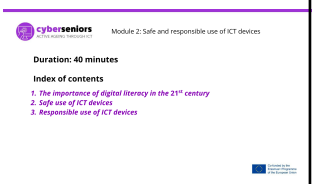
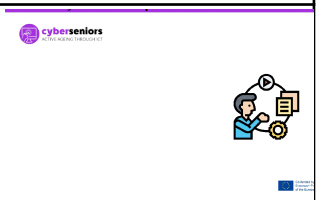
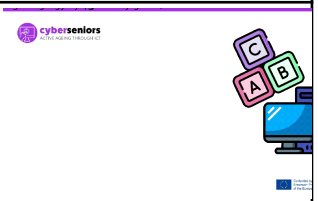
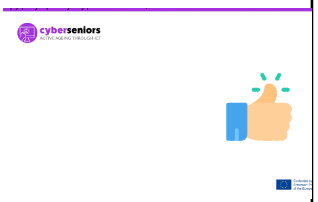
Guía formativa

Módulo 2/ Uso seguro y responsable de las TIC y los dispositivos

Antes de la sesión
• Ten todo el material necesario preparado (ordenador, presentación, pendrive, etc...) • Prepara bien tu presentación • Ten una actitud positiva y motivadora • Sé puntual

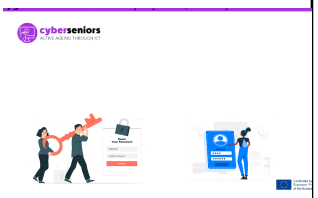
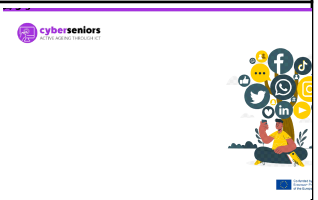
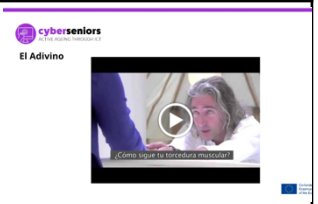
Durante la sesión		
Duración	**Duración de la sesión - 40 minutos**	Diapositiva
2 min	Durante la sesión: • Da la bienvenida a tu audiencia y preséntate para generar buen ambiente. • Sé consciente del tiempo durante todo momento para que puedas ver todo el material. • Deja un espacio al final para resolver dudas • Actúa con empatía, paciencia y cercanía • Procura cerciorarte de cuando en cuando de que tu audiencia sigue tus explicaciones	
3 min	Introducción Explicamos que Ciberseniors es un proyecto cofinanciado por la Comisión Europea a través del Programa Erasmus+, con el principal objetivo de crear recursos formativos para personas mayores de 55 años, sobre cómo manejar dispositivos móviles, y aplicaciones útiles para un envejecimiento activo y una mayor autonomía. Recordamos que toda la información, así como estos recursos, están disponibles en www.ciberseniors.org Explicaremos el índice de la sesión de hoy con el contenido que vamos a tratar, y les comentamos, en qué consisten los 4 módulos: 1. Introducción al uso de smartphone/tablet 2. Uso seguro y responsable de las Tecnologías de la Información y la Comunicación (TIC) 3. Aplicaciones TIC para móviles I (ocio, salud, comunicación) 4. Aplicaciones TIC para móviles y tabletas II (banca, necesidades diarias y accesibilidad, administración pública)	

El apoyo de la Comisión Europea para la producción de esta publicación no constituye una aprobación del contenido, el cual refleja únicamente las opiniones de los autores, y la Comisión no se hace responsable del uso que pueda hacerse de la información contenida en la misma.

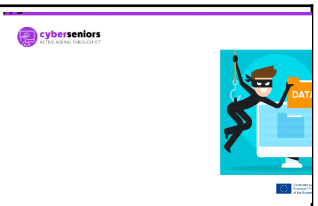
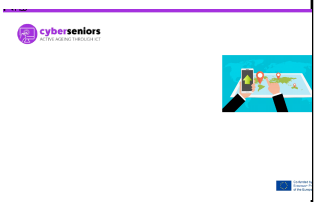
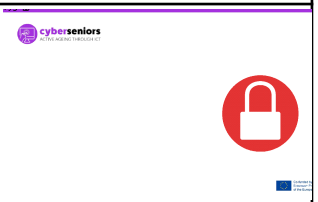
10 min	La evolución de la tecnología digital ha transformado la forma en que interactuamos con nuestro entorno y cómo llevamos a cabo nuestras actividades diarias. La alfabetización digital es una habilidad fundamental para todos nosotros, con el fin de aprender a navegar en el mundo digitalizado contemporáneo y adaptarse a las necesidades cambiantes.	
	- Necesidades diarias contemporáneas: - Correo electrónico - Comunicación virtual - Transacciones digitales - Recordatorios telefónicos	
	La alfabetización digital se refiere a: - Las habilidades requeridas para lograr competencias digitales; - El uso seguro y crítico de todos los medios técnicos para manejar las tecnologías de la información y la comunicación (TIC) para el trabajo, el ocio, el aprendizaje y la comunicación (Eurostat Glossary, 2019);	
	La alfabetización digital tiene estos beneficios: - Abre un mundo de oportunidades; - Une a la gente; - permite hacer cosas a distancia (Muy patente de la importancia ha quedado con COVID19) - Mejora las habilidades y permite el aprendizaje permanente; - Fomenta la independencia y el empoderamiento;	
15 min	Estos son algunos de los tipos de amenazas más habituales. **Suplantación**: Se pretende suplantar a otra persona en la comunicación con fin de robar datos o alterar los datos. Una técnica es la llamada “phishing”, que usa suplantación para hacernos pensar que mandamos nuestros datos a una web de confianza, cuando en realidad los está recibiendo el hacker, p.e. hacerse pasar por Facebook para robarnos nuestra contraseña de Facebook. **Troyano:** es un software disfrazado de beneficioso, y que pretende que lo instalemos para ganar acceso a nuestros datos. Puede disfrazarse de cualquier cosa, suites ofimáticas, antivirus, software de banca, etc. Por ello es fundamental que desconfiemos, que sólamente instalemos software desde	

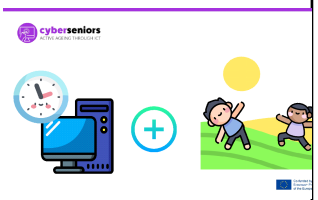
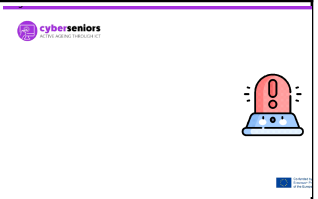
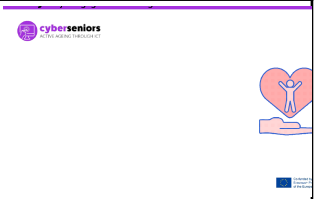
El apoyo de la Comisión Europea para la producción de esta publicación no constituye una aprobación del contenido, el cual refleja únicamente las opiniones de los autores, y la Comisión no se hace responsable del uso que pueda hacerse de la información contenida en la misma.

	fuentes confiables (app stores) y comprobemos todo software que instalemos con un antivirus. **SPAM:** el concepto de spam es muy amplio y abarca toda comunicación no deseada que se puede volver insistente y repetida, o no. Por regla general, se produce por email, pero puede producirse por cualquier otro medio, whatsapp, sms, llamada telefónica, etc. El fin puede ser conseguir tráfico hacia sitios web, robo de datos, instalación de software malicioso, etc., o también anuncios no deseados. La **ingeniería social**, explota nuestra debilidad como humanos para confiar en otros y de esa forma conseguir información necesaria para un ataque. Por ejemplo... una llamada de 'soporte' que nos pide una contraseña del servicio para solucionar un problema. También se considera Ingenieria social al estudio de la información pública (Redes sociales, webs personales, etc) de un usuario, con el fin de obtener información relevante para un ataque... p.e. Publicamos el nombre de nuestra mascota en Facebook con visibilidad universal. Un supuesto atacante añadirá ese dato a la lista de passwords que probará para entrar en sus cuentas. **Phishing:** es una técnica que lleva a la instalación de programas maliciosos, robo de datos o de dinero mediante mensajes de email, sitios web, llamadas de teléfono (vishing) o sms (smishing) que parecen legítimos en su aspecto y contexto, pero que nos llevan a sitios webs donde se nos va a robar datos, facilitar la instalación de programas maliciosos (malware), o robar dinero de nuestras tarjetas de crédito, entre otras acciones. **Adware:** es un software que nos muestra anuncios en nuestras aplicaciones o páginas web que visitamos, con el fin de generar lucro en el creador del programa malicioso, mediante nuestros clicks en los anuncios. **Spyware:** es un software que espía nuestras acciones en nuestro dispositivo. Si nuestro dispositivo dispone de funciones multimedia o sensores de localización puede espiar esa información, activar cámaras o micrófonos o acceder a nuestra localización en el móvil, etc..	

	La mitad de las personas mayores no utilizan la función de contraseña en al menos uno de sus dispositivos habilitados para Internet, lo que deja abierta la posibilidad de que cualquiera pueda acceder. Bloquee todos sus dispositivos, incluidos el ordenador, la tablet y el móvil, con contraseñas seguras. Eso las mantendrá alejadas de miradas indiscretas y supondrá una línea de defensa en caso de pérdida o robo de sus dispositivos. ¿Con qué frecuencia se necesita cambiar las contraseñas? A menos que ocurra una violación de contraseña, no hay necesidad de cambiar sus contraseñas a menudo, si cada contraseña es segura y única. Sin embargo, si cree que una de sus cuentas ha podido ser pirateada, cambie su contraseña de inmediato.	
	Al crear publicaciones en las redes sociales, puede cambiar la configuración de privacidad para seleccionar qué audiencia verá su publicación. - Los amigos que agregó en la red social, - cualquier persona - privada solo para usted. También puede especificar o no especificar su ubicación. Asegúrese de que su información privada no se comparta (contraseñas, número de teléfono, correo electrónico, etc.)	
	Este vídeo muestra algunas de las amenazas que hemos visto anteriormente y cómo actúan algunos ciberdelincuentes	
	En la comunicación a través de redes sociales, mensajería y correo electrónico, debe tener cuidado y no debe hacer clic en los enlaces que le envía una persona desconocida. Los ciberdelincuentes pueden hacerse pasar por, por ejemplo, empleados de Facebook o el servicio de seguridad de Instagram. No confíes en esos mensajes, si los recibes a través de un chat normal, una publicación o desde una página normal de Facebook. Los mensajes de seguridad se le enviarán a través de notificaciones o estarán disponibles en la configuración. Los empleados de las redes sociales nunca le pedirán su contraseña o información privada.	

El apoyo de la Comisión Europea para la producción de esta publicación no constituye una aprobación del contenido, el cual refleja únicamente las opiniones de los autores, y la Comisión no se hace responsable del uso que pueda hacerse de la información contenida en la misma.

	Si amigos o familiares le piden que los ayude en una emergencia, siempre llame para hablar con ellos personalmente y confirmar si ellos originaron el mensaje. De lo contrario, esos mensajes pueden ser de ciberdelincuentes, que pueden crear un perfil que será idéntico al perfil de su familiar o amigo e intentar obtener dinero o algún dato de usted.	
	Puede usar la herramienta "Buscar mi teléfono" de Google, si inició sesión en su cuenta de Google (gmail) en su teléfono. Primero, debe permitir que Google use los datos de su ubicación, la información del dispositivo y los eventos de conexión para ubicar sus dispositivos y accesorios. Es posible que la ubicación del dispositivo no siempre sea precisa, pero verá un mapa con la ubicación actual de su teléfono. Los datos sobre el nivel de carga y la conexión a la red móvil también estarán disponibles. Tendrá varias opciones: - Pon la alarma en tu teléfono. El dispositivo sonará durante cinco minutos incluso si el teléfono está en modo silencioso. - Bloquea tu teléfono y cierra la sesión de tu cuenta de Google. También puede mostrar un mensaje de texto en la pantalla del teléfono. - Borre los datos del dispositivo restableciendo a la configuración de fábrica. Después de eso, ya no podrá monitorear su dispositivo.	
	Consejos - Acceso seguro a tus cuentas. - Piensa antes de actuar. - En caso de duda, verifica. - Comparte con cuidado. - Usa software de seguridad. - Configura seguridad de tu navegador. - Usa antivirus (tb en móvil). - Cierra sesión. - Pide ayuda.	

5 min	Recuerda - Es necesario mantener el equilibrio mental y físico. - Gestiona las interacciones con herramientas digitales - El bienestar digital influye en nuestro bienestar general y viceversa. El mejor consejo es que encuentres un equilibrio entre ambos "mundos", pues el enriquecimiento será mayor y podrás beneficiarte de lo positivo de cada área y pormenorizar los riesgos de un excesivo uso del entorno digital, que como hemos ido viendo en la sesión de hoy puede afectarte a muchos niveles. Usa la tecnología para interactuar con el mundo físico y con nuestro entorno de una manera activa.	
	Estas son algunas de las consecuencias del abuso de la tecnología	
	- Comprenda y controle sus hábitos tecnológicos - Establezca límites - Gestione mejor sus conexiones - Tome descansos regularmente - Duerma y descanse bien por la noche, evite usar la tecnología antes de ir a dormir	
5 mins	**CONCLUSIÓN**	
	Dejaremos un tiempo hasta el final de la sesión para resolver dudas o inquietudes de lo visto en la sesión de hoy, agradeceremos su participación y les animamos a que practiquen en casa para no olvidar lo que han aprendido hoy.	

MUCHAS GRACIAS