



Cofinanciado por
la Unión Europea

MÓDULO 07

CIUDADANÍA DIGITAL

DIGITAL RURAL EUROPEAN ART
AND MEMORY



Socios del proyecto



Project DREAM
Digital Rural European Art and Memory
2025-1-SK01-KA210-ADU-000360122



Cofinanciado por
la Unión Europea

Información del proyecto:

DREAM - Digital Rural European Art and Memory
2025-1-SK01-KA210-ADU-000360122

Financiado por la Unión Europea. Sin embargo, las opiniones y posturas expresadas son responsabilidad exclusiva del/de los autor/es y no reflejan necesariamente las de la Unión Europea ni las de SAAIC. Ni la Unión Europea ni la entidad financiadora se hacen responsables de ellas.



Objetivos de aprendizaje

- Comprender la ciudadanía digital como acceso, seguridad, derechos y participación en comunidades tanto en línea como fuera de línea.
- Reconocer las dimensiones jurídica, social y práctica de la ciudadanía.
- Explicar por qué el acceso a un dispositivo o a una conexión a internet no conduce automáticamente a una inclusión digital significativa.
- Localizar sitios web, portales, avisos y puntos de contacto oficiales relacionados con los servicios públicos.
- Comprobar si la información pública está actualizada, es fiable y procede de la institución responsable.
- Aplicar la lectura lateral y la confirmación mediante dos fuentes al evaluar una página desconocida.
- Distinguir entre información desactualizada, información errónea, desinformación y estafas.
- Reconocer las señales de alerta habituales en mensajes que suplantan a una autoridad pública.
- Identificar las etapas de un procedimiento digital de un servicio público, incluidas las opciones de ayuda y las vías alternativas.
- Elaborar y revisar entre iguales una Ficha de recorrido de un servicio público.

Índice

0. Antes de empezar: mi punto de partida.....	3
1. ¿Qué es la ciudadanía digital?.....	4
2. Las tres dimensiones interrelacionadas de la ciudadanía digital	6
3. Acceso, inclusión y comunidades rurales	8
4. Derechos y principios digitales europeos	8
5. Servicios públicos digitales y recorrido del usuario por el servicio	10
6. Búsqueda de información pública oficial de la administración pública	12
7. Verificación de fuentes mediante lectura cruzada	13
8. Información obsoleta, información errónea, desinformación y estafas	14
9. Datos personales, verificación de identidad y acceso seguro	17
10. Ciudadanía digital y participación cultural	18
11. Actividad final: Ficha de procedimiento de un servicio público	19
12. Intercambio y evaluación mutua	24
13. Consejo para el bienestar digital	25
14. Glosario básico.....	26
15. Conclusión del módulo	28
Bibliografía	29

0. Antes de empezar: mi punto de partida

Antes de comenzar el módulo, evalúa cada afirmación en una escala del 1 al 5. Utiliza el **1** si aún no sabes realizar esa tarea y el **5** si eres capaz de llevarla a cabo por tu cuenta. No se trata de un examen. El objetivo es tomar conciencia de tu nivel de partida y, más adelante, reconocer tu propio progreso.

- Sé encontrar la página web oficial de un servicio público.
- Soy capaz de comprobar si la información de la administración pública está actualizada y es fiable.
- Entiendo cuándo y por qué un servicio requiere identificación digital.
- Soy capaz de detectar mensajes sospechosos que se hacen pasar por un organismo público.
- Soy capaz de explicar a otra persona los pasos principales de un trámite administrativo en línea.

Anota tus valoraciones. Volverás a estas afirmaciones al final del módulo.

1. ¿Qué es la ciudadanía digital?

La **ciudadanía** puede entenderse de varias formas interrelacionadas. Como condición jurídica, expresa la relación formal entre el individuo y el Estado, incluidos los derechos y obligaciones reconocidos. Como sentimiento de pertenencia, denota la relación con una comunidad, un lugar, una cultura o un espacio político común. Como actuación práctica, significa participar en la vida pública, colaborar con los demás, plantear preguntas, exigir responsabilidades a las instituciones y contribuir a la resolución de asuntos comunes.



Conceptos clave

La ciudadanía como condición jurídica: Relación formal entre una persona y un Estado, que incluye derechos y responsabilidades reconocidos.

La ciudadanía como pertenencia: Sentimiento de conexión con una comunidad, un lugar, una cultura o un espacio político compartido.

La ciudadanía como práctica: Participación en la vida pública mediante la cooperación, el planteamiento de preguntas, la rendición de cuentas y la contribución a asuntos de interés común.

Ciudadanía digital: Aplicación del acceso, los derechos, las responsabilidades, el criterio y la participación en los entornos digitales.

La **ciudadanía digital** traslada estos derechos, obligaciones y formas de participación al entorno digital. Representa la capacidad de participar de forma activa, constante y responsable en las comunidades, tanto en línea como fuera de línea, mediante un uso competente y positivo de las tecnologías digitales. El ciudadano digital no se limita a manejar un dispositivo. Es capaz de aprovechar las oportunidades, evaluar la información, proteger sus derechos, respetar a los demás y participar en la vida pública y comunitaria.

Por lo tanto, la ciudadanía digital no se limita únicamente a un comportamiento adecuado en Internet. También incluye la alfabetización informacional, el pensamiento crítico, la participación, la ética y la capacidad de oponerse a la exclusión o la manipulación. Este concepto aúna las habilidades prácticas con el criterio y la responsabilidad. Una persona puede

saber cómo navegar por una página web, pero aun así puede necesitar ayuda para evaluar si la página es oficial, si una solicitud es razonable o si un servicio es accesible y justo (Consejo de Europa, 2019, 2025; Richardson y Milovidov, 2022; Comisión Europea, Centro Común de Investigación, 2025).



Reflexión

Piensa en una acción digital reciente relacionada con la vida pública o comunitaria. Puede haber consistido en buscar información, solicitar una cita, ponerse en contacto con un ayuntamiento, leer un aviso público, participar en una consulta o ayudar a otra persona a completar un formulario en línea.

¿Qué dimensión de la ciudadanía estuvo presente: la condición jurídica, el sentido de pertenencia, la participación práctica o más de una de ellas?

2. Las tres dimensiones interrelacionadas de la ciudadanía digital

El Consejo de Europa (2019) describe la ciudadanía digital a través de tres dimensiones interrelacionadas: estar en línea, el bienestar en línea y los derechos en línea. Estas dimensiones se solapan entre sí. Las personas necesitan acceso y competencias, pero también seguridad, respeto, privacidad y oportunidades significativas para participar.

Estar en línea: esta dimensión abarca el acceso, la inclusión, la educación, la creatividad y la alfabetización mediática. En la vida pública cotidiana, esto puede significar, por ejemplo, encontrar el portal oficial adecuado y comprender la información que en él se ofrece.

Bienestar en línea: Esta dimensión abarca la seguridad, la salud, la empatía y el uso responsable de las tecnologías. Puede significar resistirse a la presión, reconocer los engaños, limitar el intercambio innecesario de datos personales y pedir ayuda cuando un procedimiento resulte demasiado complicado.

Derechos en línea: Esta dimensión abarca la participación, la protección de la privacidad, la concienciación del consumidor y los derechos democráticos. Puede significar utilizar un servicio público, aportar comentarios, participar en una consulta pública o solicitar información a una institución.

Estas dimensiones ponen de manifiesto por qué la ciudadanía digital tiene una vertiente tanto personal como social. El individuo necesita confianza en sí mismo y competencias, mientras que las instituciones deben proporcionar servicios comprensibles, seguros y accesibles. Las comunidades también desempeñan un papel importante, ya que las personas comparten conocimientos, se ayudan mutuamente y señalan los obstáculos que es necesario eliminar.



Tarea práctica

Elige una acción relacionada con un servicio público digital, como solicitar una cita o buscar información sobre un programa cultural. Escribe un ejemplo de lo que la persona necesita en cada una de estas dimensiones: estar en línea, bienestar en línea y derechos en línea. Identifica cuál de estas dimensiones tiene más probabilidades de generar una barrera.

3. Acceso, inclusión y comunidades rurales

La ciudadanía digital abarca el acceso, la capacidad de evaluar la información y de actuar. Una persona puede tener un smartphone y conexión a Internet, pero aun así puede verse excluida si el servicio es difícil de entender, requiere un método de identificación desconocido, utiliza un lenguaje complejo o no ofrece la posibilidad de recibir asistencia humana. Por lo tanto, la inclusión digital tiene varios niveles: el acceso a las tecnologías, las competencias necesarias para utilizarlas y la capacidad de lograr un resultado significativo (Correa y Pavez, 2016; Morte-Nadal y Esteban-Navarro, 2025).

Los servicios públicos digitales pueden resultar extremadamente beneficiosos para las comunidades rurales, ya que pueden reducir la necesidad de desplazarse, acortar los tiempos de espera y limitar la dependencia de los horarios de atención al público de las oficinas. Sin embargo, al mismo tiempo, una conexión a Internet lenta, el acceso únicamente a través del teléfono móvil, el transporte limitado, los sistemas desconocidos y la falta de puntos de contacto locales pueden dificultar el uso de estos servicios. La confianza en uno mismo, la confianza en el servicio, una información clara y la posibilidad de pedir ayuda a alguien influyen de manera significativa en que una persona complete un trámite o lo abandone.



Tarea práctica

Imagina que una persona residente necesita utilizar un servicio en línea, pero solo dispone de un teléfono móvil y de una conexión inestable. Identifica una barrera relacionada con el acceso, otra relacionada con las competencias digitales y otra vinculada a la obtención del resultado final. Para cada barrera, propone una forma de apoyo que proteja la autonomía y la privacidad de la persona.

4. Derechos y principios digitales europeos

El enfoque europeo de la transformación digital se centra en las personas. Las tecnologías deben estar al servicio de las personas, reforzar su participación en la vida social y respetar en línea los mismos derechos que se aplican fuera de línea. *La Declaración europea sobre derechos y principios digitales* marca el rumbo común hacia una transformación digital justa, segura e inclusiva.



Conceptos clave

- Las personas y sus derechos deben ocupar un lugar central en la transformación digital.
- Nadie debe quedarse atrás.
- Todas las personas deben poder adquirir las competencias necesarias para participar.
- Todas las personas deben tener acceso a servicios públicos digitales esenciales.
- Los espacios digitales deben favorecer la toma de decisiones informadas, la participación, la seguridad y la sostenibilidad.

Estos principios también son importantes a la hora de evaluar los servicios públicos. Un servicio puede ser técnicamente accesible, pero, aun así, puede excluir a algunas personas debido a un lenguaje incomprensible, procedimientos poco claros, un diseño inadecuado para dispositivos móviles o la falta de asistencia. Por lo tanto, los derechos digitales no solo se refieren a la protección frente a los perjuicios, sino también a la posibilidad real de implicarse y participar en la vida pública (Parlamento Europeo, Consejo de la Unión Europea y Comisión Europea, 2023; Comisión Europea, 2026a).



Reflexión

Elige un servicio digital que conozcas. ¿Qué principio aplica adecuadamente? ¿Qué principio podría reforzarse?

Basa tu respuesta en una característica concreta, como la accesibilidad, la claridad de las instrucciones, la información sobre privacidad, la asistencia humana o una alternativa no digital.

5. Servicios públicos digitales y recorrido del usuario por el servicio

Los servicios públicos digitales permiten a las personas obtener información, presentar solicitudes, concertar citas, remitir la documentación necesaria, recibir resoluciones o comunicarse con las instituciones públicas en línea. El programa «*Década Digital de la UE*» considera los servicios públicos digitales como uno de los cuatro ámbitos principales de la transformación digital de Europa (Parlamento Europeo y Consejo de la Unión Europea, 2022; Comisión Europea, 2026b).

Un servicio público debe entenderse como un recorrido integral del usuario, y no solo como una página web. El usuario debe, en primer lugar, encontrar la forma correcta de acceder al servicio; a continuación, comprender su finalidad; preparar los datos y documentos necesarios; verificar su identidad de forma segura; realizar la gestión necesaria; confirmar que su solicitud ha sido recibida; y saber dónde puede obtener ayuda en caso de necesidad. Un proceso comprensible abarca todas estas fases.



Conceptos clave

Encontrar: ¿Dónde está la información oficial o el portal oficial?

Comprender: ¿Quién puede utilizar el servicio y qué resultado ofrece?

Preparar: ¿Qué documentos, datos, tasas y plazos se requieren?

Autenticarse: ¿Se requiere una identidad digital, contraseña, código o firma electrónica?

Actuar: ¿Qué formulario, carga de documentos, cita, pago u otra acción se debe realizar?

Confirmar: ¿Cómo sabrá la persona usuaria que la acción ha sido recibida o completada?

Obtener ayuda: ¿Dónde puede la persona usuaria hacer una consulta, corregir un error, presentar una reclamación o utilizar otro canal?

Este recorrido ofrece una estructura práctica para analizar casi cualquier procedimiento digital de la administración pública, incluso en los casos en que los portales nacionales y los sistemas de identificación digital difieran de un país a otro (Parlamento Europeo y Consejo de la Unión Europea, 2018; Morte-Nadal y Esteban-Navarro, 2025).



Tarea práctica

Elige un servicio público que conozcas y describe su recorrido utilizando las siete etapas anteriores. No es necesario crear una cuenta ni enviar ninguna solicitud.

Indica qué etapa te resulta más fácil de comprender y cuál sería la más difícil de explicar a otra persona.

6. Búsqueda de información pública oficial de la administración pública

Los motores de búsqueda en Internet, las publicaciones en redes sociales, los artículos periodísticos y las páginas de asesoramiento privadas pueden ayudarte a orientarte sobre un tema concreto. Sin embargo, no deben sustituir a la información publicada por la institución responsable de dicho servicio. Además, los resúmenes generados automáticamente en los resultados de búsqueda pueden omitir contexto importante, mostrar datos obsoletos o dar prioridad a páginas no oficiales frente a las fuentes oficiales.

La información pública oficial suele incluir la información publicada por la institución pública responsable; un portal nacional, regional, municipal o europeo al que dicha institución remita; un anuncio oficial completo, una ley, un formulario, un procedimiento o una directriz; o un servicio de asistencia o punto de contacto autorizado (Parlamento Europeo y Consejo de la Unión Europea, 2018; Comisión Europea, Centro Común de Investigación, 2025).



Conceptos clave

La cuestión principal no es simplemente: *“¿Esta página parece oficial?”*

La pregunta más adecuada es: *“¿Quién es responsable de este servicio y puedo confirmar que esta página pertenece a esa institución o está autorizada por ella?”*

Este cambio de enfoque, de la apariencia a la responsabilidad, es esencial porque los diseños, los logotipos y los colores familiares pueden copiarse.

7. Verificación de fuentes mediante lectura cruzada

Una página web de aspecto profesional no tiene por qué ser automáticamente fiable. Los dominios de las instituciones públicas varían de un país a otro, por lo que no existe una única extensión, como por ejemplo .gov, que demuestre de forma fiable en todas partes que la página es oficial. La verificación requiere varios pasos: identificar la institución mencionada en la página, comprobar la dirección web completa, buscar la información de contacto y los datos legales, y confirmar que dicha institución es realmente la responsable de prestar el servicio (McGrew, 2024; Moore y Hancock, 2022; Comisión Europea, Centro Común de Investigación, 2025).

Los verificadores de datos profesionales suelen utilizar un método denominado **lectura lateral**. En lugar de quedarse en una página desconocida y evaluar únicamente su aspecto o su redacción, abren una nueva pestaña y buscan información sobre la fuente, la organización o la afirmación en cuestión. Buscan la página web oficial de la institución o su información legal, comprueban si alguna otra fuente pública fiable hace referencia a dicho servicio y no vuelven a la página original hasta haber confirmado quién está detrás de ella (Brodsky et al., 2021; McGrew, 2024).

La lectura cruzada resulta útil, ya que una página web puede presentar por sí misma información convincente, pero no verificada. La confirmación independiente es más fiable. La segunda fuente oficial puede ser otro portal de la administración pública, la página de inicio de la institución en cuestión, su página de contacto oficial, un servicio de asistencia autorizado o un anuncio publicado que haga referencia al mismo procedimiento.

Procedimiento sencillo de verificación

1. Indica el nombre de la institución que debería ser responsable del servicio.
2. Compruebe la dirección web completa, no solo el nombre de la página.
3. Abre una nueva pestaña y busca por separado dicha institución.
4. Busque su página de inicio oficial, su página de contacto o la información legal.
5. Confirma el servicio a través de una segunda fuente oficial o punto de contacto.
6. Vuelve a la página original solo después de haber verificado la fuente.

8. Información obsoleta, información errónea, desinformación y estafas

Al utilizar servicios públicos digitales, encontrar información en línea es solo el primer paso. También es necesario decidir si la información está **actualizada, es precisa y fiable**. Una página puede tener un aspecto profesional y, aun así, contener información desactualizada, mientras que un mensaje que parece proceder de una institución oficial puede haber sido creado en realidad para engañarte. No toda la información incorrecta o perjudicial es igual. Comprender el tipo de problema te ayuda a decidir qué debes comprobar y cómo responder.



Conceptos clave

Información desactualizada: La fuente puede haber sido correcta en su momento, pero una fecha, un formulario, una tasa o un plazo ha cambiado. La respuesta adecuada es buscar la versión oficial vigente.

Información errónea: Puede compartirse información falsa o engañosa sin intención de engañar. Verifícala antes de actuar basándote en ella o de compartirla.

Desinformación: La información falsa o manipulada se crea o difunde deliberadamente. Comprueba las pruebas y denúnciala cuando corresponda.

Estafa o suplantación de identidad: Una persona se hace pasar por una autoridad para obtener dinero, credenciales o datos personales. Detente, no hagas clic ni pagues, y ponte en contacto con la autoridad a través de una vía oficial verificada e independiente.

Estos problemas a veces pueden **solaparse**. Un mensaje fraudulento puede contener desinformación, hacerse pasar por una institución pública y dirigir al usuario a un sitio web falso. Por eso es importante comprobar no solo lo que dice un mensaje, sino también quién lo ha enviado, adónde dirige el enlace y qué te pide que hagas.

Figura 1

Ejemplo de correo electrónico de phishing bancario

From: authenticationmail@trust.ameribank7.com
To: johnsmith@email.com
Subject: **A new login to your bank account**



Bank of America

Dear account holder,

There has been a recent login to your bank account from a new device:

IP address: 192.168.0.1

Location: Miami, Florida

4 new transactions have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

<https://trust.ameribank7.com/reset-password>

Thank you,

Bank America

Nota. De Example bank phishing email [Vector graphic], por Isochrone y Belbury, 2025, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Example_bank_phishing_email.svg). CC BY 4.0.

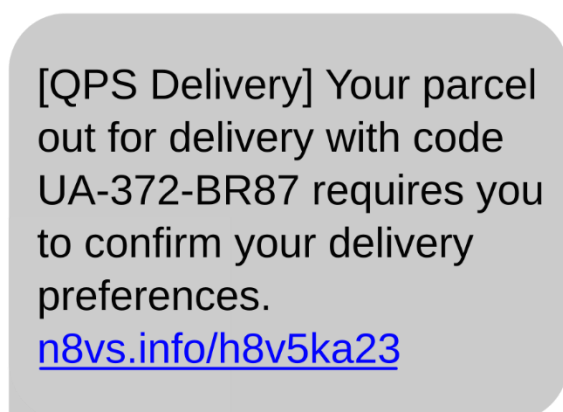
Las estafas relacionadas con los servicios públicos suelen generar presión para que la persona destinataria actúe antes de comprobar la información. Pueden copiar logotipos oficiales, utilizar un nombre de remitente similar al de una institución real o afirmar que una prestación, una multa, una cuenta o un documento están en riesgo inmediato.

Señales de alerta habituales

- Presión temporal inesperada, por ejemplo, la exigencia de actuar de inmediato so pena de perder una prestación u otra ventaja.
- Solicitud de contraseñas, códigos de acceso completo o control remoto de un dispositivo.
- Solicitud de pago mediante tarjetas regalo, criptomonedas o una cuenta privada inusual.
- Una dirección web abreviada, mal escrita o que no guarda relación con el servicio en cuestión.
- Un mensaje que pida al usuario que inicie sesión a través de un enlace en lugar de hacerlo en el portal oficial.
- Nombre del remitente que no coincide con la dirección de correo electrónico o el número de teléfono.
- Una amenaza o una indicación que disuada al usuario de verificar la información directamente con la institución correspondiente.

Figura 2

Ejemplo de SMS de phishing



Nota. Imagen que muestra un ejemplo ficticio de un mensaje SMS de phishing sobre la entrega de un paquete. De Example phishing SMS [gráfico vectorial], por Belbury, 2025, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Example_phishing_SMS.svg). CC0 1.0.

9. Datos personales, verificación de identidad y acceso seguro

Los datos personales son información que identifica a una persona concreta o que puede vincularse a dicha persona. Entre ellos se incluyen, por ejemplo, el nombre, el número de identificación, la dirección, la fotografía, los datos de localización o la información de la cuenta. Según el RGPD, los datos personales deben recopilarse con una finalidad claramente definida y su alcance debe limitarse únicamente a los datos necesarios para dicha finalidad (Parlamento Europeo y Consejo de la Unión Europea, 2016).

Cuando un servicio público solicite información, lee por qué se solicitan los datos y quién los recibirá. Relaciona cada dato solicitado con la finalidad del servicio. Evita enviar documentos de identidad a través de mensajes no oficiales o por correo electrónico. Nunca reutilices ni compartas códigos de autenticación. Los mensajes de confirmación y los certificados oficiales pueden ser importantes, pero deben guardarse de forma segura.

Normas de seguridad

- Acceda al portal oficial del servicio, no a un enlace incluido en un mensaje no esperado.
- Comprueba qué método de identificación acepta oficialmente el portal.
- Si es posible, utiliza tu propio dispositivo y cierra la sesión cuando hayas terminado.
- Nunca revele a otra persona su contraseña, su código PIN ni el código de un solo uso completo.
- No permitas que una persona desconocida te guíe durante el proceso de verificación de identidad.
- Si el procedimiento no te queda claro, solicita asistencia al servicio oficial.

10. Ciudadanía digital y participación cultural

La ciudadanía digital también incluye la participación en la vida cultural. *La Convención de Faro* vincula el patrimonio cultural con la participación, la responsabilidad compartida y la vida democrática. El patrimonio cultural no es solo algo que las instituciones protegen en nombre de los ciudadanos. Las personas pueden aportar sus conocimientos, señalar problemas, participar en la toma de decisiones y contribuir a definir la forma en que se interpretan y presentan los lugares, las tradiciones y los recuerdos locales (Consejo de Europa, 2005, 2019).

Las herramientas digitales pueden ayudar a los ciudadanos a acceder a información cultural, comunicarse con las instituciones y contribuir a las decisiones sobre el patrimonio local. El ciudadano digital puede utilizar herramientas oficiales para solicitar acceso a un archivo, informar de daños en un monumento, inscribirse en un programa cultural, plantear una pregunta, participar en una consulta pública o ponerse en contacto con la institución responsable del patrimonio.



Tarea práctica

Identifica un lugar, una tradición, una colección, un evento o una cuestión de interés para la comunidad local que pueda implicar a una institución pública. ¿Qué información o servicio podría necesitar una persona residente? Indica cuál sería probablemente la institución responsable y qué resultado práctico querría conseguir la persona.

11. Actividad final: Ficha de procedimiento de un servicio público

En parejas o pequeños grupos, preparad un procedimiento claro para utilizar un servicio público real. El servicio elegido debería estar relacionado, a ser posible, con el patrimonio cultural local o la vida comunitaria. Dado que los portales públicos y los sistemas de identificación digital varían de un país a otro, el formador puede proporcionar ejemplos nacionales o locales adecuados.



Posibles escenarios de servicios



Ejemplos relacionados con el patrimonio o la comunidad

pueden incluir

- informar de daños en un monumento o lugar de patrimonio público
- solicitar acceso a un archivo municipal o regional
- inscribirse en un programa cultural municipal
- encontrar una consulta pública sobre el desarrollo local o el patrimonio
- encontrar el procedimiento oficial para utilizar un espacio público para una actividad cultural comunitaria



Alternativas cotidianas

pueden incluir

- reservar una cita oficial
- obtener un certificado o documento oficial
- buscar información sobre empleo o ayudas sociales
- presentar una consulta o reclamación ante una autoridad
- modificar o corregir información en un registro público

Recuerda: *el resultado no debe ser una solicitud cumplimentada y no debe contener datos personales reales. Debe tratarse de una guía práctica que muestre cómo se puede encontrar, verificar y comprender el procedimiento oficial. Finaliza la actividad antes de enviar realmente la solicitud, realizar el pago o verificar la identidad.*

Hoja de trabajo sobre la ficha del procedimiento

Servicio y finalidad: qué permite el servicio y por qué una persona puede necesitarlo.

Institución responsable: Órgano o institución que gestiona dicho servicio.

Fuente oficial verificada: Portal o documento oficial y la forma en que se ha confirmado su fiabilidad.

Requisitos y preparación: quién puede utilizar el servicio, qué documentos son necesarios y qué tasas o plazos se aplican.

Pasos: Breve procedimiento numerado desde la página de inicio hasta la confirmación de la recepción.

Identificación digital: Información sobre si se requiere iniciar sesión, una identidad electrónica, una firma electrónica u otro método de verificación de la identidad.

Privacidad y seguridad: Datos personales requeridos, recordatorio de las normas de inicio de sesión seguro y una advertencia relevante sobre un posible fraude.

Ayuda y alternativas: Datos de contacto oficiales, asistencia disponible, medidas para garantizar la accesibilidad o la posibilidad de gestionar el servicio en persona.

Vínculo con la participación: La forma en que el servicio fomenta la participación comunitaria o cultural.

Paso 1: Define la necesidad del servicio

Complete la frase: „Una persona de nuestra comunidad necesita _____, porque _____“.

Indica una persona o grupo concreto, elige un servicio específico y explica el resultado práctico que necesita esa persona. Una necesidad claramente definida facilita la verificación y la explicación de todo el proceso.

Paso 2: Busca el procedimiento oficial

1. Busque el nombre del servicio junto con el nombre del municipio, ciudad, región, ministerio o institución de la UE responsable.
2. Abre el resultado que, según los datos disponibles, corresponde a la institución responsable.
3. Compruebe la dirección web completa.
4. Busque la página de inicio de la institución, la página de contacto o la información legal.
5. Confirme la veracidad del procedimiento mediante una segunda fuente oficial.

Paso 3: Realice la verificación de cinco puntos

La verificación en cinco puntos combina la comprobación de la fuente, la evaluación de la actualidad de la información, la comprobación de los datos personales solicitados y la confirmación independiente de la veracidad del procedimiento.

Organismo responsable: Indique la institución pública, el organismo o la organización designada que se encarga del servicio.

Dirección web oficial: Copie o anote la dirección web completa. Compruebe que el dominio pertenezca a la institución responsable o a un portal autorizado de servicios públicos.

Información actualizada: Anote la fecha de publicación, la fecha de actualización, la versión, la fecha límite vigente u otro dato que indique que la información sigue siendo válida.

Solicitud de datos correspondiente: Anote qué datos personales le solicita el servicio. Valore si la información solicitada es necesaria y adecuada para la finalidad indicada.

Confirmación independiente: Indique una segunda fuente oficial o punto de contacto que confirme que se trata de la vía correcta para acceder al servicio.

La lista de verificación de cinco puntos combina la verificación de la fuente, la evaluación de la actualidad de la información, el conocimiento de las solicitudes de datos personales y la confirmación independiente.

Paso 4: Describa el procedimiento

Anote el procedimiento en forma de pasos breves y numerados. Comience antes de iniciar sesión y termine antes de enviar la solicitud.

1. Abre la página web oficial del servicio.
2. Comprueba la legitimidad y la finalidad del servicio.
3. Prepara los documentos o la información necesarios.
4. Elige el método de identificación o acceso adecuado.
5. Rellene el formulario, envíelo, concierte una cita o realice cualquier otra gestión.
6. Comprueba las tasas, los plazos y el tiempo estimado de tramitación.
7. Guarde el número de confirmación o de referencia.
8. Si surge algún problema, recurre a la ayuda oficial.

La ficha debería describir todo el proceso, incluyendo la confirmación y la asistencia, y no solo la primera página del servicio.

Paso 5: Identifica el método de verificación digital y los datos personales requeridos

Requisito de inicio de sesión: Anota si no se requiere iniciar sesión, si solo se requiere para enviar la solicitud o si se requiere desde el principio.

Método de verificación: Anote los métodos aceptados, como el DNI electrónico, el monedero digital, la aplicación móvil, la contraseña, el código, la firma electrónica u otros métodos.

Datos personales requeridos: Indique únicamente las categorías de datos, nunca los datos reales de los participantes.

Finalidad de los datos: Relacione cada categoría de datos con la finalidad del servicio.

Información que no debe compartirse: Incluya contraseñas, códigos PIN, códigos de un solo uso completos y documentos que no estén relacionados con el servicio en cuestión.

Paso 6: Busca ayuda, disponibilidad y alternativas

El procedimiento completo también incluye información sobre qué hacer cuando el proceso digital ideal no funciona. Busca:

- el número de teléfono oficial o la dirección de correo electrónico
- la posibilidad de acudir a una oficina física o de concertar una cita
- un servicio digital asistido o un punto de contacto autorizado
- el procedimiento para corregir un error, presentar una reclamación o interponer un recurso

12. Intercambio y evaluación mutua

Intercambiad la ficha de procedimiento con otra pareja o grupo. Los evaluadores deben examinar primero la ficha sin que los autores la expliquen. De este modo se simula la situación en la que un miembro de la comunidad consulta las instrucciones por su cuenta.

Preguntas para la evaluación entre compañeros

- ¿Sabemos identificar el servicio y la institución responsable?
- ¿Son los pasos completos y están ordenados de forma lógica?
- ¿Se explica el método de verificación de la identidad de forma segura y comprensible?
- ¿Se indican claramente los documentos necesarios, las tasas y los plazos?
- ¿Podemos encontrar ayuda o una forma alternativa de tramitar el servicio?
- ¿Es relevante la advertencia de seguridad?



Reflexión

¿Qué parte del proceso fue más fácil de explicar? ¿Qué cambio hizo que la ficha fuera más segura, clara o inclusiva?

13. Consejo para el bienestar digital



Consejo de bienestar digital

Una pantalla, una tarea

El aprendizaje digital puede resultar agotador cuando demasiadas pestañas, mensajes y herramientas compiten por nuestra atención. Centrarse en una sola tarea visible hace que el aprendizaje sea más tranquilo y manejable.

Pruébalo: Durante el próximo periodo breve de trabajo, cierra o minimiza todo lo que no necesites. Mantén abierta únicamente la tarea, plantilla, archivo o página web que estés utilizando en ese momento.

Pregunta de reflexión: ¿Cuál es la única acción digital que necesito completar ahora?

Este hábito resulta especialmente útil durante los trámites con la administración pública, donde las distracciones pueden hacer que se pasen por alto instrucciones, se comparta información por error o queden pasos sin completar.

14. Glosario básico

Accesibilidad: Diseño de información, servicios y herramientas para que puedan utilizarlos personas con diferentes necesidades y capacidades.

Acceso digital asistido: Apoyo oficial que ayuda a una persona a utilizar un servicio digital sin que se le prive del control ni de la privacidad.

Verificación de identidad: Proceso utilizado para confirmar que una persona está autorizada a acceder a una cuenta o a un servicio.

Ciudadanía digital: Participación activa, continua y responsable en comunidades en línea y fuera de línea mediante el uso competente de las tecnologías digitales.

Identidad digital: forma o conjunto de datos que se utilizan para acreditar la identidad en el entorno digital.

Inclusión digital: Capacidad para acceder a las tecnologías, utilizarlas con las habilidades adecuadas y lograr un resultado significativo.

Desinformación: Información falsa o manipulada, creada o difundida deliberadamente con el objetivo de engañar.

Firma electrónica: Método digital para firmar o autorizar un documento o un acto.

RGPD: Reglamento General de Protección de Datos de la UE, que establece las normas para el tratamiento y la protección de los datos personales.

Lectura transversal: Abandonar una página web desconocida y consultar fuentes independientes con el fin de averiguar quién está detrás de la página y si sus afirmaciones son fiables.

Desinformación: Información falsa o engañosa que se difunde sin la intención deliberada de engañar a nadie.

Fuente oficial: Información publicada o aprobada por una institución pública responsable de un servicio concreto.

Datos personales: Información que identifica a una persona concreta o que puede vincularse a dicha persona.

Servicio público: Información, asistencia o procedimiento prestado por una institución pública, como, por ejemplo, reuniones, documentos, solicitudes o consultas.

Fraude o suplantación de identidad: intento de hacerse pasar **por** una persona o institución de confianza con el fin de obtener dinero, datos de acceso o datos personales.

Verificación mediante dos fuentes: Verificación de un procedimiento o una afirmación mediante una segunda fuente oficial independiente o un punto de contacto.

Guía de procedimientos de la administración pública: Instrucciones claras que recogen la fuente oficial, los pasos concretos del procedimiento, las advertencias de seguridad, las opciones de ayuda y las formas alternativas de utilizar los servicios públicos.

15. Conclusión del módulo

La ciudadanía digital es la capacidad de participar en la vida pública digital con el acceso necesario, el criterio adecuado, el énfasis en la seguridad y la conciencia de los propios derechos. No se trata únicamente de una competencia individual. También depende de una comunicación clara por parte de las instituciones, de servicios accesibles y de comunidades en las que las personas puedan solicitar ayuda sin perder el control sobre su información privada.

Al finalizar este módulo, deberías ser capaz de buscar y verificar información oficial de la administración pública, explicar las distintas fases del proceso de uso de un servicio público, proteger los datos personales, identificar los riesgos habituales y elaborar una guía que pueda seguir otra persona. La ficha de procedimiento de la administración pública muestra no solo lo que sabes, sino también cómo tus conocimientos pueden fomentar la participación de las personas en la vida de la comunidad.

Bibliografia

- Belbury. (2025). Example phishing SMS [Vector graphic]. Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Example_phishing_SMS.svg
- Brodsky, J. E., Brooks, P. J., Scimeca, D., Todorova, R., Galati, P., Batson, M., ... & Caulfield, M. (2021). Improving college students' fact-checking strategies through lateral reading instruction in a general education civics course. *Cognitive research: principles and implications*, 6(1), 23. <https://doi.org/10.1186/s41235-021-00291-4>
- Correa, T., & Pavez, I. (2016). Digital inclusion in rural areas: A qualitative exploration of challenges faced by people from isolated communities. *Journal of Computer-Mediated Communication*, 21(3), 247-263. <https://doi.org/10.1111/jcc4.12184>
- Council of Europe. (2005). *Council of Europe Framework Convention on the Value of Cultural Heritage for Society* (CETS No. 199). <https://www.coe.int/en/web/culture-and-heritage/faro-convention>
- Council of Europe. (2019). *Digital citizenship education handbook*. Council of Europe Publishing. <https://book.coe.int/en/human-rights-democratic-citizenship-and-interculturalism/7851-digital-citizenship-education-handbook.html>
- Council of Europe. (2025). *Digital citizenship education*. <https://www.coe.int/en/web/education/digital-citizenship-education>
- Council of Europe. (2026). *Implementation of Recommendation CM/Rec(2019)10 on developing and promoting digital citizenship education: State of play*. Council of Europe Publishing.
- European Commission. (2022). *European Declaration on Digital Rights and Principles*. <https://digital-strategy.ec.europa.eu/en/policies/digital-principles>
- European Commission. (2026a). *European Digital Rights and Principles*. <https://digital-strategy.ec.europa.eu/en/policies/digital-principles>
- European Commission. (2026b). *Europe's Digital Decade*. <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>

- European Commission. (2026c). *European Digital Identity*.
https://commission.europa.eu/topics/digital-economy-and-society/european-digital-identity_en
- European Commission, Joint Research Centre. (2025). DigComp 3.0: The Digital Competence Framework for Citizens. https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-digcomp/digcomp-30_en
- European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union, L 119, 1–88.
- European Parliament and Council of the European Union. (2018). Regulation (EU) 2018/1724 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services. Official Journal of the European Union, L 295, 1–38.
- European Parliament and Council of the European Union. (2022). Decision (EU) 2022/2481 establishing the Digital Decade Policy Programme 2030. Official Journal of the European Union, L 323, 4–26.
- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union, L 2024/1183.
- European Parliament, Council of the European Union, & European Commission. (2023). European Declaration on Digital Rights and Principles for the Digital Decade. Official Journal of the European Union, C 23, 1–7.
- Isochrone, & Belbury. (2025). Example bank phishing email [Vector graphic]. Wikimedia Commons.
https://commons.wikimedia.org/wiki/File:Example_bank_phishing_email.svg
- Jurišić, I., & Bogataj, D. (2024). Enhancing digital government engagement among older adults: Literature review and research agenda. *IFAC-PapersOnLine*, 58(3), 256-261.
<https://doi.org/10.1016/j.ifacol.2024.07.160>

- Lee-Geiller, S. (2024). The moderating effect of digital literacy on the link between e-government effectiveness and trust in government. *Journal of Policy Studies*, 39(4), 77-101. <https://doi.org/10.52372/jps.e672>
- McGrew, S. (2024). Teaching lateral reading: Interventions to help people read like fact checkers. *Current Opinion in Psychology*, 55, 101737. <https://doi.org/10.1016/j.copsyc.2023.101737>
- Moore, R. C., & Hancock, J. T. (2022). A digital media literacy intervention for older adults improves resilience to fake news. *Scientific reports*, 12(1), 6008. <https://doi.org/10.1038/s41598-022-08437-0>
- Morte-Nadal, T., & Esteban-Navarro, M. Á. (2025). Recommendations for digital inclusion in the use of European digital public services. *Humanities and Social Sciences Communications*, 12(1), 273. <https://doi.org/10.1057/s41599-025-04576-7>