Programa de Jornadas Escolares para el uso seguro y responsable de Internet por los menores

Unidad Didáctica 3

CONTROLA LA TECNOLOGÍA

La protección de dispositivos y servicios online, la gestión de contraseñas, opciones de seguridad y protección frente a aplicaciones potencialmente peligrosas.

SESIONES Y OBJETIVOS

3.1. Cierra con llave

- Valorar las consecuencias de no proteger sus dispositivos y servicios online.
- Asumir buenas prácticas para la gestión de contraseñas.
- Configurar opciones de seguridad en dispositivos móviles y redes sociales.

3.2. ¿Qué apps merecen la pena?

- Reforzar el espíritu crítico al descargar y utilizar aplicaciones móviles.
- Conocer las motivaciones que hay detrás de las aplicaciones gratuitas.
- Aprender a seleccionar aplicaciones de calidad con seguridad.

GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA Y EMPRESA
INSTITUTO NACIONAL DE CIBERSEGURIDAD
Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

SESIÓN 3.1. Cierra con llave

RESUMEN

Más allá de mostrar cómo crear una contraseña robusta, nos centraremos en enseñar hábitos de seguridad para proteger los dispositivos y la información, como es por ejemplo no compartir las contraseñas, establecer patrones de desbloqueo y ajustes de seguridad para las cuentas online.

METODOLOGÍA

Centrada en promover la reflexión sobre problemas de seguridad y posibles soluciones a través de dinámicas cooperativas. Complementariamente se plantea la práctica de ciertas técnicas para obtener contraseñas robustas.

MATERIALES

Tarjetas de juego (anexo 3.1.a) para cada alumno, listado de papeles emparejados (anexo 3.1.b) para el docente, equipo audiovisual con Internet para el grupo, equipos conectados a Internet (o en su lugar juego de caracteres [anexo 3.1.c]) para cada pequeño grupo.

DESCRIPCIÓN DE LAS ACTIVIDADES

1. **Reflexión inicial** (10')

   Reflexión grupal sobre la protección de nuestros dispositivos y servicios online haciendo una analogía entre la seguridad física de nuestra vida cotidiana (¿dejamos la puerta de casa abierta?, ¿las llaves del coche puestas?) y la ciberseguridad en nuestro día a día digital (¿y qué pasa con nuestro móvil?, ¿seguro que nadie puede acceder a nuestras redes sociales?, ¿nunca nos hemos dejado el móvil desbloqueado en un lugar con más personas?).

2. **Dinámica interactiva** (25')

   Cada participante dispone de una tarjeta de juego (anexo 3.1.a) que puede ser una herramienta de seguridad o una conducta de riesgo. Sin desvelar cuál tiene, cada uno debe buscar su pareja, es decir, quien tenga una herramienta de seguridad debe encontrar una conducta de riesgo a la que pueda hacer frente, y quien tenga una conducta de riesgo debe encontrar una herramienta de seguridad que le pueda proteger. Cada tarjeta está directamente ligada a otra (aunque puede haber varias parcialmente relacionadas), por lo que al final de la actividad todos los participantes deben estar emparejados (ver anexo 3.1.b). Terminado el tiempo, se presentarán por parejas ante el gran grupo debatiendo si efectivamente su asociación es la más adecuada, si la herramienta de seguridad protegería efectivamente frente al riesgo y si habría otras herramientas de seguridad que podrían complementarla.

3. **Juego online** (15')

   A modo de conclusión, se recuerda la necesidad de tener contraseñas seguras, con el juego online de Google "Torre del tesoro" (que nos ofrece sencillos trucos para crear contraseñas robustas y seguras) y una herramienta online para comprobar la fortaleza de una contraseña, o bien una dinámica de construcción de contraseñas utilizando distintos caracteres (anexo 3.1.c).

NOTAS PARA DOCENTES

"La mejor herramienta de seguridad es tu sentido común. La mejor prevención, tus buenos hábitos en el uso de la tecnología"

La **reflexión inicial** pretende hacer una analogía entre las medidas de seguridad de nuestro día a día (cerrar la puerta de casa, quitar las llaves del coche, etc.) y las de los medios digitales.

En la seguridad de nuestro móvil, ¿tenemos una actitud responsable o despreocupada?, si cerramos la puerta de casa, ¿por qué dejamos el móvil sin un bloqueo de pantalla seguro? (lo mínimo es un patrón de desbloqueo. Mejor una contraseña o una huella digital).

Si creemos que nadie puede acceder a nuestras redes sociales planteémonos si nunca nos hemos olvidado el móvil (aunque fuera un momento), o si nunca nos hemos dejado abierta una web en un PC del centro, o incluso si nuestra contraseña (o la pregunta de seguridad para recuperarla) es tan sencilla que alguien que nos conozca la puede adivinar.

La **dinámica interactiva** busca el diálogo y la reflexión del alumnado sobre los riesgos y problemas que se pueden encontrar online y la manera de protegerse frente a ellos.

A cada alumno se le entrega una tarjeta (anexo 3.1.a), con una "solución", herramienta o conducta de seguridad (cabecera verde clarito), o bien un "problema" de seguridad o una conducta de riesgo (cabecera gris oscuro). Cada "problema" está ligado a una "solución" (anexo 3.1.b), de modo que los participantes tienen una y solo una pareja. Su objetivo es tanto encontrar a su pareja, como ayudar a sus compañeros/as a encontrar las suyas.

Hay herramientas de seguridad que podrían hacer frente a varios riesgos, así como riesgos para los que se podrían aplicar varias herramientas de seguridad. Pero cada situación presenta ciertos matices, de modo que solo hay una combinación "ideal" para cada uno.

A la indicación de la persona dinamizadora, se moverán por el aula en busca de pareja. Deben emplear sus propias palabras para explicar su papel y su comportamiento, evitando utilizar los títulos de sus tarjetas. Han de hacer preguntas a los demás para ver si podrían ser sus parejas. Quien tenga una herramienta de seguridad debe encontrar una conducta de riesgo a la que pueda hacer frente, y quien tenga una conducta de riesgo debe encontrar una herramienta de seguridad que le pueda proteger.

Al juntarse una pareja deben continuar con el juego, yendo juntos a ayudar a sus compañeros (pueden cambiar de pareja si encuentran otra más ajustada a su papel).

Cuando se hayan formado todas las parejas se comprobarán los resultados. Cada pareja se presentará ante el grupo leyendo sus papeles y explicando por qué la herramienta de seguridad protegería frente al riesgo. De este modo se da pie a un pequeño debate sobre si es la combinación más adecuada (por ejemplo ¿algún otro compañero/a cree que su solución/problema se ajustaría mejor?). Cuando estemos de acuerdo en que se trata de la combinación correcta (anexo 3.1.b), podemos analizar si habría otras herramientas de seguridad complementarias en ese caso, por ejemplo:

- Frente a **virus/malware**: antivirus, actualizaciones de sistema y aplicaciones, copias de seguridad, desconfiar y sospechar de mensajes, publicaciones y archivos, etc.
- En **dispositivos móviles**: además de lo anterior, descargar apps solo de tiendas oficiales, comprobando la información disponible sobre ellas, sus permisos, etc.

- Para evitar que accedan a **nuestra información**: proteger la pantalla de desbloqueo, acordarse de cerrar sesión, configurar la verificación en dos pasos, utilizar contraseñas robustas, no compartirlas con nadie, dar los mínimos datos personales, etc.
- Para evitar **fraudes**: desconfiar y sospechar de mensajes, apps, no dar datos, etc.

Finalmente se plantea utilizar el **juego online** de Google "Torre del tesoro" para aprender algunos trucos que nos permitirán crear contraseñas robustas y seguras:

> Nos movemos hacia adelante, pudiendo solo girar y saltar (con las flechas del teclado) para esquivar los obstáculos y recoger los caracteres (dados ❑). En el 1º nivel solo hay dados ❑ *verdes* con letras minúsculas. Al terminarlo, formaremos palabras (en inglés) con las letras recogidas, a modo de base (sencilla de recordar) para una contraseña segura.
>
> En los siguientes niveles encontraremos también dados ❑ *azules* con letras mayúsculas y dados ❑ *rojos* con números y símbolos. Al completarlos nos aparecerá la palabra creada anteriormente, lista para combinar con las mayúsculas, números y símbolos recogidos, de modo que obtenemos una contraseña mucho más robusta sobre la misma base sencilla.
>
> Finalmente, se puede apuntar la contraseña obtenida como ejemplo para crear nuestras futuras contraseñas de manera segura, e incluso se puede acceder a una web para comprobar su fortaleza.

Como alternativa se plantea una **dinámica de construcción de contraseñas** en pequeños grupos (3-4 personas), utilizando caracteres de papel (anexo 3.1.c).

> En primer lugar a cada grupo se le facilitan las letras minúsculas. Deben repartírselas en un tiempo breve para formar cada uno una palabra sencilla. Si les faltan letras, han de llegar a acuerdos con sus compañeros (se puede utilizar letras "similares", o dejar palabras incompletas a la espera de las mayúsculas, los números y los símbolos).
>
> Seguidamente se les darán las mayúsculas para completar sus palabras o cambiar algunas minúsculas por mayúsculas. En una tercera fase se les facilitarán los números y los símbolos, de modo que puedan añadirlos o sustituir algunas letras. De este modo habrán obtenido una contraseña suficientemente robusta sobre una base sencilla de recordar.
>
> A continuación podrán debatir en pequeño grupo si las contraseñas que han obtenido les parecen más o menos seguras y por qué motivos. Deberán ponerse de acuerdo a la hora de elegir la que consideran más robusta.
>
> Finalmente se realizará una puesta en común en gran grupo de las contraseñas seleccionadas y los motivos por los que consideran que son más seguras ¿estamos todos/as de acuerdo en que son buenas contraseñas?, ¿nos ha parecido muy difícil construirlas?

RECUERDA

Si no proteges tus dispositivos y cuentas de redes sociales, te expones a multitud de problemas online. Ponte al día y revisa sus opciones de seguridad, es más sencillo de lo que parece.

SESIÓN 3.2. ¿Qué apps merecen la pena?

RESUMEN

Antes de instalar una app, valorarla críticamente en términos de necesidad, funcionalidad, desarrollador, permisos que requiere, comentarios, etc. a fin de determinar si parece útil y positiva o puede ser potencialmente peligrosa.

METODOLOGÍA

Se centra en la reflexión y el debate sobre casos ficticios (aunque realistas) de aplicaciones móviles disponibles para instalar. Complementariamente se incluyen recursos multimedia.

MATERIALES

Un equipo multimedia conectado a Internet para el grupo, fichas de apps (anexo 3.2.a) y material de escritura.

DESCRIPCIÓN DE LAS ACTIVIDADES

1. **Reflexión inicial** (10')
   Se plantean varias preguntas sobre nuestro uso de las aplicaciones móviles: ¿cuántas apps tenemos en el móvil/tablet?, ¿son todas gratuitas?, ¿nos hemos planteado alguna vez por qué pueden ser gratuitas?, ¿solemos mirar la información de una app y sus permisos antes de instalarla?

2. **Dinámica debate** (20')
   Cada grupo analizará las fichas de las apps (anexo 3.2.a) y debatirá sobre la seguridad o no de instalar cada una de ellas. Se debe plantear la relación entre la necesidad que motiva su instalación, sus funcionalidades, los permisos que solicita y el resto de información disponible sobre la misma: ¿qué apps instalaríais?, ¿cuál os parece más útil?, ¿os habéis fijado en los permisos que pide, o en la información de la ficha?, ¿son adecuados o excesivos? Asimismo, se plantean los riesgos que se pueden desprender de su uso ¿qué datos manejan sobre nosotros?, ¿Cómo podrían obtener un beneficio?
   Finalmente se pondrán en común las conclusiones a las que ha llegado cada grupo.

3. **Demostración sobre permisos y apps** (10')
   Algunas personas voluntarias enseñarán desde el PC del aula la forma en que se muestra la información de las apps y sus permisos en Google Play. Asimismo presentarán la manera de revisar los permisos de las apps instaladas en un móvil o tablet (invitando al alumnado a comprobar en casa en sus dispositivos familiares los permisos de las apps instaladas).
   Como alternativa se plantea la creación en pequeños grupos de un listado de buenas prácticas sobre la instalación y uso de apps, poniéndolo en común en gran grupo.

4. **Conclusiones** (10')
   Proyección de un vídeo a elegir: Privacidad y permisos en apps y Videojuegos "gratuitos" (PantallasAmigas), Permisos de apps (PrivacyNow). Se planteará la reflexión sobre lo que más nos haya llamado la atención del vídeo y su relación con esta sesión.
   Para terminar, se pedirá a algunas personas voluntarias que recapitulen lo aprendido en la sesión resumiéndolo en una frase o consejo.

NOTAS PARA DOCENTES

"Cuando instalas una app le das acceso a mucha información privada"

La **reflexión inicial** pretende hacernos más conscientes del uso que hacemos de las aplicaciones móviles (apps)

> En cuanto al número de apps en nuestro móvil/tablet, seguramente tenemos muchas más de las que imaginamos y de las que utilizamos a diario. Sobre la gratuidad de las apps, ¿nos planteamos cómo es posible?, ¿de dónde obtienen ingresos? Se suele pensar en la publicidad, pero también puede haber publicidad personalizada, venta de datos de perfiles personales, compras integradas en la app, etc. En este sentido, ¿solemos mirar la información de una app y sus permisos antes de instalarla o bien aceptamos los términos y condiciones sin más?

La **dinámica** plantea el **debate** en pequeños grupos sobre las fichas de apps (anexos 3.2.a y b) identificando posibles riesgos y llegando a un acuerdo sobre si es más o menos seguro instalarlas. Recordar que se trata de fichas totalmente ficticias, y con una información limitada.

> En primer lugar se distribuirán los participantes en grupos de 3-4 personas, repartiendo una ficha de app (anexo 3.2.a) a cada grupo. Deben leer cada ficha, analizar la información disponible, plantearse la necesidad que puede motivar a buscar una app así, comparar sus funcionalidades con los permisos que solicita, valorar el resto de información disponible (categoría, opiniones, fecha de última actualización, número de descargas, información del desarrollador, política de privacidad). Su objetivo es identificar los posibles riesgos de instalar esa app y debatir entre ellos si les parece o no de confianza y por qué.
>
> El tiempo para el análisis ha de ser suficiente para que haya debate en cada grupo. En cuanto se termine el análisis de una app, se intercambiará la ficha con otro grupo para analizar una nueva. En el momento en que la persona dinamizadora considere oportuno (por ejemplo tras analizar 3 ó 4 apps), se dará paso a una puesta en común donde se presentará cada app y las conclusiones de los grupos que la habían analizado.
>
> A nivel general conviene hacerse algunas preguntas sobre la seguridad de una app:
>
> - **¿De dónde la saco?** Descargar las apps siempre de las tiendas oficiales (Google Play en Android y App Store en iOS). Desconfiar de archivos descargados de Internet o de tiendas no oficiales, especialmente ante versiones gratuitas de apps de pago.
> - **¿Seguro que es ésta?** Si buscamos una app conocida, sospechar de posibles variantes en el nombre de la app, su logotipo o su desarrollador. Si no estamos seguros, mejor contrastar la información (por ejemplo visitando la web oficial del desarrollador).
> - **¿Quién está detrás?** La información del desarrollador puede ser muy escueta (basta con un nombre y un email). Desconfiar si no da su dirección o la política de privacidad.
> - **¿Qué hace con mis datos?** No es posible tener la certeza absoluta de qué pueden llegar a hacer con ellos. Los usos se han de indicar en su política de privacidad, aunque los permisos que solicita la app pueden darnos algunas pistas.
>   Es bastante habitual que los utilicen para proporcionarnos publicidad personalizada o para venderlos a otras empresas. Incluso cuando se ceden "anonimizados" (sin la información de identificación personal), sigue siendo posible unir esos datos con los de otras empresas o con datos públicos creando perfiles detallados de gustos, contactos, etc., lo que es muy valioso para marketing y publicidad.

- **¿En qué tenemos que fijarnos con los permisos?** En que sean coherentes con las funcionalidades de la app. Desconfiar si nos pide acceso a cuestiones que no están relacionadas (por ejemplo una app de linterna que pide acceso a los contactos). Siempre es útil que el desarrollador explique por qué los necesita.
- **¿Popularidad igual a seguridad?** No necesariamente. Si bien hay que desconfiar de apps que no se hayan actualizado desde hace mucho tiempo, de apps con pocas descargas, pocos comentarios y una valoración media baja, también es habitual encontrar apps poco recomendables con buenas valoraciones.

En los casos concretos de las fichas trabajadas (anexo 3.2.a), podemos ver un sencillo análisis en la tabla anexa (3.2.c). De ahí podemos extraer que con cualquier app pueden existir riesgos. No es lo mismo una app legítima, bien valorada, con detallada información del desarrollador y una política de privacidad que explique el uso de nuestros datos (normalmente con fines publicitarios y para su venta/cesión), que una app poco conocida de un desarrollador particular, sin más información sobre su funcionamiento (que también podría ser malicioso).

Obviamente para realizar un mejor análisis de riesgos habría que estudiar en detalle sus políticas de privacidad (donde indican qué datos nuestros recogen y qué hacen con ellos), y los permisos concretos que piden (por ejemplo, en la categoría "Teléfono" no es lo mismo "consultar el registro de llamadas" que "editar el registro de llamadas" o "redirigir llamadas salientes"). Asimismo, para minimizar los riesgos de posibles apps maliciosas (malware), conviene disponer siempre de un antivirus.

Respecto al beneficio económico de las apps conviene dejar claro que **nada es gratis**:

- Desarrollar una app conlleva un tiempo, un esfuerzo y unos gastos, de modo que es lógico que los desarrolladores busquen una contraprestación económica.
- Las apps "gratuitas" también nos cobran, solo que de otra manera: con compras integradas (de funciones avanzadas, objetos virtuales para un juego, etc.), con nuestros datos personales (aun tratados anónimamente, generan perfiles y tendencias de consumo para su explotación comercial) o mostrándonos publicidad (incluso personalizada según nuestro perfil e intereses).
- Las apps "de pago" no siempre son más respetuosas con nuestra privacidad. En algunos casos emplean esas mismas técnicas para obtener más ingresos.

En resumen, la app perfecta no existe. A la hora de elegir una app se ha de valorar tanto lo que nos aporta, como los riesgos que presenta, para en su caso poder asumirlos conscientemente. Además, a partir de Android 6.0 y de iOS 8 podemos permitir/rechazar cada permiso independientemente (y cambiarlo en cualquier momento). Finalmente, cuando nos deje de hacer falta una app, lo mejor es desinstalarla.

La **demostración** trata de enseñar la forma de ver los permisos y la información de las apps en Google Play y en App Store (por ejemplo con la ficha de una app) y en un dispositivo Android (ajustes – aplicaciones – permisos).

Para más información sobre los permisos se puede consultar la ayuda de Google: permisos en Android 6.0 y posteriores y permisos en 5.1 y anteriores y de Apple privacidad y localización en iOS 8 y posteriores.

Como alternativa se plantea crear un listado de buenas prácticas sobre instalación y uso de apps móviles. Para validarlas podemos fijarnos en las notas de la dinámica debate. En todo

caso se invitará al alumnado a comprobar en su casa los permisos de las apps instaladas en sus propios móviles o en los dispositivos de su familia.

En **conclusión** se refuerza la idea de la importancia de los móviles y sus apps en relación con nuestra seguridad y privacidad. Sobre los vídeos indicados destacar:

- Privacidad y permisos en apps: la app pide permiso para acceder a contactos y redes sociales y lo usa para vender información personal y publicitarse automáticamente.
- Videojuegos "gratuitos": se desbloquea una función a cambio de un pequeño pago...
- Permisos de apps: la sorpresa al "leer" los permisos de las apps que tienen instaladas.

Así pues, se animará a los participantes a relacionar los vídeos con el trabajo realizado en esta sesión. Se puede aprovechar para guiar una recapitulación de lo aprendido, concluyendo con una frase o un consejo con el que se haya quedado cada uno/a.

RECUERDA

Cuando necesitamos instalar una app, hemos de ser conscientes que puede poner en riesgo nuestra privacidad y seguridad. Siempre se debe elegir la app más adecuada, valorando sus beneficios y sus riesgos, según la información disponible.

ANEXOS

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

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

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	a	b
c	d	e	f	g	h	i
j	k	ℓ	m	n	o	p
q	r	s	t	u	v	w
x	y	z	0	1	2	3
4	5	6	7	8	9	.
-	@	€	$	&	(	)

ANEXO 3.2.a, fichas de apps (a recortar y entregar al alumnado)

Linternafest

17

limpiabrilla inc. Herramientas

PEGI 3 Contiene anuncios

La mejor app de linterna. Fácil, rápida y superluminosa. Incluye divertidos efectos de luz y sonido, con modo fiesta y luces de muchos colores para pasarlo ¡genial!

OPINIONES

3,1

17

5	8
4	1
3	
2	1
1	7

INFORMACIÓN ADICIONAL

Actualizado	la semana pasada
Descargas	1.000 – 5.000
Ofrecida por	limpiabrilla inc.
Desarrollador	limpiatdtpt98@gmail.com

PERMISOS

- Historial de aplicaciones
- Identidad
- Contactos
- Teléfono
- Fotos/multimedia/archivos
- Almacenamiento
- Conexión Wi-Fi
- ID de dispositivo y datos de llamada
- Otros

WhatsApp SuperSPY

120

Espiarwhatsapp ya Comunicación

Control parental Contiene anuncios

Descárgate las conversaciones de WhatsApp de tus amigos/as y descubre con quién hablan y qué secretos guardan ¡No se darán cuenta de que les espías!

OPINIONES

3,9

120

5	76
4	9
3	5
2	6
1	24

INFORMACIÓN ADICIONAL

Actualizado	hace seis meses
Descargas	10.000 – 50.000
Ofrecida por	Espiarwhatsapp ya
Desarrollador	thecoolkidswand@gmail.com Karphour, India www.espiarwhatsappya.com

PERMISOS

- Historial de aplicaciones
- Identidad
- Contactos
- SMS
- Conexión Wi-Fi
- Otros

ANEXO 3.2.a (continuación), fichas de apps (a recortar y entregar al alumnado)

Templete super run

RuDroide techgamer Juegos/Arcade

190.000

PEGI 7 Contiene anuncios – Ofrece compras en la aplicación

¿Serás capaz de llevarte el tesoro? Personaliza tu personaje favorito y ponte a correr, saltar, deslizarte... para poder superar todas las trampas y obstáculos, y ¡ganar!

OPINIONES

4,0

190.000

5	115.000
4	25.000
3	10.000
2	15.000
1	25.000

INFORMACIÓN ADICIONAL

Actualizado	hace un año
Descargas	10.000.000 – 50.000.000
Ofrecida por	RuDroide techgamer
Desarrollador	rdtg-tsr@rdtg-tsr.ru Moscova, 24, Proshkilon, Russia
Privacidad	www.rdtg-tsr.ru/privacy

PERMISOS

- Compras en aplicaciones
- Identidad
- Ubicación
- Fotos/multimedia/archivos
- Almacenamiento
- Conexión Wi-Fi
- Otros

Insta filtro perfecto

FilterEffect &co Fotografía

550.000

PEGI 3 Contiene anuncios – Ofrece compras en la aplicación

Mejora tus selfis, juega con diferentes efectos y filtros, personaliza tus fotos con pegatinas, emoticonos y textos *supercool* y despierta la envidia de tus amistades de Instagram.

OPINIONES

4,5

550.000

5	400.000
4	90.000
3	25.000
2	10.000
1	25.000

INFORMACIÓN ADICIONAL

Actualizado	hace un mes
Descargas	50.000.000 – 100.000.000
Ofrecida por	FilterEffect &co
Desarrollador	info@filtereffectandco.com Palo de Arriba, California, EEUU
Información	www.filtereffectandco.com

PERMISOS

- Compras en aplicaciones
- Historial de aplicaciones
- Identidad
- Contactos
- Ubicación
- Teléfono
- Fotos/multimedia/archivos
- Almacenamiento
- Cámara
- Micrófono
- Conexión Wi-Fi
- ID de dispositivo y datos de llamada
- Otros

ANEXO 3.2.a (continuación), fichas de apps (a recortar y entregar al alumnado)

Ultra moon charger

★★★★☆ 1.000

Koolappsprank Entretenimiento

PEGI 3 Contiene anuncios

¡Fin a los problemas de batería! Podrás hacer como que la batería se cargue al poner el móvil a la luz de la luna. Tarda más que nuestra app de carga a la luz del sol, pero ¡funciona de noche!

OPINIONES

4,1

★★★★☆

1.000

★ 5	750
★ 4	20
★ 3	20
★ 2	30
★ 1	180

INFORMACIÓN ADICIONAL

Actualizado	hace dos años
Descargas	100.000 – 500.000
Ofrecida por	Koolappsprank
Desarrollador	hahehi2015@gmail.com

PERMISOS

Ubicación
Conexión Wi-Fi
Otros

Teclado emojiguay

★★★★☆ 1.000.000

The emokeybrd company Personalización

PEGI 3 Contiene anuncios

Teclado emojiguay incluye cientos de emojis y emoticonos, gifs, stickers y unos tipos de letra supermolones ¡Dale nueva vida a tus conversaciones!

OPINIONES

4,2

★★★★☆

1.000.000

★ 5	650.000
★ 4	150.000
★ 3	90.000
★ 2	45.000
★ 1	65.000

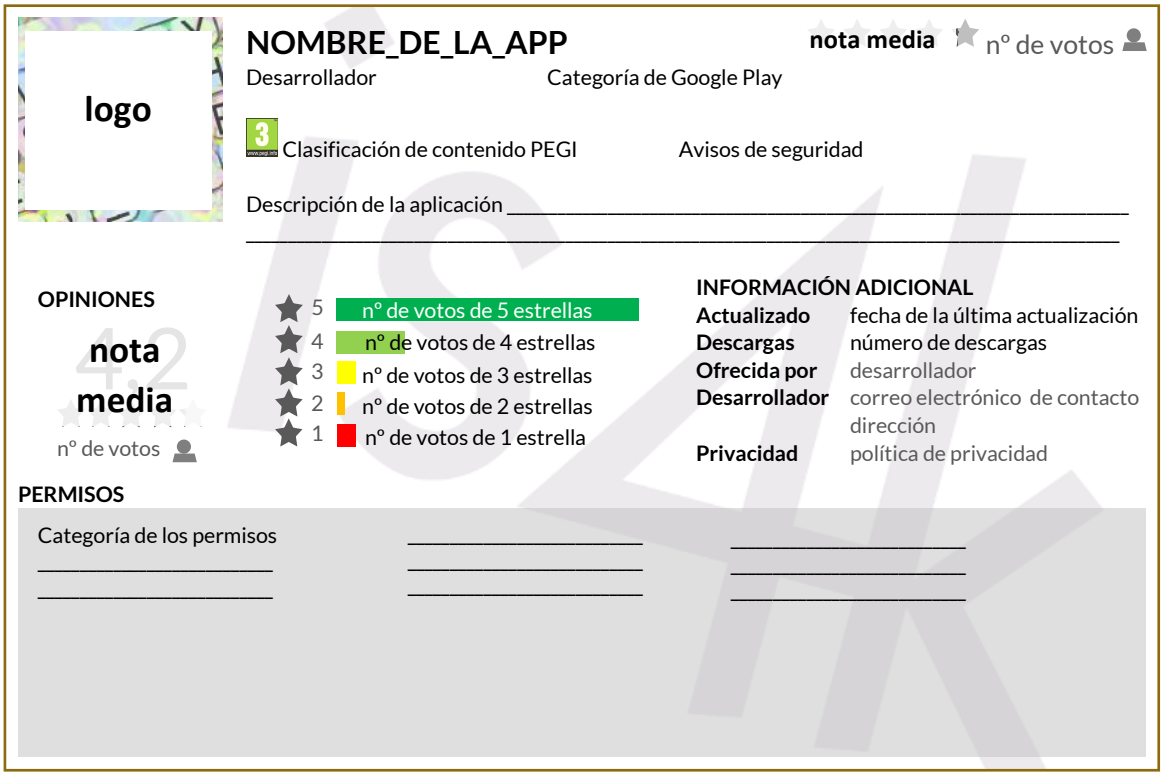
INFORMACIÓN ADICIONAL

Actualizado	ayer
Descargas	50.000.000 – 100.000.000
Ofrecida por	The emokeybrd company
Desarrollador	hello@emokeybrd.com Niantiong, China
Privacidad	www.emokeybrd.com/privacy

PERMISOS

Identidad
Calendario
Contactos
Ubicación
SMS
Teléfono
Fotos/multimedia/archivos
Almacenamiento
Cámara
Micrófono
Conexión Wi-Fi
ID de dispositivo y datos de llamada
Otros

ANEXO 3.2.b, estructura de las fichas de apps (a utilizar por los educadores)



Símbolos de las categorías de permisos de las apps

- Compras en aplicaciones
- Historial de aplicaciones
- Configuración de datos móviles
- Identidad
- Contactos
- Calendario
- Ubicación
- SMS
- Teléfono
- Almacenamiento
- Fotos/multimedia/archivos
- Cámara
- Micrófono
- Conexión Wi-Fi
- ID de dispositivo y datos de llamada
- Otros

ANEXO 3.2.c, tabla de análisis de las fichas de apps (a utilizar por los educadores)

	 **Linternafest**	 **WhatsApp SuperSPY**	 **Templete super run**	 **Insta filtro perfecto**	 **Ultra moon charger**	 **Teclado emojiguay**
Actualizada	✓	✗	✗	✓	✗	✓
Nº descargas	✗	✗	✓	✓	✓	✓
Nº opiniones	✗	✗	✓	✓	✓	✓
Nota media	✗	✗	✓	✓	✓	✓
Desarrollador	✗	✓	✓	✓	✗	✓
Política de privacidad	✗	✗	✓	✗	✗	✓
Permisos excesivos/no justificados						
Riesgos						
Comentarios	App de entre-tenimiento con excesivos permisos	Funcionalidad de espionaje falsa e ilegal	Juego de moda muy conocido entre los menores	Filtros de fotos y redes sociales llamativo para menores	Función falsa, pero categoría correcta (entre-tenimiento)	Opciones de personalización atractivas para los menores

Símbolos de los permisos

 Compras en aplicaciones
 Historial de aplicaciones
 Configuración de datos móviles
 Identidad
 Contactos
 Calendario
 Ubicación
 SMS
 Teléfono
 Almacenamiento
 Fotos/multimedia/archivos
 Cámara
 Micrófono
 Conexión Wi-Fi
 ID de dispositivo y datos de llamada
 Otros

Símbolos de los riesgos

 Malware o virus
 Publicidad
 Venta de datos personales
€ Compras integradas

Programa de Jornadas Escolares para el uso seguro y responsable de Internet por los menores

Unidad Didáctica 3
CONTROLA LA TECNOLOGÍA

www.is4k.es

@is4k Internet Segura for Kids

ENLACES DE AMPLIACIÓN DE CONTENIDOS (www.is4k.es)

- Lo que necesitas saber sobre… (uso y configuración segura de dispositivos y servicios online, privacidad, etc.)
- Centros de seguridad de las redes sociales
- Configurar un dispositivo Android o proteger un iPhone o iPad
- Guía de Privacidad y Seguridad en Internet de OSI y AEPD (fichas y videotutoriales)
- Oficina de Seguridad del Internauta (qué deberías saber sobre dispositivos, virus, herramientas gratuitas de seguridad y servicios de ayuda y asistencia)

GOBIERNO DE ESPAÑA · MINISTERIO DE ECONOMÍA Y EMPRESA

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»