ALFABETIZACIÓN MEDIÁTICA PARA MAYORES

MAYORES CON WIFI

Junta de Andalucía

ca:A Consejo Audiovisual de Andalucía

MAYORES CON WIFI

ALFABETIZACIÓN MEDIÁTICA PARA MAYORES

Manual didáctico

ca:A
Consejo Audiovisual de Andalucía

Autoría:

Consejo Audiovisual de Andalucía:

- Inmaculada Casas Delgado
- Marianela Castilla Trigo
- Ana Millán Muñoz

Edición y maquetación:

Consejo Audiovisual de Andalucía:

- Inmaculada Casas Delgado

ÍNDICE

PRESENTACIÓN

‘Mayores con Wifi’ es una iniciativa divulgativa de alfabetización mediática, impulsada por el Consejo Audiovisual de Andalucía (CAA), que promueve la inclusión socio-digital de las personas mayores en aras de facilitar su participación en esta sociedad de la información, que es cada día más tecnológica.

El CAA nace con la vocación de ser un referente social de prestigio, que colabora activamente en la tarea de garantizar la libertad de expresión, el derecho a la información veraz y la pluralidad informativa, así como el respeto a la dignidad humana y el principio constitucional de igualdad. Propicia la conciliación de los intereses de los distintos agentes económicos, socioculturales e industriales y los intereses generales de la ciudadanía andaluza. Garantiza el cumplimiento de la normativa reguladora de la programación y la publicidad, y de las condiciones de las concesiones, el cumplimiento de la eficacia y observancia de los principios establecidos en la Constitución Española, en el Estatuto de Autonomía para Andalucía, de las normativas española y europea y de los tratados internacionales relativos a la comunicación.

Entre los principios fundamentales del CAA se encuentra el impulso de todo tipo de actividades que promuevan la alfabetización mediática entre la ciudadanía andaluza. El Consejo pretende así dotarnos de las habilidades necesarias para desarrollar el espíritu crítico de la población andaluza ante los mensajes que recibimos en los medios de comunicación e Internet.

El presente manual didáctico cimenta las bases de las 10 sesiones formativas que componen el taller 'Mayores con Wifi'. El objetivo es formar a aquellas personas en riesgo de exclusión socio-digital, por edad, formación o zona de residencia, en el uso de herramientas TIC, que les ayuden a realizar tareas cotidianas en diferentes ámbitos de su vida diaria (salud, entretenimiento, trámites bancarios o administrativos, comunicación virtual, etc.) y también saber cómo utilizarlas de forma segura. De esta manera, podrán mantener su independencia y continuar realizando las actividades diarias necesarias para su día a día.

SESIÓN 1
BIENVENIDOS AL ENTORNO DIGITAL

1. Contexto y definición

- ¿Qué entendemos por digital?

  Internet y las nuevas tecnologías (conocidas como TICs) nos ofrecen todo un mundo de oportunidades a cualquier edad, siempre que se les dé un buen uso y lo hagamos de forma segura, equilibrada y saludable. Forman parte de nuestro día a día, y tanto adultos como menores las utilizamos para relacionarnos, organizarnos, entretenernos...

  Como cualquier entorno, hay que dedicar tiempo a estudiarlo y conocer cómo se maneja, cuáles son sus reglas y las herramientas más oportunas para cada uso. Acercándonos a todas las ventajas y los inconvenientes que nos ofrece, descubriremos que no todo es adecuado para todos los públicos, y algunos contenidos pueden considerarse negativos o perjudiciales.

Por eso, es importante dedicar tiempo a la búsqueda de contenidos positivos, ajustados a la madurez de cada usuario, mientras trabajamos el pensamiento crítico y la responsabilidad.

La llegada de la tecnología a nuestras vidas ha sido un proceso rápido y silencioso, incluso invasivo porque nos afecta a varios planos de nuestra vida de manera íntegra. Un uso adecuado e inteligente nos hará quedarnos con lo mejor que la tecnología nos ofrece, haciendo que nuestra vida resulte más ágil y sencilla y consiguiendo que las oportunidades superen a los riesgos. Repasemos algunas de las ventajas y desventajas.

1.2.Ventajas

Acceso global a la información. Al navegar por Internet se nos abre un mundo de posibilidades, desapareciendo el concepto de distancias y barreras. Se nos ofrece la oportunidad de acceder a los contenidos más remotos, tan sólo al hacer un clic. Podemos consultar contenidos de entretenimiento, estudio, emprendimiento, así como desarrollar nuevas aptitudes.

Instantaneidad. Uso del correo electrónico: también conocido como e-mail (del inglés electronic mail) consiguiendo realizar trámites a distancia y sin hacer uso del papel y siendo un servicio totalmente gratuito. Nos permite intercambiar información de todo tipo: texto, fotografías, vídeos, documentos..., jugando el papel tanto de remitentes, como de receptores de documentación (con tamaño limitado según qué servidor se use). Existen varias compañías con las que obtener una cuenta de correo electrónico: Gmail, Yahoo, Hotmail, etc…

Conectividad. Más allá de compartir textos es posible también estar conectados enviando y recibiendo vídeos y audios. Para ello se necesita dotar al equipo de una cámara (también conocida como webcam) y de altavoces, esto en el caso de que el equipo no los tenga integrados.

Inmediatez. La conexión en directo es una de las grandes ventajas, que nos acerca a los que tenemos lejos. Visitar en directo un programa de radio o de televisión. Asistir a un evento que esté a

cientos de kilómetros de distancia y participar como si estuviéramos presentes en tiempo y forma. O mantener una conversación o reunión con alguien que se encuentre al otro lado del planeta, de manera directa, sin interferencias ni intermediarios.

Libertad e independencia. Podemos realizar visitas de manera virtual (a todos aquellos lugares que estén disponibles con las herramientas necesarias) a destinos lejanos, disfrutando de la experiencia de acceder a ellos, como si estuviéramos allí.

1.3. Desventajas

Exceso de información publicada. Las pantallas nos imponen un ritmo frenético y confuso que en ocasiones nos produce una sensación de saturación. Toda la información que se publica, se convierte en un dato público, de ahí que un exceso de información puede hacernos vulnerables ante posibles ciberataques. Toda la información referente a nuestros gustos, aficiones, hábitos, etc. también forma parte de nuestra privacidad, y en especial, nuestros datos

personales: domicilio, número de teléfono, dirección de correo electrónico, grabaciones de vídeo, audio, fotos... Asimismo, tienen carácter privado los datos relacionados con nuestro historial sanitario (enfermedades padecidas, pruebas médicas o tratamientos), datos bancarios (número de cuenta o de tarjeta), información profesional (vida laboral, salario), los datos biométricos como las huellas dactilares, etc.

Falta de privacidad. La privacidad se define como el ámbito de la vida personal que se tiene derecho a proteger de cualquier intromisión. La privacidad proporciona seguridad y resguarda de la mirada de los otros. La privacidad es necesaria, si queremos tener una Red segura para todos. La información privada dice mucho sobre alguien o sobre su familia, entorno, etc. En función de la cantidad de datos que se publiquen se expondrá en mayor o menor medida la vida de una persona.

No tener control del tiempo. Resulta fácil que perdamos la noción del tiempo cuando estamos

conectados a las pantallas, de ahí que se muestre interesante el reflexionar sobre el tiempo que dedicamos a nuestros dispositivos móviles para saber cuánto tiempo le estamos quitando a otras cosas que nos gusta hacer, como por ejemplo leer libros, pasar tiempo con la familia, pasear, cocinar. Quizá no tengamos una sensación muy grande de perder tiempo con las pantallas, pero sí que somos conscientes de que hemos desplazado otras cosas que nos gustan mucho más por estar pendientes de nuestros dispositivos digitales. El último estudio presentado por el Observatorio Español de las Drogas y las Adicciones, refleja una tendencia preocupante: durante el confinamiento los españoles bebimos menos, fumamos menos, nos drogamos menos, pero encontramos otras adicciones, conocidas como adicciones sin sustancia, todas ellas relacionadas con el abuso de la tecnología: apuestas online, ciberpornografía, compras compulsivas. Este estudio demuestra cómo estas adicciones del siglo XXI enganchan y nos hacen sufrir los mismos síntomas de las personas enganchadas al alcohol y drogas.

Sedentarismo. Todo el tiempo que se dedica a estar frente a una pantalla, generalmente lo hacemos estando sentados, por tanto si nuestro nivel de horas dedicadas a navegar por la red aumenta, probablemente nuestro sedentarismo también lo hará, llevándonos a adquirir hábitos poco saludables que influyen de manera directa en nuestra salud.

Falta de socialización y aislamiento. El abuso de dispositivos digitales para mantener relaciones personales, familiares o profesionales nunca podrá sustituir al trato personal en vivo y en directo. Profesionales de la psicología afirman que existe un impacto negativo en las habilidades sociales, por la sobreexposición de las personas delante de las pantallas. Su uso continuado puede llevar fácilmente al aislamiento, con todo el impacto negativo que esto arroja sobre el ser humano. Es necesario promover un uso equilibrado de los dispositivos que no perjudique la salud física: respeto a las horas de sueño, la salud ocular al pasar muchas horas seguidas frente a la pantalla, practicar ejercicio físico y actividades al aire libre.

Arrastrados por la presión social. Un uso continuado y en exceso de contenidos digitales, especialmente de redes sociales, pone de manifiesto la debilidad propia del ser humano cuando se ve sometido a la presión social. Cómo el conocer de manera rápida y atropellada pero con continuidad y persistencia la opinión de otros, nos puede influir tanto en nuestro cerebro, que terminemos adoptando las opiniones y formas de pensar del otro, tan sólo por presión, por influencia, superando incluso lo que se aprecia por nuestros propios sentidos.

2. Buen uso digital

Hay expertos que afirman que el buen uso de los dispositivos digitales, pueden favorecer nuestras posibilidades de conocimiento, provoca el crecimiento de las redes neuronales, la toma de decisiones, la memoria asociativa, y el desarrollo de nuevos hábitos. Comprender cómo funciona Internet y analizar las motivaciones de las personas con las que se interactúa a través de la Red, resulta fundamental para prevenir riesgos personales, económicos y sociales.

Tiempo de pantalla. Es recomendable reflexionar sobre el equilibrio entre las horas destinadas a estar conectados a internet y el dedicado a las diferentes actividades de nuestra vida diaria. Para ello, se aconseja mirar el reloj a la hora de la iniciación y concretar un tiempo limitado de conexión. Conviene destacar la importancia de interactuar con diferentes personas y vivir experiencias variadas a lo largo de la jornada. Valorar y darle importancia a los contenidos a los que accedemos siendo libres en la elección y no navegando a base de impulsos.

Salud digital. Se mantiene una buena salud digital cuando no aceptamos como válido y veraz el contenido que recibimos por cualquier vía digital, por el único hecho de haberlo recibido. El espíritu crítico se presenta como una de las habilidades que mejor puede protegernos de los fraudes y estafas vía online. Nos llevará a reflexionar ante cualquier situación, aprendiendo con el tiempo a valorar

lo que realmente dicen y quieren las demás personas, lo que pueden llegar a interpretar de nuestras palabras y a distinguir entre lo real y lo falso. De este modo, este espíritu crítico nos ayudará a valorar las intenciones de otras personas y nos podremos proteger ante mensajes que resultan demasiado atractivos y golosos para que sean ciertos. Aprenderemos a pararnos y ser más reflexivos antes de enviar datos personales o compartir información privada.

Participación en comunidad. Participar en foros de debate, plataformas sociales, asociaciones o movimientos activos es otra de las oportunidades que nos ofrece en la Red, creando una comunidad en permanente contacto, sin que la distancia sea un obstáculo para la reunión o el encuentro. Hoy en día es frecuente que nos preguntemos: "¿Por qué nos “enganchamos” a la tecnología, al móvil?". El motivo psicológico principal es que nuestro cerebro siempre busca felicidad y junto a ella, la satisfacción de la inmediatez, el placer o la necesidad de comunicarnos con otros, informarnos, entretenernos, estar al día,

aprender... Todo eso, nos lo proporcionan nuestros dispositivos móviles en breves segundos. Diversos estudios corroboran que las pantallas disparan la secreción de hormonas como la dopamina y la adrenalina para que centremos la atención en la pantalla y nos disparan también endorfinas, porque nos disponemos a hacer algo que nos produce placer y nos gusta.

Ciudadano digital. Al igual que ocurre en el entorno off-line, en el mundo digital conviene tener en cuenta una actitud colaborativa. Habilidades como la empatía o la asertividad, nos ayudarán a buscar lazos de unión que nos conecten y nos hagan construir sobre bases comunes y no tanto focalizar en las discrepancias y diferencias que nos harán llamar a la confrontación y al comportamiento violento. Tengamos en cuenta que en las interacciones digitales no siempre podemos mirar a la cara a las personas con las que hablamos, conllevando a dos efectos fundamentales:

-Suelen ser frecuentes los malentendidos puesto que nos perdemos una buena parte de los elementos básicos de la comunicación como es el tono del mensaje, el lenguaje no verbal, la mirada…, ya que el texto puede ser interpretado de diversos modos, no acertando siempre a escoger el elegido por el remitente.

-Al tener una pantalla de por medio resulta más difícil tener presente que la otra persona también tiene sentimientos y sensibilidades. Quizás la barrera telemática nos fuerza a utilizar unas expresiones y un lenguaje que normalmente no emplearíamos de manera presencial.

Otra de las peculiaridades de nuestras relaciones online es que se selecciona tanto el radio de influencia y relación, que se acaban polarizando las opiniones. Al elegir con quien hablamos y a quien seguimos, terminamos relacionándonos solamente con aquellos que opinan como nosotros. Llegando incluso a creer

que todo el mundo está de acuerdo con todo lo que pensamos.

Todo esto nos puede llevar a perder empatía, pero no olvidemos que su práctica es clave para que el respeto a los demás y el diálogo fluyan en nuestras conversaciones de nuestros chats más frecuentes. Una práctica que se aconseja mucho es pensar antes de responder, ya que de esta manera podemos evitar dar respuestas en caliente que fácilmente se desencadenan en conflictos y enfados que hubiesen sido fácilmente evitables.

Se recomienda evitar las conversaciones conflictivas en chats compartidos formados por un amplio grupo de personas. Como solución se proponen los canales de conversación privada donde la comunicación tenga sentido de ida y vuelta entre dos personas y no más.

4. Actividades

- Consultar la cartelera, leer las noticias, visitar el Museo del Prado... ¿Sabes todo lo que puedes hacer gratis sin salir de casa, navegando por la Red?

- ¿Sabes qué es un navegador? ¿Conoces los más comunes? Consulta este vídeo de la OSI.

- Si tienes una cuenta de correo revisa las opciones que ofrece: envío de archivos adjuntos, emoticonos, edición de texto...

- ¿Conoces los servicios de almacenamiento de archivos? Revisa esta comparativa para saber cuál escoger.

- ¿Reconoces todos los símbolos de una videollamada?

- La presión social es mucho más fuerte de lo que creemos y aquí tienes un ejemplo de la serie Merlí

5. Más información

- El abuso de las nuevas tecnologías puede provocar aislamiento. Un caso extremo son los 'hikikomoris', un término japonés que denomina a los ermitaños jóvenes que viven sin salir de casa ni relacionarse con nadie, manteniendo contacto con el exterior sólo a través de las pantallas.

- Una actitud proactiva ante el uso de las pantallas ayuda a mantener el autocontrol y seleccionar quedarnos con más ventajas que inconvenientes en su uso frecuente. Dedicar tiempo a la formación en el uso de herramientas digitales, realizando cursos como 'Mayores con Wifi' o 'Experiencia Senior' de INCIBE ofrece seguridad, autonomía y nos acercan a un uso más responsable.

SESIÓN 2
CIBERSEGURIDAD

1. Contexto y definición

Internet y los servicios que se prestan a través de la Red forman parte de nuestro mundo cotidiano. Los usamos para informamos, escuchar música, ver películas, realizar trámites diversos, compras online y también para relacionarnos. En todas estas interacciones compartimos información con otras personas, como fotos o vídeos, entre otros datos. Los servicios más usados en Internet pueden prestarse gracias a la información y datos personales que los usuarios aportamos y debemos saber, en este contexto digital, cómo proteger nuestra seguridad y privacidad.

- ¿Qué es la ciberseguridad?

Es el área de la informática que tiene como objeto la protección de la infraestructura tecnológica y la información contenida en ella.

Para ello, existen protocolos y leyes, porque los fallos de seguridad pueden suponer riesgos de diversa índole, desde graves amenazas a todo un país, hasta para los datos más personales de la ciudadanía de a pie. Por eso, la ciberseguridad es un asunto de primer orden para los gobiernos, las empresas y las personas, y es éste último aspecto el que nos interesa en este taller.

Existen muchos recursos en Internet para informarse al respecto y orientar al internauta sobre los principales riesgos a los que se exponen y la manera de protegerse. Podemos citar la Oficina de Seguridad del Internauta (OSI), que se ocupa de acercar a la ciudadanía de una manera sencilla y orientativa este tipo de información, y al Consejo Audiovisual de Andalucía, que ha realizado varias actuaciones en este sentido y ha recogido en un decálogo las principales orientaciones que ayudan a tener una navegación más segura en Internet.

Entre las preocupaciones de los andaluces respecto al uso de Internet se encuentran la vulneración de la privacidad de datos, los fraudes, el robo de información personal o bancaria y la suplantación de identidad, según el último Barómetro Audiovisual de Andalucía.

Una navegación segura comienza por no dar pasos a la ligera en Internet e intentar conocer primero algunas nociones sobre seguridad para que nuestra experiencia sea positiva. En la Red uno de nuestros más preciados bienes son los datos personales.

- ¿Qué son los datos de carácter personal?

Cualquier información que nos identifique o pueda permitir que alguien lo haga, como nombre, apellidos, DNI, correo electrónico o incluso una dirección IP, que son los nombres numéricos que se asignan a un dispositivo a modo de "matrícula" para que pueda ser llamado por otros dispositivos.

También son datos personales aquellos que revelen el origen étnico o racial, opiniones políticas, religiosas, datos genéticos, biométricos o aquellos relativos a la orientación sexual.

En nuestros movimientos por la Red vamos dejando una huella, sin saberlo, que puede llegar a revelar todo sobre nosotros. Nuestros datos son nuestra responsabilidad, por ello debemos ser conscientes de lo que compartimos con otros, los datos que introducimos en las distintas páginas que visitamos o en las transacciones que realizamos. Asimismo, es muy importante conocer qué derechos tenemos sobre ellos y qué obligaciones tienen quienes los tratan. Existe una Ley orgánica sobre protección de datos, en vigor desde diciembre de 2018, que vino a adaptarse, entre otras exigencias, a la nueva realidad que introducía el mundo digital en nuestro día a día. Se trata de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Antes de dar nuestros datos en Internet, debemos preguntarnos quién nos lo pide y para qué. No es lo mismo reservar un hotel que solicitar una cita médica, por ejemplo. Dar más información de la necesaria podría acarrear en el futuro problemas ya que terceros podrían tener acceso a ella y eso nos coloca en situación de riesgo de recibir spam, o ser víctima de chantaje. Una vez que facilitemos nuestra información, perdemos el control sobre ella y, aunque tengamos derecho a que sean eliminados, un tercero ya los podría haber guardado y compartido.

A continuación se relaciona una serie de datos que, según la OSI, no deberíamos compartir nunca en Internet, ya que el riesgo para nuestra privacidad y seguridad es muy alto:

-Dirección y ubicación
-Correo electrónico y número de teléfono
-Fotos de menores
-Fotos comprometedoras
-Documentos personales

-Conversaciones privadas
-Opiniones o quejas sobre algo

Asimismo, nunca debemos facilitar información personal de terceros.

- ¿Qué es el derecho al olvido?

Recordemos que tenemos derecho a la protección de nuestros datos y que, en el caso en que queramos rectificar, o eliminarlos, existe en la ley una figura llamada 'Derecho al olvido'. Es el derecho a solicitar que los enlaces y referencias en la Red a nuestros datos personales no figuren en los resultados de una búsqueda en Internet realizada por tu nombre (práctica que se conoce con el nombre de egosurfing).

También una foto, o vídeo en el que aparezcamos es un dato de carácter personal. Si no estamos de acuerdo en aparecer, por ejemplo, en redes sociales, podemos pedir su supresión.

Puede solicitarlo la persona afectada o los progenitores o tutores de un menor de 14 años si es el caso. Primero se solicita a la plataforma responsable, y, en caso de que no surta efecto, la propia Agencia Española de Protección de Datos nos ampara en el procedimiento. Recordamos que las redes sociales más populares disponen de mecanismos para comunicarles vulneraciones de la privacidad o contenidos inapropiados mediante sus propios formularios.

2. Herramientas prácticas

- Dispositivos y conexión Wifi

Actualmente es frecuente tener uno o más dispositivos en nuestros hogares, como un smartphone, una tableta, un portátil o una Smart TV. Estamos demasiado acostumbrados a que formen parte de nuestra vida, realizamos numerosas acciones con ellos, y hay en ellos tanta información personal que su ausencia, por ejemplo, nos generaría un trastorno.

La pérdida, el robo, o el acceso de terceros a nuestros dispositivos haría que toda nuestra información se viera comprometida, es como si alguien pudiera conocerlo todo sobre nosotros. Esto puede ocurrir si no protegemos bien estos dispositivos frente a virus, o accesos no autorizados.

Se relaciona, a continuación qué resulta aconsejable o no, desde la perspectiva de la ciberseguridad y la salvaguarda de la información que se almacenan en nuestros dispositivos:

Bloqueo de pantalla. Los dispositivos tienen un sistema de bloqueo para evitar que otras personas lo usen sin nuestra autorización. Puede usarse un patrón que se dibuja sobre una pantalla táctil, por ejemplo, una clave, un PIN o, incluso, una huella digital o reconocimiento facial.

Descarga de aplicaciones. Una aplicación puede pedirnos permisos que nosotros aceptamos sin cuestionarnos si son necesarios. Se trata de autorizaciones que damos para que determinada app acceda a nuestros contactos, fotografías, vídeos, etc. Nuestros móviles, por ejemplo, tienen configuradas por defecto opciones de seguridad que evitan que nos descarguemos cualquier información desde fuentes no fiables. Algunos usuarios las desactivan, en una práctica conocida como 'Jailbreaking o Rooting'. Las consecuencias pueden ir desde la pérdida de garantía del fabricante a la instalación de malware o virus, mal funcionamiento del sistema del dispositivo o problemas al instalar actualizaciones. Además, ello puede ponernos en situación de ser blanco de fraudes del tipo suscripción a sms premiums, por los que debemos pagar y a los que nos suscribimos sin nuestro conocimiento; o configuraciones por bluetooth que permiten a un ciberdelincuente conectarse de manera remota a nuestro móvil, ordenador o tableta.

Contraseñas fuertes. Para conseguir que la información que almacenamos en nuestros dispositivos esté a salvo, necesitamos contraseñas fuertes, ya que estas son las llaves de acceso a nuestros servicios y su vulneración compromete nuestra privacidad. La gestión de las contraseñas se convierte en uno de los aspectos más importantes a nivel de empresas y también de usuarios. Aunque parezca una tarea pesada, debemos atender a lo que se nos indica en cada servicio. Hay una serie de pautas universales, como introducir una sucesión de caracteres superior a ocho que incluya mayúsculas, minúsculas, números y algún carácter diferente a los alfanuméricos. Se desaconseja usar fechas señaladas, ya que un ciberdelincuente no tardaría mucho tiempo en descifrarla. Se recomienda, también, mantener los dispositivos actualizados, siguiendo las pautas de actualización fijados en los sistemas operativos, así como cambiar las contraseñas que se nos ofrezcan por defecto.

Entre otras buenas prácticas está usar un gestor de contraseñas, activar la verificación en dos pasos, no utilizar la misma contraseña para servicios diferentes, cambiarlas periódicamente y no usar el recordatorio de contraseñas.

Antivirus. Es una buena práctica de seguridad instalar un antivirus efectivo en ordenadores, tabletas y smartphones. Muchos de estos programas, además de detección de malware, incorporan funcionalidades para validar la fiabilidad de las páginas web por las que navegamos. Existen antivirus tanto de pago como gratuitos. Se recomienda descargar el antivirus de la web oficial del fabricante y mantenerlo constantemente actualizado (aunque muchos de estos programas se actualizan de manera automática).

Copias de seguridad. Debemos hacer copias de seguridad de la información que consideremos valiosa, siempre en una ubicación distinta al equipo que contiene la información.

Carga de batería en puertos USB públicos. Los puertos USB de lugares públicos son el objetivo de un tipo de ataque conocido como Juice-Jacking: ataques para robar cuentas. Se trata de un ciberataque que puede realizarse al cargar un móvil en un puerto USB público. Estos conectores disponen de función de recarga y transferencia de datos. Un atacante puede instalar malware en esos puertos para lograr acceder a la información de nuestros dispositivos. Para evitar ser víctima de este ataque te recomendamos no conectar tu dispositivo a ningún puerto USB público.

En relación a los dispositivos, también se desaconseja conectar extraíbles cuya procedencia y contenidos desconozcamos así como mantener tapada la cámara, si la tiene incorporada, mientras no la usemos.

Configuración de la red Wifi. Como usuarios, casi todos solemos tener en nuestros hogares una red Wifi contratada con alguna compañía de telecomunicaciones a través de

un router. Este es el dispositivo que nos permite conectarnos a Internet en nuestro hogar, bien a través de un cable de red o inalámbrico, mediante la conexión Wifi. Normalmente la configuración que nos instalan por defecto, no es siempre la más segura. A través de nuestra Wifi transmitimos documentos personales, fotos, vídeos, conversaciones de chat, a lo que se suma información correspondiente al ámbito laboral, si es que trabajamos desde casa. Si nuestra Wifi no está protegida, cualquiera puede conectarse a ella y utilizarla. Aplicar unas medidas de seguridad adecuadas y revisar periódicamente la configuración de nuestro router nos proporciona seguridad. Se recomienda cambiar la contraseña de acceso que trae por defecto, modificar el nombre de la Wifi o apagar el router cuando no se esté utilizando.

- Navegación

Desde el momento en que accedemos a Internet estamos dejando un rastro: bien sea

por las cookies, el historial de navegación, o el propio caché, este rastro da información sobre nosotros. Recogemos a continuación una serie de buenas prácticas para movernos con seguridad.

El modo incógnito. Es una forma más privada de moverse en la red. Todos los navegadores disponen de este modo de navegación, que impide que cierta información se almacene, manteniendo nuestra privacidad. Si bien es cierto que esta manera de navegar tiene muchas ventajas, hay que saber que no estamos totalmente protegidos y, aún activando el modo incógnito, hemos de tener precaución con determinadas webs y conexiones Wifi, porque los ciberdelincuentes pueden tener acceso a nuestros dispositivos y rastrear nuestros movimientos desde dentro. Activar el modo incógnito es muy sencillo. Recuerda activar siempre esta opción en un dispositivo que no sea el tuyo.

Mantener actualizado el navegador. Los navegadores nos permiten acceder a las múltiples funcionalidades de Internet y a veces ni nos percatamos de su existencia. El navegador también puede estar expuesto a fallos de seguridad, por ello, actualizarlos es una garantía para hacer de nuestra navegación una experiencia más segura. Cada navegador tiene una página web oficial desde donde puede descargarse la versión actualizada (Internet Explorer, Mozilla Firefox, Google Chrome, Edge o Safari por ejemplo). Existe una manera de lograr que esta actualización se realice de manera automática.

Eliminar el historial. Es conveniente realizar esta especie de limpieza de nuestros navegadores cada cierto tiempo. Lo que hacemos es eliminar nuestro rastro de navegación, las cookies, el historial y el caché.

Webs con 'https'. Si la dirección de una web (la URL) comienza por 'https', eso indica que es una página protegida con certificados de

seguridad o protocolos de cifrado. Las letras 'https' hacen referencia a un protocolo de comunicación de Internet que protege la integridad y confidencialidad de todos los datos que se intercambian entre el equipo y el sitio web y viceversa. De este modo lo que hace es proteger la información frente a terceros, la codifica para que terceros no accedan a ella. Cuando una página web utiliza el protocolo 'https' significa que que está aplicando tres capas de seguridad a la comunicación:

1) Cifrado sobre datos que se intercambian, de manera que, si alguien espía la comunicación, no podrá saber que información se está transmitiendo.

2) Integridad, de modo que no puedan modificarse los datos intercambiados durante la transmisión.

3) Autenticación para asegurar que el usuario se está comunicando con el sitio web que quiere y no con otro que pueda estar suplantándolo.

Una web que no use este protocolo no tiene porqué ser maliciosa, aunque, ciertamente un sitio cuya URL comience por 'http' tiene menores medidas de protección frente a los ciberdelincuentes. Debemos asegurarnos de que visitamos páginas que ofrecen máximos niveles de seguridad sobre todo si vamos a realizar transacciones online, en las que necesitemos dar nuestros datos.

Bien sea a través de nuestros datos personales y privados, bien entrando a nuestros dispositivos o desde ataques a nuestra navegación, los ciberdelincuentes son muy activos y pueden socavar la seguridad en esos tres ámbitos con técnicas diversas. Por ejemplo, usando lo que se llama la ingeniería social.

Puede que la Red, al igual que el mundo off line, no pueda garantizarnos una total seguridad, por ello es necesario nuestro sentido común y responsabilidad en el mundo digital.

Antes de concluir esta unidad conviene dar a conocer la línea telefónica gratuita 017 de ayuda en ciberseguridad.

3. Actividades

- ¿Sabes cómo solicitar a las redes sociales la supresión de tus vídeos y fotos? Sigue los consejos de la Agencia Española de Protección de Datos.

- Los ciberdelincuentes tardan 5 minutos en descifrar una clave basada en una fecha de nacimiento, mientras que una contraseña fuerte requiere hasta 2 años para ser descodificada. ¿Tus claves son seguras? Si no es así, cámbialas y usa un gestor de contraseñas.

- ¿Cómo puedo configurar una Wifi segura? Sigue los 5 pasos de este vídeo explicativo de la OSI.

- Practica eliminar los datos de navegación.

3. Actividades

- Prueba a activar el modo incógnito con la ayuda de la OSI.

- ¿Sabes configurar la actualización automática del navegador? Consulta este vídeo explicativo para resolver tus dudas en los navegadores más utilizados en España: Internet Explorer, Mozilla Firefox y Google Chrome.

4. Más información

- Recomendamos consultar la Guía de la AEPD sobre los principales aspectos de seguridad y privacidad en internet.

- Si tienes dudas sobre el derecho al olvido, no te pierdas las 5 claves del derecho de supresión de la AEPD.

- Para obtener información más detallada sobre la diversa tipología de ciberataques existentes, puede consultarse la guía de ciberataques que ha editado la OSI.

- También existe una amplia variedad de recursos en andaluciaesdigital.es

SESIÓN 3
NOTICIAS FALSAS

1. Definición

Son noticias sobre temas de interés social o de actualidad, generadas con la intención de crear una alarma o atraer indebidamente la atención del mayor número de usuarios posibles. Detrás de una noticia falsa existe una clara intención de manipulación y de querer reconducir a quienes reciben la noticia en la dirección que los autores pretenden. Se hace referencia también a ellas con términos como: desinformación, fake news o bulos.

Según la Red de Periodismo Ético (EJN) la información falsa o trucada es "toda aquella información fabricada y publicada deliberadamente para engañar e inducir a terceros a creer falsedades o poner en duda hechos verificables". Esta definición debería permitirnos diferenciar más fácilmente el periodismo de la propaganda, de los "hechos alternativos" y de las mentiras malévolas.

Es por todos sabido que no se trata de algo nuevo, los falsos mitos, la mentira y la desinformación han existido desde siempre, puesto que están vinculados al ser humano, por tanto sabemos que existen desde que el hombre es hombre, solo que a través de Internet se difunden más rápido y pueden llegar a más personas, por el efecto de conectividad masiva y gran velocidad que caracteriza a la red.

En la mayoría de los casos, la propagación de una noticia falsa conlleva otros intereses, nunca mostrados de manera concisa y clara: abundan fines económicos, políticos, ideológicos o comerciales presentando un claro objetivo de crear confusión. Una noticia falsa puede hacernos tomar decisiones desacertadas, basadas en esa información falsa o clima errado tras el masivo reenvío de la misma. Habitualmente, incluyen promociones, ofertas y descuentos, especialmente en época de rebajas o compras navideñas. Suelen compartirse por redes sociales, correo electrónico o aplicaciones de mensajería instantánea como WhatsApp, y su objetivo principal es la desinformación.

2. Herramientas prácticas

- ¿Cómo puedo detectarlas?

Con idea de ayudar a detectar bulos y noticias falsas o cadenas de mensajes por parte de los usuarios de internet, el Consejo Audiovisual de Andalucía ha elaborado un decálogo que ayuda a desarrollar el espíritu crítico necesario para enfrentarse a toda la información que se recibe de manera digital. Resulta destacable indicar que debemos partir de la premisa, de que no todo lo que se publica en la Red tiene que ser verdadero.

- Decálogo #PasadelBulo y Navega Seguro

1) Pregúntate si estás ante un bulo. Producir un reportaje o noticia tan pronto como se desarrollan los acontecimientos, requiere tiempo. Desconfía de las noticias bomba que surgen en la inmediatez de los hechos. No tengas prisa, párate, piensa y decide antes de pulsar la tecla Enviar.

2) Investiga la fuente de la noticia. Poner atención en la persona, organización o entidad que remite la historia. Que sea una fuente con buena reputación por su rigor y veracidad. Si se trata de un remitente desconocido, ampliar la información a través de la web oficial, con idea de conocerlo más a fondo. Un buen consejo será comprobar la noticia a través de un buscador, como por ejemplo Google y contrastar con otras fuentes. Algunas redes, como por ejemplo Twitter verifica la oficialidad de sus perfiles marcándolos con una señal como esta:✓

3) Que no te la cuelen con la URL. Revisar que la URL sea la del servicio legítimo para detectar posibles modificaciones en el nombre que aparentemente se lee como el original, sin serlo verdaderamente. Por ejemplo, Facebok o Goggle, en lugar de Facebook o Google. Un buen truco para detectarlo es comprobar que la dirección por la que empieza incluye la letra “s” comenzando por “https”.

4) Comprueba fecha y formato. Si se detecta que el texto no está bien redactado o las imágenes no tienen buena calidad, desconfiar de esa información. Poner atención también a las fechas. Publicar una noticia como de actualidad, cuando se trata de un hecho que aconteció en el pasado, esconde una intencionalidad sospechosa. Estos pueden ser detalles que nos servirán para desenmascarar contenidos falsos y bulos.

5) Aplica el sentido común. Decidir con sentido común nos ayudará a ser equilibrados y no dejarnos llevar por la temática ni por el contexto del momento. Resulta conveniente preguntarse si el contenido es demasiado bueno para ser cierto o busca crear discordia.

6) Compara el off-line con el on-line. Aquella información que cuesta creer que sea cierta fuera de la red, ponerla en duda también al verlo publicado en Internet. Es común ver titulares sensacionalistas o muy llamativos (también conocidos como “click bait”) donde por ejemplo, nombran a algún usuario como único ganador de un fabuloso premio. Ante la duda, no hacer clic.

7) Piénsatelo antes de compartir. No se deberían reenviar mensajes en cadena de tipo alarmistas, especialmente aquellos que contengan enlaces a sitios web o a descargas de apps que se desconocen. Recordar que al reenviar sin contrastar, nos convertimos en cómplices, verificando el contenido de esa información entre nuestros contactos.

8) Navega por la red con respeto. Cuando se publican noticias que afectan a personas concretas con nombre y apellido, se debe respetar como persona que es, sin ofender, humillar o insultar. No pulsar "me gusta" sin estar de acuerdo con la información, solamente por ser el único del grupo que no lo hace. Conviene ser tolerante al leer un mensaje, dando cabida a la duda ante posibles equivocaciones o interpretaciones diferentes. Es aconsejable dedicar tiempo a la reflexión antes de dar una respuesta y hacerlo de forma constructiva.

9) Educa a los más peques. Educar a los menores desde la infancia para saber reconocer los bulos y mensajes falsos que llegarán a sus manos es sumamente importante, para evitar que caigan en la manipulación y la desinformación en el futuro. No se trata de meterles miedo, sino de concienciarles de cómo les afecta la tecnología para que puedan tomar decisiones informadas. El mejor momento para hacerles conscientes de todo ello, es AHORA.

10) Analiza sin prisa la información. Dedica unos segundos a analizar la información y a seguir las sencillas pautas antes mencionadas, bien en clase o bien en familia, fomentando el razonamiento de niños y adolescentes, e informándoles abiertamente de los riesgos y la finalidad de estos mensajes. De este modo les estaremos animando a ser más críticos con lo que comparten y a buscar contenidos positivos de calidad en Internet.

Con estos sencillos consejos conseguiremos entre todos construir una Internet más justa, sana y equilibrada.

- ¿Cómo desarrollo el espíritu crítico?

Es a través de lo que se conoce como alfabetización mediática (media literacy, en inglés), es decir, cómo desarrollamos la capacidad necesaria para saber cómo acceder a la información, analizarla y también crearla en cualquier medio, ya sea on-line, ya sea off-line.

Desarrollar espíritu crítico ante toda la información que nos llegue a nuestras manos, especialmente aquella que resulta provocadora o demasiado impactante como para ser cierta, nos ayudará a preservarnos de caer en las redes de la desinformación y los bulos. Teniendo este espíritu crítico desarrollado conseguiremos ampliar nuestra perspectiva a la hora de afrontar los temas, demandando el tener la información más completa posible a la hora de tomar decisiones en nuestra vida, tanto personal como profesional. Teniendo estas ideas en cuenta, estaremos más capacitados para:

-Detectar la confusión que suele acompañar a la desinformación.

-Localizar el contenido veraz, sabiendo hacer hincapié en él, aunque haya intención de que aparezca en un segundo plano.

Ser críticos supone tener curiosidad, investigar, leer, contrastar, consultar, para ir forjando un juicio propio que nos lleve a tomar decisiones por nosotros mismos, desoyendo las líneas de pensamiento único que pueden transmitirse como presión social. Conviene preguntarnos ¿Le damos la misma credibilidad a un rumor que nos llega de la calle que a una noticia contrastada en un medio de confianza? Pues en Internet pasa lo mismo, desarrolla el hábito de contrastar la información y no te creas nada sin antes verificar la información en otras fuentes oficiales de prestigio.

En nuestro día a día, resulta frecuente recibir, buscar y compartir información en la Red, a menudo sin pararnos a reflexionar lo suficiente. Esto nos puede llevar a acceder a contenidos falsos que estén enmascarados como si se tratara de información real. Nos pueden llegar a través de nuestras publicaciones en redes sociales, con mensajes privados, foros o chats de grupos familiares, vídeos, etc… que suelen ser nuestros canales de información más frecuentes.

Desarrollar espíritu crítico ante toda la información que nos llegue a nuestras manos, especialmente aquella que resulta provocadora. Por eso se recomienda no ser impulsivos a la hora de compartir o difundir una información, ya que podríamos convertirnos en un elemento más de la cadena de transmisión del bulo.

A veces es difícil diferenciar las noticias falsas del humor o la sátira. Para salir de dudas, comprueba si la fuente de la noticia es conocida por sus parodias, y si los detalles y el tono de la historia sugieren que esta se ha escrito en clave de humor.

Hoy día las 'fake news' están evolucionando de forma rápida hacia contenidos más difíciles de detectar debido a su mayor realismo, como es el caso de los 'deepfakes', que son video-montajes hiperrealistas que manipulan el mensaje o la acción de una persona, aplicando herramientas y técnicas digitales muy avanzadas. El resultado que se consigue suele parecer muy real.

- ¿Cómo debo reaccionar ante una noticia falsa?

Conocer que las noticias falsas existen y que están presentes en nuestro día a día forma parte de la realidad que nos ocupa a los ciudadanos del siglo XXI. Pero esto no debe coartarnos ni restringirnos la libertad de uso y convivencia en la red.

Ya hemos visto algunos trucos que nos ayudan a identificar los bulos y falsas noticias. A continuación veremos cómo reaccionar ante una posible noticia falsa, según nos recomienda el Centro de Seguridad en Internet para menores de edad en España, más conocido como Internet Segura for Kids (IS4K):

1. Transmitir calma y prudencia. Los menores deben aprender a actuar en Internet, como en la vida real, de forma reflexiva y cauta. Merece la pena dedicar unos minutos a analizar la información antes de confiar en un contenido.

2. Contrastar la información. Comprobar la veracidad de la noticia, observando si está publicada en sitios de reconocido prestigio informativo, y desconfiando de aquellos medios que parezcan poco profesionales. Podemos apoyarnos en páginas web especializadas en verificación de información (fact-checking).

3. No compartir las noticias falsas. Es recomendable eliminarla del dispositivo y evitar su difusión descontrolada. Rompiendo la cadena estamos impidiendo que otras personas reciban la información.

4. Reportar la noticia falsa. Las redes sociales y muchas páginas web ya ofrecen la opción de denuncia de estos contenidos desde la propia publicación. También podemos contactar con los administradores de la web, o con entidades especializadas en verificación de información, como algunas de las anteriormente mencionadas, para avisar del riesgo de difusión.

5. Informar a nuestros contactos. Tanto la persona que la ha enviado, como las personas receptoras de la misma, agradecerán saber que se trata de un contenido falso. Podemos indicarles las características o motivos que nos han permitido reconocer la noticia falsa o bulo.

6. Pedir ayuda a una persona de confianza. A menudo, las temáticas y razonamientos que se esconden detrás de las fake news pueden resultar demasiado complejas y escapar a la comprensión de los menores o de aquellos usuarios noveles. Crea un entorno cotidiano seguro para hablar con naturalidad y sin miedos de estos temas con la familia y amigos. Ante cualquier sospecha de duda, se puede denunciar llamando a través de la Línea de Ayuda en Ciberseguridad de INCIBE en el número gratuito y confidencial 017, disponible los 365 días del año en horario de 9:00 – 21:00.

4. Actividades

- Un ejemplo de 'deepfake' es el anuncio publicitario de Cruzcampo titulado 'Con mucho acento' con Lola Flores como protagonista. Si quieres saber cómo se hizo pincha en este enlace. ¿Sabrías reconocer un vídeo manipulado? Sigue los consejos de la OSI para detectarlo.

- La desinformación sobre la pandemia ha aumentado la difusión de bulos como aquel que decía que la ingesta de agua tibia prevenía la infección por coronavirus. Visita las páginas web de Efe Verifica, Maldita, Newtral, y la sección de 'Avisos de Seguridad' de la Oficina de Seguridad del Internauta (OSI) y comprueba si alguna de estas plataformas de verificación ya han desmentido alguna noticia que hayas recibido por redes sociales y creas que es falsa.

4. Más información

- Debemos diferenciar entre la información y la sátira. Un ejemplo de ello es 'El Mundo Today' un diario satírico online, cuyo contenido es totalmente ficticio y humorístico, pero usando el formato de prensa tradicional para crear la parodia.

- Resulta de utilidad consultar la web 'Infopirina', una herramienta digital para combatir la desinformación, creada por la Asociación de Universidades Populares de Extremadura (AUPEX). Esta página aúna en un mismo lugar conceptos, datos, enlaces de interés, consejos y un test para medir nuestro grado de inmunidad ante las noticias falsas.

SESIÓN 4
FILTRO BURBUJA

1. Contexto

- ¿Cómo nos informamos actualmente?

  El 78,5% de la población andaluza utiliza Internet para estar al día de la actualidad, según el Barómetro Audiovisual de Andalucía 2020 (BAA), elaborado por el CAA. Tras los diarios digitales, al que recurren un 59,5% de los encuestados para obtener información, el 47% de los usuarios andaluces de Internet afirma que lo hace a través de las redes sociales. Le sigue en orden de preferencia el uso del WhatsApp, con un 21,9%, mientras que un 7,1% accede a la información a través de alertas o suscripciones a algún medio o servicio de noticias.

- ¿Por qué aumenta su uso frente a otros medios?

  La instantaneidad, gratuidad y facilidad de acceso a las noticias son los motivos principales, pero también la diversidad de opiniones que ofrece.

De hecho, los andaluces otorgan a Internet el mayor grado de confianza respecto al pluralismo político (5,4), seguido de la radio (5,3) y, en último lugar la televisión con una media de 4,8, según el BAA. En concreto, este estudio revela que un 27,4% de las personas consultadas posicionan el pluralismo de Internet en el segmento 6–10 y el 15,5% lo hacen en el segmento 5.

- ¿Internet me garantiza una información plural?

En teoría la pluralidad está garantizada. La Red te permite acceder de forma rápida y gratuita a cientos de noticias sobre un mismo asunto. Introducir las palabras clave de un hecho en el buscador de Google nos ofrecerá resultados procedentes de diarios digitales, webs de televisiones, radios, blogs… Con suscripción puedes leer una amplia variedad de periódicos y revistas digitales europeas a través de Kiosco y más. Sin embargo, ¿leemos más de un diario?, ¿contrastamos las noticias que recibimos por Whatsapp o las redes sociales? Seamos sinceros, la falta de tiempo o la costumbre hace que no aprovechemos esas herramientas y confiemos en

una única fuente, a la cual recurrimos con frecuencia.

- ¿La información que circula en la Red es fiable?

  No siempre lo es. Hay empresas, grupos de presión, partidos políticos que utilizan la Red en su propio beneficio propagandístico o publicitario. Los andaluces somos conscientes de ello, porque un 39,5% de las personas consultadas en el BAA creen que Internet está politizado. Lo cierto es que debemos adquirir una actitud crítica ante los mensajes que recibimos, ya que las nuevas tecnologías facilitan la proliferación de noticias falsas mediante la manipulación de imágenes e incluso, vídeos. Debemos tener cuidado de no ser víctimas o cómplices de bulos o mensajes de discurso de odio.

- ¿Qué es el discurso de odio?

  La pandemia mundial ha creado un clima propicio para el aumento del discurso de odio en la Red.

Nos referimos a mensajes peyorativos hacia una persona o colectivo concreto, basados en estereotipos o actitudes intolerantes. Según el informe del CAA sobre la expansión del discurso de odio en Internet durante los meses de confinamiento en 2020 se propagaron vídeos en Youtube que acusaban a la comunidad asiática como causante de la creación y propagación del coronavirus. Otros vídeos señalaban a la etnia gitana como "irresponsable" en el cumplimiento de las medidas para frenar la propagación de la COVID-19, incluso, se detectaron ataques xenófobos dirigidos contra las personas migrantes y refugiados.

- ¿Por qué es necesario contrastar la información?

En los últimos años la polarización política se ha incrementado, es decir las distancias entre ideologías aumentan, creando un clima constante de crispación social, que dificulta el consenso y fomenta la parcialidad de la información. Es algo que se aprecia en los titulares de distintos medios, que en ocasiones distan mucho, según su posicionamiento ideológico.

Es por ello que contrastar la información es una buena herramienta para obtener una información completa, libre de noticias falsas y discurso de odio.

2. Definición y características

- **Los mensajes y noticias que leo reafirman la misma idea, ¿esa es la correcta?**

Tendemos a pensar que no es necesario dudar de la veracidad de los mensajes que recibo porque coinciden entre sí. Creemos que navegamos libres por la Red, que no hay censura, pero Internet nos marca el camino. Dirige nuestras decisiones. No hay nada aleatorio o casual. Eso se debe al filtro burbuja o burbuja de filtros, término acuñado en 2011 por el ciberactivista Eli Pariser en su libro homónimo. Así explica él mismo este fenómeno: "Internet nos muestra lo que piensa que queremos ver y no necesariamente lo que tenemos que ver. El filtro burbuja es el universo propio, personal y único de información que vives en la Red. Lo que haya en el filtro burbuja depende de quién eres y lo que haces.

El problema reside en que tú no decides qué entra en tu filtro. Y lo más importante es que no vemos qué es lo que se elimina".

En otras palabras, el filtro burbuja o burbuja de filtros es el proceso mediante el cual un servidor web muestra al usuario resultados ajustados a sus intereses, tomando información previa como su ubicación, gustos o búsquedas realizadas. Aunque puede resultar una herramienta útil de selección personalizada también conlleva riesgos porque puede provocar el aislamiento intelectual del usuario. El internauta recibe noticias que reafirman sus creencias y, por tanto, obtiene una perspectiva incompleta de la realidad al no contrastar con contenidos de diferente ideología. Por ejemplo, la existencia del filtro burbuja, se puede comprobar haciendo la misma búsqueda distintas personas, las cuales puede que obtengan resultados distintos.

- ¿Cómo se hace esa selección?

Mediante los algoritmos de búsqueda de Internet

y las cookies se va generando información sobre tu navegación. Páginas que visitas, cuánto tiempo… Un algoritmo es una operación lógica que realiza un cálculo para dar solución a un problema. Los algoritmos recurren a los datos, que consciente e inconscientemente facilitamos en la Red, para personalizar los resultados de nuestras búsquedas. Esos datos se extraen, entre otras cosas, a través de las cookies, que son archivos de las páginas webs que guardan los datos de navegación, es decir, recuerdan tus preferencias y proporcionan contenido basado en tu ubicación. Esa es la razón por la que te aparece publicidad personalizada, es decir, anuncios de un producto tras haber hecho una búsqueda del mismo.

- Ventajas e inconvenientes del filtro burbuja

El filtrado no hace sino reforzar las creencias del usuario a base de noticias o informaciones alineadas a su postura ideológica, lo cual le incapacita a la hora de contrastar diversas perspectivas o valorar realmente lo que ocurre a su alrededor.

- Argumentos a favor:

A gusto del consumidor. El usuario disfruta de una experiencia ajustada a sus gustos, a lo que realmente le apasiona o interesa. Para quienes acceden de manera puntual a la Red, puede ser beneficioso encontrarse directamente con aquello que les atrae.

Simplificación. La navegación se hace mucho más intuitiva y accesible para el internauta, lo cual puede agradecerse a la hora de afrontar el inmenso universo online.

Instantaneidad. El filtro burbuja tiene la capacidad de aligerar los plazos y procesos de búsqueda, sirviendo en bandeja de plata la información requerida, a la que se llega mucho más rápido y de forma sencilla.

Individualización. Antaño, la información y el entretenimiento ofrecían parrillas limitadas y poco flexibles para el usuario. Sin embargo, Internet abre la puerta a la construcción de un menú audiovisual absolutamente personalizado.

- Argumentos en contra:

Problemas de privacidad. Para generar el filtrado, la web recurre a nuestras búsquedas anteriores, a nuestra ubicación o, incluso, a nuestros 'Likes' en redes sociales. Es, por tanto, evidente que el desarrollo del filtro burbuja pone nuestra intimidad en entredicho.

Distorsión de la realidad. Como se apuntó anteriormente, el compendio de informaciones que llegan al usuario debido al filtro burbuja suele estar profundamente sesgado, lo cual impide el debate y genera una realidad ficticia y alejada del mundo original.

Herramienta de censura. Aunque parezca una obviedad, el hecho de recibir solo un tipo de información impide que te lleguen otras. Por mucho que se alejen de tus gustos, si la Red impide la transmisión de ciertos contenidos, los está censurando.

Homogeneización social. Contradictoriamente, las redes sociales, creadas originalmente para conectar gente de muy diversa índole, recurre al filtro burbuja, atentando contra sus propios fundamentos. Nuestro comportamiento en ellas nos une a perfiles similares con facilidad, pero no así con quienes piensan distinto.

Espacio para las noticias falsas. El ser humano goza de una peligrosa tendencia a necesitar que le den la razón. Poco hay más gratificante que leer en un artículo exactamente lo que piensas, más allá de la veracidad del mismo. Tomando tal premisa, la práctica del filtro burbuja es ideal para la proliferación de bulos.

3. Herramientas prácticas

- **¿Cómo puedo salir del filtro burbuja?**

La peligrosidad del filtro burbuja se hace patente si tenemos en cuenta que Internet es para muchos usuarios la base o su única fuente de información. Por lo tanto, es notablemente perjudicial que ésta llegue sesgada y notablemente filtrada mediante criterios unipersonales.

Algunas recomendaciones para erradicar o disminuir los riesgos del filtro burbuja son:

Apuesta por la diversidad. El usuario es tan responsable del filtro burbuja como la web. Aceptamos sus aspectos negativos porque deseamos los positivos. Es necesario, consecuentemente, hacer autocrítica y construir, para nosotros mismos, un espacio online mucho más sano y enriquecedor, diversificando nuestras búsquedas. Es tan fácil como dar de vez en cuando 'Likes' a noticias opuestas a tu ideología para ampliar el abanico de informaciones que puedas recibir.

Alterna buscadores. Existe cierta tendencia a utilizar un único motor de búsqueda, por diversos motivos. Bien sea porque nos parece estéticamente mejor o porque sea más intuitivo, no solemos cambiar de navegador. Es aconsejable, en este punto, despojarnos de esa mentalidad e ir alternando entre los distintos buscadores existentes.

Rechaza las 'cookies'. Cuando accedes por primera vez en una página web aparece una ventana emergente que te pregunta si quieres aceptar las 'cookies'. La ventana no te permite ver por completo la página hasta que no decides, de ahí, que los usuarios suelan aceptar sin más esa advertencia. Te recomendamos que dediques unos segundos a ese mensaje y desactives las 'cookies' para que no se rastree tu navegación dando a 'Rechazar todo' o 'Guardar mis preferencias'.

Instala extensiones. Uses el buscador que uses, tienes la posibilidad de potenciarlo y hacerlo más seguro con la aplicación de ciertas extensiones como AdBlock, que trabajan contra la acción del filtrado. Es tan sencillo como instalarlas.

Recurre a verificadores de noticias. Haz que tu información sea lo más amplia posible y no te quedes satisfecho con lo primero que te llegue. Ante la duda, puedes consultar en webs dedicadas a desmentir noticias falsas como: Efe Verifica, Maldita, Newtral, Salud sin Bulos o AFP España, entre otros.

4. Actividades

- Lee los titulares de una misma noticia en distintos medios de comunicación ¿Aprecias diferencias?

- Compara el apartado de noticias de tu teléfono móvil con el de otra persona ¿Coinciden?

- Si tienes una red social revisa tu perfil y analiza si las informaciones que recibes son de ideologías opuestas.

- Haz una búsqueda en Google y apunta los 5 primeros resultados que obtienes. Pide a alguien que haga lo mismo. ¿Concuerdan los resultados?

5. Más información

- El filtro burbuja o burbuja de filtros también se le conoce como burbuja informativa o burbuja de opinión. Son distintos términos para un mismo fenómeno, sobre cuyas negativas consecuencias reflexionan distintos académicos, tal y como se expone en los vídeos enlazados.

- Otro concepto relacionado con el filtro burbuja y la polarización de la sociedad es la cámara de eco, un espacio social que amplifica y reitera una idea, que no es rebatida al estar dentro de un sistema cerrado, donde apenas tienen cabida las visiones diferentes.

- Estar inmersos dentro de un filtro burbuja dificulta nuestras posibilidades de estar bien informados al recibir contenidos sesgados. Es por ello que recomendamos consultar Learn to Check, un proyecto pedagógico contra la desinformación.

SESIÓN 5
CÓMO CONSTRUIR MI YO DIGITAL

1. Definición

Siempre que se navega por Internet vamos dejando información sobre nosotros mismos en los diferentes sitios que visitamos, lo que indica a otras personas cómo somos, qué opiniones tenemos, gustos, aficiones, etc. Todo esto forma parte de lo que se conoce como mi yo digital, huella digital o identidad digital.

Todos tenemos una identidad, algo que hace que el resto de personas nos identifique rápidamente y, que a la vez, nos hace distintos de los demás. Se nos puede identificar por nuestra profesión, amistades, familia, físico, forma de escribir o de vestir... En el mundo digital sucede algo parecido, ya que al participar en las funcionalidades de la Red, ofreces una representación de ti mismo, que es como tu «yo» virtual, y lo vas creando con tus actividades y las de los que interaccionan contigo.

Si eres un usuario habitual de Internet, habrás utilizado algunos servicios como foros, suscripciones a sitios web, redes sociales, blogs, habrás subido imágenes y vídeos, comentado noticias... Por tanto, puede haber una gran cantidad de datos personales tuyos existentes en la Red.

Una misma persona puede tener diferentes identidades utilizando herramientas diversas, o tener sólo una. Al igual que en el mundo real, se pueden emplear identidades diferentes para distintos contextos. Por ejemplo, alguien puede tener la identidad de un seguidor de un equipo de fútbol, de un fan de un cantante, ser voluntario de una ONG, amigo de una persona... Y todas esas identidades pertenecen a esa misma persona.

Esta identidad digital, puede coincidir o no con la identidad del mundo real, es decir, puede haber características asociadas a tu identidad digital que no se correspondan contigo, por lo que, para muchas personas, resulta importante gestionar la propia reputación y privacidad en la Red.

La identidad digital, es tu tarjeta de presentación ante los demás. Es por esto que se recomienda seguir una línea coherente entre tu vida off-line y tu identidad dentro del mundo on-line. Con esto se evitarán confusiones y malos entendidos. Al repasar la identidad digital de alguien se obtiene una aproximación al perfil de esa persona.

Conviene tener en cuenta que todo lo que se publica, habla de ti, por tanto aporta impactos negativos tener un comportamiento o publicar opiniones en el entorno digital, que no seas capaz de defender fuera de la red.

Toda la información que conforma tu identidad digital, se encuentra fragmentada en los diferentes servicios que utilizas: puedes tener opiniones en un foro, perfil en una red social, artículos en un blog, etc. También puede haber información sobre ti que hayan publicado otras personas, imágenes que hayan subido o comentarios que hagan en los que se te mencione.

Es posible conocer tu identidad digital, mediante el Egosurfing, que consiste en buscar información sobre uno mismo en Internet, con el objetivo de comprobar qué es lo que aparece de manera pública en la Red sobre nosotros. Podemos utilizar alguna de las herramientas que hay creadas para tal fin:

- Buscadores: te muestran toda la información relativa a una persona.

- Presencia en Internet, o como se llama en inglés, Me on the Web, es una nueva herramienta de Google que permite configurar alertas para recibir notificaciones en tu dirección de correo si alguno de los datos personales que indiques aparecen en Internet (nombre, dirección de correo...)

2. Herramientas prácticas

A) Uso personal - Uso profesional

Internet y las redes sociales han demostrado ser una herramienta satisfactoria y de gran al-

cance. La publicación de imágenes, vídeos y chats interactivos son un escaparate digital para muchas organizaciones que se valen de estas aplicaciones para llegar a un gran número de usuarios, de una manera mucho más personal si lo comparamos con cómo se presentaba cualquier organización o entidad antes de la llegada de la creación de su propia página web. Aporta gran valor al uso que damos a estas herramientas, si entendemos bien el uso que queremos darle y sobre todo en qué contexto. Existen grandes diferencias a tener en cuenta si le damos un uso únicamente personal frente al uso profesional.

USO PERSONAL	USO PROFESIONAL
Conoces a tu interlocutor	Tu interlocutor es un desconocido
Lenguaje coloquial, informal y cercano	Lenguaje más formal
Tu interlocución se muestra relajada en cuanto a las formas	Prestas más atención a seguir unas formas en tu interlocución
Compartes información personal	No compartes información personal
Incluyes imágenes de tus seres queridos	No incluyes imágenes de seres queridos
Utilizas apodos o nombres cariñosos	No utilizas apodos o nombres cariñosos
Lenguaje no verbal no tan presente	Cuidas más el lenguaje no verbal

B) Conocer bien las reglas de juego

Al igual que cuando comenzamos a circular por vez primera, no nos lanzamos a la carretera sin conocer las normas establecidas por el código de circulación, es conveniente al incorporarnos al mundo digital, tener presente, cómo funciona y ser consciente de que no se trata de un camino que cada uno de nosotros recorre solos, sino que nos incorporamos a una comunidad compartida por más integrantes donde tener sentadas unas buenas prácticas, hará que tengamos una experiencia en la red saludable y satisfactoria.

Mantener una actitud prudente, nos ayudará a pensar antes de hacer clic y no navegar de manera impulsiva. La prevención pasa por tomar diversas pautas de seguridad, tanto dirigidas a reducir las posibilidades de que los riesgos se conviertan en problemas reales, como para limitar las consecuencias negativas en caso de que así sea.

Las grandes compañías que operan en el entorno digital, a las que se les denomina GAFA (acrónimo de Google, Apple, Facebook y Amazon) son empresas cuyo fin no es otro más que ganar dinero. Este principio comercial, que es tan lícito como el de cualquier otra empresa comercial, es la razón de su existencia, pero tenemos que saber los usuarios qué es lo que estas empresas venden y qué papel jugamos nosotros en este escenario. La industria tecnológica invierte cada año cantidades ingentes de dinero cuya finalidad no es otra que conseguir capturar nuestra atención para que cada uno de nosotros (clientes potenciales) pase el mayor tiempo posible conectado. Nosotros somos sus clientes y generamos ingresos cada vez que hacemos clic o creamos contenido o descargamos una imagen o un video, etc. También generan ingresos los servicios de pago conocidos como Premium, que ofrecen un servicio mejorado, con mayores ventajas frente al servicio estándar. Por tanto cuando estamos interactuando estamos haciendo que esas empresas generen ingresos.

Llegados a este punto es fácil preguntarse ¿dónde está el negocio, si en internet todo lo que hago es gratuito? La respuesta es bien sencilla y conoceremos una palabra que será importante tener en cuenta en adelante, el negocio son nuestros DATOS. Nuestra información personal vale mucho de ahí que haya quien denomina a los datos como el nuevo oro del siglo XXI. Al conocer nuestros datos, se puede conocer con exactitud nuestros gustos y necesidades por lo que las nuevas estrategias de marketing se aproximarán a ser capaces de vendernos aquello justo que necesitamos en el tiempo y forma apropiada para que lo compremos o nos suscribamos o lo compartamos. Esto se consigue con el diseño de algoritmos que relacionan nuestras búsquedas frecuentes con nuestros datos personales aportados a la hora de abrir una cuenta en redes sociales o suscribirnos a algún portal.

C) Haz que tu tiempo sume

El uso frecuente de las pantallas y la velocidad de Internet nos imponen un ritmo frenético y confuso. Por la propia naturaleza de lo digital, donde el lenguaje se vuelve muy intuitivo y atractivo para nuestro cerebro, mucho más que los formatos lineales analógicos, es fácil perder la noción del tiempo. El hecho de utilizar lo que llamamos hipervínculos anexados en la redacción de textos, hace que una simple consulta que podría llevarnos unos minutos, vea triplicado su tiempo porque de una página saltamos a otra y esta a su vez a otra, sin fin. Como sabemos que no todo lo que hay en internet puede interesarte, es conveniente concentrar nuestra atención dirigiendo hacia dónde queremos llevar nuestra búsqueda.

Como el tiempo es limitado para todos, se recomienda ponernos una limitación a la hora de iniciar una consulta. Con esto se desarrolla la habilidad de autocontrol, marcándonos por ejemplo unos 30 minutos y una vez que estos transcurran finalizamos la navegación.

D) No te refugies en el anonimato

Llegados a este punto ya conocemos la gran viralidad que pueden tener los contenidos en Internet. Es muy fácil que algo que digamos o hagamos en línea pueda llegar a muchas personas que no esperamos, tanto si se trata de algo positivo como negativo. Pero ojo, porque el mundo digital facilita el poder participar incluso interactuar sin ser vistos, ampliando el campo del anonimato. Se aconseja que nuestro comportamiento sea coherente con quienes somos, por lo que todo aquello que no seas capaz de decir ni hacer en la vida real, no lo hagas refugiado en ese anonimato que ofrece internet. Ese anonimato nos hace poder estar en contacto con personas que no forman parte de nuestro entorno, acercándonos a ellas con facilidad.

Existe una teoría que dice que cada ser humano está conectado con cualquier otro por una cadena de unos 6 conocidos de media. Sin embargo, una investigación realizada por Facebook encontró que dentro de su red social

una persona podía llegar a cualquier otra pasando sólo por 3,57 personas más. Dicho de otra forma, entre los amigos, de los amigos de mis amigos podría estar cualquier persona. Las redes sociales son herramientas muy útiles para poner en contacto a las personas con las ventajas que eso supone a la hora de compartir aficiones e intereses comunes, aunque no podemos olvidar el hecho de que el contacto con personas desconocidas supone un riesgo para la seguridad, (engaños, chantajes, fraudes etc.). Normalmente un contacto de tu amigo, no es tu amigo. Al igual que una persona con la que contactas tan solo de forma telemática, no es tu amiga. Conviene tenerlo en cuenta para evitar situaciones incómodas.

E) Vela por tu seguridad

Uno de los pasos previos para acceder a la mayoría de redes sociales, foros o chats es crear un perfil o una cuenta a la que accedes con una contraseña personal también conocida como password.

En general se trata de construir contraseñas robustas y distintas en cada página. Al menos con 8 caracteres, combinando mayúsculas, minúsculas, números y símbolos. Sin incluir palabras reales, ni información personal (nombres, DNI, teléfono, fecha de nacimiento…), ni letras o números consecutivos (abc, 123).

Además, se deben cuidar, no compartirlas con nadie, ni teclearlas delante de otras personas o en ordenadores públicos. Cambiarlas de vez en cuando, guardarlas en gestores de contraseñas, usar teclados virtuales y verificación en dos pasos (si es posible). Configurar las opciones de recuperación (sin respuestas sencillas a las preguntas de seguridad, con un número de teléfono de recuperación). Es conveniente, configurar las opciones de privacidad de las redes sociales, indicando que por defecto solo los contactos puedan ver lo que compartimos, limitando las búsquedas desde el exterior (por ejemplo Google o Bing) e incluso, seleccionando a los

usuarios o grupos de usuarios que puedan ver solo algunas cosas de las que compartimos.

Cada uno de nosotros decidimos la información que damos y los mensajes que compartimos en Internet. Si nos centramos en darles un tono positivo, dejaremos una huella mejor en la Red y en los demás, mejorando nuestras relaciones y evitando problemas. Conseguiremos humanizar la tecnología y que se convierta en un medio de disfrute que nos facilite y no nos complique la vida.

3. Actividades

- Prueba a activar la alerta de Presencia en Internet de Google para recibir notificaciones si tus datos personales se muestran públicamente.

- Repasa en 5 minutos tu identidad digital, consultando los perfiles que tengas en diferentes redes sociales y aplicaciones, así como los últimos movimientos que hayas realizado en webs, blogs, consultas en buscadores, compras, etc…..

- ¿Te sientes identificado con tu huella digital (lo que se ve de ti en la Red) ¿Realmente eres lo que publicas?

4. Más información

- El universo de Internet se mueve a gran velocidad, de ahí, que en tan sólo un minuto se llevan a cabo millones de interacciones en las plataformas y aplicaciones más populares. En concreto, en 60 segundos del año 2021 se suben 500 horas de contenidos en Youtube, se producen 2 millones de visualizaciones en Twitch, 5.000 descargas en Tik Tok, se envían 69 millones de mensajes por WhatsApp, hay 28.000 suscriptores viendo Netflix y se comparten 695.000 historias en Instagram, según una infografía realizada por @LoriLewis y @OfficiallyChadd.

SESIÓN 6 GESTIONES ADMINISTRATIVAS ONLINE

1. Contexto

La mayoría de la población andaluza (69,6%) utiliza Internet habitualmente, según el Barómetro Audiovisual de Andalucía 2020 (BAA), elaborado por el CAA. Este estudio revela que no sólo accedemos a la Red para informarnos o entretenernos, porque el 23% de los encuestados también realiza gestiones administrativas online, sobre todo bancarias.

Este dato manifiesta una tendencia, que sospechamos irá en aumento los próximos años, ya que las nuevas tecnologías facilitan trámites administrativos que antes requerían desplazarnos y esperar largas colas, mientras que ahora sólo necesitamos un dispositivo electrónico (móvil, ordenador o tableta) conectado a Internet.

Pedir una cita médica, consultar los resultados de una analítica, hacer una transferencia bancaria o registrar documentación en una institución son algunas de las muchas interacciones telemáticas que podemos desarrollar en la modalidad online de forma gratuita y cómodamente desde casa. Conozcamos algunos recursos digitales a nuestro alcance para realizar todas esas gestiones:

2. Definiciones y características

El Sistema Sanitario Público de Andalucía pone a disposición de la población andaluza recursos telemáticos para facilitar los servicios de atención sanitaria, nos referimos a ClicSalud+, Salud Responde y Salud Andalucía. Conozcamos las prestaciones que ofrecen cada una:

ClicSalud+ es una web con una sesión personalizada para cada usuario que permite realizar todo tipo de gestiones relacionadas con la atención sanitaria. Podemos resumirlas en los siguientes puntos:

- Citas, pruebas y listas de espera: Solicitud, cambio o anulación de cita previa para consultas de atención primaria (medicina de familia o pediatría), enfermería ·o vacunas. Acceso a la consulta de la información relativa a citas hospitalarias, pruebas diagnósticas e inscripción en el registro de demanda quirúrgica.

- Histórico de medicación, vacunas, bajas, etc: Consulta de los tratamientos prescritos electrónicamente, de las vacunas administradas a partir del año 2010, analíticas realizadas, incapacidades laborales, informes de hospitalización, consultas externas o urgencias hospitalarias, y pruebas de imagen que consten en su historia clínica electrónica.

- Certificado COVID: Solicitud del Certificado COVID Digital que posibilita la libre circulación por la Unión Europea, acreditando la vacunación, el resultado negativo en una prueba o la recuperación tras padecer la enfermedad.

- Cambios de acceso a los servicios: Tramitación de solicitudes tanto de elección de un profesional de medicina de familia en nuestra propia localidad, como de desplazamiento temporal que permite elegir el centro y profesional de atención primaria de otro municipio andaluz con validez entre un mes y un año de duración

- Renovación de la tarjeta sanitaria: Gestión de la renovación de una tarjeta sanitaria en caso de deterioro, pérdida o robo, la cual se recibe por correo ordinario en el domicilio del usuario solicitante.

- Datos personales al día: Comprobación de nuestros datos personales de contacto y actualización de los mismos, en caso de cambio de domicilio, correo electrónico o teléfono, por ejemplo.

Estos mismos servicios también los ofrece Salud Responde, un recurso multicanal de asistencia sanitaria disponible las 24 horas del día, todos los días del año y desde cualquier lugar de Andalucía. Se puede acceder a través de los siguientes canales:

-Número de teléfono: 955 545 060

-Email: saludresponde@juntadeandalucia.es

-Aplicación móvil homónima, disponible para su descarga gratuita en Google Play para los sistemas operativos Android y en iOS para los iPhones.

Esta aplicación requiere darse de alta como usuario introduciendo el número de tarjeta sanitaria, fecha de nacimiento y DNI. Entre su amplia cartera de servicios destacamos los consejos sanitarios sobre alergias, gripe, coronavirus, asma o los efectos del calor en la sección 'Salud Andalucía 24 horas'.

Asimismo, resulta de utilidad inscribirse en la sección 'Envejecimiento Saludable' para recibir mensajes para la promoción del bienestar físico y emocional, la autonomía personal y la prevención del aislamiento.

En cuanto a la aplicación móvil de descarga gratuita, Salud Andalucía, es un catálogo que reúne en un mismo espacio la actualidad sanitaria, herramientas sobre la COVID-19 (certificado, autoevaluación y asistente virtual) y todas las aplicaciones sobre salud homologadas por el Sistema Sanitario Público de Andalucía, incluidas ClicSalud+ y Salud Responde. El resto de apps son:

- Dona Sangre, un buscador con las localizaciones más cercanas al usuario donde donar sangre y que facilita información sobre las campañas de donación.

- Mi Prescripción, un asistente para gestionar tratamientos, ya sean prescritos o no, con la posibilidad de activar avisos de las tomas del medicamento.

- Vacunas, histórico de las vacunas que ha recibido el usuario y sus beneficiarios, que incluye información general sobre planes de vacunación.

- Radar COVID, sistema de aviso a la ciudadanía, con garantías de anonimato, del contacto con una persona contagiada de coronavirus.

Los nuevos hábitos adquiridos por la pandemia mundial han impulsado los sistemas de pago digitales con el fin de evitar el contacto interpersonal mediante el uso de efectivo. La aplicación Bizum es un sistema de pago a través del móvil que realiza transferencias instantáneas tanto a particulares como a ONGs y comercios online asociados.

No requiere conocer la cuenta bancaria del receptor del dinero enviado, sólo su número de teléfono móvil. Para acceder a ella es necesario tener descargada la aplicación móvil de nuestro banco y dentro de ella buscar la pestaña correspondiente a este servicio de pago. En general los envíos oscilan entre un mínimo de 50 céntimos y un máximo 1.000 euros, aunque estos límites varían en cada entidad bancaria. Dentro de Bizum hay que buscar la opción 'Enviar y recibir dinero', introducir el número de móvil o seleccionar el destinatario de nuestra lista de contactos, indicar el importe y pinchar en 'Enviar'.

La mayoría de las entidades bancarias españolas están afiliadas a esta aplicación, que cumple con las medidas de seguridad exigidas para este tipo de transacciones monetarias. . No obstante, la Oficina de Seguridad del Internauta (OSI) viene advirtiendo en los últimos años de algunas estafas de falsos envíos de dinero por Bizum con la intención de conseguir información personal clave para violar nuestra seguridad.

Uno de esos fraudes se realiza a través de avisos por WhatsApp o llamadas telefónicas de un supuesto reembolso de gran importe por parte de la Seguridad Social. El estafador asegura que vamos a recibir el dinero por Bizum y para cobrarlo nos pide datos personales y bancarios. Para evitar ser víctimas de esta clase de timos hay que tener en cuenta estos consejos:

- Tus credenciales no son necesarias para cobrar. Este servicio de pago no exige introducir las credenciales bancarias del receptor para recibir dinero. Si el mensaje recibido lo requiere, estamos ante un fraude. Si el receptor no es usuario de esta aplicación recibirá un SMS con unas instrucciones para recibir el dinero, sin necesidad de dar información personal.

- No aceptes solicitudes de envío de dinero sospechosas. Si no tienes constancia previa de que un conocido o familiar te vaya a pedir dinero por esta aplicación, rechaza la solicitud porque podría ser una estafa.

- Revisa regularmente tu cuenta bancaria. Si en los detalles de pago de la aplicación de tu banco aparecen pagos hechos por Bizum que no reconoces, ponte de inmediato en contacto con el servicio de atención al cliente de tu entidad bancaria para saber cómo actuar.

El registro oficial de documentación dirigida a la Administración Pública también se ha adaptado a la modalidad digital mediante el Registro Electrónico Común (REC), una aplicación que permite registrar telemáticamente solicitudes o comunicaciones dirigidas a cualquier organismo integrado en el Sistema de Interconexión de Registros (SIR). Son muchas las instituciones dentro de SIR: todos los ministerios, gobiernos autonómicos, entidades locales, universidades, el Defensor del Pueblo, la Agencia Española de Protección de Datos, etc. Para asegurar la confidencialidad de la gestión, este registro únicamente puede realizarlo la persona interesada, no siendo posible delegar en gestores o asesores que actúen en nombre de terceros.

Este sistema destaca por su flexibilidad horaria, al permitir el registro las 24 horas del día durante los 365 días del año. La solicitud electrónica permite hasta un máximo de 5 archivos adjuntos en distintos formatos (doc., jpg, pdf, txt, png, tif…), cuyo tamaño conjunto no puede superar los 15Mb. Además, este trámite administrativo online tiene todas las garantías de seguridad y efectividad, generando un acuse de recibo electrónico para que el usuario pueda justificar el registro. Ese recibo contiene el número de registro individualizado, la fecha y hora de presentación, copia del escrito enviado y en caso de archivos adjuntos, la enumeración y denominación de los mismos. Otra ventaja que ofrece REC es conocer el estado de nuestra solicitud seleccionando la opción de 'Notificación' ya sea por SMS y/o correo electrónico. Cualquier duda al respecto puede resolverse a través de los siguientes canales de atención ciudadana:

-Teléfono 060
-Buzón de Atención
-WebChat

3. Herramientas prácticas

A pesar de las ventajas de los trámites administrativos digitales, entre los mayores de 65 años son minoría (un 12,8%) aquellos que emplean estos nuevos recursos a su disposición, según el BAA 2019. Las reticencias de la población de edad avanzada quizás estén motivadas por el desconocimiento de estas nuevas herramientas o el miedo a la vulneración de su privacidad. Este último motivo, el temor a los ciberataques, supone la mayor preocupación de la población andaluza respecto al uso de Internet, con un 58,4% de las respuestas obtenidas en el BAA 2020.

Esa inquietud es razonable, pero cabe señalar que las sedes electrónicas de los organismos públicos exigen el acceso a través del DNI electrónico o Certificado Digital, de esta manera se avala la seguridad en la transmisión de la información y la autenticidad de la persona que realiza la gestión, evitando así la suplantación de identidad.

El Certificado Digital de Persona Física es un documento identificativo de carácter individual y electrónico, expedido por la Fábrica Nacional de Moneda y Timbre (FNMT), que garantiza que sólo nosotros y nuestro interlocutor podemos ver los datos que compartimos en una aplicación oficial, sin intervención de terceras personas. Mediante este certificado podemos identificarnos dentro de las páginas web oficiales de los organismos nacionales, autonómicos y locales para llevar a cabo todo tipo de gestiones online con la Administración Pública. Junto con la firma electrónica de documentos y formularios oficiales de todo tipo, otros trámites que permite realizar este certificado son:

-Presentación y liquidación de impuestos
-Presentación de recursos y reclamaciones
-Cumplimentación de los datos del censo
-Consulta e inscripción en el padrón municipal
-Consulta de multas de circulación
-Consulta y solicitud de subvenciones
-Consulta de asignación de colegio electoral
-Actuaciones comunicadas

El Certificado Digital se puede obtener de dos formas diferentes, siguiendo los pasos indicados por la FNMT:

A) Utilizando el DNI electrónico

"Configuración previa. Para renovar el certificado es necesario instalar el software que se indica en este apartado.

Solicitud con Certificado. Asegúrese de tener un certificado válido con el que identificarse para solicitar su Certificado de Persona Física. Al final de este proceso le enviaremos a su correo electrónico el Código de Solicitud que necesitará para poder descargarse el certificado.

Descarga de su Certificado de Persona Física. Aproximadamente 1 hora después de la solicitud y haciendo uso del código de solicitud que le hemos remitido a su cuenta de correo electrónico, desde aquí podrá descargar e instalar su certificado y realizar una copia de seguridad (RECOMENDADO)".

B) Como archivo descargable en el ordenador

"Configuración previa. Para solicitar el certificado es necesario instalar el software que se indica en este apartado.

Solicitud vía internet de su Certificado. Al finalizar el proceso de solicitud, usted recibirá en su cuenta de correo electrónico un Código de Solicitud que le será requerido en el momento de acreditar su identidad y posteriormente a la hora de descargar su certificado.

Acreditación de la identidad en una Oficina de Acreditación de Identidad. Una vez completada la fase anterior y esté en posesión de su Código de Solicitud, para continuar con el proceso deberá Acreditar su Identidad en una de nuestras Oficinas de Acreditación de Identidad. Para su comodidad, puede usted hacer uso de nuestro servicio LOCALIZADOR DE OFICINAS".

"Descarga de su Certificado de Usuario. Aproximadamente 1 hora después de que haya acreditado su identidad en una Oficina de Acreditación de Identidad y haciendo uso de su Código de Solicitud, desde aquí podrá descargar e instalar su certificado y realizar una copia de seguridad (RECOMENDADO)".

Una vez tengamos instalado el Certificado Digital conviene hacer un uso prudente y responsable del mismo, siguiendo estos sencillos consejos de seguridad:

- Personal e intransferible: Al igual que no entregamos nuestro DNI a alguien para que se presente en nuestro nombre, no debemos dejar que alguien instale nuestro certificado en su equipo, ni compartir nuestras claves para que firme por nosotros. De lo contrario, ponemos en riesgo nuestra identidad digital.

- Uso privado: No debemos instalar el certificado en un ordenador de uso público o compartido con personas que no sean de plena confianza.

- Copia de seguridad: Es recomendable guardar una copia del Certificado Digital en algún dispositivo de almacenamiento (pendrive o disco duro externo) como medida de seguridad ante un posible robo, pérdida o fallo del ordenador en el que esté instalado.

En resumen, disponer de un DNI electrónico o Certificado Digital puede ser de mucha utilidad para realizar gestiones telemáticas como las aplicaciones sanitarias anteriormente explicadas o el registro online de documentación en la Administración Pública, que exigen disponer de estos identificadores para poder acceder a estos servicios.

4. Actividades

- Presta atención a las indicaciones de los tutoriales enlazados y prueba a:

  -Pedir cita previa en atención primaria

  -Consultar tu medicación prescrita electrónicamente

  -Elegir tu centro y profesional de medicina de familia

- ¿Sabes presentar un documento por el Registro Electrónico Común? Sigue los pasos de este vídeo explicativo.

- Churriana (Málaga) fue el escenario escogido para una divertida campaña publicitaria de Bizum. ¿Te animas a activarlo y probarlo?

- Practica a solicitar tu Certificado Digital de Persona Física por la modalidad software con la ayuda de estos consejos de la FNMT.

5. Más información

- Para cualquier duda sobre el funcionamiento de ClicSalud+, dispones de un interesante listado de videotutoriales.
- Si necesitas alguna aclaración o más detalles sobre la aplicación Salud Responde puedes llamar al 955 006 300 o ver este tutorial.
- Asimismo, puede ser de utilidad este vídeo sobre Salud Andalucía.
- Antes de registrar una solicitud por REC te recomendamos consultar su Manual de Usuario.
- El Manual de Solicitud del Certificado Digital también puede ayudarte a resolver las preguntas que tengas al respecto.

SESIÓN 7
COMPRAS ONLINE

1. Contexto y definición

Si ha habido un sector que ha experimentado una verdadera revolución con Internet, éste ha sido el comercio. La tecnología ha provocado profundos cambios en nuestros hábitos como consumidores y compradores. En la actualidad, uno de cada tres españoles realiza sus compras por Internet lo que mueve un volumen de negocio en nuestro país de más de 51.500 millones de euros.

Esta posibilidad ofrece numerosas ventajas tanto a las empresas como a los consumidores, pues la Red permite que, sólo a golpe de clic, pueda realizarse todo el proceso de compra hasta la entrega de un producto en nuestro propio domicilio, o hasta el consumo de un bien o contratación de un servicio. Pueden realizarse compras online desde productos de primera necesidad, hasta ocio, tecnología o contratación de seguros, por ejemplo. Esta evolución ha hecho que aparezcan los denominados 'marketplace' y las plataformas de 'e-commerce'.

Los primeros son una especie de centro comercial virtual en el que se pueden encontrar productos muy diversos de diferentes marcas y empresas. Algunos ejemplos de 'marketplace' son Amazon, eBay, AliExpress, o Mercado Libre. Las 'e-commerce' son plataformas o webs que pertenecen a una marca o tienda concreta, la cual es responsable última de la venta de su producto o servicio y se encarga de hacérselo llegar al cliente.

Internet es, pues, un escaparate global en el que encontramos todo lo que buscamos. El comercio electrónico ofrece ventajas indudables como rapidez, comodidad, personalización, pero ¿nos movemos con seguridad en él?

2. Compras seguras

Esta unidad tiene una relación estrecha con los conocimientos desarrollados en el tema dedicado a la Ciberseguridad. El tema configura la condición básica para realizar en Internet operaciones como las compras.

Además de los consejos básicos con los que nos movemos a la hora de realizar compras presenciales, debemos añadir el conocimiento sobre elementos de seguridad que hemos de tener en cuenta a la hora de navegar en internet, sobre todo porque la realización de transacciones implica la cesión de una serie de datos sensibles, como nuestro nombre completo, nuestra dirección postal o nuestros datos bancarios, sin contar con la cantidad de preferencias que revelan nuestros movimientos, cuyo rastro se queda en la Red, como ya vimos anteriormente.

Para que tanto la calidad del producto o servicio que adquirimos a través de Internet sea una garantía, así como para que nuestros datos personales y bancarios estén protegidos durante todo el proceso, debemos detenernos en los siguientes apartados fundamentales:

a) Seguridad en dispositivos y red
b) Fiabilidad de la tienda online
c) Medios de pago
d) Derechos y garantías

a) Seguridad en dispositivos y red

Es fundamental que podamos contar con un entorno seguro en Internet para que el proceso de compra se desarrolle con totales garantías como consumidores, de forma que cualquier posibilidad de convertirnos en objeto de fraude, suplantación de identidad o robo de datos, quede disipada.

Es importante dotar a nuestros dispositivos de los elementos básicos de seguridad como un antivirus, así como observar una adecuada configuración de la red WiFi. Es conveniente analizar el dispositivo antes de realizar cualquier operación de compra por si éste estuviera infectado. Así, comprobamos que exista un buen antivirus o que el sistema operativo del dispositivo esté actualizado. Del mismo modo podemos revisar programas y aplicaciones y eliminar aquellos que no se estén utilizando, ya que eso sólo dificulta un mejor rendimiento y puede ralentizar su funcionamiento.

Para la realización de transacciones no se aconseja el uso de ordenadores u otros dispositivos públicos, ni tampoco una WiFi pública,

pues no sabremos con seguridad el grado de protección que nos ofrece y nuestros datos podrían ser objeto de robo, interceptación o ataques maliciosos sin que nos percatásemos de ello.

Las nociones más básicas de ciberseguridad nos advierten de que no se realicen operaciones que supongan el intercambio de datos u otro tipo de información sensible a través de una conexión mediante red WiFi pública.

Asimismo, se recomienda que cuando nos encontremos fuera del alcance de nuestras redes WiFi se deshabilite la opción de conectarse automáticamente a este tipo de redes, pues podría darse el caso de que haya atacantes que suplanten algunas de nuestra lista de favoritos, haciendo que nos conectemos a ella de forma automática y sin que estemos siendo conscientes de ello.

b) Fiabilidad de la tienda online

Conviene elegir una tienda que inspire confianza.

Evitaremos sorpresas y fraudes si nos aseguramos de que realizamos nuestras compras en una tienda que reúna unos mínimos requisitos de seguridad y cuya web sea fiable. Pero ¿cómo saber si es así?

La información que la web debe proporcionarnos de una manera clara y accesible es la relativa a la identificación de la empresa y sus protocolos de seguridad:

Quién es: debe identificar a su responsable, el nombre de la empresa; su número de identificación fiscal (NIF); datos de contacto, domicilio fiscal, condiciones de venta y devolución, etc. Normalmente esta información podrá encontrarse en un enlace bajo la denominación de 'aviso legal'.

Qué datos nos pide y qué hace con ellos: la web debe informarnos sobre los datos personales que recoge y para qué los utiliza. Normalmente, estas condiciones se recogen en la sección de'privacidad'o en la de 'términos y condiciones' del servicio.

Un candado en la barra de direcciones: sabremos si una página es segura si la dirección web que aparece en la barra de direcciones del navegador comienza por https: (conexión segura). También, si en el inicio de la URL vemos el icono de un candado.

Certificado digital en vigor: cuando accedemos a un sitio web que utiliza el protocolo https: su servidor utiliza un certificado para demostrar la identidad del sitio web a los navegadores. Pichando en el icono del candado podremos comprobar los datos del certificado de la página, que viene a garantizar, por un lado, que la página es legítima y auténtica y, por otro, que el sitio web funciona con información cifrada.

Si en nuestro proceso de compra online no podemos comprobar fácilmente los elementos citados, es aconsejable no continuar con la operación.

c) Medios de pago

Dentro de una página web han de identificarse claramente los modos de pago aceptados.

Una tienda online legítima ha de posibilitar diversas maneras de poder realizar el pago a fin de que sea el cliente quien decida cuál se ajusta más a sus preferencias, necesidades o le ofrece mayor nivel de confianza. Si se aceptan varios sistemas, pero finalmente el abono se limita a una o dos modalidades, como por ejemplo el uso de tarjeta o la transferencia bancaria, no deberíamos fiarnos y antes de completar el proceso deberíamos informarnos más a fondo sobre la autenticidad del comercio.

Como formas de pago más seguras en el comercio online pueden citarse la modalidad contra reembolso, el abono con tarjetas de prepago; el uso de plataformas virtuales como PayPal o el empleo de los llamados 'wallets', término inglés que significa billetera. Es una cartera virtual en el que gestionamos nuestros activos económicos digitales.

Veamos detalladamente cuántas modalidades de pago existen, en qué consiste cada una, cuáles son más aconsejables y qué principales ventajas o desventajas tienen:

En efectivo. Es la forma en la que se envía dinero a cambio de un bien o servicio, incluso puede existir la modalidad de envío anónima, por lo que puede resultar, también, difícil de identificar al receptor. Se desaconseja desde el Instituto Nacional de Ciberseguridad (Incibe), para compras virtuales, pues, aunque con este sistema se evita intercambiar los datos bancarios del comprador a través de internet, que puedan realizarse envíos anónimos no deja constancia de quién envía el dinero, o de quién lo recibe, de manera que, ante una incidencia en el proceso, será muy difícil ejercer un derecho de reclamación o devolución o si se es víctima de una estafa.

Contra reembolso. Podría decirse que ha quedado algo anticuado, dado el avance tan vertiginoso de la tecnología. No obstante aún hay compradores que lo prefieren.

Se trata de un sistema muy seguro para el comprador porque no ha de introducir datos bancarios en la red y el pago sólo se realiza cuando el producto se recibe. Es el propio repartidor quien cobra al cliente en el momento de la entrega. Para los vendedores no es una opción tan ventajosa, ya que requiere contar con repartidores o empresas con equipamiento y autorización para gestionar y mover el dinero. Asimismo, para el vendedor es un riesgo enviar un producto por el cual aún nadie ha pagado y puede que también se exponga a asumir costes mayores cuando, en el momento de la entrega, el cliente no se encuentra en la dirección indicada. Ha de tenerse en cuenta que el pago contra reembolso supone normalmente un coste adicional para el comprador.

Transferencias bancarias. Se envía una cantidad de dinero entre dos cuentas bancarias. Permite que no se tengan que introducir datos financieros en Internet, pero cuenta con la desventaja de que el comprador realiza un pago por un producto cuando aún no tiene evidencia de su compra.

Puede ser difícil de recuperar el dinero en caso de incidencias en el proceso, ya que una devolución no podrá tener lugar si el receptor del pago no la autoriza.

Pago con el móvil. Su uso se va extendiendo en función de la innovación tecnológica y del mayor empleo del dispositivo móvil. Hay marcas que ya ofrecen estas aplicaciones, como Samsumg – Samsung Pay—Básicamente necesita que se configuren los datos de una tarjeta en la aplicación, de manera que con el propio terminal puede pagarse acercando el móvil a cualquier TPV tradicional y autenticando la transacción con una huella dactilar, por ejemplo. Con el desarrollo tecnológico han surgido nuevas soluciones para pagos a través del móvil, como los wallet, una cartera digital donde se guardan las tarjetas de crédito. Además del citado arriba, pueden enumerarse otros como Apple Pay o Google Pay. Los bancos han respaldado ampliamente esta modalidad, y poseen sus propios wallets como BBVA Wallet, Bankinter Pay, CaixaBank Pay, Santander Wallet, Bankia Pay, etc.

Pago a través de intermediarios o terceros: Se trata de plataformas dedicadas exclusivamente a la gestión de cobros y pagos electrónicos. La plataforma actúa como intermediario en la realización de esta función entre comprador y vendedor. También se usa para pagos entre particulares. Aquí destaca Paypal, que es ya una referencia en el mundo de los pagos en internet. Ofrece gran seguridad y su uso está muy extendido, por lo se ha convertido en un medio muy utilizado por aquellos clientes que compran a menudo online. Es también muy versátil y cómodo para gestionar devoluciones. Los usuarios la consideran como una de las más fiables y seguras. Para usarla, sólo es necesario hacerse una cuenta en la plataforma, vincular a esa cuenta una tarjeta y un correo electrónico. El cliente no tiene que dejar sus datos personales en la tienda online, por lo que en todo el proceso se mantiene en un alto nivel de seguridad y privacidad. Cuenta también con el respaldo de las entidades financieras.

Como desventajas pueden citarse que puede conllevar comisiones o que, en el caso de ser receptor de cobro, el dinero, primero, va a una cuenta de Paypal y, posteriormente, a la cuenta bancaria personal, con lo que el proceso no es inmediato.

Tarjeta bancaria. Es el modo más parecido al procedimiento offline, con un sistema de securización semejante al de los TPV convencionales y permite usar la misma tarjeta y las mismas claves. Se trata del medio más usado para el cobro por el comercio virtual en nuestro país. La información que se necesita está contenida en la propia tarjeta de crédito o débito. Además, con ellas se evitan recargos adicionales por el uso de la tarjeta por parte de los beneficiarios de los pagos. Es un método seguro y cómodo, tanto para compradores habituales, como esporádicos. Permite, asimismo, detectar y actuar con eficacia frente a operaciones fraudulentas o cargos erróneos. También es un sistema garantista frente al vendedor, en caso de eventuales incidencias por parte del comprador.

Ofrece mucha seguridad, ya que es un servicio de comercio electrónico que ofrecen la mayoría de entidades bancarias y al que se adscriben los comercios online a través de un contrato. En el momento de la tramitación del pedido por Internet, el comprador accede a la pasarela de pago de un determinado banco en la que puede abonar su compra a través de su tarjeta de crédito o débito. De este modo, será el banco quien se encargue de autentificar la tarjeta y proteger los datos del cliente.

Si la tienda online no usa estas pasarelas, la protección sobre los datos bancarios del comprador recae sobre el propio comercio y los mecanismos de seguridad que tenga implantados. Incibe recomienda no facilitar los datos de la tarjeta si existen dudas sobre la fiabilidad de la web.

Tarjetas prepago. Es un tipo de tarjeta que no está asociada a una cuenta bancaria y que se puede recargar cuando se necesite. Es también un modo de hacer pagos que goza de un gran nivel de seguridad.

De este modo, si tiene lugar cualquier incidencia en el proceso de compra, un ciberatacante no podría acceder a nuestras cuentas bancarias ni tampoco robar el dinero, ya que las tarjetas suelen disponer de saldos justos y limitados y cada usuario decide cuánto recargar. Pueden usarse desde el móvil con aplicaciones específicas, de modo, que, ante cualquier sospecha de movimiento extraño, el usuario puede bloquear la tarjeta desde su dispositivo.

d) Derechos y garantías

Es la normativa europea la que marca las grandes líneas sobre los derechos y deberes a los que han de acogerse empresas y consumidores en las transacciones comerciales y operaciones de comercio electrónico. Esta legislación abarca desde los derechos que amparan la tan sensible protección de datos de carácter personal, hasta la regulación de las obligaciones que han de estar presentes en todos los procedimientos comerciales realizados en la Unión Europea para que el proceso de compra y venta online sea seguro y satisfaga a ambas partes.

Sobre los datos personales: Después de haber realizado cualquier operación online en un comercio, el establecimiento podrá conservar nuestros datos de carácter personal y usarlos para fines sobre los que previamente haya informado y nosotros, autorizado.

Sobre el producto adquirido: Desistimiento y devoluciones. Tenemos el derecho a anular y devolver el pedido en un plazo de 14 días, por cualquier motivo y sin justificación alguna. Este llamado 'período de reflexión' finaliza a los 14 días de la fecha de recepción de los productos (o de la celebración de un contrato de servicios). Se trata del llamado derecho de desistimiento. Existen algunos productos sobre los que no se aplica el derecho de desistimiento: Billetes de avión y tren, entradas de conciertos, reservas de hotel, alquiler de vehículos y suministro de comidas para fechas específicas, comida a domicilio, artículos personalizados, software informático desprecintado, contenidos digitales online, contratos de reparaciones o productos comprados a particulares y no a empresas.

Reembolso por devolución. El vendedor debe reembolsar el importe abonado en un plazo de 14 días a partir de la recepción de la solicitud de anulación. No obstante, puede aplazar el reembolso si no ha recibido los productos o la prueba de que han sido devueltos. El reembolso debe incluir todos los gastos de envío que se hayan abonado al hacer la compra.

Garantías. Existe el derecho a una garantía mínima de dos años sin coste alguno siempre. Dentro de la UE, si el producto adquirido está defectuoso, o no es el anunciado, el vendedor debe repararlo o cambiarlo gratuitamente, ofrecer un descuento o devolver el importe íntegro abonado. Las garantías a las que tiene derecho el consumidor también se aplican a productos de segunda mano, aunque aquí el plazo máximo es de un año en defecto de pacto entre comprador y vendedor. El consumidor tiene derecho a recibir un producto en perfecto estado siempre.

3. Herramientas prácticas

Ser un comprador atento y observador evitará que podamos ser víctimas de estafas y fraudes. Ten especial cuidado con:

- Los banners. Se trata de un formato publicitario de contenido gráfico, muy común en Internet, cuyo objetivo es atraer tráfico hacia el sitio del anunciante. Aunque su finalidad no es engañar al usuario, sí que han acabado por convertirse en instrumento para realizar estafas. Hay una enorme cantidad de 'banners' en Internet que imita a firmas conocidas. Pon atención antes de pinchar en uno y usa los conocimientos adquiridos en este taller para evitar ser víctima de un engaño.

- Páginas falsas. Actualmente resulta sencillo para los 'hackers' crear una página web falsa, de manera que parezca ser un comercio online. Se trata de un fraude, ya que detrás de dicha página web no existe ningún soporte comercial. Realiza tus compras en páginas legítimas.

- Diseño de la web, imágenes sin calidad y textos con errores. Si las imágenes no son buenas, aparecen pixeladas o incluyen marcas de agua; si la web aparenta ser la página legítima de una determinada marca, si aparecen textos mal traducidos, etc, se trata de elementos suficientes para que desconfiemos de esos sitios.

- Desconfía de las gangas y ofertas de productos gratuitos. Podría tratarse de productos falsificados o robados. Si el comprador adquiere productos a sabiendas de su falsedad, podría incurrir en un delito. Si ves gangas imposibles y sospechas de su falsedad, denúncialo.

- Apps maliciosas. Debemos asegurarnos de descargar aplicaciones oficiales, es decir, que no se trata de una suplantación de la legítima. Algunos buenos consejos son conocer qué permisos solicita al instalarse y para qué. Valorar si éstos son razonables o consultar los comentarios y la valoración que han realizado otros usuarios.

4. Actividades

- Consulta un par de páginas que conozcas donde puedas comprar productos y comprueba que tienen certificado digital, siguiendo los consejos de la Oficina de Seguridad del internauta (OSI).

- Atrévete a realizar una compra en Internet con todas las garantías de seguridad, siguiendo los pasos de este interesante tutorial de Andalucía Compromiso Digital.

- ¿Cuánto sabes sobre compras seguras online? Comprueba tus conocimientos al respecto con un rápido cuestionario de la OSI.

5. Más información

- Los sellos de confianza son un tipo de certificaciones que utilizan las tiendas online para ganarse la confianza de los usuarios, acreditando que utilizan mecanismos de seguridad y buenas prácticas que aseguran la protección y privacidad de los consumidores. Si quieres saber más, la OSI te lo explica con este sencillo vídeo.

- En el comercio electrónico tienes derechos como consumidor que debes conocer. Te recomendamos prestar atención a esta entrevista de Andalucía Compromiso Digital a Santiago Hoya, Jefe del Servicio de Educación y Promoción de las Personas Consumidoras de la Junta de Andalucía.

SESIÓN 8
INTERACCIONES SOCIALES DIGITALES

1. Contexto

En los últimos años el uso de Internet se ha convertido en un elemento fundamental en nuestra rutina como herramienta de trabajo, aprendizaje, socialización y entretenimiento. Los datos que se extraen del Barómetro Audiovisual de Andalucía 2020 (BAA), reflejan el protagonismo cada vez mayor de la Red como medio de ocio con múltiples prestaciones a nuestra disposición: redes sociales, aplicaciones de mensajería, plataformas audiovisuales online… En concreto, el 86,6% de la población andaluza dice usar Internet para entretenerse, y dentro de este porcentaje destacan los servicios que facilitan la interacción social entre personas, a pesar de la distancia geográfica entre ellas. Nos referimos al uso de las redes sociales, que es la opción preferida para distraerse, según el 65% de los encuestados.

No hace tanto tiempo necesitábamos reunirnos personalmente con alguien para poder verle en directo, enseñarle las fotos de nuestras últimas vacaciones o prestarle un libro, pero todo eso ya pertenece al pasado. Relacionarse con los demás ya no exige la presencialidad, ventaja que nos ha acercado a nuestros seres queridos que viven lejos o no son convivientes, como ocurrió durante el confinamiento. En esos meses del año 2020 fueron muchos los mayores que tuvieron que aprender de forma apresurada a conectarse telemáticamente con su entorno. Incluso, algunos se quedaron desconectados del mundo por no saber hacer una videollamada, mandar un email o acceder a los archivos familiares guardados en la nube.

En esta sesión repasaremos algunos de los servicios más populares de interacción social digital como el correo electrónico, el envío de archivos pesados por WeTransfer, el servicio de mensajería WhatsApp y el almacenamiento remoto. Además, os daremos algunas pautas de buen uso para garantizar nuestra seguridad.

2. Definiciones y características

En la actualidad la mayoría de los adultos dispone de una o más cuentas de correo electrónico, ya sea para uso personal o profesional, y desde distintos proveedores gratuitos como Gmail, Outlook (antiguo Hotmail) o Yahoo. Los emails nos permiten enviar y recibir mensajes electrónicos y archivos adjuntos al instante, siempre y cuando tengamos conexión a Internet. Sin embargo, son pocos los usuarios que saben gestionar eficientemente su email, ya que desconocen todos los recursos que ofrecen estas plataformas, de los cuales destacamos:

- Programar envíos: ¿Te gustaría enviar una felicitación de cumpleaños a un amigo justo ese día, pero no estarás disponible para entonces? Con la opción 'Programar envíos' puedes dejar redactado un correo y elegir la fecha y hora que quieres que lo reciba tu destinatario.

- Posponer mensajes: ¿Has leído un email que debes responder en un momento inoportuno y temes olvidarlo más tarde? Utilizando la herramienta 'Posponer mensaje' recibirás un recordatorio en tu bandeja de entrada del correo electrónico en la ocasión exacta que tú prefieras.

- Crear etiquetas: ¿Te resulta complicada la búsqueda de emails de distintos emisores y asuntos, pero que guardan algo en común? Cuando guardes un correo es recomendable asignarle una 'Etiqueta', que puedes crear, editar y eliminar. Este simple gesto te ayudará a organizar tu cuenta de correo, facilitando además, tus futuras búsquedas.

- Respuesta automática: ¿Cómo puedo avisar a mis contactos de que no podré responder a sus emails en los próximos días? Una solución rápida es activar una 'Respuesta automática', es decir, un correo electrónico que puedes redactar a tu gusto, el cual recibirán todas aquellas personas que te envíen un email hasta que desactives esta opción.

Un problema habitual en los emails es la imposibilidad de enviar varias fotos o vídeos de gran calidad, que pueden superar los 20 o 50 MB, que suele ser el límite habitual de tamaño de los archivos adjuntos en los principales servicios de correo electrónico. ¿Cómo podemos compartir esa clase de archivos pesados? Una alternativa es WeTransfer, un servicio de transferencia de ficheros, que funciona mediante el almacenamiento temporal de archivos enviados por los usuarios, a los cuales pueden acceder a través de un enlace de descarga que se genera automáticamente. Esta herramienta cuenta con una versión gratuita para compartir ficheros de hasta 2 GB de tamaño en un mismo envío y que no requiere registro previo, por lo que el proceso apenas dura un minuto. Veamos paso a paso cómo funciona:

- En la parte izquierda de la web oficial de WeTransfer hacemos clic con el ratón en 'Añade tus archivos' o 'Selecciona una carpeta', donde podremos adjuntar ficheros que tengamos guardados en nuestro ordenador.

- En los espacios pertinentes debemos escribir la dirección de correo electrónico desde la que enviamos el mensaje y la dirección del receptor del mismo. Si es una transferencia dirigida a varias personas debes saber que hay un límite de 20 destinatarios diferentes en un mismo envío.

- Pulsamos el botón 'Enviar' y al instante veremos un mensaje en la pantalla solicitando un código de verificación de 6 cifras, el cual llegará a los pocos segundos a nuestra dirección de correo. Lo copiamos, lo pegamos en el espacio indicado, hacemos clic en 'Verificar' y se enviarán los archivos.

- Poco después recibiremos un email de confirmación de envío y se nos informará cuando el destinatario descargue el contenido, al cual tendrá acceso durante 7 días. Pasado ese tiempo el enlace dejará de funcionar.

Cabe subrayar que las interacciones sociales digitales por parte de la población andaluza no se limitan al envío de correos electrónicos y archivos. De hecho, el 46% de la población andaluza utiliza WhatsApp como herramienta de entretenimiento, según el BAA 2020. El éxito de este servicio de mensajería instantáneo, gratuito y sin límite de caracteres, quizás se deba a los diversos recursos que ofrece. No sólo sirve para chatear, mandar emoticonos, fotos y mensajes de voz; también permite realizar llamadas y videollamadas entre dos personas o grupales con un límite de 8 personas. Incluso, el número de participantes en una videollamada colectiva puede aumentar hasta 50 si se crea una sala. Además, WhatsApp nos ayuda a compartir:

-Ubicación, una función muy útil cuando quieres indicar una dirección a alguien.

-Documentos de todo tipo (Word, PDF, hojas de cálculo…) de hasta 100 MB.

-Contacto, que permite pasar un teléfono de tu agenda a otro usuario.

Aunque WhatsApp es uno de los más populares, no es el único servicio para hacer videollamadas, hay otras aplicaciones sin coste como FaceTime, Google Hangouts, Skype o Zoom, entre otros. ¿Cuál es la mejor? La respuesta depende de las necesidades de cada usuario, ya que tienen funcionalidades y características de seguridad comunes y propias. Incluso, hay diseños que parecen más intuitivos a unas personas que a otras.

Hay personas reacias al uso de esta clase de servicio de mensajería, porque temen que se vulnere la privacidad de sus conversaciones o de los archivos que comparten. Sin embargo, la mayoría de estas aplicaciones cuenta con algún sistema de seguridad para proteger las comunicaciones, a saber:

- Cifrado extremo a extremo: Garantiza que el mensaje enviado (texto, imagen, vídeo, audio o archivo) viaje cifrado de un dispositivo a otro. Es decir, solo tú y el receptor pueden verlo, sin intermediación de terceros, ni siquiera la empresa desarrolladora de la aplicación.

- Cifrado TLS: A diferencia del anterior sistema éste asegura el cifrado del mensaje (texto, imagen, vídeo, audio, etc.) desde tu dispositivo hasta el servidor de la aplicación, lo cual implica que la empresa dueña de la aplicación podría acceder a tus mensajes.

- Verificación en dos pasos: Es un método adicional de seguridad para comprobar que el usuario que accede al servicio es quien dice ser, para lo cual debe verificar su identidad con un código. En otras palabras, se garantiza que nadie utilice tu cuenta sin tu permiso.

Asimismo, es recomendable descargarse estas aplicaciones en espacios de confianza como la página web oficial del servicio de mensajería escogido o plataformas legítimas como Google Play o Apple Store. De lo contrario, corremos el riesgo de instalar una aplicación falsa que dañe nuestro dispositivo con un virus o acceda a nuestros mensajes.

Otras prestaciones menos conocidas de WhatsApp son WhatsApp Web y WhatsApp Escritorio, que son extensiones de nuestra cuenta que nos permiten usar esta aplicación en un ordenador, pudiendo mandar y recibir mensajes en dicho dispositivo y en el móvil. La diferencia entre una y otra es que la primera se puede usar desde cualquier navegador, mientras que la segunda requiere descargarse la aplicación en un ordenador. Ambas funciones pueden ser de gran utilidad cuando queremos ver en pantalla grande algún archivo que nos envían o necesitamos vaciar la memoria del móvil, guardando fotos o vídeos directamente en una carpeta de nuestro ordenador personal.

Al cabo de un solo día podemos acumular muchos archivos en nuestros dispositivos móviles, sobre todo, fotografías y vídeos, que suelen ocupar bastante espacio de memoria, el cual, recordemos, no es ilimitado. Una sobrecarga de archivos conlleva complicaciones como ralentizar las funcionalidades de nuestro teléfono móvil.

Para evitar este problema se recomienda eliminar aquellos archivos innecesarios, y los que queremos conservar pasarlos a un ordenador, un sistema de almacenamiento externo (pendrive, memoria externa) o un servicio de alojamiento mediante un servidor remoto. Esta última opción se conoce comúnmente como la nube, disponible a través de Dropbox , iCloud o Google Drive, entre otras plataformas. ¿Qué ventajas nos ofrece este sistema?

- Accesibilidad universal. Siempre que dispongas de un dispositivo (teléfono móvil, ordenador o tableta) con conexión a Internet podrás acceder en cualquier momento a tus archivos depositados en la nube, sin importar tu ubicación física.

- Seguridad extra. Guardar una copia de tus ficheros en la nube es una alternativa de seguridad ante una posible pérdida o daño de tu ordenador y tu disco duro portátil, porque al ser un lugar externo tus documentos no correrán ningún peligro en situaciones como esas.

- Gratuidad. Estos servicios disponen de versiones de pago y sin coste. La mayor diferencia entre una y otra es el espacio de almacenamiento disponible, el cual es notablemente superior en las opciones con coste, llegando a ser ilimitado el alojamiento de archivos en algunos casos.

- Colaboración a distancia. En general se piensa que la nube sólo sirve para conservar ficheros, pero también tiene otra función muy útil, el trabajo en equipo. Si añades como editor de un documento a una o más personas estas puedes realizar cambios que pueden verlos todos los integrantes del equipo.

No obstante, debemos advertir de que estos servicios no son infalibles y también tienen sus inconvenientes. Por un lado, no nos permiten acceder a nuestros ficheros sin conexión a la Red. Por otro, perdemos el control directo de nuestra privacidad, porque dejamos en manos de dicho proveedor la seguridad de los mismos.

Como los servicios en la nube también son susceptibles de ciberataques conviene no depender sólo de este sistema para guardar nuestros archivos. Es mejor tener varias copias de seguridad en distintos formatos (físico y online).

3. Herramientas prácticas

Ya hemos visto que existen diversas y útiles formas de interaccionar con nuestros familiares y amigos a través de Internet, pero no hay que bajar la guardia, porque siempre hay riesgos en este tipo de comunicaciones. Te recomendamos seguir estos consejos de seguridad:

- Cuida tu privacidad. Igual que no gritamos por la calle nuestros datos confidenciales tampoco debemos hacerlo por correo electrónico, mensaje de WhatsApp o videollamada. Aunque estos servicios disponen de cifrados de seguridad eso sólo te protege de terceras personas ajenas a esa conversación, pero no garantiza que el receptor del mensaje no reenvíe tu mensaje.

- No hagas clic en enlaces dudosos. No es recomendable seguir las instrucciones de un mensaje que te exige pulsar un enlace para ver su contenido completo. Son mensajes fáciles de reconocer porque suelen captar nuestra curiosidad con noticias de carácter sensacionalista, alertas, premios o falsos descuentos.

- Pon límites a los grupos. A veces nos añaden a grupos masivos que no son de nuestro interés y nos interrumpen con notificaciones constantes. Puedes silenciar estos avisos o salir del grupo. Incluso, tienes la opción de restringir qué contactos pueden añadirte en grupos y así recibirás una invitación para decidir si quieres entrar o no. Asimismo, hay que poner especial hincapié en no compartir archivos o datos comprometedores en grupos de WhatsApp o videollamadas grupales, ya que a veces puede haber un participante que desconocemos o que no es de nuestra plena confianza.

- Videoconferencias seguras. Si organizamos una videoconferencia debemos configurar una contraseña de acceso a esa reunión, que enviaremos sólo a los integrantes del mismo, a los cuales hay que alertar de que no la compartan con terceros ni la publiquen en redes sociales. Además, podemos activar la opción de 'Sala de espera' que asegura que el administrador de la videollamada autorice o no a esa persona a que se una.

- Cifra tus ficheros de la nube. Al cifrar un archivo aseguramos que nadie pueda ver su contenido, porque será ilegible para aquellos que no dispongan de una clave secreta. Este proceso se realiza a través de alguna herramienta gratuita de cifrado como VeraCrypt o Cryptomator. Si tienes dudas, consulta los pasos indicados por la Oficina de Seguridad del Internauta (OSI).

En definitiva, todas estas aplicaciones facilitan nuestra manera de relacionarnos con los demás, pero lo digital no puede sustituir completamente la interacción presencial.

4. Actividades

- ¿Sabes gestionar de manera eficaz tu correo electrónico? Sigue los pasos de este taller online de Andalucía Compromiso Digital para cuentas de Gmail y Outlook.

- ¿Crees que tu email es seguro? Comprueba que cumples las siguientes recomendaciones de la OSI para proteger tu correo.

- Prueba a enviar un archivo pesado por We Transfer a un amigo o familiar. En Youtube tienes a tu disposición videotutoriales como el de EducaTIC, que te explican cómo hacerlo.

- Mejora la privacidad de tus conversaciones en WhatsApp con OSI: confirmando los códigos de seguridad, activando la verificación en dos pasos o restringiendo qué contactos pueden visualizar tu foto de perfil o de estado.

- Practica a hacer una videollamada por WhatsApp, Google Duo o Skype con la ayuda de Andalucía Compromiso Digital.

5. Más información

- Utilizar contraseñas seguras o el cifrado de emails pueden ser herramientas útiles para proteger tu cuenta de correo electrónico. Si necesitas más detalles puedes ver este tutorial de Andalucía Compromiso Digital.

- El Centro de Ayuda de WhatsApp puede resolver tus dudas sobre el uso de esta aplicación. Consúltalo.

- Antes de instalar, revisa las infografías de la OSI sobre la seguridad y privacidad de las plataformas de videoconferencia y de los servicios de almacenamiento en la nube más conocidos.

SESIÓN 9
TODO SOBRE LAS REDES SOCIALES

1. Contexto

A lo largo de la última década el Consejo Audiovisual de Andalucía ha constatado el aumento del uso de las redes sociales entre la población andaluza, según el Barómetro Audiovisual de Andalucía 2020. En concreto, en el año 2012 el 53,9% de los encuestados afirmaban usar Facebook, Twitter o Instagram para entretenerse; una cifra que se ha incrementado hasta alcanzar un 65% en 2020. Aunque el perfil del usuario de redes sociales suele ser joven, cada vez son más los mayores que abren una cuenta para interactuar con sus familiares y amigos. Si quieres unirte a esta tendencia o ya formas parte de una red social, te recomendamos que consultes esta sesión donde repasaremos las características de las redes sociales, los nuevos hábitos de consumo digital y os daremos algunos consejos de buenas prácticas para evitar riesgos en la Red.

2. Definiciones y características

Las redes sociales son plataformas digitales formadas por comunidades de personas u organizaciones con vínculos entre sí, ya sea de amistad, parentesco, trabajo, etc. Su objetivo es permitir el contacto entre individuos y/o empresas, además de constituir un medio de comunicación y de intercambio de información. Nos facilitan interactuar con contenidos textuales y audiovisuales, los cuales podemos crear o compartir, o participar comentando o valorando la publicación de otro usuario. Podemos resumir sus funciones de la siguiente manera:

-Alternativa de entretenimiento digital.
-Fuente de información.
-Medio de contacto personal y profesional.
-Plataforma de intercambio de contenido multimedia (fotos, vídeos, etc.).
-Foro de debate.
-Instrumento publicitario para dar a conocer a una persona, colectivo o empresa.

- ¿Qué beneficios pueden tener las redes sociales para la población mayor?

-Implica la mejora de las habilidades cognitivas. Empezar a usarlas trae consigo el aprendizaje de algo nuevo, tratándose de un reto intelectual. Y más allá de aprender a utilizarlas, sirven como medio para alcanzar nuevos conocimientos, resolver dudas, investigar, interaccionar, leer, escribir, etc. Por lo que suscita la facultad de razonamiento y también aviva la actividad cerebral, ayudando incluso a prevenir enfermedades como la demencia.

-Es un instrumento de ocio. Las limitaciones de desplazamiento por problemas físicos o circunstanciales dificultan nuestras opciones de divertirnos en la calle. Es por ello que el uso de las redes sociales sea una buena alternativa contra el aburrimiento para entretenernos de mil y una maneras sin salir de casa: leyendo, viendo vídeos y fotos, chateando, jugando a juegos…

-Ayuda a reducir el sentimiento de soledad. Las redes sociales pueden servir para que no estemos solos y aislados de la sociedad, al ponernos en contacto con conocidos, amigos, hermanos, hijos, nietos, etc. Incluso, nos permite conocer a gente nueva. Con las redes compartimos opiniones, experiencias, pensamientos…, y nos ponemos al día de la vida de nuestros amigos al visitar sus perfiles. Además, se trata de una manera muy sencilla de sentirse acompañado sin tener que salir de casa. No obstante, esta experiencia digital nunca puede sustituir completamente el contacto en persona.

-Vía para encontrar nuevas oportunidades. Las redes son una fuente de información casi inagotable y en constante actualización. Un medio sencillo para encontrar información u ofertas de todo tipo, tanto de productos o servicios que nos interesan o que se encuentran en nuestro entorno, como de otros que desconocemos o que están a miles de kilómetros de distancia, pero que podemos necesitar o querer.

- ¿Cuáles son las redes sociales más populares?

  Facebook, Instagram, Youtube y Twitter son las más exitosas y ya llevan más de una década en nuestras vidas. Facebook engloba todas las características anteriormente descritas como plataforma de intercambio de textos, fotos, vídeos entre una comunidad digital concreta. En cambio, Instagram y Youtube son esencialmente audiovisuales, mientras que Twitter se caracteriza por sus textos breves que no superan los 280 caracteres, aunque se pueden mandar fotos, vídeos y mensajes de voz de 140 segundos.

- ¿Qué les diferencia entre sí?

  La popularidad de Instagram radica en su funcionalidad como una sencilla herramienta para editar fotografías mediante filtros, los cuales no sólo pueden mejorar la iluminación de una imagen, sino modificar nuestro rostro o añadir toda clase de objetos inexistentes en la instantánea original.

Twitter es la red social más adecuada para informarse de una manera ágil sobre la actualidad de todo el mundo. Puedes saber qué está pasando y dónde a tiempo real. Un claro indicador de qué asunto o persona está generando más interés en un momento concreto son los 'trending topic', es decir, las palabras clave más repetidas por los usuarios de Twitter.

El contenido que se comparte en Youtube son vídeos de un tamaño máximo de 256 GB que podemos publicar, reenviar y comentar. El límite de los vídeos no puede superar los 15 minutos a excepción de las cuentas verificadas, cuya duración es mucho mayor.

- ¿Hay redes sociales centradas en un tema concreto?

Claro que sí, hay cientos de redes sociales de toda clase de temáticas. Podemos poner como ejemplo LinkedIn, TripAdvisor y Pinterest.

LinkedIn es una red social que permite darte a conocer si buscas trabajo o ponerte en contacto con millones de profesionales. TripAdvisor se trata de una plataforma que proporciona un espacio donde publicar y recibir reseñas de contenido relacionado con viajes, esencialmente, hoteles, restaurantes, monumentos, actividades… Pinterest se trata de un espacio que permite a sus usuarios encontrar y recopilar imágenes mediante la creación de tableros personales temáticos. La consulta del perfil de otros usuarios es muy útil para descubrir ideas para nuestros proyectos y aficiones.

- **¿Existen redes sociales específicas para personas de edad avanzada?**

  Formar parte de la tercera edad no es un problema para relacionarse con otros en Internet. De hecho, hay redes sociales enfocadas a este sector de la población. Veamos un par de ejemplos:

-Post55: Su uso requiere tener un perfil en Facebook, porque es una comunidad dentro de esta red social. Engloba diversos grupos creados según los intereses de los miembros. Es un espacio recomendable para conocer gente nueva o contactar con amigos, interactuar, entretenerse, encontrar propuestas de ocio, noticias, chistes…

-Ourtime: Destinada especialmente a la búsqueda de pareja en la madurez, concretamente desde los 50 años. Por un lado, tienes la opción de crearte un perfil con tus datos e intereses y buscar personas afines a ti. Por otro, puedes acudir a actividades creadas para solteros mayores, una buena manera de conocer gente sin el reparo de una cita.

- **¿Qué es un 'challenge'? ¿Cuáles son las redes sociales de última moda?**

  Es un reto que se difunde de forma viral por las redes sociales. Algunos son solidarios, pero otros promueven conductas peligrosas.

Estos 'challenges' causan furor entre los adolescentes y veinteañeros que suelen compartir vídeos o fotos donde demuestran si superan o no el reto propuesto. Aunque puedes recibir uno de estos desafíos a través de cualquier red social o servicio de mensajería, los 'challenges' más actuales suelen proceder de las aplicaciones más exitosas entre los jóvenes en la actualidad: TikTok y Twitch.

-TikTok, que está basada en compartir vídeos musicales de 1 minuto de duración, los cuales se pueden crear y editar. Permite, además, aplicar varios efectos y añadirles un fondo musical.

-Twtich es una plataforma para realizar retransmisiones en directo en la que puedes interactuar con el receptor, conocido como 'streamer', enviándole mensajes en un chat. Tiene un amplio público entre los aficionados a los videojuegos, pero posee más contenidos como 'Música', 'Aire libre y viajes', 'Comida y bebida', 'Eventos especiales'...

- ¿Cuáles son los nuevos hábitos de consumo audiovisual?

  Twitch es uno de los muchos ejemplos de nuevos hábitos de consumo audiovisual en la actualidad. La televisión ya no es el único medio para disfrutar de contenidos audiovisuales, porque Internet nos abre todo un nuevo mundo de posibilidades. Nos referimos sobre todo a servicios de suscripción de vídeos a la carta como Netflix, Amazon Prime, Disney+ o HBO. Estas plataformas digitales de pago dan acceso a cientos de películas, series y documentales, tanto recientes como antiguas, de origen estadounidense, principalmente. Para los amantes del cine español se recomienda el servicio FlixOlé y para los aficionados al cine independiente, Filmin.

  Cabe señalar, que las cadenas de televisión españolas ya tienen la mayoría de sus programas y series disponibles en Internet para disfrutar de estos contenidos en cualquier momento (RTVE Play, Atresplayer, Mitele...).

3. Herramientas prácticas

No podemos olvidar que un uso irresponsable de las redes sociales conlleva riesgos: engaños online, desinformación, suplantación de identidad, robos… Debemos proteger nuestros datos personales, porque son más valiosos de lo que creemos. En los Cuadernos del Audiovisual Nº9 del CAA se reflexiona, entre otras cosas, de este asunto y al respecto, la profesora de la Universidad de Navarra, Charo Sádaba, advierte de la comercialización de nuestros datos personales: "A veces no somos conscientes de que la información de carácter personal que compartimos en las redes sociales deja de estar bajo nuestro control e incluso en ocasiones, deja de ser nuestra. Los términos de uso y compromiso que aceptamos cuando abrimos un perfil en una plataforma social esconden en el farragoso lenguaje legal sorpresas. Y es que, cuando no pagamos con dinero por un servicio que estamos recibiendo, tenemos que preguntarnos cómo lo estamos haciendo y, en el mundo digital, lo más probable es que sea con nuestros datos".

- Protege la información vulnerable. Nuestro número de teléfono y el correo electrónico personal son datos que no deben publicarse en Internet. De lo contrario estamos expuestos a recibir emails o llamadas fraudulentas. Tampoco conviene mencionar si no tienes compañía en casa ni compartir nuestra ubicación y domicilio porque los ladrones podrían saber cuándo está deshabitado. Asimismo, al crear un perfil de una red social solicitan tu fecha de nacimiento, pero no la dejes visible públicamente, porque es otro dato vulnerable ante ataques de suplantación de identidad.

- Configura tus preferencias de privacidad. Revisa qué condiciones de privacidad ofrece la red social en la que tengas un perfil y reflexiona qué contactos son de confianza para que vean tu actividad y quiénes pueden contactar contigo. Recuerda, además, utilizar contraseñas seguras, es decir, una secuencia alfanumérica con mayúsculas y minúsculas, que no coincida con datos fácilmente deducibles (nombre, fecha de nacimiento…).

- No aceptes invitaciones de amistad sospechosas. Si no solemos interactuar con desconocidos por la calle, ¿por qué hacerlo en Internet? Detrás de un perfil aparentemente inofensivo puede encontrarse un delincuente o un 'bot'. Un 'bot' es un programa informático que simula el comportamiento humano en Internet. Es muy frecuente su uso en redes sociales mediante perfiles falsos, cuya finalidad, entre otras cosas, es la difusión de noticias falsas.

- Imágenes que debes guardar. Evita exponer públicamente en las redes sociales fotografías de tu tarjeta de crédito o cualquier documento identificativo (DNI, pasaporte, carné de conducir…). Tampoco compartas imágenes de conversaciones privadas o fotos en las que aparezcan terceras personas sin su consentimiento previo. Además, los menores requieren una protección mayor, por eso es mejor no publicar fotos de niños y adolescentes en la Red.

4. Actividades

- Internet ofrece un variado catálogo de aplicaciones y algunas pueden ayudarnos a incrementar nuestra capacidad de concentración, mejorar nuestra memoria y fomentar nuestra creatividad. ¿A qué esperas para probarlos? En este taller te lo cuentan todo al respecto.

- Anímate a crear un perfil en una red social, pero asegúrate de construir una identidad digital positiva en las redes sociales, como recomienda la Oficina de Seguridad del Internauta (OSI).

- Las redes sociales saben más de nuestra vida privada de lo que creemos. Limita el acceso de terceras personas o empresas a tus datos personales con estos consejos sobre ajustes de privacidad en Instagram y YouTube de Andalucía Compromiso Digital.

5. Más información

- Los mayores también pueden triunfar en las redes sociales, como la onubense Guadalupe Fiñana, más conocida como 'Abuela de Dragones', que tiene miles de seguidores y asegura que las redes sociales le han cambiado la vida.

- Aunque TitkTok es la red social con más éxito entre adolescentes o jóvenes, muchos mayores también se han unido, como 'Los Abuelos Tiktokers' de una residencia de ancianos en Granada, cuyos vídeos arrasaron durante la pandemia.

- Si quieres conocer cómo funciona y las claves del éxito de TikTok no te pierdas este taller de Andalucía Compromiso Digital.

SESIÓN 10
ORIENTACIÓN A MENORES

1. Contexto

El doctor en Filosofía, Ricardo Yepes Stork, define la educación como la enseñanza "no sólo de conocimientos teóricos, sino sobre todo de modelos y valores que guíen el conocimiento práctico y la acción, y ayuden a adquirir convicciones e ideales, logrando una educación en los valores y en la virtudes. Educar es entonces cumplir la función perfectiva de la autoridad: comunicar la excelencia".

Esta acción corresponde no sólo a los padres, sino también a los educadores, ya sean en el aula o en casa. Aquí cabe destacar la figura de los abuelos, que pueden ser grandes educadores, puesto que comparten horas de cuidado y dedicación a los menores, en colaboración con sus padres, quienes confían en ellos el cuidado y custodia de los más pequeños, con idea de buscar la conciliación entre la vida profesional y familiar.

En esta labor de educar a los nietos resulta de gran utilidad y ayuda poder compartir los conocimientos y la experiencia acumulada de la vida con los más pequeños de la casa.

El entorno digital forma ya parte del mundo en el que vivimos y está muy presente en el día a día de los más pequeños. De hecho, la población andaluza menor de 18 años está muy familiarizada con las redes sociales y los servicios de mensajería instantánea, siendo WhatsApp (77,5%), Instagram (65,8%) y Tik Tok (29,7%) los más utilizados, según el Barómetro Audiovisual de Andalucía 2020. Las nuevas tecnologías pueden convertirse en una herramienta educativa beneficiosa, pero al mismo tiempo un uso indebido de las mismas plantea serias amenazas, especialmente al público más vulnerable, como son los menores, poniendo en riesgo tanto su desarrollo personal como sus relaciones sociales. Ante tales circunstancias conviene asumir una actitud proactiva mediante la mediación parental.

2. Definición y características

- ¿Qué es la mediación parental?

Según expone el Instituto Nacional de Ciberseguridad (INCIBE), "el objetivo de la mediación parental es formar a los propios menores para que sean capaces de enfrentarse a los riesgos de Internet de forma responsable. Para ello, la mediación engloba la educación, acompañamiento y protección de los menores en su proceso de aprendizaje digital. De este modo, los adultos debemos enseñarles cómo utilizar la tecnología de forma segura, para que su entrada en el mundo digital sea progresiva y consciente".

Asimismo, en INCIBE distinguen entre la mediación activa (estar a su lado cuando naveguen por la Red y darles ejemplo de un uso responsable) y la mediación restrictiva (imponer normas para controlar el uso de las nuevas tecnologías cuando no estén acompañados).

- ¿Qué podemos hacer como mediadores?

Esta es una de las grandes cuestiones que los adultos nos hacemos. ¿Qué podemos hacer para formar y educar en el correcto uso de Internet? Repasemos algunas ideas sencillas que nos facilitará orientar a los menores desde que son pequeños en el uso correcto de Internet.

-Mejor acompañados. Permitir navegar por la Red siempre que haya un adulto delante, que pueda comprobar en qué webs navega, que conozca el historial de visitas, a qué 'influencers' sigue, sobre qué temas expresa su opinión con 'Me gusta'. Hacerlo delante de ellos, no como espías, sino como parte de su educación y de su formación.

-Provocar conversaciones que nos faciliten hablar acerca de noticias o temas de actualidad, que nos hagan comprobar qué ha leído y qué información ha recibido. Esta actividad es una gran arma de prevención de noticias falsas y bulos.

-Preguntar de forma directa por ese 'influencer' que sabemos que le encanta y pedir que describa por qué le sigue y qué le gusta de ese personaje. Que destaque 2 o 3 aspectos positivos de esa figura le ayudará a tener un pensamiento reflexivo.

-Instalar recursos de control parental como filtros que restrinjan la información tanto de entrada como de salida, así como las conexiones a páginas webs con contenidos no convenientes para los menores. Los hay que son gratuitos y muy accesibles para su instalación como, por ejemplo, Google Family Link. Esta aplicación ayuda a que los menores consuman contenido de calidad.

-Promover que tengan criterio propio. Hacerles pensar, que no todo se base en navegar sin control. Conviene que paren, piensen y después actúen de forma que vayan adquiriendo un pensamiento crítico ante toda la información que reciben.

-Conocer su lista de contactos, es decir, sus amigos virtuales. Esto nos dará una pista de los temas que les unen y más les interesa.

-No se aconseja el uso de dispositivos de manera individual y solitaria, por ejemplo en su habitación. Para ello se recomienda instalar el ordenador en alguna zona común de la vivienda, como el cuarto de estar, la salita, el pasillo. No conviene que tenga una televisión o tableta para uso privado en su cuarto.

-Establece límites de tiempo al uso de las pantallas. Por tanto, estar pendiente a qué hora se conecta y negociar cuánto tiempo le va a dedicar. Se desaconseja permitir el uso del dispositivo electrónico sin límite horario, ya que esto afecta no solamente a su salud ocular, sino también al impacto que produce en su cerebro. Por ejemplo, en el caso de videojuegos suele ser de gran utilidad medir los tiempos según las partidas. Autorizar el jugar una única partida y después apagar el dispositivo.

-Facilitar la comunicación. Demuéstrale que tienes confianza en él o ella. Asegúrate de que se siente cómodo pidiéndote ayuda. Evita la sobrerreacción y el juicio rápido. Si el menor cree que se meterá en problemas al hablarte de algún comportamiento inadecuado, o que perderá algún privilegio (como el acceso a Internet o el teléfono móvil) será más reticente para solicitar tu ayuda. Y eso puede provocar que intente resolverlo por sí mismo, acrecentando así el problema.

En definitiva, el papel del adulto debe ser el de orientar, acompañar y guiar al menor en su participación en el entorno digital. No tanto siguiendo la figura de un inspector de policía o un espía, que se limita a controlar sus acciones, sino más bien, el de un socorrista o vigilante de la playa, cuya finalidad principal es prevenir de las amenazas y peligros que puedan acecharles, permitiendo que al minimizar riesgos y evitando malas prácticas, gocen de una experiencia más educativa, saludable y constructiva para ellos.

3. Herramientas prácticas

Cada vez son más las instituciones y organizaciones que nos proveen de instrumentos para orientar a los niños y adolescentes en un uso responsable de las nuevas tecnologías. Conozcamos algunas de ellas y las herramientas que ponen a nuestra disposición:

Internet Segura for Kids (Is4k). Es el Centro de Seguridad en Internet para menores de edad en España. Desarrolla campañas de sensibilización y divulgación para promocionar un uso seguro y beneficioso de la Red. En su web reúne todo tipo de información y materiales (guías, tests, juegos didácticos...) y además, ofrece servicios de asistencia online para casos problemáticos (ciberacoso escolar, discursos de odio, contenidos inapropiados, uso excesivo de las TIC, etc.). Puedes contactar con Is4K tanto para resolver dudas en su 'Línea de ayuda' como para denunciar contenidos dañinos que encuentres en la Red en su 'Línea de reporte'. Resultan muy útiles las instrucciones para configurar el control parental en todo tipo de plataformas de contenidos, sistemas operativos, videojuegos...

Empantallados. Es una plataforma que apuesta por el activo acompañamiento familiar en el mundo digital como una oportunidad para educar a los más jóvenes de la casa. En su web encontramos estudios y todo tipo de recursos (vídeos, podcasts, infografías...) que fomentan el desarrollo de niños y niñas como usuarios saludables de las nuevas tecnologías. Destacamos sus consejos para que naveguen por la Red con seguridad sin que se sientan espiados por los adultos: instalando controles parentales en los móviles, acompañándoles en sus inicios en Internet, estableciendo normas sobre el tiempo de uso o educándoles para que tengan una sana autoestima, que no dependa de los 'Likes' que reciban en las redes sociales.

Consejo Audiovisual de Andalucía. La autoridad audiovisual pública andaluza ha elaborado en los últimos años varias recomendaciones y otros materiales de interés sobre la protección de menores en Internet, como los Cuadernos del Audiovisual 9, en colaboración con expertos en la materia.

PantallasAmigas. Esta entidad es uno de los portales españoles de referencia en educación digital desde 2004. Su labor se desarrolla a través de proyectos y recursos para la capacitación de habilidades digitales saludables. Entre las temáticas abordadas subrayamos el 'ciberbullying', 'sexting', 'sextorsión', o el 'grooming', problemáticas estas, cada día más frecuentes entre los jóvenes y que nos ayudan a afrontarlos. Los recursos que ofrecen son amplios: apoyo a padres y profesores, denuncia online, formación, sensibilización, guías, campañas... en especial, os recomendamos su canal de Youtube con múltiples vídeos animados, que explican de forma amena todo tipo de situaciones cotidianas sobre nuestra relación con Internet.

4. Actividades

- ¿Tienes claro qué es la mediación parental? Internet Segura for Kids (Is4k) te ayuda en un vídeo con 23 consejos por edades en tan sólo 3 minutos.

- También puedes consultar un ejercicio práctico en la web de Is4K sobre cómo afrontar una situación complicada al descubrir que tu hijo o hija ve contenidos violentos en su tableta.

- ¿Qué tipos de controles parentales existen? En Empantallados nos dan algunas interesantes claves.

- ¿Sabes configurar el control parental? PantallasAmigas te lo explica y subraya que estos sistemas se deben complementar dando ejemplos a los niños y niñas en el uso de las pantallas, educando en el pensamiento crítico y ganándonos su confianza.

4. Actividades

- TikTok es la red social favorita de los adolescentes, muchos de los cuales desconocen cómo gestionar las opciones de privacidad y requieren de un adulto que les oriente. En este taller de Andalucía Compromiso Digital puedes aprender sobre ello.

- ¿Qué consejos darías a un menor sobre noticias falsas, ciberseguridad o acoso en Internet? Busca entre el variado catálogo de recursos educativos de Internet Segura for Kids, Empantallados, PantallasAmigas y el Consejo Audiovisual de Andalucía.

- ¿Qué hacer si tu nieto o nieta te dice que de mayor quiere ser 'influencer'? Internet Segura For Kids nos sugiere un juego didáctico de cartas sobre los riesgos de exponer tu vida en Internet con el fin de concienciar a los más jóvenes de las pautas de seguridad que deben tener en las redes sociales.

5. Más información

- El Consejo Audiovisual de Andalucía convoca anualmente los Premios Andaluces 'El Audiovisual en la Escuela', un certamen para concienciar al profesorado y alumnado de los centros educativos de nuestra comunidad autónoma sobre la importancia de la alfabetización mediática. Recomendamos el visionado de los vídeos ganadores, disponibles en el canal del CAA, que abordan distintos asuntos de actualidad sobre Internet y los medios de comunicación desde una óptica original y crítica.

- ¿Cómo reaccionar ante un conflicto con un menor sobre el uso de los dispositivos y las redes sociales? En Is4k se enumeran algunas pautas a tener en cuenta como el fomento del diálogo, buscar la ayuda de un especialista o la denuncia en casos graves.