

Reto Rural digital

Actualización Octubre/2025

DigiEmprende

Guía del Alumnado

Muévete con seguridad. Resuelve problemas en Entornos Digitales

LABURO, Soc. Coop. Mad.

Calle de la Alameda, 22

28014 Madrid (Madrid)

+34 91 954 19 64 +34 604 51 89 59

administracion@laburo.es

1. INTRODUCCIÓN

Queremos darle la bienvenida a esta experiencia formativa, esperando que sea una oportunidad de aprendizaje para ampliar sus habilidades digitales y mejorar su vida cotidiana.

Muévete con seguridad. Resuelve problemas en entornos digitales, forma parte del Programa "Reto Rural Digital" para proyectos de capacitación digital en el marco del Plan de Recuperación, Transformación y Resiliencia que subvenciona el Ministerio de Transición ecológica y el Reto Demográfico con el compromiso de reducir la brecha digital.

Este curso tiene como fin ofrecer a las personas emprendedoras, autónomas y desempleadas herramientas para mejorar el uso crítico, responsable y creativo de las tecnologías, fundamental para aprovechar las oportunidades que nos brindan los avances tecnológicos.

Además, el curso integra contenidos transversales de igualdad, promoviendo una mirada inclusiva y equitativa sobre el uso y acceso a la tecnología, y favoreciendo actitudes de respeto, corresponsabilidad y cooperación en el ámbito digital.

La competencia digital implica usar tecnologías digitales de forma eficaz y segura, ampliar los conocimientos con la búsqueda de información, la comunicación y la colaboración, un uso responsable de servicios digitales y la resolución de problemas técnicos todo ello desde una perspectiva de igualdad, respeto y bienestar digital.

Cada participante, con el apoyo de la orientación y acompañamiento que ofrecerá el equipo docente, identificará y aplicará prácticas útiles para el uso seguro de las herramientas digitales y la solución a problemas técnicos que se le puedan presentar.

2. OBJETIVOS

Proteger los dispositivos.

Proteger los datos personales y la privacidad.

Proteger la salud y el bienestar.

Resolver problemas técnicos.

Identificar necesidades y respuestas tecnológicas a esas necesidades.

Identificar áreas de mejora en las propias competencias digitales.

3. CONTENIDOS Y APRENDIZAJES

3.1. Protección y privacidad en los dispositivos y aplicaciones

3.1.1. Contenidos

Configuración de opciones de privacidad en móviles.

Cómo evitar compartir información personal inadvertidamente.

Medidas básicas para proteger los dispositivos y aplicaciones (contraseñas, actualizaciones).

Contraseñas seguras y autenticación en dos pasos.

Protección contra phishing y malware.

Políticas de privacidad y tratamiento de datos personales en páginas web, listas de distribución o redes sociales.

3.1.2. Aprendizajes

Ajustar la configuración de privacidad en su dispositivo y aplicaciones. como por ejemplo, un patrón o PIN seguro para bloquear el móvil.

Crear contraseñas seguras y diferentes para el correo, la banca online y las redes sociales.

Actualizar periódicamente las aplicaciones y el sistema para mantener la seguridad del dispositivo.

Comprobar que su antivirus o la protección básica del dispositivo está activa.

Comprender que aceptar una política de privacidad significa autorizar el uso de sus datos personales.

Revisar y ajustar la configuración de privacidad en Redes sociales como Facebook o LinkedIn para mostrar solo la información adecuada.

Limitar las cookies en el navegador para reducir el seguimiento de su actividad en internet.

Distinguir un correo legítimo de uno fraudulento o de phishing.

Identificar un intento de phishing que suplanta a una empresa de empleo o a una plataforma de pago.

3.2. Seguridad en la comunicación y la navegación

3.2.1. Contenidos

- Reconocimiento y bloqueo de spam o mensajes molestos.
- Principales tipos de estafas y fraudes en Internet: ejemplos reales.
- Precauciones al realizar compras en línea: métodos de pago seguros y webs fiables.

3.2.2. Aprendizajes

- Bloquear correos o contactos sospechosos.
- Detectar páginas web inseguras antes de comprar o registrarse.
- Aprender a denunciar o reportar un intento de fraude.
- Analizar ejemplos de estafas reales para aprender a reconocerlas.
- Evitar abrir enlaces sospechosos en mensajes que ofrecen empleos o productos demasiado atractivos.

3.3. Proteger la salud y el bienestar

3.3.1. Contenidos

- Concienciación sobre el impacto del uso excesivo de dispositivos digitales.
- Estrategias para mantener un equilibrio saludable entre la vida digital y offline.
- Impacto ambiental del uso de dispositivos tecnológicos.

3.3.2. Aprendizajes

- Reconocer que el uso excesivo del móvil o del ordenador puede generar estrés y fatiga visual.
- Establecer horarios para separar el tiempo de trabajo digital del tiempo personal.
- Silenciar notificaciones en la noche para favorecer el descanso.
- Aprender a organizar la jornada con un calendario que incluya momentos de desconexión.
- Valorar la importancia de dedicar tiempo offline a la familia y actividades de ocio para equilibrar la vida profesional y personal.
- Identificar buenas prácticas para reducir el impacto ambiental del uso tecnológico.

3.4. Resolución de problemas técnicos

3.4.1. Contenidos

Principales problemas en el uso del mail y soluciones.

Principales problemas técnicos y sus soluciones.

3.4.2. Aprendizajes

Aprender qué hacer si no pueden adjuntar un archivo en un correo electrónico.

Resolver un problema común cómo recuperar la contraseña olvidada del correo.

Identificar cómo actuar si un correo importante aparece en la carpeta de spam.

Practicar cómo reiniciar el router cuando no hay conexión a internet.

Comprobar los pasos básicos cuando el ordenador o móvil va lento (cerrar pestañas, liberar espacio).

3.5. Identificar áreas de mejora en las propias competencias digitales

3.5.1. Contenidos

Evaluación de las competencias.

3.5.2. Aprendizajes

Comparar los resultados iniciales con los obtenidos tras varias sesiones formativas.

Reconocer que equivocarse en la evaluación es parte del proceso de aprendizaje.

Usar herramientas de autoevaluación para planificar nuevas metas digitales en su negocio o búsqueda de empleo.

Explorar recursos online gratuitos para seguir mejorando sus competencias después del curso.

4. DESARROLLO DE LAS SESIONES

Este curso consta de cuatro sesiones con una duración de dos horas cada una, en las que trataremos todos los contenidos citados anteriormente de la siguiente manera:

Sesión 1. Protege tus dispositivos y tus datos personales. Aprenderemos a proteger la información personal y mantener los dispositivos seguros y conoceremos cómo protegernos de acciones relacionadas con el phishing y malware.

Sesión 2. Navega y comunícate de forma segura. Trabajaremos en cómo mantener la seguridad al comunicarnos y navegar por Internet. Reconoceremos aspectos para identificar estafas y fraudes en Internet.

Sesión 3. Uso responsable y saludable de la tecnología. Tomaremos conciencia de cómo usamos las tecnologías y trataremos de cómo mantener el equilibrio saludable entre la vida digital y la offline.

Sesión 4. Mis herramientas digitales para seguir aprendiendo. Esta sesión estará destinada a fortalecer la autonomía digital y el aprendizaje continuo. Y daremos herramientas para poder enfrentarnos a algunos problemas técnicos comunes.

5. METODOLOGÍA

Este curso se desarrollará en la modalidad presencial, con una duración de ocho horas, complementado con un Café Virtual para resolver dudas surgidas en la clase, así como para ampliar información de los temas de interés.

El curso se fundamenta en metodologías activas, en las que el alumnado protagoniza su propio aprendizaje: adquiriendo capacidades, conocimientos y destrezas significativas para su desarrollo personal, social y/o profesional. Atenderemos en medida de lo posible las necesidades e intereses de cada participante, lo haremos mediante el acompañamiento de prácticas individuales.

Se trabajará en grupo para generar un aprendizaje con el que compartir experiencias previas enriquecedoras para el grupo. Además, de dotar espacios para propiciar la autonomía, el pensamiento crítico y la confianza tecnológica.

Para ello, utilizaremos recursos digitales al alcance del alumnado para poder adaptarnos a su contexto y necesidades. Se propondrán tareas prácticas que se pueden presentar en su día a día y trabajaremos para resolverlas, así los contenidos tendrán un carácter más significativo.


6. SISTEMAS DE EVALUACIÓN Y SEGUIMIENTO

6.1. Evaluación

6.1.1. Evaluación inicial

Esta evaluación se llevará a cabo con una dinámica participativa en la que el alumnado responderá a cuestiones como: qué saben de algunas competencias digitales básicas, qué esperan aprender del curso y qué dificultades diarias tienen en relación a los entornos digitales.

6.1.2. Evaluación continua



Necesaria para reajustar los contenidos debemos tener un seguimiento continuo de los aprendizajes que va adquiriendo el alumnado.

Utilizaremos la observación directa y el diálogo con las personas participantes. Se valorarán la adquisición de contenidos, autonomía y confianza, así como el grado de participación y los métodos usados para resolver las prácticas propuestas..

6.1.3. Evaluación final

La evaluación final tiene como propósito valorar la consolidación de conocimientos, habilidades y capacidades a lo largo del curso.

Para ello, se entregará un breve cuestionario de autoevaluación para que cada participante reflexione sobre sus avances en las competencias digitales.

Al finalizar el curso se entregará a cada alumno/a un diploma acreditativo de aprovechamiento de la acción formativa.

6.2. Seguimiento

6.2.1. Café Virtual

El café virtual tiene como propósito servir de encuentro informal para que las personas participantes puedan intercambiar experiencias, inquietudes y dificultades sobre los contenidos ofrecidos en el curso.

Este espacio estará guiado por el equipo docente cuya función será moderar y dinamizar el espacio y si fuera necesario aportar nuevos recursos que fortalezcan las habilidades digitales trabajadas durante la acción formativa.

Su periodicidad será mensual, pero podrá realizarse de forma quincenal.