de colectivos destinatarios. Este impacto se manifiesta no solo en términos cuantitativos, sino también en cambios cualitativos en la percepción, comprensión y gestión de la privacidad por parte de la ciudadanía.

8.1. Impacto cuantitativo

Las principales actuaciones desarrolladas en el marco de la Escuela de Privacidad permiten acreditar los siguientes indicadores de impacto:

- Más de 200 escolares han participado en sesiones educativas centradas en privacidad, consentimiento digital y prevención de la violencia digital, contribuyendo a la adquisición temprana de hábitos responsables en el uso de tecnologías y redes sociales.
- Más de 100 formadores y agentes educativos han sido capacitados específicamente en materia de violencia digital y protección de datos personales, actuando como multiplicadores del mensaje preventivo en sus respectivos ámbitos de intervención.
- Se ha llevado a cabo un desarrollo continuado de acciones formativas dirigidas a personas mayores, orientadas a la prevención de estafas, fraudes y usos indebidos de datos personales, reforzando su autonomía y capacidad de autoprotección en el entorno digital.
- Se han realizado formaciones adaptadas a personas con discapacidad, incorporando criterios de accesibilidad, claridad comunicativa y adaptación metodológica, con el objetivo de prevenir situaciones de abuso o exclusión digital y facilitar el ejercicio efectivo de sus derechos.
- La sección semanal estable en COPE Más Zaragoza ha permitido alcanzar un impacto ciudadano estimado superior a 500.000 impactos anuales, consolidándose como un espacio continuado de alfabetización social en protección de datos personales.
- Las publicaciones periódicas en Heraldo Escolar han generado un impacto anual estimado cercano a 400.000 lectores, especialmente en el ámbito educativo y familiar, reforzando la concienciación en privacidad desde edades tempranas.

8.2. Impacto cualitativo

Más allá de los datos cuantitativos, el impacto cualitativo del proyecto se refleja en una serie de resultados educativos y sociales relevantes, entre los que destacan:

- una mejora apreciable en la comprensión de los riesgos digitales por parte de las personas participantes, especialmente en relación con la exposición de datos personales y el uso de redes sociales;
- una mayor conciencia sobre la importancia del consentimiento, la intimidad y el respeto a los datos personales propios y ajenos;
- la adopción de hábitos más responsables en el uso de dispositivos, aplicaciones y entornos digitales;

- el refuerzo de la capacidad de autoprotección digital en colectivos vulnerables, favoreciendo decisiones informadas y una mayor confianza en el ejercicio de sus derechos.

En conjunto, estos resultados evidencian que la Escuela de Privacidad no solo alcanza a un número significativo de personas, sino que contribuye de manera efectiva a la construcción de una cultura de la privacidad, orientada a la prevención, el empoderamiento ciudadano y la protección real del derecho fundamental a la protección de datos personales.

9. Replicabilidad y sostenibilidad

El modelo desarrollado por la Escuela de Privacidad presenta un alto grado de replicabilidad y sostenibilidad, al apoyarse en principios pedagógicos claros, recursos educativos reutilizables y una estructura organizativa flexible, orientada a la continuidad del proyecto y a su adaptación a distintos contextos sociales y territoriales.

9.1. Replicabilidad

El proyecto es fácilmente replicable en otros territorios y ámbitos sociales, ya que combina de forma coherente distintos elementos que pueden trasladarse con adaptaciones mínimas:

- Formación presencial adaptable a distintos públicos, con contenidos y metodologías ajustables a las características de cada colectivo y contexto local.
- Materiales didácticos propios y reutilizables, que permiten mantener la coherencia del mensaje educativo y facilitar su implantación en otros entornos.
- Colaboración con administraciones públicas y entidades sociales, integrando la protección de datos en programas y estructuras ya existentes.
- Utilización de medios de comunicación locales como espacios estables de educación ciudadana, favoreciendo la difusión y normalización de la cultura de la privacidad.

Esta estructura modular permite reproducir el modelo de la Escuela de Privacidad en otros ámbitos geográficos o sectoriales, manteniendo su eficacia pedagógica y su coherencia conceptual.

9.2. Sostenibilidad

La sostenibilidad del proyecto se fundamenta en una combinación de factores que garantizan su permanencia en el tiempo y su capacidad de evolución:

- la continuidad de las colaboraciones institucionales y sociales, que refuerzan la integración del proyecto en el tejido educativo y comunitario;
- la actualización periódica de los contenidos formativos, en respuesta a la evolución de los riesgos digitales y de la normativa aplicable;
- la reutilización y mejora continua de los recursos educativos desarrollados, optimizando su impacto y alcance;
- la integración de la Escuela de Privacidad en redes educativas y sociales ya existentes, favoreciendo sinergias y evitando duplicidades.

Este enfoque asegura que la Escuela de Privacidad no sea una iniciativa puntual, sino un proyecto educativo estructural, con vocación de continuidad y capacidad de adaptación a los nuevos retos tecnológicos y sociales en materia de protección de datos personales.

10. Conclusión

La Escuela de Privacidad representa una apuesta decidida por situar la protección de datos personales en el centro de la vida ciudadana, no como un concepto jurídico abstracto, sino como un derecho fundamental vivo, cotidiano y ejercitable. En un contexto de creciente complejidad tecnológica, la educación en privacidad se convierte en una herramienta esencial para preservar la libertad, la dignidad y la autonomía de las personas.

Este proyecto demuestra que la formación y la concienciación, cuando se abordan de manera estructural, accesible y continuada, son capaces de transformar la relación de la ciudadanía con sus datos personales. A través de la combinación de educación presencial, recursos didácticos propios, campañas de sensibilización, colaboración institucional y educación ciudadana a través de los medios de comunicación, la Escuela de Privacidad ha construido un modelo educativo integral, orientado a la prevención de riesgos y al empoderamiento real de la ciudadanía.

La transversalidad del proyecto, presente en sus públicos, metodologías y canales de actuación, constituye uno de los principales valores añadidos de la Escuela de Privacidad como iniciativa de educación ciudadana en derechos digitales

Su enfoque preventivo, inclusivo y socialmente comprometido, con especial atención a colectivos vulnerables como menores, personas mayores y personas con discapacidad, acredita una comprensión profunda de los desafíos actuales en materia de derechos digitales. El impacto educativo y social alcanzado, junto con su capacidad de replicación y sostenibilidad, convierten a la Escuela de Privacidad en un proyecto con vocación de permanencia y proyección más allá de su ámbito territorial.

La Escuela de Privacidad no solo forma e informa: construye cultura cívica, refuerza la conciencia colectiva sobre el valor de los datos personales y contribuye a que la protección de datos sea entendida como un pilar esencial de la convivencia democrática en la sociedad digital. Por todo ello, este proyecto se presenta como una iniciativa ejemplar de formación, educación y concienciación al servicio de la ciudadanía, plenamente alineada con los valores y objetivos del Premio de la Agencia Española de Protección de Datos.

11. Relación de anexos

Con el fin de acreditar la realidad, continuidad y coherencia de las actuaciones descritas, se incorporan como anexos los siguientes documentos:

- **Anexo I.** Presentación institucional de Aragón Privacidad.
- **Anexo II.** Documento marco del proyecto Escuela de Privacidad.
- **Anexo III.** Guía práctica de privacidad para personas mayores.
- **Anexo IV.** Programas y materiales educativos dirigidos a menores y adolescentes.
- **Anexo V.** Programas de talleres sobre prevención de la violencia digital.
- **Anexo VI.** Índice completo de la sección semanal en COPE Más Zaragoza.
- **Anexo VII.** Publicaciones y colaboraciones en Heraldo Escolar.
- **Anexo VIII.** Documentación de jornadas y actividades públicas organizadas por Aragón Privacidad.

La presente relación de anexos refuerza el carácter verificable, estructural y sostenido en el tiempo del proyecto presentado.

ARAGÓN
PRIVACIDAD

ARAGÓN
PRIVACIDAD

Aragón Privacidad nace con la vocación de aglutinar a los profesionales de la privacidad y cumplimiento normativo que desarrollan su actividad en Aragón, como respuesta a una necesaria intervención en nuestra profesión y actuando desde la proximidad de nuestro territorio.

La imparable velocidad adquirida por la aplicación del RGPD, los nuevos paquetes normativos o la irrupción de la IA, entre otros, hace necesario agrupar esfuerzos y sinergias, sumando el talento que inspira Aragón de tal modo que podamos aunar iniciativas y poner en valor nuestra figura profesional.

NUESTROS OBJETIVOS

1. Integrar a todas las personas físicas o jurídicas que en el ejercicio de su Actividad se dediquen a la protección de datos de carácter y /o el cumplimiento normativo.

2. Colaborar con la Agencia Española de Protección de Datos, así como otras autoridades del territorio nacional, acercando su figura a la ciudadanía como principal garante de sus derechos.

3. Colaborar con las Administraciones Públicas para acercar el cumplimiento a los ciudadanos. Así como para servir de apoyo en sus misiones de interés público y respectivas obligaciones legales que requieran.

4. Difundir la cultura de la privacidad y las buenas prácticas, a través de todos los medios a nuestro alcance y ser un vinculo con los medios de comunicación

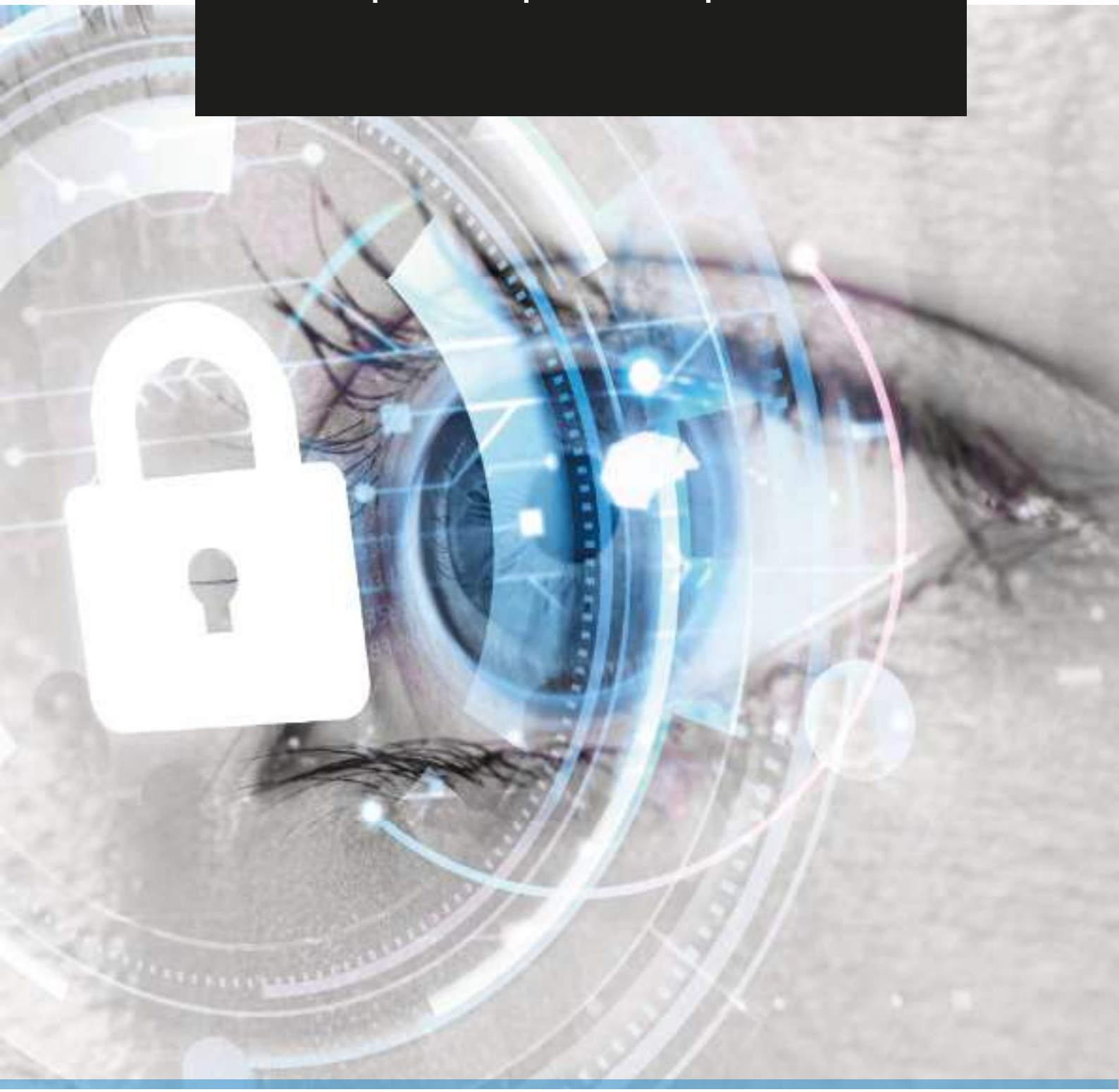
5. Velar por el prestigio profesional del Delegado de Protección de Datos y denunciar prácticas ilegales.

6. Informar y asesorar a los asociados en todos los temas que puedan ser de interés para perfeccionar la prestación profesional.

7. Impartir, participar y desarrollar acciones formativas que favorezcan el perfil del profesional en privacidad y cumplimiento normativo.

8. Establecer y mantener contactos y colaboraciones con entidades nacionales e internacionales de análoga naturaleza y finalidad, así como de intereses confluyentes.

Agrupamos, potenciamos y defendemos la privacidad, a los profesionales de la privacidad y cualquier ciudadano y/o entidad que nos pueda requerir



¿POR QUÉ FORMAR PARTE DE ARAGÓN PRIVACIDAD?

Relaciónate con profesionales expertos, conoce el sector de forma profunda y amistosa

Aprovecha las sinergias, a nivel profesional y personal, conocerás a otras personas, que podrán proporcionarte información y un apoyo relevante, así como ayudarte a conseguir nuevos clientes y proyectos.

Mejora tu perfil profesional, participar de Aragón privacidad indica que estas comprometido con el sector y participas activamente en su evolución.

Podrás **compartir y debatir** sobre las últimas noticias, tendencias, resoluciones, publicaciones e información sobre privacidad y cumplimiento normativo, lo cual es clave para predecir tendencias, conocer nuevos escenarios y conseguir información relevante.

ARAGÓN
PRIVACIDAD

Proyectamos formación específica, por y para los socios, que es un aspecto clave para mejorar la competitividad, además nuestros eventos formativos te facilitaran el cumplimiento de horas exigido para las renovaciones de las certificaciones profesionales.

Aragón Privacidad es **la voz del sector** con la administración pública, Gobierno de Aragón, Diputaciones Provinciales, Ayuntamientos, Comarcas, favoreciendo la interacción público-privada.

Aragón Privacidad **refuerza tu marca de empresa o personal**, como una marca de confianza y proyecta una imagen positiva.

En Aragón Privacidad **promovemos la excelencia a través de los premios** que reconocen la labor en torno a la privacidad en Aragón.

Podrás obtener acceso a **programas de ahorro en costes**.

¿CÓMO HACERTE SOCIO?

Ponte en contacto con Aragón Privacidad a través de nuestra web y rellenando el formulario de alta como socio en:

WWW.ARAGONPRIVACIDAD.COM/ALTA-SOCIOS

WWW.ARAGONPRIVACIDAD.COM

INFO@ARAGONPRIVACIDAD.COM

ARAGÓN

PRIVACIDAD

ESCUELA DE PRIVACIDAD

ARAGÓN

PRIVACIDAD

Escuela de Privacidad: Proyecto Educativo para la Protección de Datos

1. Presentación del proyecto

La Escuela de Privacidad es una propuesta educativa pionera promovida por la Asociación Aragón Privacidad. Su objetivo principal es difundir y concienciar a la sociedad sobre la importancia de la protección de los datos personales. Esta escuela surge como respuesta al reto que supone acercar la privacidad y la protección de datos a la vida cotidiana, facilitando la comprensión ciudadana ante una legislación compleja. Así, la iniciativa se configura como un proyecto permanente, social y flexible, diseñado para evolucionar y dar respuesta a los desafíos que surgen en el ámbito de la privacidad y la protección de datos.

Se concibe como un espacio de participación para diferentes colectivos sociales y profesionales, fomentando la colaboración, el aprendizaje y el debate. La Escuela de Privacidad aspira a convertirse en un referente en Aragón, así como en un modelo que pueda ser replicado en otros territorios, favoreciendo la creación de una comunidad comprometida con el respeto a la privacidad.

2. Fundamentación y sentido

La proliferación de tecnologías digitales y el uso masivo de internet han incrementado los riesgos sobre la intimidad y la identidad de las personas. En la actualidad, la protección efectiva de los datos personales depende en gran medida del nivel de conocimiento y conciencia de la ciudadanía acerca de los datos que genera, su procesamiento, quién puede acceder a ellos y cómo protegerse de posibles amenazas. Por ello, educar en privacidad es una medida preventiva clave para evitar abusos, fraudes y situaciones de vulnerabilidad.

En este sentido, la Escuela de Privacidad surge como respuesta a la necesidad de dotar a la sociedad de herramientas y conocimientos prácticos, promoviendo la autonomía y el empoderamiento digital. Además, el proyecto contribuye a reforzar valores como el respeto, la responsabilidad y la convivencia en el entorno digital, fundamentales para una sociedad democrática y plural.

3. Objetivos

- Fomentar una cultura de privacidad y el empoderamiento ciudadano, promoviendo una actitud proactiva en la defensa de los derechos digitales.
- Clarificar la normativa vigente en materia de protección de datos, facilitando su comprensión tanto para la ciudadanía como para las organizaciones.
- Proporcionar herramientas prácticas para que las personas gestionen su información personal de forma segura y responsable, y puedan identificar y prevenir riesgos.
- Prevenir fraudes, suplantaciones de identidad y reducir la brecha digital, especialmente entre colectivos vulnerables.
- Atender específicamente a colectivos vulnerables, como mayores, menores, jóvenes y personas con discapacidad, adaptando los contenidos a sus necesidades.
- Promover valores de respeto, solidaridad y comunidad en torno a la privacidad, contribuyendo a un entorno digital más seguro y ético.
- Impulsar la formación continua y el debate social sobre los retos actuales y futuros de la privacidad en la era digital.

4. Públicos destinatarios

La Escuela de Privacidad adapta sus contenidos y metodologías a la diversidad de los grupos sociales, garantizando así una formación inclusiva y eficaz:

- Mayores: Se imparten talleres específicos para prevenir fraudes, reconocer engaños en internet y usar dispositivos tecnológicos de forma segura, con un enfoque práctico y sencillo.
- Menores y jóvenes: Los programas se centran en el uso responsable de las redes sociales, la prevención del ciberacoso y la protección de la reputación digital, promoviendo la reflexión sobre las consecuencias de compartir información personal en línea.
- Personas con discapacidad: Se elaboran recursos accesibles y adaptados para facilitar la comprensión y aplicación de buenas prácticas en privacidad, así como para detectar posibles abusos o discriminación en entornos digitales.
- Ciudadanía y profesionales: Se ofrecen criterios claros y actualizados sobre el manejo responsable de datos personales en la vida cotidiana y laboral, incluyendo sesiones para profesionales de la educación, salud, trabajo social y otros sectores clave.
- Familias: Se proporcionan recursos y espacios de apoyo para que padres, madres y tutores acompañen a los menores en el uso seguro y responsable de la tecnología.

5. Metodología

La metodología empleada por la Escuela de Privacidad se fundamenta en varios principios:

- Uso de un lenguaje claro, evitando tecnicismos y facilitando la comprensión a todos los niveles.
- Presentación de ejemplos prácticos y situaciones cotidianas para identificar riesgos y aplicar soluciones concretas.
- Fomento de la participación activa mediante dinámicas grupales, debates, role playing y resolución de casos prácticos.
- Adaptación cultural y contextual de los contenidos, considerando la diversidad de los destinatarios.
- Generación de confianza y promoción de hábitos responsables para reforzar la capacidad de tomar decisiones informadas en el uso de la tecnología.
- Evaluación continua del aprendizaje y recogida de sugerencias para la mejora constante de materiales y actividades.

6. Líneas de actuación

- Formación presencial y talleres: Programas estructurados impartidos en centros educativos, asociaciones, centros de mayores y otros espacios comunitarios.
- Charlas y jornadas sobre privacidad: Encuentros abiertos con expertos, mesas redondas y conferencias para difundir buenas prácticas y resolver dudas.
- Recursos educativos y guías descargables: Elaboración de materiales didácticos, infografías, vídeos y guías prácticas en distintos formatos.
- Itinerarios temáticos: Módulos específicos para contextos como la escuela, el entorno laboral, la salud, los servicios sociales y el uso de tecnología en la vida diaria.
- Colaboraciones institucionales: Trabajo conjunto con entidades públicas, privadas y del tercer sector para ampliar el alcance y eficacia del proyecto.
- Campañas de sensibilización: Difusión de mensajes clave a través de medios de comunicación, redes sociales y eventos públicos.

7. Materiales propios

La Escuela de Privacidad desarrolla sus propios recursos pedagógicos para atender a los distintos públicos:

- Materiales didácticos para menores sobre privacidad, consentimiento y prevención de la violencia digital, adaptados a su edad y en formatos atractivos.
- Guías prácticas para mayores y personas con discapacidad sobre seguridad en internet, protección de dispositivos y detección de fraudes.
- Material audiovisual y multimedia para reforzar el aprendizaje y facilitar la difusión de los contenidos.
- Juegos educativos y dinámicas de grupo para interiorizar conceptos clave de manera lúdica.
- Test y autoevaluaciones para medir el nivel de conocimientos y la mejora de las competencias digitales.

8. Proyección social

El proyecto busca empoderar a la sociedad general, facilitando el acceso a la información y las herramientas necesarias para proteger la privacidad de manera efectiva. Promoviendo la convivencia digital basada en el respeto y la responsabilidad, la Escuela de Privacidad contribuye a la construcción de un entorno digital más seguro, inclusivo y equitativo. Además, fomenta la participación ciudadana en el debate público sobre protección de datos, reforzando el compromiso social con los derechos fundamentales en el entorno digital. Se pretende, asimismo, inspirar a otras regiones y entidades para replicar el modelo y multiplicar la concienciación y la formación en privacidad.

9. Replicabilidad y sostenibilidad

El modelo de la Escuela de Privacidad es fácilmente replicable y sostenible gracias al uso de recursos reutilizables, metodologías sencillas y adaptables, y la colaboración activa con agentes locales, instituciones y entidades sociales. El proyecto se mantiene actualizado para responder a los retos tecnológicos y normativos emergentes, garantizando su vigencia y relevancia. Se prevé la creación de una red de formadores y colaboradores para expandir el proyecto y asegurar su sostenibilidad a largo plazo, así como la búsqueda de alianzas estratégicas que refuercen su impacto social.

10. Cierre

La Escuela de Privacidad apuesta firmemente por acercar la protección de datos a la ciudadanía, haciendo que la información y el conocimiento en esta materia sean útiles y accesibles para todos. Bajo el lema “La privacidad es un derecho de todos”, el proyecto pone el conocimiento al servicio de la sociedad, contribuyendo a la formación de ciudadanos más libres, informados y responsables en la era digital.

GUIA

PROTECCIÓN DE DATOS PERSONALES

PROTEJA SUS DATOS PARA PROTEGER
SU DIGNIDAD, LIBERTAD Y BIENESTAR

ARAGÓN PRIVACIDAD

Zaragoza AYUNTAMIENTO

¿QUÉ ES
LA PROTECCIÓN DE DATOS?

La protección de datos son los derechos que le permiten decidir el uso de la información personal que las empresas y administraciones tienen sobre usted.

La ley exige respetar la privacidad y el consentimiento que usted dé al uso de esos datos.

¿CUÁLES SON SUS DATOS PERSONALES?

Toda aquella información que permita identificarle de manera directa o indirecta.

- Nombre y apellidos
- Número de DNI o NIE
- Dirección
- Números de teléfono · Correo electrónico
- Datos bancarios o económicos
- Imágenes, grabaciones de voz o vídeo
- Huella dactilar u otros datos biométricos
- Historial médico, diagnósticos o tratamientos
- Creencias y afiliaciones religiosas o políticas
- Número de la tarjeta sanitaria · Estado civil

¿CUÁNDO PUEDEN PEDIRLE DATOS PERSONALES?

Solo pueden pedirle datos cuando sea necesario para contratar un servicio que usted haya solicitado, como al darse de alta en un centro de salud o un hotel, apuntarse a una actividad o contratar un plan telefónico.

CUANDO LE PIDAN DATOS, DEBEN EXPLICARLE:

1. El uso que darán

2. Quién será el responsable legal

3. Cuánto tiempo los guardarán

4. Cómo ejercer sus derechos

SUS **DERECHOS** SOBRE SUS DATOS.

ACCESO. Solicitar qué datos tienen sobre usted, su uso y con quién los comparten.

PORTABILIDAD. Solicitar una copia en formato digital de los datos que tienen de usted.

OPOSICIÓN. Puede negarse a que se usen sus datos para ciertos fines, como publicidad.

SUPRESIÓN. Puede solicitar que borren todos los datos que tengan sobre usted.

RECTIFICACIÓN. Puede corregir errores o datos incompletos.

LIMITACIÓN. Puede pedir que se suspenda el uso de sus datos en ciertas situaciones.

Estos derechos pueden ejercerse fácilmente escribiendo a la empresa o entidad que tiene sus datos. Si no le responden o no atienden su petición, puede acudir a la Agencia Española de Protección de Datos (www.aepd.es).

¿QUIÉN SE LOS PIDE?

Si alguien le pide datos personales, usted mismo debe hacerse estas preguntas:

1. ¿Es una persona o empresa de confianza?

2. ¿Tengo relación con esta persona o entidad?

3. ¿Puedo comprobar su identidad?

USTED TIENE DERECHO A DECIR NO.

1. Pregunte sin miedo para qué necesitan estos datos.

2. Diga que lo pensará y responderá más tarde.

3. Hable con alguien de confianza antes de decidir.

4. No firme nada sin leerlo. Tómese su tiempo.

RECUERDE: Nadie puede obligarle a dar más datos de los necesarios. Si alguien le presiona, le habla con prisas o le promete regalos a cambio de información, sospeche. Puede estar ante un engaño o un uso indebido de su confianza.

DATOS DE **SALUD**

Los datos relacionados con la salud, como su historial médico, tratamientos y situación de dependencia, son los más delicados. Estos datos solo pueden ser solicitados y usados por:

- Personal médico o sanitario con razón justificada.
- Entidades públicas cuando lo exija la ley.

Su médico de cabecera puede consultar su historial, pero **no puede compartir esa información sin su permiso**.

SU PRIVACIDAD **EN CASA**

No deje a la vista documentos con información personal, como facturas, recetas, cartas del banco ni contraseñas anotadas.

Rompa cartas y extractos al tirarlos.
Mejor aún si los tritura.

SU PRIVACIDAD **FUERA DE CASA**

Proteja sus **documentos** personales y su móvil, evitando dejarlo **sin vigilancia** o con la pantalla **desbloqueada**.

No hable de temas **privados** ni diga **datos personales en voz alta** en lugares públicos.

SU PRIVACIDAD EN INTERNET

Acceda solo a páginas web seguras que empiecen por "**https://**" y tengan un **candado** en la barra del navegador.

Evite **formularios que no conoce** o llegan por **enlaces dudosos**.

No instale **programas que no necesite** o no vengan de sitios **oficiales**.

Cierre sesión al terminar, especialmente en equipos compartidos.

No dé su número de tarjeta en webs que no conozca.

Instale un antivirus. La mayoría tiene opciones sencillas de usar.

CUIDADO CON EL TELÉFONO Y EL CORREO SI...

Le llaman diciendo ser de un banco, empresa o administración, pero le **piden datos que ellos ya deberían tener.**

Le dicen que **ha ganado algo pero debe dar datos** para recibirlo.

Le **apremian para tomar decisiones importantes** en ese momento.

Recibe notificaciones donde le dicen que debe **actualizar datos**.

CONSEJOS PRÁCTICOS

No confíe **solo porque digan su nombre o dirección**.

Si no está seguro de quién llama nunca dé su número de cuenta, DNI, **ni pulse teclas** si se lo piden durante una llamada.

Revise bien los sobres y remitentes de las cartas y correos. Si ve errores ortográficos o nombres sospechosos, desconfíe.

No devuelva llamadas a números que no conoce.

Cuando tenga dudas, **consulte con un familiar**, **vecino** o **profesional** de confianza.

¿NECESITA AYUDA?

Agencia Española de Protección de Datos
www.aepd.es

Oficina de Seguridad del Internauta
www.incibe.es

Lista Robinson (para no recibir publicidad)
www.listarobinson.es

Aragón Privacidad
www.aragonprivacidad.com

Zaragoza
AYUNTAMIENTO

La privacidad, tu mejor defensa.

ARAGÓN
PRIVACIDAD

1

¿Qué vamos a ver?

- Qué es la violencia digital
- Riesgos comunes en nuestro día a día
- Qué es y cuál es la importancia de la privacidad
- Herramientas para protegerse
- Denuncia de violencia digital y robo de datos
- Sugerencias finales y puntos de vista

ARAGÓN
PRIVACIDAD

2

3

- ¿Tengo tableta o móvil propio?
- ¿Me supervisan de alguna forma?
- ¿Quién hay detrás de ese perfil?
- ¿Hasta dónde llega lo que publico en RRSS?

Introducción

ARAGÓN
PRIVACIDAD

4

Qué es la violencia digital

- Cyberbulling
- Violencia de género digital
- Desinformación

ARAGÓN PRIVACIDAD

5

Riesgos en nuestro día a día

ARAGÓN PRIVACIDAD

6

Oversharing **Control y manipulación**

Violencia en grupos **Phising y estafas**

Impacto en la salud **Doxing**

ARAGÓN PRIVACIDAD

7

Un CTF

Tenemos que buscar donde se hizo esta foto.

La única pista que tenemos es que el niño se llama Ruperto.

ARAGÓ PRIVACIDAD

8

La privacidad

ARAGÓN
PRIVACIDAD

9

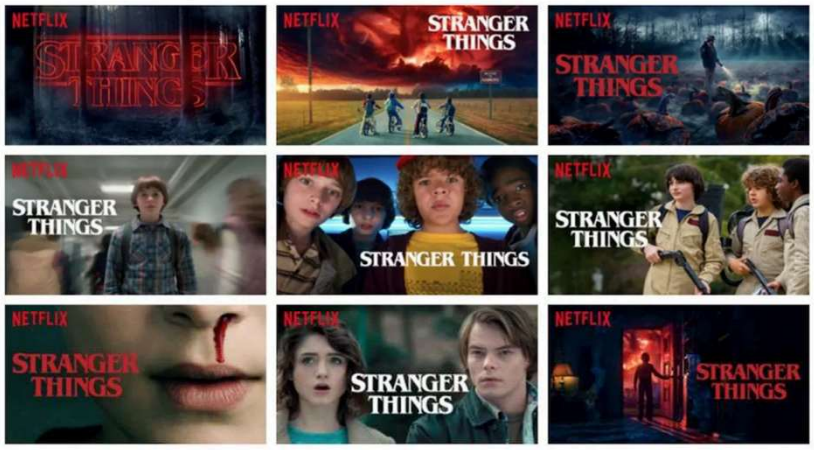
Qué es y cuál es la importancia de la privacidad

- Protección y control sobre tu información personal.
- Desde dónde empieza nuestra privacidad.
- Tu experiencia en redes sociales marca un objetivo.

ARAGÓN
PRIVACIDAD

10

Un ejemplo, NETFLIX



ARAGÓN PRIVACIDAD

11

Caso Cambridge Analytica

ARAGÓN PRIVACIDAD

12

Riesgos de NO proteger la privacidad

ARAGÓN PRIVACIDAD

13

Dispositivos de Hacker

EVIL CROW

BADUSB

ARAGÓN PRIVACIDAD

14

Otro CTF

SZXPVIH

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

HOLA → SLOZ

ARAGÓN PRIVACIDAD

15

Herramientas

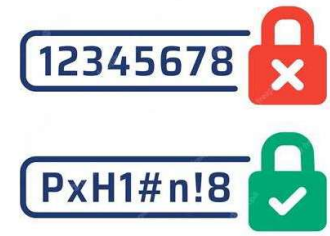
ARAGÓN PRIVACIDAD

16

Herramientas

Contraseñas y autentificación

- Longitud adecuada: Utiliza contraseñas de al menos 12 caracteres.
- Diversidad de caracteres: Incluye letras mayúsculas y minúsculas, números y símbolos
- Evita información personal: No uses nombres, fechas o palabras comunes.
- Actualización regular: Cambia tus contraseñas periódicamente y no las reutilices en diferentes servicios.
- Uso de gestores de contraseñas: A través de un gestor, podéis almacenar, o incluso crear a través de él contraseñas muy seguras que no tenéis que recordar.



ARAGÓN PRIVACIDAD

17

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

HIVE SYSTEMS

› How did we make this? Learn at hivesystems.com/password

18

Crea tu contraseña segura

ARAGÓN PRIVACIDAD

19

Herramientas

Configuraciones de privacidad

- Activar privacidad RRSS
- Desactivar geolocalización
- Mantener RRSS en privado
- Subir contenido en diferido

20

Navegación segura

- VPN e incógnito
- Derecho al olvido de Google

Google Report content on Google

Formulario de solicitud de retirada de datos personales

Por motivos de privacidad y de protección de datos (por ejemplo, en virtud del Reglamento General de Protección de Datos de la UE), tienes derecho a solicitar que se retiren determinados datos personales relacionados contigo.

Con este formulario, puedes solicitar que se retiren determinados resultados de la Búsqueda de Google devueltos en consultas que incluyen tu nombre. Google LLC es el responsable del tratamiento de los datos personales que se lleva a cabo al determinar los resultados que se muestran en la Búsqueda de Google y, además, gestiona las solicitudes de retirada enviadas mediante este formulario.

Si quieres solicitar la retirada de datos personales de otro producto de Google, envía una solicitud mediante el formulario del producto correspondiente, disponible en nuestra página Cómo retirar contenido de Google. Por ejemplo, si quieres solicitar la retirada de datos personales de Blogger, envía una solicitud a través del formulario de Blogger correspondiente.

Cuando Google recibe una solicitud, busca el equilibrio entre tus derechos de privacidad y protección de datos y si es de interés público tener acceso a esa información, así como el derecho de otros usuarios a distribuirla. Por ejemplo, podemos negarnos a retirar determinada información sobre estafas financieras, negligencia profesional, condenas penales o comportamientos impropios de funcionarios públicos. Consulta más información en este artículo del Centro de Ayuda.

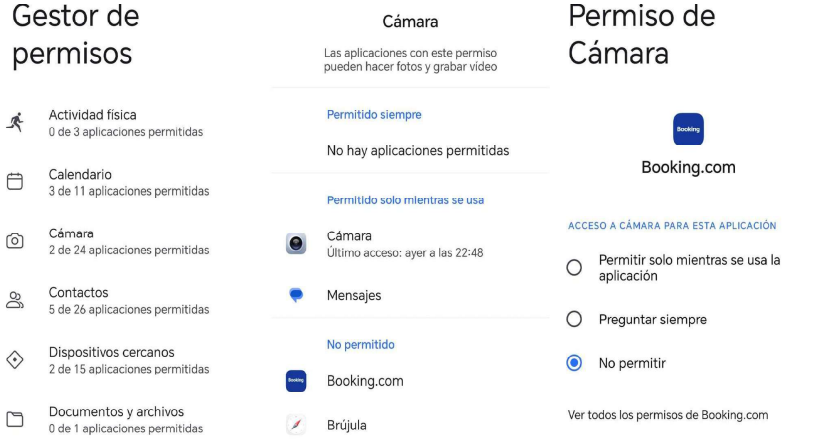
País cuya legislación se aplica (normalmente, en el país donde resides)

Herramientas

ARAGÓN PRIVACIDAD

Apps y permisos

- Revisa qué permisos das (¿por qué una app de linterna necesita tu cámara?)
- También rechazar permisos en la IA para que tus datos no sean usados para el entrenamiento.



Gestor de permisos

Actividad física
0 de 3 aplicaciones permitidas

Calendario
3 de 11 aplicaciones permitidas

Cámara
2 de 24 aplicaciones permitidas

Contactos
5 de 26 aplicaciones permitidas

Dispositivos cercanos
2 de 15 aplicaciones permitidas

Documentos y archivos
0 de 1 aplicaciones permitidas

Cámara

Las aplicaciones con este permiso pueden hacer fotos y grabar vídeo

Permitido siempre

No hay aplicaciones permitidas

Permitido solo mientras se usa

Cámara
Último acceso: ayer a las 22:48

Mensajes

No permitido

Booking.com

Brújula

Permiso de Cámara

Booking.com

ACCESO A CÁMARA PARA ESTA APLICACIÓN

Permitir solo mientras se usa la aplicación

Preguntar siempre

No permitir

Ver todos los permisos de Booking.com

Herramientas

ARAGÓN PRIVACIDAD

¿Cómo denunciar?

ARAGÓN PRIVACIDAD

23

Contar lo sucedido a alguien de confianza. Si no tenéis a nadie hay personas dispuestas a ayudaros: 017, 024, 112..

Recabar evidencias: capturas, lista de llamadas, fotos, audios... cuanto más puedas conseguir, más sencillo será el proceso

Con las pruebas recabadas, cortar todo contacto con el agresor

Ahora sí, ir a los cuerpos de seguridad y denunciar

Denuncia ante la violencia digital

ARAGÓN PRIVACIDAD

24

Reglamento General de Protección de Datos: garantiza el control de nuestros datos

¿Cómo denuncio un robo, un uso sin mi consentimiento o quiero ejercer mi derecho al olvido? → a través de la Agencia Española de Protección de Datos rellenando su formulario.

El responsable de estas acciones puede llegar a tener multas de entre 40.000-300.000 euros, y en casos graves hasta 20 millones de euros.

Proceso denuncia ante AEPD

ARAGÓN PRIVACIDAD

25

CONCLUSIÓN

ARAGÓN PRIVACIDAD

26

1. Bienvenida e introducción (10 min)
Objetivo: Conectar con el grupo, explicar qué es la privacidad y motivar.

Guion formador/a:
- Hola a todos. Hoy vamos a aprender cómo cuidar nuestra información personal en Internet.

- La privacidad es como una caja fuerte: dentro guardamos cosas importantes. Si la caja está abierta, cualquiera puede mirar; si está cerrada, solo nosotros tenemos la llave.

Dinámicas:
- ¿Quién tiene móvil? ¿Quién usa WhatsApp, TikTok, YouTube…?

- Escribe en la pizarra/cartulina las apps que digan.

- Conecta: Todas estas apps saben cosas de vosotros. Por eso tenemos que aprender a proteger nuestra información.

Cierre:
Nuestra información personal es valiosa y hay que cuidarla como cuidamos nuestras cosas.

2. ¿Qué es la privacidad? (15 min)
Objetivo: Aprender a distinguir entre lo que se puede compartir y lo que se debe guardar.

Guion formador/a:
- Los datos personales son cosas como nombre, dirección, fotos, teléfono, contraseñas.

- Algunos se pueden compartir (ej. aficiones), pero otros debemos guardarlos.

- Es como cuando hablas con un amigo de confianza (seguro) o con un desconocido en la calle (peligroso).

Dinámicas:
- Dinámica 1 – Clasificación de tarjetas: El grupo coloca las tarjetas en columnas (Compartir o Guardar).

- Dinámica 2 – Caja fuerte simbólica: ¿Qué meterías dentro para protegerlo? (ej. dirección, foto familiar).

Cierre:
No todo se comparte. Algunas cosas son solo nuestras.

3. Riesgos en Internet y cómo evitarlos (20 min)
Objetivo: Identificar situaciones de riesgo y aprender qué hacer.

Guion formador/a:
- A) Ciberacoso: No contestar, guardar pruebas y pedir ayuda a un adulto.

- B) Contenidos inapropiados: Cierra la pantalla, no lo compartas y pide ayuda.

- C) Amigos en línea: Un verdadero amigo se conoce en persona. Nunca dar datos a desconocidos.

Dinámicas:
- Role play: leer un mensaje ofensivo y preguntar '¿Qué hacemos?'

- Pregunta rápida: 'Si veo un vídeo que me da miedo, ¿qué hago?'

- Escenario: 'Un contacto dice que te dará un juego si le das tu dirección. ¿Qué haces?'

Cierre:
Ante un riesgo en Internet: no contestar, cerrar, pedir ayuda.

4. Buenas prácticas de privacidad (15 min)
Objetivo: Aprender rutinas seguras para el día a día.

Guion formador/a:
- Piensa antes de compartir: ¿me gustaría que lo viera todo el mundo?

- Contraseñas seguras: letras, números y símbolos.

- Tiempo equilibrado: Internet es divertido, pero también hay que jugar y descansar.

Dinámicas:
- Dinámica 1 – Contraseña segura: crear contraseñas fuertes en grupo.

- Dinámica 2 – Semáforo de la privacidad: frases para clasificar en verde, amarillo o rojo.

Cierre:
Con buenos hábitos, podemos disfrutar de Internet de forma segura.

5. Cierre y recordatorio final (5 min)
Objetivo: Reforzar ideas clave y acabar con un mensaje positivo.

Guion formador/a:
- La privacidad protege nuestra información.

- No todo se comparte.

- Ante un problema: no contestar, cerrar, pedir ayuda.

- Las contraseñas fuertes son nuestra llave.

- ¡Nunca estamos solos, siempre podemos pedir ayuda!

Dinámicas:

Cierre:
Internet puede ser divertido y útil si lo usamos con cuidado. Vosotros tenéis la llave para proteger vuestra información.

Protección de Datos y Violencia Digital: la privacidad como frontera de la dignidad

ARAGÓN PRIVACIDAD

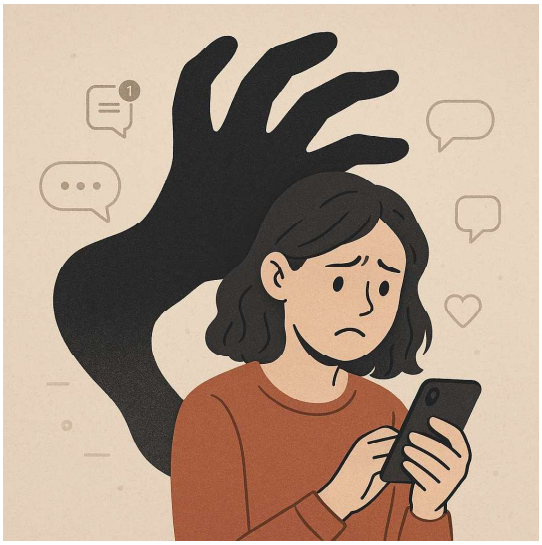
1

La violencia digital: un daño silencioso

> La violencia ya no siempre es visible: puede llegar a través de una notificación, una imagen reenviada sin permiso o mensajes constantes.

> 7 de cada 10 mujeres jóvenes han sufrido acoso digital; 2 de cada 3 no lo denuncian.

> Proteger los datos personales es proteger a las personas.



ARAGÓN PRIVACIDAD

2

¿Qué es la violencia digital?
Conductas dañinas ejercidas a través de tecnologías, redes sociales o Internet, que afectan la intimidad, dignidad y libertad.

Ejemplos frecuentes:
- Acoso y control por mensajes o ubicación
- Vigilancia y presión en redes sociales
- Espionaje digital (spyware)
- Censura y exigencia de contraseñas
- Coerción para obtener material íntimo
- Difusión no consentida de imágenes o vídeos

ARAGÓN PRIVACIDAD

3

Marco legal: justicia en el entorno digital
Reconocimiento legal
El Derecho español ya reconoce la violencia digital como forma de violencia psicológica, de género y contra menores.
Se aborda desde el ámbito penal, civil y admistrativo.

Principales normas
LO 10/2022 Libertad sexual : incluye *revenge porn*, *sextorsión* y *deepfakes*.
LO 1/2004 Violencia de género: incorpora control y acoso digital.
LO 8/2021 Protección de la infancia: reconoce la violencia digital hacia menores.
Código Penal tipifica acoso en redes, difusión no consentida de imágenes y amenazas online. (169,171,172 ter,197.7, 197 bis, 401)
RGPD+LOPDGG
Ámbito laboral, educativo y sanitario se promueven **protocolos de actuación frente a ciberacoso o difusión no consentida de contenidos**.

Perspectiva actual
Enfoque integral: prevención + educación + reparación.
Campañas y canal prioritario de la AEPD para retirar contenido íntimo.
Eje específico en la Estrategia Estatal de Erradicación de la Violencia contra las Mujeres (2022–2025)

ARAGÓN PRIVACIDAD

4

Denunciar y preservar la prueba: del miedo a la acción

Dar el paso cuesta. Muchas víctimas minimizan el acoso por miedo o culpa. Pero denunciar frena al agresor y activa protección.

Buenas prácticas:
- No borrar nada.
- Capturas claras con fecha, hora y usuario.
- Relato cronológico de incidentes.
- Acta notarial o peritaje informático.

Denuncia ante Policía Nacional, Guardia Civil o juzgado. Teléfonos: 016 (violencia de género), 017 (INCIBE). La denuncia rompe el aislamiento y abre el camino de la protección.

ARAGÓN PRIVACIDAD

5

Derechos digitales de las víctimas: privacidad, honor y "olvido"

El RGPD y la LOPDGDD garantizan derechos de supresión (olvido), oposición y limitación del tratamiento. La víctima puede exigir la eliminación de contenidos que perpetúan el daño.

La Ley 4/2015 (Estatuto de la Víctima) protege la identidad, evita la revictimización y prevé vistas a puerta cerrada. La privacidad es reparación: recuperar el control es recuperar la paz.

ARAGÓN PRIVACIDAD

6

El Canal Prioritario de la AEPD: privacidad en acción

El Canal Prioritario permite retirar de inmediato contenidos sexuales o violentos publicados sin consentimiento. La AEPD puede ordenar la eliminación en cuestión de horas y abrir procedimiento sancionador. La protección de datos es una herramienta real de defensa y dignidad.

ARAGÓN PRIVACIDAD

7

La importancia de quien acompaña

Ninguna herramienta funciona si la primera persona que escucha a la víctima no sabe cómo hacerlo. Hace falta formación en privacidad para policías, juristas, sanitarios, educadores y comunicadores.

En Aragón Privacidad trabajamos precisamente aquí: formar y sensibilizar a quienes son la primera línea de contención, para evitar revictimización y asegurar una respuesta humana y eficaz.

ARAGÓN PRIVACIDAD

8

Educación y prevención: cultura de privacidad

La mejor respuesta es prevenir. La privacidad debe enseñarse como autonomía y respeto, no como prohibición.

Educar en privacidad es educar en libertad.

ARAGÓN PRIVACIDAD

9

Cooperación institucional y recursos

La violencia digital exige red: AEPD, Interior, Justicia, Igualdad, INCIBE, comunidades y entidades civiles.

Aragón Privacidad aporta formación, acompañamiento y cultura de privacidad.
La privacidad es tarea colectiva.

017 TU AYUDA EN CIBERSEGURIDAD incibe_

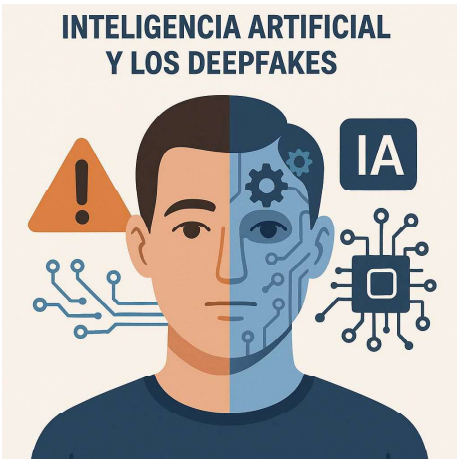
aepd agencia española protección datos

Zaragoza IGUALDAD

ARAGON PRIVACIDAD

ARAGÓN PRIVACIDAD

10



Retos inmediatos: IA, deepfakes y control algorítmico

La inteligencia artificial y los deepfakes abren una nueva amenaza: imágenes falsas hiperrealistas. La respuesta jurídica avanza, pero la alfabetización digital y la ética son esenciales.

ARAGÓN
PRIVACIDAD

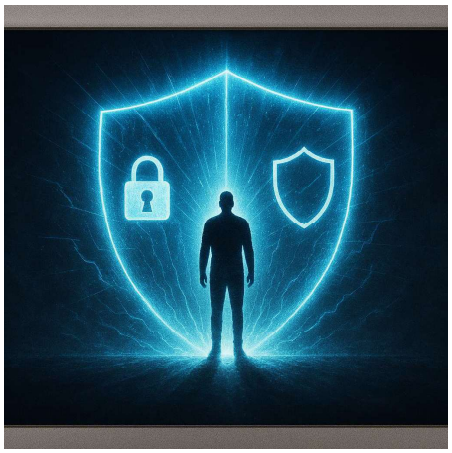
11

La privacidad como frontera de la dignidad

La privacidad no es un lujo: es la frontera de la dignidad humana. Nos permite decidir qué mostramos, qué guardamos y con quién. Respetar esa frontera fortalece la libertad.

Desde Aragón Privacidad reafirmamos nuestro compromiso con la formación, el acompañamiento y la defensa de la privacidad como valor social.

Cuando protegemos datos, protegemos personas. Y cuando protegemos personas, preservamos la dignidad. La privacidad no solo protege datos, protege vidas.



ARAGON
PRIVACIDAD

12

ARAGÓN

PRIVACIDAD

info@aragonprivacidad.com

13

CONTENIDOS COPE 2025-2026

Bloque 1 · Privacidad en la vida diaria
1. ¿Qué es la privacidad y por qué debería importarte?
2. ¿Por qué hay que pensar antes de publicar en redes?
3. Consejos para proteger tu móvil del cotilleo ajeno.

4.-los sistemas de control de acceso y control horario

5.-los sistemas de control de acceso y control horario 2

6. ¿Cómo evitar que te escuchen sin darte cuenta? Micrófonos y asistentes de voz.
7. ¿Qué es el rastro digital y cómo se borra?
8. Contraseñas: cómo crear una buena y no olvidarla.
9. ¿Es legal que te graben sin permiso?
10. ¿Te pueden grabar en el trabajo?
Bloque 2 · Privacidad y menores
11. ¿Debemos publicar fotos de nuestros hijos?
12. ¿Cómo enseñar privacidad digital a los peques?
13. TikTok, Instagram y compañía: riesgos para menores.
14. ¿Qué hacen los videojuegos con los datos de los niños?
15. ¿A qué edad debería un menor tener redes sociales?
Bloque 3 · Publicidad y privacidad
16. ¿Por qué me salen anuncios justo de lo que he hablado?
17. Cookies: qué son y qué aceptamos sin leer.
18. ¿Cómo evitar llamadas y correos publicitarios?
19. ¿Qué son las listas Robinson?
Bloque 4 · Privacidad y tecnología
21. ¿Qué datos compartes al instalar una app?
22. ¿Tu coche también sabe por dónde te mueves?
23. Inteligencia artificial y privacidad: ¿nos espían las máquinas?
24. ¿Son seguros los códigos QR?
25. ¿Qué pasa con tus datos cuando usas Wi-Fi gratis?
Bloque 5 · Derechos y reclamaciones
26. ¿Sabías que tienes derecho a que borren tus datos?
27. Derecho al olvido: ¿puedo desaparecer de internet?
28. ¿Qué hacer si han publicado una foto tuya sin permiso?
29. ¿Cómo denunciar un uso indebido de tus datos?
30. ¿Qué hace la Agencia Española de Protección de Datos?
Bloque 6 · Privacidad en ámbitos específicos
31. ¿Te pueden obligar a dar tu DNI?
32. Videovigilancia: ¿pueden grabarte en la tienda?
33. ¿Pueden leer tu correo en el trabajo?

34. ¿Es legal que te pidan una foto para entrar a una discoteca?
35. ¿Qué pasa con tus datos cuando te haces socio de un gimnasio?
Bloque 7 · Privacidad y vulnerabilidad
36. Cómo proteger a personas mayores frente a estafas digitales.
37. ¿Qué riesgos corren las personas migrantes con sus datos?
38. Privacidad y violencia de género: cómo protegerse digitalmente.
39. ¿Por qué es tan importante la privacidad en salud mental?
40. Cómo evitar que una expareja controle tus dispositivos.

41, Confidencialidad y anonimato canal de denuncias y protocolos

escolar

Suplemento de HERALDO DE ARAGÓN
Miércoles **22 de octubre de 2025**

TE INTERESA

DÍA INTERNACIONAL DE LAS BIBLIOTECAS

Este viernes 24 de octubre se conmemora el Día de las Bibliotecas bajo el lema 'Contra la desinformación: bibliotecas', que busca destacar el papel fundamental que desempeñan todas las tipologías de bibliotecas (públicas,

TU OPINIÓN CUENTA

Escuela sin papeles

«La burocracia nos ahoga». ¿Qué docente no firmaría esta afirmación? Bien, de acuerdo. Cumplimentar documentación es una pesada carga que nos supone un esfuerzo, decimos, que podríamos emplear en causas más nobles.

Ahora bien, dispuestos al debate, ¿significa esto que renunciamos a la documentación sabiendo que, dado el caso, nos ampara cuando la necesitamos para defender nuestros derechos?

Hubo un tiempo en que estos mecanismos de control y supervisión se mantenían en unos niveles razonables. Incluso los vimos como un apoyo que favorecía el desarrollo de nuestros proyectos. Hoy, sin embargo, vivimos en un ecosistema donde impera una cierta confusión, en el que se asocia la burocracia con una extrema fiscalización de nuestra práctica educativa.

Tan absurdo es sepultar a los docentes con exigencias excesivas como rechazar un requerimiento documental, por muy razonable que sea.

Proclamo mi fe en el compromiso y el esfuerzo común y expreso mi escepticismo ante la improvisación y la desinformación. Por ello, creo que documentar nuestra práctica es asegurar que somos fiables y responsables, recorrer un camino cómplice que nos invita a creer en nuestra obra y nos aproxima a la certeza.

Conviene, así, formar a los docentes en el manejo de la documentación, propiciando herramientas útiles y mejorando la gestión del tiempo. Este último es un aspecto crucial, cuya mejor gestión nos ayudaría a ser más eficientes y a acercarnos a un mayor bienestar.

Por:
Juan Antonio Pérez Bello

INSTITUTOS HISTÓRICOS

Museos vivos del patrimonio pedagógico de Aragón

Se crearon hace 180 años en las tres provincias aragonesas y almacenan un material inédito utilizado a lo largo de los años en el ámbito de la enseñanza, además de las huellas de ilustres alumnos

Fue en 1845 cuando la reina Isabel II rubricó la ley Pidal y nacieron los institutos públicos en España. Este hito histórico es fielmente recreado en el cortometraje 'La firma', gracias a la inteligencia artificial (IA) y al buen hacer de la profesora Nuria Calvo, jefa del Departamento de Inglés y Coordinadora del Patrimonio Histórico del IES Goya.

El documental, que se presentó el pasado 30 de septiembre como uno de los principales actos conmemorativos del 180 aniversario del instituto zaragozano, muestra la función de los centros de segunda enseñanza en el país. «Cumplían un papel preparatorio para la universidad, además de profesionalizar», explica Concha Gaudó, exprofesora de Geografía e Historia del centro y miembro de la Asociación Innovación y Patrimonio IES Goya. Para ella, la condición de 'instituto histórico' es «una gran responsabilidad, tanto por llevar 180 años educando como por conservar el patrimonio pedagógico».

El del Goya es muy rico y diverso, con fondos de todo tipo. Se recogen los expedientes de todo el alumnado, incluidos los de personajes ilustres como María Moliner o Luis Buñuel, entre otros. También hay de asignaturas que ya no se imparten, como la de Agricultura en el siglo XIX o de materiales que ya no se utilizan, como los grabados para enseñar Arte, como explica Gaudó. En definitiva, su legado lo forman el archivo histórico, la biblioteca histórica, los bienes culturales de los departamentos de Biología y Geología, Física y Química, Geografía e Historia, el museo de Ciencias Naturales y los cinco cuadros en depósito del Museo del Prado de Madrid.

Museo de Ciencias del IES Ramón y Cajal de Huesca. V. LACASA

Bienes en el instituto turolense. IES V. TURIA

Biblioteca histórica del IES Goya, en Zaragoza. RUBÉN LOSADA

Mención aparte merece la visita que realizó Albert Einstein en 1923, reflejada en una de las actas del claustro del instituto. Precisamente este hecho histórico se recogerá en otro vídeo conmemorativo elaborado con IA que se presentará próximamente.

Aquellos institutos provinciales

Sucesores de los antiguos institutos provinciales, el IES Ramón y Cajal, de Huesca; y el IES Vega del Turia, de Teruel cierran la nómina de institutos históricos de Aragón. El primero de ellos fue sede el pasado año de las XVII Jornadas Nacionales de Institutos Históricos. Su directora, María Costa Rey, aclara el esfuerzo organizativo que supuso desarrollar un programa de tal envergadura y afirma con rotundidad que «en la actualidad seguimos trabajando para defender nuestro patrimonio, mantener y restaurar muchos de los bienes que conservamos en el centro». Que son abundantes, pues el instituto oscense, en el que estudiaron el propio Ramón y Cajal o Joaquín Costa, cuenta con un Museo de Ciencias que reúne una gran colección zoológica y geológica, y con el Museo Sertoriano, que rescata el legado de una de las universidades más antiguas de España, fundada en 1354 y que desapareció en 1845, convirtiéndose en aquel instituto provincial.

El IES Vega del Turia, por cuyas aulas pasaron Antonio Mingote o José Antonio Labordeta de profesor, tiene previsto organizar actividades de difusión en el vigente curso académico para dar a conocer a su propio alumnado la «relevancia» del patrimonio que alberga el instituto más antiguo de Teruel, tal y como apunta Rosa María Galán, directora del centro. «La sociedad turolense no es consciente del valor de nuestros fondos y de nuestra vocación de servicio que, al final, es lo que define a cualquier centro educativo», añade. Como ejemplo de esta labor, la directora refiere que han recibido valiosas donaciones de particulares y que, a su vez, el propio instituto ha colaborado con el Museo de Teruel cediéndole bienes. En su amplio catálogo de bienes históricos hay herbolarios de otro siglo, libros antiquísimos o ejemplares faunísticos, entre otras joyas.

Por: ***Carolina Iglesias***

escolares, universitarias, especializadas y nacionales/regionales) en la lucha contra la desinformación. Las bibliotecas la combaten a través de sus recursos y de un uso adecuado de las nuevas tecnologías. Y, por encima de todo, gracias a su personal bibliotecario, que trabaja como curador de contenidos.

SÍGUENOS EN INSTAGRAM
@heraldoescolar

EXPERIENCIAS

¡Qué interesante es la paleontología!

Con motivo del Día Internacional de la Geodiversidad, los escolares de primaria de los municipios turolenses de Mas de las Matas, Castellote y Galve participaron los días 6, 8 y 9 de octubre en una serie de actividades formativas centradas en la divulgación científica que se agruparon bajo el nombre 'Guardianes del territorio: niños por la conservación paleontológica'.

En cada municipio y dentro del horario lectivo, se impartió una charla sobre fósiles y su conservación, con ejemplos basados en la paleontología local, que contó con el respaldo de la Fundación Conjunto Paleontológico de Teruel-Dinópolis (Museo Aragonés de Paleontología).

Dos de sus especialistas, Raquel Ferrer y María Pilar Castellano, fueron las encargadas de conducir las actividades, que tuvieron una gran acogida entre los escolares. Castellano señala que «les gusta mucho ver los restos fósiles que les enseñamos de su entorno y, sobre todo, saber que son muy importantes. Muchos saben de ellos, pero no los conocen ni se hacen a la idea de lo valiosos que son». De entre todas las iniciativas, destaca el interés que despierta el taller de réplicas: «Primero hacen un molde de un fósil y luego sacan una copia. Cuando desmoldan la escayola se sorprenden muchísimo del resultado. También les llama la atención los materiales que utilizamos para los talleres, las siliconas, la arcilla y la escayola». Y añade: «Más de uno dice que le gustaría ser paleontólogo de mayor y encontrar un gran dinosaurio».

Por: ***Heraldo Escolar***

Las actividades planteadas buscan despertar el interés de los escolares. FUNDACIÓN CONJUNTO PALEONTOLÓGICO DE TERUEL-DINÓPOLIS

Creatividad sanadora. El alumnado de 1º de ESO del IES Baix Matarranya, en el municipio de Maella, ha trabajado el punto en Educación Plástica, Visual y Audiovisual, inspirándose en la obra de la artista japonesa Yayoi Kusama, que utiliza su arte como una forma de terapia.

Contra la soledad no deseada. El alumnado de Psicología del Colegio Madre María Rosa Molas de Zaragoza salió a la calle con sus 'Mesas contra la soledad', un espacio para conversar, conectar y recordar que, a veces, un rato compartido puede marcar la diferencia.

SUEÑOS DE COLOR: un globo aerostático

Clara Antón Allué, de 3º de primaria
CEIP Moncayo, Tarazona

NUESTRA PRÓXIMA HISTORIA: 'Patio incógnita'.
Shackleton es una chica corriente. No tiene amigos ni enemigos hasta que, un día, se nombra capitana del barco Polaris y zarpa hacia el Polo Norte. Casi toda su clase se suma a este viaje y las aventuras se suceden. **Dibuja para la semana que viene:** el Polo Norte, con sus habitantes, sus animales y sus características casas.

CÓMO ENVIAR LOS DIBUJOS
Independencia, 29. 50.001-Zaragoza o escolar@heraldo.es. El proyecto de literatura infantil y juvenil de Santillana **Loqueleo** premiará al ganador con dos libros que recibirá en su colegio.

'Patio incógnita'. Autor: Bruno Puelles. Loqueleo. Más de 10 años. Temáticas: acoso escolar, amistad, aventura, colegio, convivencia.

ESCUELA DE PRIVACIDAD

Proteger tus datos también es cosa de héroes

Imagina que un día subes una foto con tu camiseta del cole y alguien la comparte sin que lo sepas. O que publicas dónde vas a jugar y un desconocido lo ve. Puede parecer que no pasa nada, pero tus datos cuentan quién eres y merecen protección, igual que cuidas tus tesoros más valiosos.

- Tus datos no son solo tu nombre o tus fotos: también son tus dibujos, vídeos, mensajes y gustos. Son parte de ti, como tu escudo de superhéroe. Antes de publicar o compartir, pregúntate: ¿Lo vería alguien que no conozco?, ¿Me sentiría bien si lo viera mi profe o mi abuela?, ¿Quiero que se quede en internet para siempre?
- No compartas contraseñas con amigos ni uses fechas fáciles de adivinar. Usa claves fuertes, como si fueran la llave de tu fortaleza secreta, que solo tú y tus padres conozcan.

Si algo en internet te hace sentir raro o incómodo, cuéntalo a tus padres o a un adulto de confianza. No es chivarse: es proteger tu seguridad y la de tu mundo.

- Cuidar tu privacidad no es tener miedo, es ser valiente e inteligente. Así podrás disfrutar de juegos, vídeos y redes sin preocuparte de que alguien use tu información para hacer daño o reírse de ti.

Recuerda: tus datos son tuyos. Tú decides qué compartir y con quién. Si tienes dudas, es mejor preguntar antes de publicar.

- Internet es un lugar increíble para aprender, crear y divertirte, pero ser un héroe digital significa proteger tu privacidad en cada paso. ¡Con pequeños gestos puedes ser grande en internet!

Además, cuando cuidas tus datos, cuidas a tus amigos. Un héroe de verdad protege a los demás mientras se divierte. ¡Tú puedes ser ese héroe digital cada día!

Por: ***Fernando Andreu***
Aragón Privacidad

TUS AMIGOS Y TÚ ¿AÚN NO CONOCÉIS...?

'Contamos contigo', de Diego Arboleda y José Fragoso

Un buen puñado de escritores e ilustradores de literatura infantil y juvenil han unido sus teclados, sus plumas y sus pinceles para construir este libro de relatos híbrido y mestizo.

Editado por la editorial valenciana Sargantana, el volumen reúne los textos de 26 autores y autoras y las ilustraciones de 22 artistas gráficos que han colaborado de manera totalmente desinteresada. Los beneficios obtenidos con su venta se destinarán íntegramente a la reconstrucción de nueve bibliotecas municipales de las zonas más afectadas por la DANA.

Fantasía, amor, humor, algún poema y hasta un cómic forman parte de esta selección que tiene como nexo de unión el amor por las palabras, la solidaridad y la generosidad de un grupo de autores que saben que recuperar la normalidad, recuperar la vida... pasa por recuperar las historias, los libros y los espacios donde compartirlos.

En esta semana de las bibliotecas, corred a las librerías a encargar este libro que os llenará de aventuras y permitirá que otros retomen las suyas.

Por: ***Pepe Trivez***

escolar

TE INTERESA

SANTA'S ENGLISH WORKSHOP
El próximo 12 de diciembre, a las 18.00, el Ámbito Cultural de El Corte Inglés organiza, junto a Number16 School, Santa's English Workshop, una de las actividades más mágicas y traviesas de la Navidad. Los más pequeños se convertirán en elfos ayudantes mientras juegan, cantan y aprenden inglés sin darse cuenta. Entre risas y sorpresas del Polo Norte, vivirán una experiencia llena de color y espíritu navideño. Las plazas son limitadas, es imprescindible inscripción previa y confirmación en el *mail*: acultural_zaragoza@elcorteingles.es

TU OPINIÓN CUENTA

El profesorado tiene voz

El lunes se presentó la Unidad de Apoyo al Profesorado, que persigue cuidar de quienes sustentan el sistema educativo. ¿Cuidar de o cuidar a?
El título parece un poema al revés. Sospecho que los docentes no hablamos, que somos como un verso dirigido a una sociedad que escucha poco y vive de espaldas a la palabra de quien aún creemos en la vocación. ¿Los docentes hablamos? En realidad, muy poco. Quizás porque nos han puesto entre la dificultad y la ignorancia. O porque vivimos para que el sistema educativo mire de frente a los ojos de la gente.
Cuando el docente habla, cuenta que le gustaría un sistema de acceso a la carrera que valorase también valores. Quiere decir que cree en otra distribución de los tiempos, otra organización de los espacios y un nuevo diseño de los equipos didácticos. Desea hablar de que es necesario que los equipos directivos lo sean porque quieren, saben y pueden. Y pretende que se le crea cuando se refiere a las familias como cómplices incondicionales cuyo apoyo tanto bien hace. ¡Ah! Y que confíen en ellos. Por eso necesitamos que se nos conozca de verdad, que sepan cómo somos, por qué somos y, muy importante, con quién somos. Hace falta más verdad y menos titulares.
¿Hablamos poco? Pues entonces es preciso que seamos mensajeros de nuestra vida. Que compartamos nuestro trabajo, opiniones e ideas. La sociedad tiene que conocernos y eso depende de ellos, de ti y de mí. Es una asignatura pendiente.

Por: ***Juan Antonio Pérez Bello***

DÍA DE LA ELIMINACIÓN DE LA VIOLENCIA CONTRA LA MUJER

¿Cómo celebraron el 25-N los colegios aragoneses?

Todos los colegios e institutos aragoneses deben incluir en su proyecto educativo de centro un plan de convivencia e igualdad

De múltiples formas reivindicaron y conmemoraron las aulas aragonesas el Día Internacional de la Eliminación de la Violencia contra la Mujer. Pero en todas ellas el mensaje era el mismo: ni una víctima más.

Según indican desde la Dirección General de Política Educativa, Ordenación Académica y Educación Permanente del Gobierno de Aragón, en el curso 2025-2026, más de 50 centros se han beneficiado de una dotación económica extraordinaria por realizar proyectos coeducativos para el desarrollo de los planes de convivencia e igualdad y la prevención de la violencia de género.

Además, dentro de las medidas desarrolladas en el Pacto de Estado contra la Violencia de Género, el Departamento de Educación y el IAM ofrecen teatro de sensibilización y formación especializada en este ámbito.

Por: ***Heraldo Escolar***

@ies_avempace Con una intervención artística colectiva en torno al acto de tejer. «Tejer complicidades, tomar conciencia y proponer acciones de mejora de la calidad de vida de las mujeres».

@cpilajota Con un Jardín de la Igualdad para «reflexionar sobre la importancia del respeto, la convivencia y la igualdad, aportando su creatividad y su compromiso para construir un entorno más justo y seguro».

@iesejimeno Con una reflexión sobre la importancia de romper con los estereotipos de género «que nos ha permitido cuestionar y comprender mejor cómo influyen en nuestro día a día».

@ceipcerbin Con un mural que plasma «comportamientos que están mal, como los insultos o el control; y conductas que están bien, como la igualdad, el apoyo mutuo, la comunicación sana y el respeto».

@ceipmaella Con títeres, cuentos y canciones para «celebrar la igualdad entre niños y niñas» y entender por qué hay un día dedicado a aquellas mujeres que sufren violencia.

@iesmcatalanzgz Con un mural reivindicativo y «llenando las paredes del instituto con el nombre de las mujeres asesinadas desde 2018 por violencia machista. Para que los números lleguen algún día a cero».

SÍGUENOS EN INSTAGRAM

@heraldoescolar

EXPERIENCIAS

Navidades sostenibles

Queda muy poco para la Navidad y el ambiente festivo de estos días se empieza a respirar en las calles. Se acerca una época llena de luces, magia e ilusión en la que los niños y las niñas son los protagonistas.

Durante estos días, nuestro mayor deseo debería ser aprovechar las vacaciones en familia y con amigos para crear bonitos recuerdos que nos acompañen siempre. Una buena forma de conseguir esos momentos que recordaremos con cariño más adelante es llevar a cabo manualidades en familia. Que todos los miembros de la casa trabajen juntos utilizando su y la creatividad.

Algunas ideas de manualidades para hacer con los más pequeños. P. E.

Puede resultar muy divertido usar materiales reciclados para crear figuras. Por ejemplo, decorar rollos de papel como elfos, renos o, incluso, Papá Noel; crear copos de nieve con botellas de plástico, pintura y rotuladores de tiza líquida; construir pueblos navideños con cajas de leche, témperas de colores y luces; o hacer postales de Navidad decoradas y personalizadas, listas para enviar. Y como durante estos días tenemosm ás tiempo para jugar, podemos rescatar algunos clásicos como el tres en raya, el hundir la flota o el juego del *stop*, para los que solo es necesario papel y boli.

Todas estas actividades tienen como base principal la diversión, pero también nos enseñan a dar una nueva vida a objetos que ya no se utilizan antes de tirarlos, a trabajar en equipo y a sentirse orgullosos de ver el resultado de nuestro trabajo.

La Navidad es para disfrutarla con mucha ilusión, pero no nos olvidemos de conectar con lo que realmente importa.

Por: ***Patricia Estela***

a+NHORABUENA!ƒ Carlos Larraz, estudiante del ciclo formativo de grado medio de Instalaciones Eléctricas y Automáticas del CPIFP Pirámide, ha sido reconocido como Mejor Instalador Novel 2025 en la XVIII edición del Concurso Nacional de Jóvenes Instaladores organizado por FENIE.

¶ƒLEER DESDE PEQUEÝOS¥ En el CEIP Concepción Gimeno Gil de Alcañiz han pasado unas tardes muy entretenidas acompañados de las familias y de la escritora Sandra Araguás. ¿El objetivo? Fomentar la lectura a los 3, 4 y 5 años, y saber más sobre los cuentos clásicos y la tradición oral.

SUEÑOS DE COLOR: un dinosaurio

¡GANADOR!

Pablo Guaus Penella, de 1º de primaria
CEIP Monzón 3, Monzón

4; +9: 8¶ƒ68»>/3 ¶ƒ /9: 58/¶^ƒ
Un nuevo comienzo. Píntalo dorado 1. Lenlen es patinadora y tiene un sueño: competir en los Juegos Olímpicos de 2030. Y, aunque los saltos se han convertido en su cruz personal, ¡no piensa rendirse!
Dibuja para la semana que viene: baloncesto, fútbol, balonmano, gimnasia rítmica, kárate, tenis, atletismo, *datchball*... ¿Cuál es tu deporte favorito?
ƒ
)»3 5ƒ+4</¶8ƒ59ƒ /(; 059ƒƒ Independencia, 29. 50.001-Zaragoza o escolar@heraldo.es. El proyecto de literatura infantil y juvenil de Santillana **Loqueleo** premiará al ganador con dos libros que recibirá en su colegio.

; N/NUEVO/COMIENk ZO¥ƒ/NTALO/DORADOƒ
****Autora: Andrea Tomé. Loqueleo. Más de 12 años. Temáticas: adolescencia, amistad, autoestima.

ESCUELA DE PRIVACIDAD

Ser libre también es saber decir no

Cuidar tu privacidad es cuidar de ti. Y respetar la de los demás también. En internet, muchas formas de violencia empiezan cuando se rompe esa barrera: se publica una foto sin permiso, se reenvía un mensaje privado, se difunde un rumor, se graba sin consentimiento o se expone algo íntimo para ridiculizar. Detrás de cada imagen o dato hay una persona. Lo que parece un juego, una gracia o un reto puede convertirse en una herida digital que deja huella, que hace daño y que no siempre se borra ni se olvida.
Aunque no haya gritos ni empujones, la violencia digital también hiere. Y decir no ante eso requiere valor, más del que parece. La libertad no es hacer cualquier cosa sin pensar. Es elegir con empatía, con responsabilidad, con respeto, con sentido común y con coraje. Ser libre es decidir lo correcto incluso cuando cuesta. Ser responsable es entender que lo que compartes, grabas, reenvías o comentas deja marca en los demás... y también en ti.
Si algo en internet te hace sentir mal, te incomoda, te asusta o invade tu intimidad, puedes pararlo. Puedes contarlo. Puedes pedir ayuda. Eso no es chivarse: es proteger tu dignidad, tu privacidad y tu bienestar emocional. Mereces sentirte seguro también en lo digital. Y puedes ayudar a que otros también se sientan protegidos.
Y si tú no eres quien sufre, pero lo ves, también puedes actuar. No rías, no compartas, no participes. A veces, frenar una cadena de daño empieza con una sola persona que se atreve a respetar. Ayudar también es cuidar. Y respetar lo privado es siempre el primer paso.
Cada *clic* cuenta. Cada palabra, cada imagen, cada gesto, cada silencio. Defender la privacidad propia y ajena es también defender la libertad. Tú puedes hacerlo. También en la red.

Por: ***Fernando Andreu***
Aragón Privacidad

¿QUÉ ME ESTÁS CONTANDO?

Historias para no dormirme

Miraba Mateo su libro de ciencias con desesperación: «Estoy *reventao*, ¿cómo voy a recordar Mercurio, Venus, Tierra, Marte, Júpiter, Saturno, Urano y Neptuno? Y además por orden, es una locura». Sus neuronas, en huelga, pedían refuerzos. Entonces ideó un plan para aprendérselo. Con las iniciales de los planetas creó una frase que fuera fácil de visualizar: «Me vendió un tigre tu madre el jueves satánico con uñas negras». Se imaginó la escena con el máximo nivel de detalles y lo memorizó fácilmente. ¡Lo tenía! Entusiasmado con su idea, inventó otra frase para recordar las 7 islas Canarias: «Paloma te hizo un gol gracioso lanzando furiosa». Al día siguiente, fue precisamente esta una de las preguntas del examen, y, mientras la contestaba, Mateo se rió imaginando a su amiga Paloma furiosa corriendo con el balón en un partido de fútbol. No solo lo recordaba todo, sino que hasta se había divertido estudiando. Eso sí, seguía *reventao*.

- **Claves para lograrla:**
  Elegir palabras clave, aplicar reglas nemotécnicas y usar acrónimos y acrósticos, creando imágenes ingeniosas.
- **Consecuencias:**
  Es más ameno estudiar y recordarás lo aprendido durante mucho tiempo.

Por: ***Fundación Piquer. Programa Escuela Activa***

ARAGÓN PRIVACIDAD

PROGRAMA

9:00	**Bienvenida y presentación de las jornadas** ***D. Miguel Angel García Muro*** Concejal Delegado Ayto. Zaragoza de Transformación Digital
9:15 - 10:00	MESA 1 **Panoramas PD 2025 | *Francisco Pérez Bes*** - Adjunto presidencia AEPD
10:00 - 10:45	MESA 2 **Privacidad y relaciones laborales** ***Herminia Lombarte Laviña*** - Directora de Zona Adecco Aragón ***Ivana Larrosa Ibáñez*** -Profesora de Derecho Internacional Privado y Arbitraje Internacional
10:45 - 11:15	**Coffe Break**
11:15 - 12:00	MESA 3 **La desconexión digital en la práctica** ***Eva Barrabino*** - Directora Departamento de Administración RRHH y RRLL de Hiberus ***Rosa García Torres*** -Directora Área Relaciones Laborales y Sostenibilidad CEOE Aragón
12:00 - 12:45	MESA 4 **Privacidad, menores y patria potestad en el entorno digital** ***Ramón Arnó*** - Abogado especialista en aspectos jurídicos del entorno digital
12:45 - 13:30	MESA 5 **Protrección de la infancia en el entorno digital** ***Alexandra Juanas*** **-** DPO de MasOrange ***María Doussinague*** **-** Manager Social Impact MasOrange
13:30 - 15:30	**Comida libre / insitucional**
15:30 - 16:15	MESA 6 **Automatizar la privacidad: cuando la anonimización se convierte en ventaja competitiva** ***Mario Garcés*** - The Mindkind ***Pedro Luís Gimeno*** -Elan Asesores ***Oscar Villanueva*** - Nymiz - Personal Data Masking
16:15 - 17:00	MESA 7 **Privacidad, el DPD y el talento** ***María Cristina Martínez Tercero*** - Responsable Consultoría Legal en Integra Platform
17:00 - 17:45	MESA 8 **Ciberseguridad y protección de datos** ***David López*** - Fundador MADAC ***Vitori Hernandez*** - Women4Cyber
17:45 - 18:15	**Entrega de premios y clausura**

E&K Pro Privacidad Estratégica · audidat · CEOE ARAGÓN · SANVALERO grupo · coloriuris generando confianza · ARAGÓN PRIVACIDAD · Zaragoza AYUNTAMIENTO

IV Jornadas Aragonesas de Protección de Datos

Aragón Privacidad nace con la vocación de aglutinar a los profesionales de la privacidad y cumplimiento normativo que desarrollan su actividad en Aragón, como respuesta a una necesaria intervención en nuestra profesión y actuando desde la proximidad de nuestro territorio.

La imparable velocidad adquirida por la aplicación del RGPD, los nuevos paquetes normativos o la irrupción de la IA, entre otros, hace necesario agrupar esfuerzos y sinergias, sumando el talento que inspira Aragón de tal modo que podamos aunar iniciativas y poner en valor nuestra figura profesional.

Panoramas Protección de Datos en 2025, por Francisco Pérez Bes

Tras la inauguración institucional, la primera intervención corrió a cargo de Francisco Pérez Bes, adjunto a la presidencia de la Agencia Española de Protección de Datos (AEPD), quien ofreció una ponencia magistral centrada en las tendencias regulatorias y tecnológicas que marcarán la evolución de la privacidad en los próximos años.

Pérez Bes abrió su intervención subrayando que el volumen y la sensibilidad de los datos tratados en la actualidad hacen imprescindible consolidar estructuras sólidas de cumplimiento, tanto en el sector público como en el privado. Rechazó frontalmente la idea de que la normativa en protección de datos actúe como freno a la innovación, reivindicando que el RGPD, además de garantizar derechos fundamentales, habilita una libre circulación de la información basada en la seguridad y la confianza.

De hecho, insistió en que uno de los principales retos actuales no es la existencia de regulación, sino su correcta interpretación y aplicación en entornos altamente tecnológicos y cambiantes.

Uno de los ejes centrales de su ponencia fue la llamada "avalancha regulatoria" que, desde Bruselas, está redefiniendo el marco normativo en el que operan las organizaciones. Mencionó como hitos especialmente relevantes el Reglamento de Inteligencia Artificial, la Directiva NIS2 sobre infraestructuras críticas, la Digital Services Act, la Digital Markets Act, el Data Act y otros textos que, en conjunto, componen un ecosistema jurídico interconectado pero fragmentado en términos operativos.

En esta línea, defendió el papel del Delegado de Protección de Datos como figura esencial en la arquitectura de cumplimiento, no solo por su función consultiva, sino como garante interno de legalidad, transparencia y eficiencia, llamando a fortalecer su protagonismo.

Entre ellas, destacó las auditorías algorítmicas, los principios de privacidad desde el diseño (*privacy by design*) y por defecto, la ingeniería de privacidad, la implantación de cuadros de mando de transparencia y la existencia de protocolos específicos para incidentes de seguridad. Lejos de considerar el RGPD como una norma estática, lo definió como un marco vivo, en constante evolución.

Pérez Bes dedicó también una parte sustancial de su intervención al análisis de los riesgos tecnológicos emergentes. Enumeró entre ellos la expansión de la inteligencia artificial generativa, los deepfakes, los datos sintéticos, la biometría avanzada, el internet de las cosas (IoT) y la computación cuántica, tecnologías que ponen en cuestión los sistemas actuales de cifrado y las bases tradicionales del consentimiento informado.

Alertó del uso creciente de dispositivos que recopilan datos fisiológicos, emocionales o neurológicos, y defendió la necesidad de abordar cuanto antes los neuroderechos.

Asimismo, advirtió que la protección de datos ya no es únicamente una cuestión legal o de cumplimiento formal, sino que se ha convertido en una cuestión estratégica de gobernanza. Cada vez más, afirmó, las decisiones de inversión están condicionadas por el estado de la ciberseguridad y el nivel de madurez en privacidad de las organizaciones.

En este sentido, alertó sobre el impacto reputacional, legal y financiero que puede derivarse de una gestión deficiente de los datos, especialmente en un contexto en el que se multiplican las demandas colectivas por brechas de seguridad. Recordó que ya existen precedentes en los que incidentes en protección de datos han afectado directamente a la cotización bursátil de compañías tecnológicas, y llamó a no subestimar esta dimensión del riesgo.

Privacidad y relaciones laborales, por Herminia Lombarte e Ivana Larrosa

La segunda mesa la protagonizaron Herminia Lombarte, Directora de Zona de Adecco Aragón, e Ivana Larrosa, profesora de Derecho Internacional Privado y Arbitraje Internacional, aportando una perspectiva ofreciendo por un lado la experiencia de una gran empresa de recursos humanos, y por otro, el marco normativo y jurisprudencial que delimita los derechos fundamentales de los trabajadores en entornos digitalizados.

Lombarte expuso las claves del tratamiento de datos personales en los procesos de selección de Adecco, una de las principales firmas de empleo en Aragón, donde se reciben y procesan más de 150.000 candidaturas, destacando la dificultad de conjugar el volumen masivo de datos con la inmediatez que exigen los clientes, lo que obliga a adoptar sistemas digitales sin comprometer la privacidad.

Explicó detalladamente el recorrido que realiza un dato desde su entrada en la base hasta su eventual supresión o anonimización, destacando el uso de la plataforma Salesforce como eje de la trazabilidad y seguridad del tratamiento.

El proceso comienza con la entrada digital de información por diversas vías: formularios web, redes sociales o candidaturas espontáneas. En todos los casos, se garantiza la aceptación de la política de privacidad mediante trazabilidad electrónica, asegurando el consentimiento expreso y el cumplimiento de los requisitos legales. Las comunicaciones comerciales, explicó, requieren un consentimiento adicional mediante un check específico, y en caso de no ser aceptado, el sistema revoca el alta de forma automatizada en un plazo de siete días.

La ponente también detalló las medidas adoptadas para segmentar la base de datos de candidatos, identificar perfiles aptos para las ofertas disponibles y garantizar comunicaciones seguras, todo ello bajo criterios de cumplimiento normativo y seguridad informática. Destacó que las cláusulas legales se integran en todas las comunicaciones mediante footers informativos, y que el ejercicio de derechos se canaliza a través de un enlace directo, que remite la solicitud al departamento jurídico de la compañía.

En cuanto a la política de retención, se aplican tres mecanismos: borrado automático tras tres años sin interacción, supresión permanente a solicitud del interesado, y anonimización como alternativa en determinados casos.

Según concluyó, estas prácticas reflejan el compromiso de Adecco con el cumplimiento del RGPD y la transparencia en la gestión de datos laborales.

Larrosa abordó el marco jurídico que regula la protección de datos personales en el entorno laboral desde una perspectiva multinivel, analizando el entramado normativo que abarca la legislación europea, el derecho internacional y la normativa estatal. Mencionó el RGPD, el Reglamento de Inteligencia Artificial, el Comité Europeo de Protección de Datos, así como las obligaciones establecidas en la Constitución Española, la LOPDGDD y el Estatuto de los Trabajadores.

Subrayó que cualquier juicio sobre una posible vulneración de derechos debe atender a tres filtros: idoneidad, necesidad y proporcionalidad de la medida, en coherencia con los principios derivados del Derecho Europeo. Larrosa centró buena parte de su intervención en la jurisprudencia del Tribunal Europeo de Derechos Humanos, citando los casos Bărbulescu II y López Ribalda.

En el primer caso, se estableció el conocido "Test Bărbulescu", que obliga a los tribunales a ponderar si una medida empresarial —como el control de comunicaciones— era idónea, necesaria y proporcionada. En el segundo, relativo a videovigilancia en supermercados, el TEDH avaló las medidas tomadas por la empresa en un contexto excepcional, validando el uso de cámaras ocultas bajo ciertas garantías.

La profesora también analizó cómo la irrupción de la inteligencia artificial en el ámbito laboral introduce nuevos desafíos, especialmente en lo relativo a procesos de decisión automatizada y evaluación de desempeño. Señaló que el uso de IA en estos contextos debe estar sujeto a criterios estrictos de transparencia, prevención de sesgos y respeto a los derechos fundamentales del trabajador, como el honor y la intimidad.

La mesa concluyó con la constatación de que la gestión de datos en el ámbito laboral exige una combinación cada vez más precisa entre herramientas tecnológicas, diseño jurídico y criterios éticos. Tanto desde la empresa como desde el derecho, se reivindicó la necesidad de fortalecer una cultura de cumplimiento que ponga el foco en la persona trabajadora, reconociendo la privacidad como un derecho operativo, y no como un obstáculo, dentro de la lógica organizativa.

La desconexión digital en la práctica, por Eva Barrabino y Rosa García

La tercera mesa de las jornadas se centró en el derecho a la desconexión digital. Rosa García Torres, directora del Área de Relaciones Laborales y Sostenibilidad de CEOE Aragón, y Eva Barrabino, directora del Departamento de Administración, Recursos Humanos y Relaciones Laborales de Hiberus.

Rosa García Torres abrió la mesa destacando que el derecho a la desconexión digital no era una mera formalidad legal, sino una herramienta esencial para garantizar el bienestar psicosocial de las plantillas en un entorno marcado por la inmediatez, la ubicuidad tecnológica y la presión constante por la productividad. Señaló que, si bien el teletrabajo y la conectividad ofrecían ventajas operativas, también introducían riesgos asociados al tecnoestrés, la tecnofatiga, la ansiedad digital o incluso la adicción al trabajo.

Abogó por la integración sistemática de evaluaciones de riesgos psicosociales, recomendando que se informara a las personas trabajadoras sobre su realización y finalidad. Señaló que la desconexión digital no solo tenía una dimensión psicológica, sino también física: el uso prolongado de dispositivos digitales conllevaba problemas musculoesqueléticos y daños oculares, como la fatiga visual, la sequedad ocular o trastornos de visión a largo plazo.

Destacó que todas las organizaciones debían contar con una política interna de desconexión, adaptada a su tamaño, sector y estructura operativa. Evitar prácticas como el envío de correos electrónicos fuera del horario laboral y que las políticas sean consensuadas con los representantes de los trabajadores o con estos, incluyendo medidas claras de conciliación, periodos definidos de desconexión y excepciones pactadas. La experta recomendó, además, la creación de comités internos por áreas y la necesidad de revisar los convenios colectivos para introducir los acuerdos sin generar contradicciones normativas o desigualdades.

A continuación, Eva Barrabino aportó el punto de vista empresarial desde su experiencia en Hiberus, donde la política de desconexión se había orientado a una adaptación real del entorno laboral, más allá del cumplimiento normativo. Subrayó que el compromiso con esta política requería acciones concretas, comenzando por la sensibilización interna y continuando con la medición y control de aquellas prácticas que pudieran comprometer el descanso digital.

Explicó que, en su organización, se habían definido protocolos específicos que contemplaban excepciones justificadas —como situaciones de riesgo grave o emergencias operativas— en las que se activaba un procedimiento especial. En estos casos, el tiempo dedicado se computaba como tiempo efectivo de trabajo, y se contaba con un equipo de soporte disponible bajo acuerdo previo de disponibilidad.

Barrabino insistió en que, para que la desconexión digital fuera efectiva, debía ser concebida como parte integral de la cultura corporativa, lo que implicaba revisar procesos, identificar hábitos perjudiciales y adoptar herramientas tecnológicas alineadas con este objetivo. Reforzó así la idea previamente expuesta por García Torres: sin una voluntad clara por parte de las organizaciones —expresada tanto en sus políticas internas como en su conducta diaria—, el derecho a la desconexión podía quedar reducido a una declaración simbólica sin impacto práctico.

Privacidad, menores y patria potestad en el entorno digital, por Ramón Arnó

La cuarta mesa de las jornadas abordó: la protección de los menores en el ámbito familiar. La intervención corrió a cargo de Ramón Arnó, abogado especializado en aspectos jurídicos del entorno digital, quien ofreció un análisis preciso sobre el ejercicio de la patria potestad en contextos marcados por la presencia ubicua de dispositivos tecnológicos y el acceso temprano a Internet.

Arnó recordó la patria potestad como una institución del derecho de familia que conlleva un conjunto de derechos y deberes tanto para los progenitores como para los hijos, donde se articula el principio del interés superior del menor, pero también la obligación de obediencia y respeto derivada de la filiación. A partir de esta base, explicó el concepto del ius corrigendi, entendido históricamente como el derecho de corrección y castigo ejercido por los padres.

Explicó que hasta 1981, este derecho incluía incluso la posibilidad de sanciones físicas, si bien las reformas legislativas posteriores han delimitado este derecho exclusivamente al ámbito de la corrección razonable. En este marco, defendió que ciertas actuaciones cotidianas, como requisar el teléfono móvil de un hijo en contextos de desobediencia o uso inadecuado, pueden y deben enmarcarse en el ejercicio legítimo de la patria potestad, tal como recoge el artículo 162 del Código Civil, sin constituir una vulneración de la intimidad del menor si se adoptan en función educativa y dentro de los límites.

El ponente también trató las consecuencias jurídicas que pueden derivarse del incumplimiento grave de los deberes filiales, especialmente cuando los hijos ya han alcanzado la mayoría de edad, recordando figuras como la indignidad para suceder, la desheredación o la extinción del deber de alimentos, aplicables en casos de ruptura grave del vínculo familiar y falta de respeto a los deberes de convivencia.

Un eje central de su exposición fue la necesidad de proteger y garantizar los derechos digitales del menor. En este punto, Arnó afirmó con claridad que la existencia de una brecha digital entre generaciones no puede justificar la pasividad de los progenitores ante la vida digital de sus hijos. Citó, como pilares normativos, el artículo 5 de la Ley Orgánica de Protección Jurídica del Menor, el artículo 84 del Reglamento General de Protección de Datos, y el artículo 45 de la Ley Orgánica de protección integral a la infancia y la adolescencia frente a la violencia, cuya exposición de motivos ya reconoce la urgencia de actuar sobre la exposición tecnológica de los menores.

Desde una perspectiva jurisprudencial, aludió a la Sentencia del Tribunal Supremo de 10 de diciembre de 2015 y a las contribuciones doctrinales de Antonio Torres del Moral, que han contribuido a consolidar un marco interpretativo donde se equilibra el respeto a la autonomía progresiva del menor con los deberes de protección que pesan sobre padres, tutores y educadores.

Por último, propuso como instrumento jurídico de creciente utilidad el contrato digital parental, una fórmula basada en el acuerdo entre padres e hijos para regular de forma explícita los usos tecnológicos en el entorno doméstico. Esta herramienta, afirmó, permite trasladar los principios del derecho civil a la práctica cotidiana, favoreciendo el diálogo, clarificando límites y

reconociendo responsabilidades mutuas. Lejos de ser una imposición, este contrato contribuye a reforzar una cultura de corresponsabilidad digital dentro del núcleo familiar.

Protección de la infancia en el entorno digital, por María Doussinague y Alexandra Juanas

María Doussinague, manager de Impacto Social en MasOrange, y Alexandra Juanas, Delegada de Protección de Datos (DPO) de la misma compañía, condujeron la quinta mesa redonda. Ambas expusieron, desde sus respectivos ámbitos de responsabilidad, un enfoque basado en datos y los retos regulatorios que impone la actual legislación en materia de privacidad infantil.

María Doussinague presentó los principales hallazgos del Informe de Impacto Social 2025 elaborado por MasOrange, un estudio pionero en el que el sector teleco analiza su responsabilidad en la protección de los menores. Según los datos recogidos, el 93 % de los menores reconocía la necesidad de cambiar sus hábitos tecnológicos.

Sin embargo, un 14 % afirmaba que sus propios progenitores hacían un uso más intenso del móvil que ellos, revelando una contradicción en los modelos de referencia digital dentro del hogar. En cuanto a los usos principales de la tecnología, el 93 % la empleaba para socializar, el 90 % para ver contenidos audiovisuales o jugar online, y un 70 % para actividades formativas, incluidas aquellas que implican el uso de inteligencia artificial.

Entre sus principales preocupaciones, el 81 % se declaraba sensibilizado ante los riesgos digitales, y más de la mitad citaba específicamente aspectos relacionados con la privacidad, la protección de datos y la huella digital. Llamó también la atención el nivel de familiaridad con conceptos como los deepfakes, cuya comprensión por parte de los menores revela una creciente sofisticación en la alfabetización digital.

El informe también identificó desafíos importantes en el entorno familiar: el 50 % de los padres reconocía que sus hijos manejaban mejor las tecnologías que ellos; un 47 % expresaba dificultades en el uso de las plataformas digitales; y un 37 % señalaba la carencia de recursos o formación para acompañar adecuadamente el desarrollo digital de sus hijos. Ante este escenario, Doussinague formuló recomendaciones dirigidas a distintos actores: a las familias, se

les instó a asumir un papel activo como referentes tecnológicos, acompañando a los menores en su uso de las TIC, generando espacios seguros para el diálogo, y siendo conscientes del impacto de compartir imágenes o información de los hijos en redes sociales.

Al profesorado se le encomendó la tarea de contribuir a la formación de una ciudadanía digital responsable; a los propios adolescentes, se les animó a equilibrar su vida digital con actividades analógicas como el deporte o los hobbies; y al sector tecnológico, se le exigió el desarrollo de herramientas de protección avanzadas, integrando la inteligencia artificial como un complemento educativo y no como sustituto del juicio pedagógico.

En esta línea, se presentó el servicio "TuYo" de Orange, una solución diseñada para facilitar el uso seguro del móvil entre menores, que permite modular el acceso a funcionalidades según el grado de madurez del niño, mediante sistemas de control de horarios, bloqueo de contenidos, geolocalización o detección de evasiones. Finalmente, Doussinague subrayó la importancia de las alianzas estratégicas como la colaboración con UNICEF o el programa internacional "Todo por aprender", cuyo objetivo es reducir la brecha digital y garantizar que el acceso a lo digital constituya una oportunidad real de equidad educativa.

Por su parte, Alexandra Juanas profundizó en los retos legales que plantea el tratamiento de datos de menores desde el punto de vista de los profesionales de la privacidad, tomando como referencia el nuevo Proyecto de Ley de Protección al Menor aprobado el 11 de abril. Esta norma refuerza el marco de protección de los derechos fundamentales en entornos digitales, introduciendo cambios significativos como el aumento de la edad de consentimiento de los 14 a los 16 años.

Esta modificación obliga a revisar la validez de los consentimientos otorgados previamente y a implementar sistemas de verificación más robustos; por otro, requiere que las evaluaciones de impacto y los análisis de riesgo incorporen de manera sistemática el principio del interés superior del menor. Además, la legislación prohíbe expresamente el uso de datos de menores con fines publicitarios, lo cual plantea dificultades para el sector del marketing digital, particularmente por la falta de mecanismos fiables para distinguir la edad real de los usuarios.

Juanas abordó también los límites de los actuales sistemas de verificación de edad, señalando que, aunque existen iniciativas como el uso de códigos QR vinculados a operadores móviles, la eficacia de estos controles sigue dependiendo en gran medida de la diligencia de los padres.

En cuanto al impacto económico de esta legislación sobre los proveedores de servicios digitales, explicó que, si bien los beneficios obtenidos en España por muchas plataformas extranjeras ya eran bajos, las nuevas exigencias pueden agravar la tensión regulatoria con operadores internacionales que no comparten el mismo estándar de protección. En conjunto, la mesa evidenció que la defensa de los derechos digitales de la infancia exige un esfuerzo compartido entre familias, sector público, empresas tecnológicas y comunidad educativa, bajo un enfoque que combine regulación eficaz, responsabilidad social y acompañamiento activo.

Automatizar la privacidad: cuando la automatización se convierte en ventaja competitiva, por Mario Garcés, Pedro Luis y Óscar Villanueva

La sexta mesa de las IV Jornadas Aragonesas de Protección de Datosreunió a tres expertos procedentes de distintas áreas del ecosistema tecnológico y jurídico: Mario Garcés (The Mindkind), Pedro Luis Gimeno (Elan Asesores) y Óscar Villanueva (Nymiz).

Mario Garcés se centró en la opacidad estructural de los modelos actuales de inteligencia artificial basados en redes neuronales profundas. Explicó que, aunque el desarrollo de una inteligencia artificial general aún no se ha conseguido por ninguna entidad, en The Mindkind han creado una tecnología intermedia que denominan "ETR 0.5".

Su solución permite resolver problemas de trazabilidad y explicabilidad sin recurrir a reentrenamientos completos, lo que representa una diferencia sustancial respecto a los modelos actuales. Con su enfoque se puede conocer qué datos han sido utilizados, cómo se han procesado, y qué variables han influido en decisiones concretas. El sistema permite también fusionar modelos previamente entrenados, incorporar casos nuevos en tiempo real y eliminar sesgos identificados de manera deliberada.

Sobre el uso de información pública por parte de modelos generativos, señaló la necesidad de establecer mecanismos que limiten el acceso a datos sensibles y permitan verificar qué información ha sido utilizada en cada respuesta ya que se puede hacer reversing de estos. También abordó la cuestión de la computación cuántica, diferenciando entre su utilidad futura en problemas complejos y el riesgo que supone para los actuales sistemas de cifrado ya que grandes potencias ya almacenan información cifrada con la expectativa de desencriptarla cuando la tecnología cuántica sea viable a gran escala.

Óscar Villanueva presentó los servicios de Nymiz, una plataforma centrada en la anonimización de datos personales que ofrece herramientas para identificar, tratar y proteger datos sensibles en más de cien idiomas y en formatos no estructurados como presentaciones, hojas de cálculo, PDFs o documentos legales.

Nymiz aplica técnicas de anonimización, pseudo-anonimización, enmascaramiento, redacción y sustitución por tokens o datos sintéticos, todo ello con el objetivo de evitar brechas de seguridad y asegurar que los tratamientos de datos se mantengan bajo control. Subrayó que muchas compañías operan fuera del ámbito europeo y no respetan la normativa vigente, lo que sitúa a los datos en un terreno de incertidumbre. Por ello, argumentó que la generación de datos sintéticos puede servir para neutralizar estos riesgos, ya que elimina cualquier posibilidad de trazar la información original.

También señaló que uno de los desafíos es trasladar estas soluciones a las pymes, donde la implantación suele ser más compleja, pese a que el riesgo es igualmente elevado. Recalcó que el diseño de las herramientas de privacidad debe permitir una automatización accesible, capaz de mejorar el rendimiento operativo sin depender de conocimientos técnicos avanzados, y ajustarse en todo momento a los marcos legales europeos. Finalmente, hizo un llamamiento a que las herramientas de tratamiento de datos no sean solo aplicables por grandes corporaciones, sino también por pequeñas entidades que deben enfrentar los mismos retos regulatorios.

Privacidad, el DPD y el talento, por María Cristina Martínez

La séptima mesa de la jornada corrió a cargo de María Cristina Martínez Tercero, responsable de Consultoría Legal en Integra, abogada especializada en derecho digital, inteligencia artificial y propiedad intelectual, con una trayectoria de más de quince años. En su intervención articuló una reflexión técnica y estratégica sobre el papel del Delegado de Protección de Datos (DPD) como figura clave en la gobernanza del talento dentro de las organizaciones.

Partiendo de su experiencia en la implantación de protocolos de IA desde el área jurídica, defendió que el DPD debe posicionarse como un motor de confianza y cultura organizativa, alineando cumplimiento normativo, innovación tecnológica y gestión de personas. Martínez subrayó que el Reglamento General de Protección de Datos (RGPD) no concibe al DPD como responsable último de las decisiones empresariales, sino como garante de legalidad y asesor clave.

Esta posición, explicó, cobra especial relevancia ante el nuevo Reglamento Europeo de Inteligencia Artificial y el Data Act, normativas que exigen un conocimiento profundo de los flujos de datos, la evaluación de riesgos, la rendición de cuentas y la formación interna.

Señaló que muchas pymes carecen de los recursos necesarios para implantar dichas exigencias con medios propios, por lo que abogó por modelos híbridos de DPD interno-externo, especialmente en grupos empresariales con estructuras diversas. Insistió en que la imparcialidad, la formación jurídica, el conocimiento sectorial y las habilidades interpersonales son cualidades imprescindibles del DPD actual, que actúa también como mediador, formador y actor transversal en las políticas internas de protección de datos.

En la segunda parte de su intervención, centrada en la relación entre el DPD y el talento, Martínez trazó un mapa detallado del ciclo de vida del dato en la gestión laboral, desde la captación e incorporación de personal hasta la desvinculación. Argumentó que el DPD debe participar en el diseño de cláusulas contractuales, en la gestión de bajas, en la supervisión de herramientas de análisis de desempeño y en la revisión de accesos a cuentas corporativas.

Asimismo, reivindicó el papel del DPD en el fortalecimiento de la confianza organizativa, facilitando canales seguros para el tratamiento de incidentes, e impulsando la formación

continua en protección de datos como obligación empresarial, ya recogida en el artículo 4 del Reglamento de IA bajo el término de "alfabetización".

Alertó también sobre los sistemas de IA clasificados como de alto riesgo, especialmente aquellos que impactan en la selección de personal o la evaluación automatizada del desempeño, recordando que estos deben someterse a estrictas evaluaciones de impacto y procesos de gobernanza.

Finalmente, destacó que el DPD, aunque a menudo relegado a una función meramente técnica, debe ser comprendido como una figura estratégica imprescindible para la sostenibilidad legal y reputacional de las organizaciones. A través de ejemplos concretos, advirtió que la ausencia de una gestión adecuada de datos personales en contextos laborales puede derivar en conflictos internos, sanciones regulatorias o deterioro de la imagen de marca.

Ciberseguridad y protección de datos, por David López y Vitori Hernández

La última mesa de las IV Jornadas Aragonesas de Protección de Datos abordó el vínculo entre la ciberseguridad y la protección de datos. La sesión contó con la participación de David López, fundador de MADAC y director de Cibergob, y Vitori Hernández, destacada representante de Women4Cyber.

López presentó una intervención estructurada desde la experiencia acumulada a lo largo de varios años de trabajo en el desarrollo e implementación del Esquema Nacional de Seguridad (ENS), especialmente en administraciones públicas locales. Relató los desafíos iniciales para introducir el ENS en instituciones, donde era inexistente la conciencia sobre las obligaciones en materia de protección de datos. Mencionó el cambio normativo de 2021, momento en que las empresas proveedoras de servicios a la Administración pública pasaron a estar obligadas a cumplir el ENS.

Explicó que fue un punto de inflexión ya que supuso una expansión de la demanda del este servicio, abarcando desde microempresas hasta grandes corporaciones. En su valoración sobre el estado actual, López denunció que, pese a existir voluntad institucional, persisten múltiples

fricciones: falta de recursos, escasa capacitación técnica, resistencias internas y una visión deficiente sobre la seguridad como inversión estratégica. Subrayó que muchos responsables siguen tratando la ciberseguridad como un añadido posterior, en lugar de integrarla como condición de partida en el diseño de sistemas y servicios.

David López también abordó también el papel del usuario como eslabón débil del ecosistema digital. Criticó duramente la banalización del riesgo en el uso cotidiano de la tecnología, alertando sobre el desconocimiento generalizado que existe en torno a la trazabilidad digital y la cesión inconsciente de datos. Reivindicó la necesidad de comprender que la privacidad no es únicamente proteger lo que ya se ha entregado, sino también gobernar activamente lo que generamos como usuarios.

Finalmente puso valor en la necesidad de abordar la ciberseguridad desde una triple capa: tecnológica, humana y procedimental. Señaló que no basta con tener tecnología robusta ni con formar a los usuarios; es imprescindible también diseñar procesos seguros y sostenibles. De este modo, defendió que el cumplimiento normativo, lejos de ser una imposición burocrática, debe entenderse como una palanca para la mejora continua, la eficiencia y la transparencia en las organizaciones públicas y privadas.

A continuación, Vitori Hernández intervino situando el foco en la diversidad como condición indispensable para construir una ciberseguridad más justa, accesible y eficaz. Como profesional técnica en, explicó las barreras que ha debido superar como técnica en un entorno marcadamente masculinizado para emprender de lo suyo. Su relato se estructuró en torno a la experiencia directa con Women4Cyber, organización con la que ha colaborado estrechamente para generar programas de mentorización, formación y acompañamiento a mujeres emprendedoras.

Expuso con claridad las líneas de acción de estos programas, entre ellas, el combate al síndrome de la impostora, la creación de redes de apoyo y la generación de espacios de visibilidad. Compartió el impacto de su participación en la aceleradora de Google for Startups y cómo estas iniciativas han permitido consolidar empresas tecnológicas lideradas por mujeres, muchas de ellas desde entornos rurales o periféricos. Destacó la necesidad de contar con referentes cercanos y reales, que muestren que es posible liderar en tecnología sin renunciar a la autenticidad ni a la identidad personal.

Su intervención subrayó que la ciberseguridad no puede abordarse de forma plenamente eficaz si excluye a la mitad de la población. Aportar perspectivas diversas no es una cuestión ideológica, sino una necesidad estructural para que las soluciones de seguridad contemplen escenarios más completos, respuestas más creativas y mejores capacidades de adaptación frente a amenazas complejas y cambiantes; que defender y visibilizar el talento femenino no es solo una cuestión de justicia, sino también una estrategia de fortalecimiento del ecosistema profesional.

Coloriuris, Premio Aragón Privacidad 2025, firma de colaboración con Womans4Cyber y clausura del evento

La jornada concluyó con un acto de clausura en el que se hizo entrega del Premio Aragón Privacidad 2025. En esta edición, la distinción fue concedida a la empresa Coloriuris, en reconocimiento a su labor en el ámbito de la protección de datos y su apuesta por el desarrollo de soluciones jurídicas y tecnológicas orientadas a la soberanía digital.

El reconocimiento fue entregado por el presidente de Aragón Privacidad, Fernando Andreu Royo, quien destacó la coherencia del recorrido profesional de Coloriuris, su capacidad de adaptación a los desafíos normativos del entorno digital y su constante implicación en la defensa de los derechos fundamentales. Se firmó la colaboración con Womans4Cyber.

Editores

La elaboración, redacción y maquetación de esta memoria institucional ha sido llevada a cabo por D.ª Ana-Belén Lor Gallego y D. Rubén-Vasile Marcu Ungureanu, en el marco de la colaboración interna de la Asociación Aragón Privacidad para la documentación técnica y comunicativa de sus actividades. Ambos han trabajado con el objetivo de ofrecer un documento riguroso, estructurado y fiel al espíritu de las IV Jornadas Aragonesas de Protección de Datos, cuidando tanto la precisión del contenido como la claridad formal de su presentación.

IMAGEN DE LA CAMPAÑA DE DIFUSIÓN REALIZADA EL 28 DE ENERO DE 2025