COMPRENSIÓN LECTORA 2 DEPARTAMENTO DE TECNOLOGÍA		
CURSO: 2023/2024	**TEMPORALIZACIÓN:** 5 Sesiones de 30 minutos cada una repartidas de lunes a viernes	**GRUPOS:** 3º y 4º ESO
DISTRIBUCIÓN DE LAS SESIONES		
Sesiones	**Título**	**Material a utilizar**
1	¿Qué es (y qué no es) información?	Documento 1.2
2	Qué es la desinformación y por qué hablamos tanto de eso	Documento 2.2
3	¿Por qué se desinforma?	Documento 3.2
4	Cómo identificamos la desinformación	Documento 4.2
5	Creadores de desinformación	Documento 5.2. Actividad

Documento 1- ¿Qué es (y qué no es) información?

Televisión, radio, periódicos digitales, Twitch...Todos los días recibimos mensajes a través de muchos canales y no siempre es fácil saber si lo que tenemos delante es información, opinión, una mezcla de las dos cosas o nada que ver con una noticia (es decir, desinformación).

La información debe estar contrastada y ser lo más objetiva posible. El periodista tiene que evitar sesgos o juicios de valor y basarse en datos y hechos contrastados.

La noticia es el principal género informativo. Su objetivo es transmitir de forma objetiva hechos y acontecimientos de interés público. Para que una entrevista sea considerada información debe estar contrastada por el periodista. Es decir, la persona entrevistada puede responder con una mentira y es labor del periodista detectarla para desmentirla o no publicarla.

¿Y qué pasa con una columna de opinión, una tertulia televisiva o una emisión en Twitch? Suelen ser géneros mixtos, que pueden mezclar información contrastada y la opinión del autor. ¿Cómo sabemos en estos casos si lo que nos están contando es información u opinión? Hay que fijarse, por ejemplo, si está apoyado en fuentes y datos públicos y fiables. Y oye, que la opinión no está mal, pero hay que saber que es precisamente eso: la opinión de una persona.

Además, hay que tener mucho ojo porque en ocasiones los desinformadores disfrazan la opinión de información contrastada: nos presentan como noticia algo que no lo es, que no aporta datos ni hechos, para intentar colárnosla. Asimismo, la opinión puede incluir mentiras que pueden desmontarse con datos y hechos.

Los desinformadores también tratan de hacer pasar por noticias y medios de comunicación cosas que no lo son. Es decir: no todo lo que parece una noticia lo es, ni todas las webs son medios (aunque tengan una cabecera o secciones). Y por supuesto, una captura de pantalla que llega a través de WhatsApp puede ser un bulo, aunque tenga apariencia de noticia.

<u>Comunicar e informar: ¿son lo mismo?</u>

Informar no es lo mismo que comunicar. Cuando comunicamos es esencial el vínculo con el comunicador (si nos gusta cómo se expresa, si nos interesa el tema, si la plataforma es adecuada a nuestros intereses, etc.). En otras palabras, cuando nos comunicamos importa tanto la forma como su contenido.

Cuando hablamos de informar, lo más importante es el mensaje y que esté basado en datos y hechos. Para informar hace falta una metodología, unas reglas. Los periodistas estudian y aplican metodologías para buscar y organizar información, valorar correctamente hechos y datos, contrastar declaraciones y aprender a evaluar correctamente sus fuentes.

<u>Las 5W</u>

Las noticias deben intentar responder a las 5W: who (quién), what (qué), when (cuándo), where (dónde), why (por qué):

- ¿QUÉ?: Los acontecimientos, los hechos o conceptos que forman la noticia. La esencia del hecho. ¿Qué ha sucedido? ¿De qué se trata? ¿Está contrastado?
- ¿QUIÉN?: ¿Quién o quiénes son los protagonistas de la noticia?
- ¿CUÁNDO?: ¿Cuándo se produjo el hecho del que estamos hablando? ¿Cuándo fueron recopilados los datos a los que se refiere la información? (ojo, porque los malos hacen pasar sucesos antiguos por actuales para desinformar).
- ¿DÓNDE?: ¿En qué lugar ocurrió? (cuidado, porque algunos contenidos sitúan un hecho real en un lugar equivocado y eso genera desinformación).
- ¿POR QUÉ?: ¿Por qué se produjo? ¿Cuál ha sido la causa? ¿Qué pasó antes?

Además, se podrían añadir otra pregunta: ¿CÓMO? y señalar cómo sucedieron los hechos.
Si al recibir un enlace o una captura de pantalla no sabes si se trata de una información o de otro tipo de comunicación (bromas, opinión, crítica cultural, etc..) puedes fijarte en:
- La firma: ¿El contenido está firmado por algún periodista y/o medio de comunicación reconocible? ¿Si utilizas un buscador encuentras más contenido firmado por el periodista o el medio de comunicación?
- El lenguaje: ¿El lenguaje es objetivo y prescinde de opiniones, adjetivos y construcciones sensacionalistas?
- El objetivo: ¿El objetivo es narrar la realidad transmitiendo hechos o acontecimientos de interés público?
- Las fuentes: ¿El contenido incluye las fuentes en las que se basa? Si cita estudios, estadísticas u otros contenidos, ¿Pone un link a esas fuentes?
¿Es localizable? ¿Si buscas por las palabras del titular o por el nombre del medio dentro de un buscador puedes encontrarla?
Si has contestado que sí a todas las preguntas es probable que se trate de una noticia (pero para asegurarte haz clic en el enlace o busca el texto que aparece en el pantallazo en un buscador).
Para saber más:
1) ¿Has escuchado que para hacer buen periodismo debemos dar voz a los dos lados? Los medios de comunicación no deben dar voz a los dos lados sino contar los datos y las evidencias y destapar las mentiras. Por ejemplo, entrevistar a un difusor de bulos y luego a científicos especializados en esa área significa poner a los dos al mismo nivel en la argumentación, dando al primero un peso que no merece y dando más visibilidad a sus patrañas.
2) Porque confundir la opinión de un columnista con la opinión del medio en el que escribe crea bulos y desinformaciones. https://bit.ly/3xnfEKV

Documento 2- Qué es la desinformación y por qué hablamos tanto de eso

Hoy en día casi todos tenemos internet y un smartphone. Y eso ha cambiado la forma en que se produce y se consume la información. Piensa en lo que costaba antes hacer un periódico en papel, un programa de radio o un programa de televisión: no era ni fácil ni barato. Ahora cualquier persona puede publicar, compartir y producir contenidos de manera fácil y rápida. Como resultado, tenemos más acceso que nunca a la información, pero constantemente circulan bulos y patrañas.

Cada día recibimos contenidos falsos o manipulados que se hacen pasar por "informaciones" y tenemos que aprender a reconocerlos y así poder tomar decisiones informadas. Hay que entender que la información veraz y de calidad es un derecho fundamental en una democracia.

En 2020 llegó la pandemia y también la ola más grande de desinformación que hemos visto: más desinformación y más peligrosa que nunca, bulos que han generado más incertidumbre de la que ya había y que han dañado a personas.

Cambios en nuestra forma de consumir información

La desinformación no es un fenómeno nuevo, pero desde la llegada de internet se ha popularizado. Consumimos información sobre todo en Internet y mucha de ella nos llega por redes sociales. En el estudio Digital News Report (2021), del Reuters Institute, podemos ver el crecimiento de las plataformas como fuentes de difusión de noticias en España:

- 78% de las personas consumen noticias de fuentes online.
- 73% lo hacen a través del móvil.
- 55% utilizan las redes sociales para informarse.
- 35% de los españoles consultados consumen información a través de WhatsApp.

Antes, cuando buscábamos información, leíamos un periódico en papel, escuchábamos los pitidos que anunciaban un informativo de radio o encendíamos la tele y veíamos el telediario. Teníamos lo que llamamos 'anclas' que nos ayudaban a identificar que lo que teníamos delante era información. Ahora gran parte de los contenidos que nos llegan viene en formato de captura de pantalla sin fuente, fecha o autor, haciendo más difícil que sepamos si son o no son periodismo. Cuando nos envían una captura en WhatsApp, no tenemos esas anclas que nos dicen "esto es un medio" o "esto es una página web que no es un medio", o "esto es sátira". Hemos perdido esas anclas y en ese proceso debemos reaprender cómo consumir información.

Video: ¿Qué es la desinformación? https://www.youtube.com/watch?v=0AiA0ufgjbw

Debatir los pensamientos al respecto en clase.

Documento 3- ¿Por qué se desinforma?

Sabemos que con la expansión de los móviles con acceso a internet ha aumentado el acceso a la información. Pero dentro de los contenidos que consumimos cada día, muchos pueden ser bulos, patrañas o incluso timos.

Pero ¿por qué se desinforma? Algunas veces se hace para obtener beneficios económicos, otras por influir en una batalla ideológica o simplemente por pura maldad.

En Maldita.es se han identificado las motivaciones más frecuentes:

● Interés económico: intentan que hagas clic en una página con titulares engañosos o bulos para generar ingresos publicitarios. También se conoce como “clickbait”. Existe otra práctica conocida como “phishing”, en la que los timadores buscan hacerse con tus datos personales o bancarios haciéndose pasar por una empresa o institución que conoces.

● Interés ideológico: tratan de modificar nuestra percepción de la realidad y presentan unos hechos distorsionados que fomentan el discurso de odio o favorecen que apoyemos una determinada ideología. Por ejemplo, la desinformación sobre migraciones.

● Interés en crear caos o “trolear”: bulos que, en apariencia, solo buscan sembrar el caos. Con el tiempo pueden hacer que desconfiemos de todo lo que nos llega de los medios y las fuentes oficiales.

En Maldita.es se han caracterizado a los diez personajes que más frecuentemente alimentan el ecosistema de la desinformación, personas que tienen distintas intenciones a la hora de crear y/o compartir bulos.

LOS 10 PERSONAJES DE LA DESINFORMACIÓN

La desinformación tiene muchos formatos: webs, capturas de pantalla, audios, vídeos, etc y detrás de ellos siempre hay personas que los crean, todas ellas tienen distintas intenciones.

1 GENERADOR DE ODIO

Crea mensajes falsos para atacar a grupos específicos como mujeres, población LGBTI+, migrantes o grupos minoritarios. Busca viralizar el odio.

2 CONSPIRANOICO

Crea teorías sin pruebas, evidencias científicas o datos contrastados. Ante situaciones de crisis o miedo son consumidas y se viralizan como reales.

3 IMITADOR

Imita a un medio de comunicación o se hace pasar por periodista. Quiere que hagas click en su sitio y veas la publicidad por la que recibe dinero o que su mensaje político se viralice.

4 ESTAFADOR

Crea contenido falso imitando marcas o aprovechando una crisis para obtener datos o dinero con el engaño.

5 POLÍTICO

El poder da credibilidad y algunos políticos aprovechan esa confianza para esparcir sus mentiras e intentar cambiar el debate público.

6 FAMILIAR

Las personas confían más en familiares o amigos cercanos. Reenvía bulos o contenidos sin pruebas y el receptor se los cree porque confía en quien lo manda.

7 FALSO INFILTRADO

Afirma que tiene información real sobre un lugar donde supuestamente vive o trabaja y pide que confíen en ella porque tiene datos "desde dentro". Lo hace sin pruebas.

8 BROMISTA

Crea una broma, pero alguien no la entiende y la comparte a otros como si fuera real; se convierte en un bulo.

9 CELEBRIDAD

Su notoriedad le da credibilidad y distribuye bulos o contenidos sin pruebas.

10 BOT

Persona contratada para manejar cuentas falsas de redes sociales para difundir desinformación con el fin de influir en el discurso público.

MALDITA.ES

Fuente: elaboración propia

Formatos de la desinformación

Fuente: Maldita.es (elaboración propia)

Cómo se amplifica la desinformación

Fuente: Maldita.es (elaboración propia)

- Opinión personal sobre las tablas, ¿conoces algún perfil de personaje de desinformación cerca tuya? ¿Compartes noticias falsas o desinformación en algún formato presentado más arriba? ¿Estás de acuerdo en cómo se va amplificando la desinformación? ¿Es igual en tu entorno más cercano?
- Haz autocrítica y piensa a través de dónde te llega la desinformación en tu día a día y trata de ponerle nombre según las tablas mostradas más arriba. Propón medidas para evitar que esto ocurra.

Documento 4- Cómo identificamos la desinformación

Ver vídeo https://cutt.ly/zRQ5CYI (Fuente: Maldita.es)

Para identificar la desinformación es necesario que analicemos siempre:
● El lenguaje: el lenguaje de los bulos casi siempre es sensacionalista para atraer nuestra atención y para apelar directamente a nuestras emociones (miedo y enfado son las preferidas).
● Las evidencias: la mayoría de bulos nunca aportan ninguna evidencia como pruebas, enlaces o datos concretos.
● Las fuentes: tampoco esperes que los contenidos falsos te indiquen cuáles son sus fuentes porque o no las hay o no las conoce nadie.

Consejos básicos para la lucha contra la desinformación

Obstáculos informativos: sesgos, burbujas y polarización

Además de identificar la desinformación debemos tener en cuenta que las personas procesamos la información de manera distinta. Para entender cómo se distribuye la información (y la desinformación) en internet es fundamental conocer un poco de cómo nos afectan los algoritmos, los filtros burbuja, las cámaras de eco y nuestros sesgos cognitivos.

Los sesgos cognitivos

Nuestro cerebro utiliza atajos mentales para simplificar la vida diaria, porque a veces tenemos que tomar decisiones de forma rápida.

Estos atajos responden a la necesidad evolutiva de realizar un filtrado selectivo de los estímulos que nos llegan para así liberarnos de la cantidad de procesos mentales que tendríamos que realizar si procesáramos cada vez toda la información sensorial que recibimos.

El problema es que esos atajos nos pueden llevar a juicios incorrectos o interpretaciones erróneas: esto son los sesgos cognitivos.

En este vídeo te explicamos cómo puedes entender mejor cómo funciona nuestro cerebro y en qué nos debemos fijar para intentar aprender a protegernos:

Ver vídeos: https://youtu.be/kx07LKnyydY?si=4RpPsuqNs_7QOWdc Fuente: Maldita.es

Cámara de eco, filtro burbuja y polarización

Cuando seleccionamos contenido dentro de buscadores, compramos en tiendas on-line o pinchamos “me gusta” en páginas comerciales permitimos, aunque sin darnos cuenta, que las plataformas almacenen informaciones valiosas: nuestros gustos, nuestra localización, nuestra edad, nuestros hábitos de consumo. Configuramos un entorno a nuestra medida (o mejor, a medida de las empresas que nos puedan vender algo). Esta colección de datos condiciona los resultados de los motores de búsqueda que son personalizados construyendo lo que se conoce como “filtro burbuja” (filter buble). En otras palabras, la información y los formatos en que se me presentará este contenido depende de mis anteriores búsquedas, compras e interacciones.

Los motores de búsqueda y las plataformas están constantemente experimentando para que su contenido sea lo más satisfactorio posible para el usuario y, consecuentemente el más lucrativo. Con el paso del tiempo, los filtros burbuja pueden evolucionar y formar las “cámaras de eco” (echo chambers), creando grupos de usuarios que no tienen acceso a información contraria a sus creencias, lo que puede derivar en una gran polarización.

Los fact-checkers o verificadores

La figura de los fact-checkers o verificadores no es nueva: la precisión, el rigor y la información basada en datos y hechos están en la base del periodismo de calidad y, en este sentido, la verificación es parte de una buena práctica periodística.

Con el aumento de la desinformación online, la necesidad de fact-checkers se hizo aún más evidente: además de verificar el discurso político y periodístico había que verificar el discurso público, lo que circula en redes sociales. La verificación, que ya era parte de la metodología periodística, pasa a ser considerada también un género aparte y hoy día una de las variantes más importantes dentro del ecosistema periodístico digital.

El objetivo de la verificación es dotar a la ciudadanía de herramientas e información que les permita crearse opiniones con todos los datos y los hechos contrastados en la mano y tomar decisiones informadas. La desinformación puede influir sobre cómo está pensando la sociedad y cómo se está enfrentando a los problemas del día a día y, por eso, los verificadores tienen como misión central arrojar luz y datos sobre esas cuestiones.

Actividades:

1. ¿Qué páginas de internet conoces o usas para contrastar información?
2. Debate a cerca de la lectura

Documento 5.2. Actividad - Creadores de desinformación

En esta actividad, asumimos el rol de creadores de desinformación. Escribe un bulo en forma de un pequeño texto en formato periodístico, respondiendo a las 5W del periodismo (quién, qué, cuándo, dónde y por qué) para presentar el suceso de manera sencilla y completa. El tema es libre, pero tiene que estar relacionado con un suceso real. La narrativa tiene que ser verosímil y estar escrita de acuerdo con las características más frecuentes de los bulos.
La «noticia» tiene que tener título y, por lo menos, dos párrafos. Al acabar la tarea, cambia tu bulo con el de un compañero o compañera y analiza las características de su texto que indican que se trata de desinformación. Algunas ideas para abrir el debate:

- ¿Qué deberías observar para comprobar que se trata de un bulo?
- ¿Qué características tiene este contenido que nos indican que puede ser falso?
- ¿Cuál era el objetivo de difundir esta mentira? (Publicidad, trolear, timos, sembrar el caos, interés ideológico u otros)
- ¿Qué pruebas necesitas para confirmar que es un bulo?
- ¿Cómo podrías convencer a tus amigos de que se trata de desinformación?
- ¿Crees que este contenido podría viralizarse dentro de tu instituto?
- ¿Cuál sería el impacto de publicar la historia sin saber si es real o no?
- ¿Qué personas o colectivos serían perjudicados con este bulo?

ANEXO 3.1.a, tarjetas de juego (a recortar y entregar al alumnado)

Antivirus Instalar un antivirus en el móvil y mantenerlo siempre actualizado	**Antivirus** Instalar un antivirus para PC y mantenerlo siempre actualizado	**Actualizaciones** Mantener siempre actualizado el sistema operativo, el antivirus y las aplicaciones
Pantalla de desbloqueo Proteger el desbloqueo de pantalla con huella digital, contraseña, pin o un patrón	**Cerrar sesión** Cerrar sesión siempre al terminar de trabajar con la página de Instagram, Facebook o Twitter	**Acceso/login en 2 pasos** Configurar la verificación en dos pasos: cada vez que se intente entrar en tu correo, lo tendrás que autorizar desde tu móvil
Contraseñas robustas Poner en el correo electrónico una contraseña robusta: larga, con mayúsculas, minúsculas, números y símbolos y sin seguir un patrón predecible	**Contraseñas secretas** Mantener las contraseñas siempre en secreto	**Tiendas de apps oficiales** Instalar aplicaciones solo desde las tiendas oficiales (Google Play y App Store)
Apps sospechosas Antes de instalar una app, comprobar su información, desarrollador, nº de comentarios y valoraciones, si son positivas o negativas...	**Permisos de una app** Antes de instalar una app, asegurarse de que los permisos que nos pide están justificados y parece lógico que los necesite	**No dar datos personales** Evitar dar información personal, ni números de teléfono en Internet
Desconfiar y sospechar Desconfiar de mensajes muy llamativos a través de las redes sociales, para ver un vídeo no hace falta instalar nada	**Desconfiar y sospechar** Desconfiar de mensajes alarmantes sobre fallos de seguridad de tu móvil. Si te ofrecen instalar algo para solucionarlos, no piques	**Copias de seguridad** Realizar copias de seguridad de tus contactos, documentos, fotos, etc. periódicamente para no perderlos si sufres un problema de seguridad

ANEXO 3.1.a (continuación), tarjetas de juego (a recortar y entregar al alumnado)

Malware/virus archivos Recibes un email en el móvil y tiene un archivo adjunto infectado con un malware o virus	**Malware/virus archivos** Te dejan una memoria USB con información para un trabajo y tiene un archivo infectado con malware o virus	**Malware/virus genérico** Hace meses que no actualizas el ordenador, el antivirus ni los programas y de repente empieza a hacer "cosas raras"
Acceso no deseado Te olvidas el móvil en el recreo y está desbloqueado, con lo que cualquiera puede ver tus cosas	**Acceso no deseado** Sales del aula de informática y te dejas la página de Instagram, Facebook o Twitter con la sesión abierta	**Acceso no deseado** Alguien te ve poner la contraseña en el aula de Informática, y se mete en tu correo electrónico
Acceso no deseado Alguien intenta adivinar tu contraseña para entrar en tu correo electrónico	**Acceso no deseado** Tu mejor amigo/a tiene tu contraseña y entra en tu cuenta de Instagram	**Malware/virus y apps** Instalas un juego desde una tienda de apps (market) no oficial donde lo anuncian gratis, pero infecta tu móvil con un malware o virus
Malware/virus y apps Instalas una nueva app de filtros y efectos para tus fotos pero el móvil hace cosas raras y publica en tu nombre publicidad en tu Instagram	**Malware/virus y apps** Instalas una app de linterna y te pide permiso de acceso a Internet, GPS, identidad, cuentas, contactos, memoria, etc.	**Fraudes/SMS Premium** Para desbloquear un nivel y seguir jugando tienes que meter tu número de móvil y empiezas a recibir mensajes SMS Premium
Malware/virus y redes sociales Un amigo/a te manda un vídeo que es "alucinante", y que "no te lo vas a creer", pero al reproducirlo te pide instalar algo que infecta tu móvil	**Malware/virus y navegación** Te salta un mensaje de alerta "tu batería está infectada" y pinchas en el botón que sale para "solucionarlo", pero... no para de salir publicidad	**Malware/virus, ransomware** Tu ordenador ha sido "secuestrado", no puedes usarlo ni acceder a tus trabajos y fotos hasta que no pagues un rescate

ANEXO 3.1.b, listado de papeles emparejados (a utilizar por los educadores)

Nº	Herramientas y conductas de seguridad	Riesgos y problemas de seguridad
1	**Antivirus** Instalar un antivirus en el móvil y mantenerlo siempre actualizado	**Malware/virus archivos** Recibes un email en el móvil y tiene un archivo adjunto infectado con un malware o virus
2	**Antivirus** Instalar un antivirus para PC y mantenerlo siempre actualizado	**Malware/virus archivos** Te dejan una memoria USB con información para un trabajo y tiene un archivo infectado con malware o virus
3	**Actualizaciones** Mantener siempre actualizado el sistema operativo, el antivirus y las aplicaciones	**Malware/virus genérico** Hace meses que no actualizas el ordenador, el antivirus ni los programas y de repente empieza a hacer “cosas raras”
4	**Pantalla de desbloqueo** Proteger el desbloqueo de pantalla con huella digital, contraseña, pin o un patrón	**Acceso no deseado** Te olvidas el móvil en el recreo y está desbloqueado, con lo que cualquiera puede ver tus cosas
5	**Cerrar sesión** Cerrar sesión siempre al terminar de trabajar con la página de Instagram, Facebook o Twitter	**Acceso no deseado** Sales del aula de informática y te dejas la página de Instagram, Facebook o Twitter con la sesión abierta
6	**Acceso/login en 2 pasos** Configurar la verificación en dos pasos: cada vez que se intente entrar en tu correo, lo tendrás que autorizar desde tu móvil	**Acceso no deseado** Alguien te ve poner la contraseña en el aula de Informática, y se mete en tu correo electrónico
7	**Contraseñas robustas** Poner en el correo electrónico una contraseña robusta: larga, con mayúsculas, minúsculas, números y símbolos y sin seguir un patrón predecible	**Acceso no deseado** Alguien intenta adivinar tu contraseña para entrar en tu correo electrónico
8	**Contraseñas secretas** Mantener las contraseñas siempre en secreto	**Acceso no deseado** Tu mejor amigo/a tiene tu contraseña y entra en tu cuenta de Instagram

ANEXO 3.1.b (continuación), listado de papeles emparejados (a utilizar por los educadores)

Nº	Herramientas y conductas de seguridad	Riesgos y problemas de seguridad
9	**Tiendas de apps oficiales** Instalar aplicaciones solo desde las tiendas oficiales (Google Play y App Store)	**Malware/virus y apps** Instalas un juego desde una tienda de apps (market) no oficial donde lo anuncian gratis, pero infecta tu móvil con un malware o virus
10	**Apps sospechosas** Antes de instalar una app, comprobar su información, desarrollador, nº de comentarios y valoraciones, si son positivas o negativas…	**Malware/virus y apps** Instalas una nueva app de filtros y efectos para tus fotos pero el móvil hace cosas raras y publica en tu nombre publicidad en tu Instagram
11	**Permisos de una app** Antes de instalar una app, asegurarse de que los permisos que nos pide están justificados y parece lógico que los necesite	**Malware/virus y apps** Instalas una app de linterna y te pide permiso de acceso a Internet, GPS, identidad, cuentas, contactos, memoria, etc.
12	**No dar datos personales** Evitar dar información personal, ni números de teléfono en Internet	**Fraudes/SMS Premium** Para desbloquear un nivel y seguir jugando tienes que meter tu número de móvil y empiezas a recibir mensajes SMS Premium
13	**Desconfiar y sospechar** Desconfiar de mensajes muy llamativos a través de las redes sociales, para ver un vídeo no hace falta instalar nada	**Malware/virus y redes sociales** Un amigo/a te manda un vídeo que es “alucinante”, y que “no te lo vas a creer”, pero al reproducirlo te pide instalar algo que infecta tu móvil
14	**Desconfiar y sospechar** Desconfiar de mensajes alarmantes sobre fallos de seguridad de tu móvil. Si te ofrecen instalar algo para solucionarlos, no piques	**Malware/virus y navegación** Te salta un mensaje de alerta “tu batería está infectada” y pinchas en el botón que sale para “solucionarlo”, pero… no para de salir publicidad
15	**Copias de seguridad** Realizar copias de seguridad de tus contactos, documentos, fotos, etc. periódicamente para no perderlos si sufres un problema de seguridad	**Malware/virus, ransomware** Tu ordenador ha sido “secuestrado”, no puedes usarlo ni acceder a tus trabajos y fotos hasta que no pagues un rescate