Programa de Jornadas Escolares

Promoción del uso seguro y responsable de Internet entre los menores

---

Protección ante virus y fraudes

Unidad Didáctica y contenidos de apoyo al docente

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

Licencia de contenidos

CONTENIDO

1. Presentación de la Unidad Didáctica

El día a día quienes usan Internet diariamente está marcada por el acceso a los muchos servicios que facilita (trámites, compras, comunicación, diversión y ocio, etc.), pero también por los virus y fraudes a los que se exponen. No es extraño que 'compañeros digitales' alerten sobre **virus** que pueden afectar a dispositivos, o sobre **fraudes** que, aprovechando la viralidad que Internet y las redes sociales propician, acechan.

Siendo esta la realidad, es del todo necesario que el alumnado conozca aquellas pautas y herramientas que pueden protegerle de los distintos **virus y fraudes** que circulan por Internet, apelando a aquellas estrategias y recomendaciones que ayudan a prevenir de este tipo de situaciones.

Por ello, el objetivo de esta Unidad Didáctica será orientar el aprendizaje del menor en pautas básicas de mantenimiento, actualización y seguridad, introduciéndole en los conceptos de fraude y virus informático. Se abordará tanto la evolución de éste en los últimos años como la importancia de proteger nuestros datos personales en todas las comunicaciones que se realizan a través de Internet. Específicamente se tratarán los conceptos de virus /antivirus, sus consecuencias y medidas de prevención (filtros/software de protección/ configuración del sistema operativo, navegadores y programas). Se explicarán los riesgos relacionados con la descarga de archivos, también de su intercambio, los posibles riesgos de instalar software pirata, los riesgos asociados a la webcam, las medidas de prevención en peticiones de amistad de desconocidos, la importancia de realizar copias de seguridad, etc., haciendo hincapié en la necesidad de **aplicar el sentido común y apelar a la responsabilidad personal a la hora de mantener protegidos (y actualizados) todos los dispositivos.**

2. Ficha descriptiva.

Destinatarios		Alumnado de 6º de Primaria y ESO
Duración		2 sesiones de 50 minutos
Objetivos didácticos	**General**	Informar y capacitar al alumnado para actuar de manera proactiva frente a los riesgos asociados a virus y fraudes informáticos extendidos a través de Internet, ofreciéndole recomendaciones, pautas y herramientas para su prevención y/o actuación en caso de verse afectados por ellos
	Específicos	• Conocer qué son y cómo funcionan los virus informáticos y los fraudes para poder prevenirnos ante ellos. • Aplicar medidas y pautas para la protección de ordenadores y dispositivos móviles ante los virus. • Reconocer en qué consiste el fraude electrónico y sus principales riesgos.

<table>
<tr><td colspan="2">Contenidos de aprendizaje</td><td>

Qué son los virus.

Objetivo de los virus.
Métodos de infección utilizados.
Ejemplos de virus informáticos.
Riesgos de ser infectados por virus informáticos y programas maliciosos.
Mecanismos para la prevención y actuación frente a los virus.

Concepto de fraude electrónico e ingeniería social.

Tipos de fraudes.
Cómo pueden afectar a los menores.
Casos reales de fraudes electrónicos.
Mecanismos y pautas de prevención ante el fraude electrónico.

</td></tr>
<tr><td rowspan="2">Áreas competenciales</td><td>Digitales</td><td>
Área Información. El alumnado será capaz de navegar y buscar información en Internet sobre virus informáticos y fraudes electrónicos, filtrando información y comparando diferentes fuentes sobre la temática.

Área Comunicación (nº 2.1. Interacción mediante nuevas tecnologías). El alumnado será capaz de relacionarse por medio de diversos dispositivos y aplicaciones digitales, adquiriendo habilidades que le permitan una interacción positiva a través de las TIC, gestionando eficazmente su comunicación digital y siendo crítico con la información relativa a virus y fraudes electrónicos.

Área Seguridad (nº 4). El alumnado será capaz de evitar y protegerse ante los posibles riesgos relacionados con virus informáticos y fraudes electrónicos, estableciendo medidas de seguridad y estrategias activas, que le permitan identificar conductas inadecuadas y métodos de engaño a través de la ingeniería social.

*Referencia “Marco Común de la Competencia Digital Docente” INTEF[1] (Instituto de Tecnologías Educativas y de Formación del Profesorado) (2013)
</td></tr>
<tr><td>Clave</td><td>

Comunicación lingüística (CCL): el alumnado conocerá y aprenderá a utilizar lenguaje específico relacionado con virus y fraudes electrónicos y sus posibles riesgos, medios de infección y métodos de engaño.
Aprender a aprender (CPAA): adquirirá habilidades para iniciarse en su propio aprendizaje, de forma cada vez más eficaz y autónoma en relación a diferentes casos y ejemplos de virus y fraudes informáticos, así como a las formas de prevención frente a éstos.

</td></tr>
</table>

[1] Marco Común de Competencia Digital Docente V 2.0

		• **Sentido de la iniciativa y Espíritu emprendedor (SIE)**: será capaz de desenvolverse adecuadamente y de forma independiente ante la presencia de riesgos provocados por virus y fraudes informáticos, siendo capaz de tomar sus propias decisiones y buscar alternativas frente a ellos.

3. Temporalización y secuenciación.

Sesión	Contenido / actividad	Duración	Metodología
Sesión 01	Actividad 01 (Introducción a la temática)	15 min.	Expositiva + Interrogativa y Debate en grupo
	Actividad 02 (Nuevas estrategias de engaño)	20min.	Expositiva + Debate en grupo
	Actividad 03 (Prevenir mejor que curar)	15 min.	Expositiva y Trabajo en grupo
Sesión 02	Actividad 03 (Continuación actividad anterior)	10 min.	
	Actividad 04 (Apps maliciosas)	15 min.	Expositiva + Debate
	Actividad 05 (Entidades y servicios de referencia)	15 min.	Expositiva + Elaboración de un cartel
	Actividad 06 (Autoevaluación)	10 min.	Autoevaluación individual/Crucigrama

4. Orientaciones didácticas.

4.1. Metodología.

A lo largo de esta Unidad Didáctica, el formador impulsará la reflexión y actitud crítica acerca de los contenidos trabajados, facilitando la participación y el debate en torno a los riesgos a los que se enfrentan los menores asociados a virus informáticos y fraudes electrónicos, capacitándoles para actuar de manera proactiva frente a éstos, mediante hábitos básicos y recomendaciones de prevención, así como de pautas de actuación a implementar en caso de verse afectados por ellos.

Se proponen para ello sesiones que combinan los **métodos expositivo** [2](centrado en la transmisión de información, que facilita ésta de forma rápida y generalizada, por parte de un/a experto en la materia), **interrogativo** [3] y **demostrativo** [4](centrados ambos en la aplicación práctica del contenido a trabajar), incorporando a éstos la visualización de contenido audiovisual (vídeos), que animarán el debate y reflexión compartidos, sobre ideas, inquietudes y dudas relacionadas con la temática expuesta. Se propondrá el debate y la participación del alumnado tanto en dinámicas de grupo, como a través del trabajo y la reflexión individual, favoreciendo en todo momento la motivación del alumnado, por medio de actividades y herramientas específicas como:

- **Debate en grupo**: tiene como fin el intercambio informal de ideas e información sobre un tema, que ha de ser cuestionable y dar lugar a diferentes enfoques e interpretaciones, elegido de antemano por el/la docente. Este/a conducirá el debate como moderador, a través de preguntas previamente preparadas que faciliten la discusión, estimulando el pensamiento crítico, el análisis, el trabajo colectivo, la comprensión y la tolerancia.
- **Generación de crucigramas**, por parte del docente, con el fin de utilizar éste para afianzar definiciones y conceptos, trabajados a lo largo de la Unidad Didáctica.

En todo caso, el formador asesorará y facilitará recursos e información relacionados con la temática, que a través de ejemplos vinculados a la realidad objetiva del alumnado, promuevan el aprendizaje permanente y la reflexión crítica. Utilizará un lenguaje acorde al nivel de conocimientos previos del alumnado para favorecer la comprensión de las actividades propuestas y contribuir a su buen desarrollo.

4.2. Recursos necesarios

Recursos requeridos para el desarrollo de la Unidad Didáctica:

- Recursos logísticos:
  - Ordenador con conexión a Internet para el docente, conectado a un proyector VGA o pizarra electrónica, capacitado para la emisión de vídeo (con altavoces de buena resolución, que faciliten la escucha entre foros grandes de personas).
  - Pizarra o papelógrafo.
  - Ordenadores con conexión a Internet para actividades del alumnado (al menos 1 ordenador por cada 2 alumnos) y altavoces (tipo auricular/cascos, para la escucha individual).

[2] **METODOLOGÍA EXPOSITIVA:** centrada en la transmisión de información, posibilita la transmisión de conocimientos ya estructurados, facilitando demostraciones de tipo verbal y la transmisión de información y conocimiento, de manera rápida y generalizada.

[3] **METODOLOGÍA INTERROGATIVA**: centrada en el proceso de aplicación del contenido a trabajar, basada en el proceso de comunicación que se establece entre docente y grupo, a través de **la pregunta**. Esta se convierte en elemento dinamizador, que desencadena el proceso de enseñanza aprendizaje.

[4] **METODOLOGÍA DEMOSTRATIVA**: centrada también en el proceso de aplicación del contenido a trabajar, en la que el formador/a es el modelo de acción ante el grupo, ejemplificando las tareas y acompañándolas de las diferentes explicaciones, para la posterior imitación por parte del alumnado. Más información sobre "Métodos didácticos" en este enlace.

- Recursos didácticos:
  - Presentación de contenidos dirigida a los menores, que acompaña a la presente Unidad Didáctica.
  - Sitios web, imágenes y vídeos previamente seleccionados por el docente. Con este objeto, se adjuntan a esta Unidad Didáctica, en la descripción de cada actividad propuesta y en el **epígrafe Bibliografía /Documentación complementaria,** una pequeña muestra de posibles ejemplos a utilizar (a modo orientativo) por el docente.

4.3. Descripción de las actividades a abordar.

Actividad 01. Definiendo conceptos: malware, virus y riesgos relacionados con éstos

Descripción	Actividad expositiva y de debate abierto en el aula para introducir la temática.
Metodología	Expositiva + Interrogativa y Debate en grupo.
Duración	15 minutos.
Recomendaciones	Teniendo en cuenta la información introductoria sobre la temática que hemos resumido en el epígrafe **"Marco teórico de apoyo al docente"** de la presente Unidad Didáctica, presentaremos al alumnado, un breve resumen sobre **qué son los virus informáticos, cuál es su objetivo, sus métodos de infección y algunos ejemplos** que les ayuden a comprender el riesgo que representan. Con este objetivo, el formador podrá utilizar diferentes **vídeos** – enumeramos a continuación algunos de ellos, relacionados con la temática a trabajar a lo largo de esta primera sesión – para su visualización en el aula, a modo de **vídeo introductorio:** • **'Conozca los riesgos de la tecnología'**, que aborda la utilidad y extensión del uso de la tecnología en nuestra vida cotidiana, destacando los riesgos derivados de los virus informáticos y nuestra responsabilidad, como usuarios, de conocer y actuar frente a esos riesgos, para minimizar su daño. • **¿Qué sabemos sobre los virus informáticos?** Un poco más actualizado, con información específica sobre virus informáticos, su historia y evolución, las consecuencias que acarrean para quien los padece o sufre, así como el rol de los 'antivirus' y las últimas tendencias en virus, extendidos rápidamente a través de Internet. • **Seguridad informática**: otro vídeo, con consejos importantes, que pueden servir de arranque a la UD, en el que se analiza la necesidad de proteger nuestros datos personales, del "ataque" de hackers y ciberdelincuentes. Tal como se recoge en el artículo **"Ponte al día con los virus informáticos"**, publicado en la página web de la Oficina de Seguridad del Internauta (una de las fuentes que el docente tomará como referencia a lo largo de la Unidad Didáctica), entendemos por "malware" o **virus**: aquel programa malicioso capaz de colarse en un ordenador, smartphone o tableta con algunos fines como

robar datos privados, hacer que el dispositivo deje de funcionar correctamente o tomar su control para llevar a cabo otras acciones maliciosas. Para entender mejor el concepto y algunas de las principales tipologías de software malicioso existentes (como Ransomware, Spyware o Keylogger), proponemos analizar, a continuación, **la siguiente infografía** en la que se detallan, en cada caso, sus riesgos, métodos de infección y principales medidas frente a ellos. (Las medidas a tomar se reflejan en el apartado "No me gusta" de la infografía).

El análisis del anterior contenido, puede dar pie a establecer un **breve debate en el aula**, que nos permita sondear el grado de familiarización del alumnado con estos términos y con las consecuencias y riesgos que los virus informáticos representan, a través de preguntas del tipo:

- ¿Qué tipos de virus conocéis?
- ¿Os habéis visto amenazados en alguna ocasión por alguno de ellos?
- ¿Cuál ha sido el 'detonante', la acción que ha activado y extendido ese virus?
- ¿Cuáles creéis que son los métodos más habituales de infección?
- ¿Qué crees que se podría haber hecho para evitarlos?
- ¿Afectan sólo a ordenadores? ¿Habéis detectado algún virus en vuestros dispositivos móviles?
- ¿Tenéis instalado y configurado un antivirus en vuestro smartphone o tablet?

Tras el debate, repasaremos con el alumnado los **principales mecanismos y medios de infección:**

- **Correo electrónico.** Es una de las principales vías de entrada de virus, a través de ficheros adjuntos peligrosos o enlaces a páginas web maliciosas.
- **Dispositivos de almacenamiento externo** (USB, discos duros, tarjeta de memoria), al copiar archivos infectados de un USB a nuestro equipo. En ocasiones, simplemente por el hecho de conectar un USB a nuestro equipo podemos resultar infectados, ya que algunos virus tienen la capacidad de auto-ejecutarse.
- **Descarga de ficheros desde Internet.** Al abrir o ejecutar ficheros (programas, contenido multimedia, documentos, etc.) pueden traer camuflado/escondido algún tipo de malware. Hay que tener especial precaución con lo que descargamos mediante programas de compartición de ficheros (P2P) u obtenemos en las distintas páginas web de descarga de contenidos, ya que pueden ser más propensos a contener virus.
- **Páginas web maliciosas**, preparadas para infectar al usuario que las visita aprovechando **problemas de seguridad de un navegador no actualizado** o de los complementos instalados: Java, Flash, etc. También a través de páginas web legítimas que han sido manipuladas por ciberdelincuentes, **redirigiéndonos a webs maliciosas o fraudulentas**. Una forma de llegar a éstas podría ser, por ejemplo,

haciendo clic en **enlaces acortados** en Twitter (u otras redes sociales) o en enlaces facilitados en correos electrónicos fraudulentos.

- **Redes sociales,** utilizadas para infectar los dispositivos debido a la gran cantidad de usuarios que las frecuentan y el alto grado de propagación que facilitan. Hay que ser precavidos frente a publicaciones con enlaces a páginas web con mensajes o titulares llamativos que resulten "raros" o poco fiables, solicitudes para instalar programas para poder acceder o visualizar un contenido, o aplicaciones que solicitan autorización no justificada para el acceso a nuestra **información personal**.
- **Vulnerabilidades y fallos de seguridad** en los sistemas operativos, navegadores, aplicaciones, plugins o programas instalados en el dispositivo. Son aprovechadas por los ciberdelincuentes para infectar los equipos, a veces, sin que el usuario tenga que realizar una acción que le haga consciente de ello. El ejemplo comentado en este caso por el formador puede ser el **Fallo de seguridad de Abobe Flash Player**. A través de este fallo de seguridad, un atacante pudo tomar el control remoto de un dispositivo y realizar cualquier acción, como por ejemplo instalar malware**.** Para evitarlos, es importante mantener actualizados nuestros dispositivos. El docente comentará que precisamente la actualización del programa ante la vulnerabilidad detectada en Adobe Flash, permitió que la incidencia se solventara con total rapidez.

Así como los principales **mecanismos de actuación y consecuencias de los virus:**

MECANISMOS DE ACTUACIÓN	CONSECUENCIAS. RIESGOS
• Bloquea o toma el control del ordenador infectado, en algunos casos solicitando un ingreso económico para desbloquearlo, previa suplantación de identidad, es decir haciéndose pasar generalmente por una organización, empresa o entidad conocida con cierta reputación y prestigio.  Ejemplo "**Virus de la Policía**" • Captura de pulsaciones del teclado, para hacerse con claves	• Cifrado y/o borrado de la información almacenada en el dispositivo.  Ejemplo "**Falsa factura de Endesa**" • Ralentización o inutilización del dispositivo. • Espionaje y/o robo de información personal: fotografías, datos bancarios, números de tarjetas de crédito,

y contraseñas de acceso a los servicios online.

- Espionaje, mientras permanece el virus oculto en el sistema, sin mostrar actividad aparente y escondiéndose del antivirus.
- Aprovechando fallos de seguridad en plugins y aplicaciones que los usuarios utilizan habitualmente (Adobe Flash Player, Java, Acrobat Reader, etc.).
- Introduciendo un pen-drive USB o conectándose a una página web infectada.
- Abriendo un archivo adjunto de imagen (aparentemente inocua), que contiene un código que se ejecuta de forma automática en el momento en que se visualiza ésta.
- Activando la webcam del usuario sin que éste sea consciente de que está siendo grabado.

documentación importante, etc.

- Suplantación de identidad. Envío de correos electrónicos en nombre de la víctima, publicar en sus perfiles en redes sociales, realizar transferencias económicas a otras cuentas bancarias, realizar compras y pagos online, etc.
- Uso del ordenador de la víctima para realizar ataques a otros ordenadores infectándolos para obtener información de sus usuarios, realizar estafas o el envío de publicidad.
- Envío de SPAM desde el ordenador de la víctima sin que ésta sea consciente.

Como material de apoyo al contenido de esta actividad, el docente podrá utilizar varios enlaces y documentos referenciados en el apartado **Bibliografía / Documentación complementaria** de esta Unidad Didáctica, como el **Monográfico sobre protección ante virus y fraudes,** elaborado por Red.es y el artículo **Ponte al día con los virus informáticos**, de la Oficina de Seguridad del Internauta.

Actividad 02. Conociendo algunos fraudes muy extendidos

Descripción	Análisis de ejemplos y casos reales de los últimos fraudes electrónicos que circulan a través de Internet, tras el cual iniciaremos una exposición de experiencias propias o conocidas, evaluando sus consecuencias y distintas formas de actuación frente a éstos.
Metodología	Exposición de contenido y experiencias + debate en grupo
Duración	20 minutos
Recomendaciones	Al inicio de esta actividad se abordará la definición de dos conceptos importantes: • **Fraude electrónico:** entendido éste como la actividad delictiva que se lleva a cabo a través de medios como Internet, ordenadores y dispositivos móviles. • **Ingeniería social:** engaños y manipulaciones dirigidos a embaucar a los usuarios a que realicen alguna acción y conseguir así información que posteriormente será utilizada para sustraerle claves de acceso, contraseñas, infectar sus dispositivos, etc. En definitiva, la ingeniería social es la técnica que utilizan los ciberdelincuentes para materializar sus fraudes. Para facilitar la asimilación de este contenido, presentaremos al alumnado ejemplos relativos a distintos tipos de fraudes electrónico propagados a través del correo electrónico, redes sociales (Facebook, Twitter, Instagram), juegos online y apps de mensajería (WhatsApp, Snapchat): • **Phishing:** una de las técnicas más usadas por los ciberdelincuentes (sobre la que puedes saber más a través de **este artículo**) en la que, haciéndose pasar por una compañía o empresa conocida, solicitan al usuario sus claves de acceso a un servicio online, datos bancarios, descargar un fichero malicioso, etc. Ejemplos: ○ **Falsa factura electrónica de Endesa intenta infectar tu equipo:** La noticia se hace eco de la campaña fraudulenta que, a través de la suplantación de la identidad de la empresa *Endesa,* instala malware en el equipo de la víctima, cifrando los ficheros e impidiendo su acceso, para pedir un rescate por su 'liberación'. ○ **Suplantan a Apple para intentar robarte credenciales y la tarjeta de crédito.** En este caso, la campaña de correos electrónicos fraudulentos (phishing) suplantan la identidad de la compañía Apple a través de un mensaje de alerta a los usuarios para que verifiquen su información de iCloud o en caso contrario su cuenta será cerrada. El objetivo es robar el usuario y la clave de acceso al servicio, además de información personal y datos bancarios. ○ **Correos y Telégrafos NO te ha enviado ninguna notificación.** Convertido en uno de los fraudes más extendidos, el malware

que utiliza la imagen corporativa de Correos y Telégrafos de España infecta los dispositivos con un malware que cifra los ficheros, haciendo irrecuperable la información que en ellos se almacena así como la de las unidades de red mapeadas, pendrives conectados, etc.

- **Virus de la Policía.** Se trata de un virus que bloquea el ordenador del usuario para a continuación solicitarle un ingreso de dinero a cambio del desbloqueo. Todo ello bajo la excusa del pago de una multa por alguna actividad supuestamente ilegal en Internet.

- **Robo de datos personales** de forma engañosa o sin nuestro consentimiento. Ejemplos:
  - **Falsa página de Mercadona**. El robo de datos se realizaba a través de una página preparada específicamente para robar datos personales a los usuarios que introdujesen su información personal en ella bajo la excusa de que dichos datos eran necesarios para obtener un supuesto premio.
  - **Webcam controlada desde otro ordenador.** A consecuencia de un virus que toma el control del ordenador accediendo a la información captada desde ella, sin consentimiento del usuario. **Ver artículo**.
- **Falsos vídeos y nuevas estafas, a través de redes sociales**. Ejemplo:
  - **Falso vídeo en Facebook.** Este malware no solo infecta el equipo con troyanos para el robo de información, sino que además instala una extensión en el navegador para publicar en Facebook de forma automática y seguir propagando el contenido entre más usuarios.
  - **Las nuevas estafas de las redes sociales.** La Policía Nacional alerta de los nuevos fraudes, estafas, timos y bulos que se propagan con especial rapidez a través de redes sociales y aplicaciones de comunicación, como WhatsApp, y que pretenden lograr beneficio económico al margen de la ley.
- **Suscripción a servicios Premium o de pago**. Ejemplo:
  - **Videollamadas de WhatsApp.** Los mensajes de esta nueva campaña ofrecen a los usuarios activar videollamadas para el sistema de mensajería instantánea WhatsApp (a día de hoy esta funcionalidad no la ofrece la app). La promoción fraudulenta se propaga a través de redes sociales en teléfonos móviles con mensajes que contienen un enlace que dirige a una web que trata de suplantar la identidad de WhatsApp, desde la que le anima a "Descargar Videollamadas" remitiéndole a una web desde la que se intentará subscribir al usuario a un servicio SMS Premium.

	○ **Vales descuento de Lidl.** Una campaña de correo electrónico que ofrece supuestos vales descuento de la cadena de supermercados Lidl. El objetivo es obtener datos personales y suscribir a un servicio de recepción de ofertas con un coste de 24,90€ mensuales. • Fraudes **asociados a juegos online**: ○ Suscripciones ocultas y con coste, mediante publicidad incorporada al videojuego. ○ Robo de datos. **Estos y otros muchos ejemplos, son recogidos a través de la sección de 'Avisos' de la Oficina de Seguridad del Internauta (OSI), que nos alerta de forma permanente sobre nuevo software malicioso y fraudes informáticos, facilitándonos importantes consejos y recomendaciones, tanto para prevenir la infección como para atajarla, una vez infectado nuestro ordenador o dispositivo.** Tras el análisis de algunos de los ejemplos presentados, iniciaremos una **exposición de experiencias propias o conocidas similares,** qué problemas ocasionaron y cómo se actuó. Para estimular el debate y la intervención de la mayor parte del alumnado, se propone una serie de preguntas: • ¿Conocéis a algún familiar o amigo que haya sido víctima de un fraude electrónico? • ¿Qué consecuencias han tenido? • ¿Cuál es el último engaño o fraude que os ha llegado al teléfono móvil? • ¿Creéis que un buen antivirus puede protegernos de fraudes? • ¿Cuál ha sido el 'detonante', la acción que ha activado la amenaza? Ejemplo: descargar e instalar un archivo adjunto; hacer clic en el enlace que mostraba el texto recibido; cumplimentar los datos que solicitaba la página Web; etc. • ¿Qué creéis que se podría haber hecho para evitarlos? • ¿Tomáis actualmente alguna precaución ante este tipo de amenazas en la Red? • ¿Sabes que existen virus que no se muestran al usuario? La respuesta individual y colectiva a cada una de estas preguntas dará pie al análisis de los casos y ejemplos reales, destacando algunos de los riesgos y amenazas más importantes de los virus y fraudes informáticos.

Actividad 03. ¡Prevenir mejor que curar!

Descripción	Después de haber trabajado en detalle su tipología y características mediante ejemplos destacados de virus y fraudes informáticos, así como de sus riesgos, buscamos ahora conocer medidas de prevención a aplicar frente a ellos.
Metodología	Expositiva y trabajo en grupo.
Duración	25 minutos[5]
Recomendaciones	Como hemos visto tras el contenido trabajado en las 2 actividades anteriores, conocer los **riesgos** a los que expone el software malicioso o los fraudes es importante. Esto obliga a hacer un uso responsable de la tecnología y a actuar, de manera proactiva para la **prevención** de este tipo de incidencias. En esta línea, proponemos trabajar estas **medidas de seguridad y prevención** apoyándonos en el video: **'Usa un escudo e impide el avance de los virus'**. La información se complementará con una visita guiada a la **página de OSI,** donde encontraremos, entre otras cosas, información sobre **herramientas gratuitas para proteger nuestros dispositivos**, haciendo más segura nuestra navegación por Internet. Como veremos tanto en el vídeo como en la web de OSI, los consejos y recomendaciones genéricas para prevenir y protegernos ante virus y fraudes, son sencillos y aplican el **sentido común,** fomentando el uso responsable de la tecnología a través de sencillas pautas entre las que destacamos: • Llevar a cabo instalaciones seguras que no comprometan nuestros dispositivos, a través de sitios oficiales de descarga. • Instalación y correcta actualización de programas antivirus, tanto en ordenadores como en tabletas y smartphones, descargándolos desde la web oficial del fabricante. • Activación de cortafuegos (integrado en el sistema operativo) que bloquea el acceso no autorizado a los dispositivos, permitiendo las comunicaciones que sean autorizadas. • Mantener actualizado el sistema operativo, los navegadores, complementos así como el resto de programas. • Realización de copias de seguridad. • Cifrado de la información. • Limitación de permisos de usuarios a través del perfil de 'usuario administrador', único con permiso para la instalación de aplicaciones y actualizaciones del sistema operativo. Tras el repaso a estos consejos y recomendaciones, se puede proponer en el aula un **trabajo en grupo**. El alumnado elaborará, en grupos de 4-5 personas, una lista con todas las medidas que conoce y/o recuerda para la prevención de virus y fraudes en

[5] Proponemos dividir esta actividad entre las 2 sesiones previstas para la Unidad Didáctica, dedicándole 15 minutos en la primera sesión y 10 más, ya en la segunda sesión.

	sus dispositivos. Con las respuestas recogidas, que se apuntarán en una pizarra o dispositivo, se elaborará una **lista conjunta de pautas y recomendaciones** que permita al alumno anotar éstas en su cuaderno de trabajo, marcando con una X aquellas que ha utilizado hasta la fecha. Entre esas pautas y recomendaciones no pueden faltar: • Mantener actualizado todo el software instalado en un determinado dispositivo (sistema operativo, navegador, antivirus y demás programas). • Gestionar el acceso a dispositivos compartidos con cuentas de usuario limitado, que permiten la instalación de aplicaciones o modificaciones en la configuración sólo a través del perfil "administrador". • Realizar copias de seguridad. • Llevar a cabo una buena gestión de contraseñas (secretas, robustas y no repetidas). • Cambiar periódicamente la contraseña de la conexión wifi del router. • Tomar precauciones al utilizar dispositivos públicos y conectarse a redes wifi públicas. • Tener precaución con los enlaces cortos (tipo bit.ly; goo.gl;) antes de acceder a ellos – sobre todo desde Twitter y otras redes sociales, donde se usan para ahorrar caracteres -, ya que pueden dirigirnos a páginas web fraudulentas que contienen malware. • Descargar programas y aplicaciones sólo desde páginas oficiales. • Evitar la navegación por páginas web sospechosas. Configurar adecuadamente la privacidad en las redes sociales. • Evitar conectar a los dispositivos medios de almacenamiento extraíbles (USB) de dudosa procedencia, ya que pueden ser una puerta de entrada para los virus. Se les invitará a valorar algunas de las medidas destacadas que aún no han implantado en su rutina diaria para mejorar su prevención ante posibles ataques derivados de virus y fraudes informáticos. El docente encontrará, en el resumen facilitado en el en el epígrafe **"Marco teórico de apoyo al docente",** éstas y otras recomendaciones a seguir tanto en la prevención como en la intervención ante la presencia de virus y fraudes informáticos.

Actividad 04. Apps maliciosas. Cómo nos afectan

Descripción	El objetivo de esta actividad es alertar y proporcionar recomendaciones básicas que prevengan de la posible descarga e instalación de aplicaciones maliciosas en smartphones y tabletas.
Metodología	Expositiva + Debate
Duración	15 minutos
Recomendaciones	Los dispositivos móviles, tabletas y especialmente smartphones han conseguido introducirse en nuestras vidas, dotando a la conectividad y al uso de Internet de una apreciada característica: la movilidad. Pero este boom no ha pasado desapercibido para quienes han visto en él una oportunidad inigualable para extender virus y fraudes informáticos a través de numerosas aplicaciones móviles que podrían acabar siendo descargadas e instaladas, tal y como muestran los vídeos recomendados para su visualización con el alumnado como introducción a la temática de esta actividad: • **Cómo proteger nuestros dispositivos móviles de los ataques de los virus**, sobre la presencia de virus, chantajes y fraudes en ordenadores, tabletas o teléfonos móviles. • **La principal puerta de entrada de malware en dispositivos es la descarga de aplicaciones**. Es importante saber cómo proteger los dispositivos móviles de aplicaciones maliciosas. No debemos olvidar que el riesgo de infección puede tener serias consecuencias debido a que éstos: • Permiten la escucha y grabación de las llamadas realizadas y recibidas en los teléfonos móviles. • El envío de mensajes SMS Premium, que incrementan el coste de la factura sin que el usuario sea consciente de esta acción. • La activación del GPS del dispositivo móvil, obteniendo datos sobre la posición geográfica del dispositivo. Por ello, se proporcionarán al alumnado **soluciones y recomendaciones** que le prevengan de las consecuencias de la posible descarga e instalación de aplicaciones maliciosas en smartphones y tabletas, como: • Instalar y mantener actualizado un antivirus en los dispositivos móviles. • Descargar aplicaciones sólo desde markets oficiales: Play Store, Apple Store o Microsoft Store entre otras. • Revisar los permisos que las apps solicitan al instalarse. • Leer las cláusulas y condiciones que se suelen aceptar (sin leer los detalles) cuando se accede a comprar algún elemento (ayudas, versiones extendidas, etc.) a través de un juego o aplicación.

	• Eliminar apps que no se estén utilizando. • Instalar la aplicación CONAN Mobile, si se dispone de Android, para la protección de sus dispositivos móviles. Se abordará al final de la actividad un pequeño **debate sobre el uso y aplicación de estas medidas y recomendaciones,** tratando de resolver las dudas que pueden surgir sobre ellas e invitando al alumnado a que elija 2 de ellas que aún no haya llevado a cabo hasta la fecha, implementándolas a lo largo de los dos próximos días y debiendo reportar al profesorado su experiencia tras esa fecha.

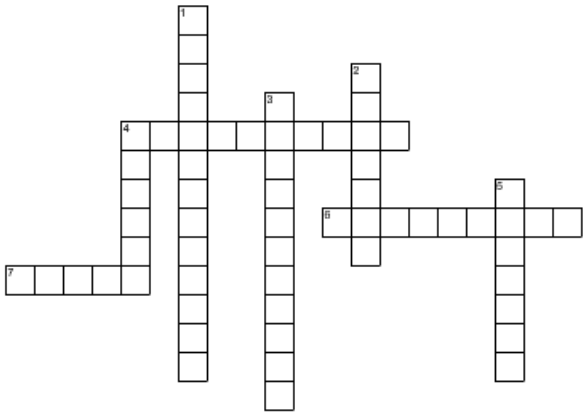
Actividad 05. Estar informado fortalece tu protección

Descripción	Presentaremos al alumnado entidades y servicios de referencia que les permitirán tanto el acceso a información permanente relativa a nuevas modalidades y casos de software malicioso, como la denuncia ante la sospecha de estar siendo víctima de éstos.
Metodología	Expositiva + Elaboración de un cartel/anuncio
Duración	15 minutos
Recomendaciones	Comprender que la tecnología evoluciona constantemente y con ella, la elaboración de nuevas formas de infectar dispositivos electrónicos y engañar a sus usuarios. Esto obliga a permanecer en alerta e informados a través de **entidades y servicios de referencia** que también debemos utilizar ante la sospecha de estar siendo víctima de software malicioso o fraude electrónico. **Comentaremos con el alumnado el interés de conocer y permanecer atentos a las recomendaciones y herramientas facilitadas por entidades como:** • La Guardia Civil cuenta con el **Grupo de Delitos Telemáticos** (GDT), con el que se puede contactar a través de la **sección *colabora* de su página web** o utilizar su formulario de denuncia que, una vez rellenado, generará un documento de denuncia en formato PDF que se puede presentar en un centro policial para interponer la denuncia. Desde su **canal en Twitter**, informan de manera permanente sobre las últimas novedades y avisos relacionados con delitos telemáticos. • La **Brigada de Investigación Tecnológica** (BIT) del Cuerpo Nacional de Policía, creada para combatir la delincuencia que utiliza los medios que proporcionan las nuevas tecnologías de la información y que permite la denuncia de este tipo de fraudes a través del teléfono **902 102 112**, su **página web** o en cualquier **comisaría,** así como a través del correo electrónico **delitos.tecnologicos@policia.es**. La Policía Nacional dispone también de un **canal en Twitter**, reconocido y premiado en España por su gran labor a la hora de alertar e informar sobre las últimas novedades relacionadas, entre otras, con delitos informáticos. • INCIBE que, a través de la Oficina de Seguridad del Internauta (OSI), facilita un buzón de correo electrónico: **incidencias@certsi.es** y un número de teléfono (**901 111 121**) para la consulta y resolución de

	incidentes de seguridad relacionados con el uso de las TIC. **Desde este enlace,** OSI destaca toda la información relativa a cómo y dónde reportar información sobre fraudes electrónicos. Además, la OSI ofrece la interesante opción de suscribirse a las últimas novedades en seguridad informática **a través de este enlace**, facilitando tan solo una dirección de correo electrónico. Es interesante destacar también, dentro del **portal OSI**, otros contenidos como: • Los **avisos de seguridad**, para estar actualizado de las últimas alertas de seguridad. • El **Blog,** dónde se publican noticias de actualidad referentes a la seguridad. Todos los contenidos están escritos con un lenguaje sencillo y cercano para el usuario al que le resulta difícil leer textos con un lenguaje más técnico y dirigidos a un público más profesional. Además, en la página de Internet Segura for Kids hay información enfocada a menores (**https://www.is4k.es**) con secciones dirigidas específicamente a familias y profesorado, con su propio **blog**. • **Historias reales**. Sección qué informa a los ciudadanos sobre los **últimos fraudes y timos** relacionados con **Internet**. Son los propios ciudadanos los que contactan a través del **buzón de correo** para contar su historia. Existen casos en los que el usuario ha sido víctima de un fraude. En otros casos, los usuarios han sido capaces de identificar el timo y han sabido evitarlo y protegerse adecuadamente. En ambos casos su propósito es contar su caso para evitar que otros se conviertan en víctimas de esas estafas. • **Servicio Antibotnet**, que te permite identificar si desde tu conexión a Internet (dentro de España) se ha detectado algún incidente relacionado con botnets (ordenadores infectados, controlados por ciberdelincuentes, para llevar a cabo acciones maliciosas). • **Conan Mobile**, una aplicación gratuita que te permite conocer el estado de seguridad de tu dispositivo móvil. Tras la presentación y navegación por estos servicios y herramientas de la web, a ser posible haciendo uso del proyector, como actividad final se animará al alumnado a **realizar en grupo un cartel** que resuma las herramientas de soporte y denuncia comentadas. El cartel puede ser elaborado en un formato grande y llamativo, de forma que pueda permanecer en un lugar visible en el centro educativo, fácilmente accesible para todo el alumnado.

Actividad 06 Autoevaluación

Descripción	Test de autoevaluación individual
Metodología	Autoevaluación individual
Duración	10 minutos

Recomendaciones	Se ha elaborado **un test de autoevaluación** sencillo (de uso individual), que evalúa los criterios marcados en el siguiente epígrafe (‘**Criterios de evaluación’**), facilitando la verificación de que el alumnado ha entendido y asimilado conceptos y buenas prácticas relacionados con cada uno de los contenidos trabajados. De modo complementario a éste, se propone la opción de introducir como herramienta de evaluación un **crucigrama** específico[6] que sirva de repaso a los principales conceptos recogidos a lo largo de la Unidad Didáctica. En el **Anexo 3** a esta Unidad Didáctica, se muestra también la solución al crucigrama propuesto. VIRUS Y FRAUDES  Horizontal 4. Red de ordenadores infectados que, sin saberlo, estan siendo controlados de forma remota 6. Programa que detecta la presencia de un virus informatico y generalmente, lo elimina 7. Programa informatico que busca alterar el funcionamiento de dispositivos electronicos Vertical 1. Actividad delictiva orientada a tener un beneficio economico ilicito, a traves de dispositivos electronicos 2. Actividad delictiva que busca obtener de forma ilicita nuestras claves de acceso 3. Sistema que previene el uso y acceso desautorizados a tu ordenador 4. Falsos antivirus que infectan nuestros dispositivos 5. Servicios que utilizan la red de telefonia para enviar contenido a tu telefono, previo pago por este servicio

[6] Generado a través de herramientas sencillas como el Generador de crucigramas de Educima, utilizado como ejemplo en la creación del crucigrama propuesto o cualquier otro, elegido por el docente, que cumpla esta función.

4.4. Criterios e instrumentos de evaluación.

Se ha elaborado un **Test de Autoevaluación (Anexo 1)** relacionado con las competencias alineadas con la Unidad Didáctica que, tomando como referencia el "**Marco Común de Competencia Digital Docente**"[7]. **Evalúa tanto los conceptos de virus y fraude informático como los principales recursos y mecanismos de prevención, así como el desarrollo de actitudes responsables para el adecuado uso de ordenadores y dispositivos móviles.** En el **Anexo 2** se muestran las respuestas al Test.

El test de autoevaluación se ha elaborado con el objetivo de que el alumnado compruebe los conocimientos como actividad final de la presente Unidad Didáctica. El test de autoevaluación también puede ser utilizado al inicio y al final. Al inicio como actividad nº 0, con objeto de que el alumnado sea consciente de los conocimientos que tiene sobre la temática, y al final estableciendo una comparativa y observando los avances obtenidos tras la realización de todas las actividades.

También se puede pedir al alumnado que aporte alguna pregunta más a incluir en el test. Desafiar a sus compañeros siempre es un reto atractivo; de esta manera se fomentará su curiosidad y espíritu competitivo en beneficio del aprendizaje. La resolución del test de forma grupal preguntando al alumnado los motivos de escoger cada respuesta puede ayudar a hacer más atractiva la actividad. La evaluación atenderá de este modo al interés y participación del alumnado, tanto en ésta como el resto de las actividades planteadas a lo largo de la Unidad Didáctica.

Como ya se describía en la **Actividad 06**, de modo complementario al test se puede introducir como herramienta de evaluación un **Crucigrama** específico que sirva también de repaso a los principales conceptos recogidos a lo largo de la Unidad Didáctica. En el **Anexo 3** se muestra la solución al crucigrama.

5. Marco teórico de apoyo al docente

Se incluyen a continuación orientaciones y recomendaciones para abordar los distintos conceptos que integran esta Unidad Didáctica.

5.1. Definición de virus

Este término se refiere, a lo largo de la Unidad Didáctica, a programas informáticos que buscan alterar el funcionamiento de los dispositivos (ordenadores, tabletas, teléfonos móviles, etc.) y, en muchos casos, robar información del usuario[8].

A día de hoy estos virus informáticos son creados con el principal objetivo de **obtener información de los usuarios infectados** (datos bancarios, número de tarjetas de crédito, información personal, contraseñas de acceso al correo electrónico y redes sociales, etc.) que les pueda comprometer y obtenerse un **beneficio económico con ellos**. Para ello utilizan técnicas como las siguientes:

- Poner en circulación estafas y fraudes a través del email y redes sociales.
- Suplantar la identidad de la víctima.

[7] Marco Común de Competencia Digital Docente V 2.0

[8] Definición extraída del Monográfico sobre Protección ante virus y fraudes, elaborado por RED.ES (recogido en el apartado Bibliografía / Documentación complementaria de esta Unidad Didáctica).

- Enviar masivamente publicidad maliciosa.
- Colar aplicaciones móviles maliciosas en las tiendas oficiales, como Google Play o Apple Store u otras alternativas.
- Facilitar la descarga de contenidos infectados como películas, series, programas, música, etc. a través de portales que ofrecen estos materiales de "manera gratuita".
- Instalar plugins y complementos maliciosos.
- Intentar suscribir a los usuarios a servicios de tarificación especial desde sus dispositivos móviles.
- Etc.

Los virus actuales más comunes no requieren siquiera de la acción humana para ser activados en un determinado dispositivo electrónico. Son propagados fácilmente a través de **mecanismos y vías de infección** utilizando técnicas denominadas de ingeniería social para engañar y manipular al usuario, infectar sus dispositivos y sustraer su información personal y privada. Principales vías de infección:

- **Correo electrónico.** Es una de las principales vías de entrada de virus a través de ficheros adjuntos peligrosos o enlaces a páginas web maliciosas.
- **Dispositivos de almacenamiento externo** (USB, discos duros, tarjeta de memoria). Al copiar archivos infectados de un USB a un equipo, en ocasiones simplemente por el hecho de conectar un USB, puede resultar infectado, ya que algunos virus tienen la capacidad de auto-ejecutarse.
- **Descarga de ficheros desde Internet.** Al abrir o ejecutar ficheros (programas, contenido multimedia, documentos, etc.) pueden traer camuflado/escondido algún tipo de malware. Hay que tener especial precaución con lo que se descarga mediante programas de compartición de ficheros (P2P) o se obtiene en las distintas páginas web de descarga de contenidos, ya que pueden ser más propensos a contener virus.
- **Páginas web maliciosas.** Preparadas para infectar al usuario que las visita aprovechando **problemas de seguridad de un navegador no actualizado** o de los complementos instalados: Java, Flash, etc. También a través de páginas web legítimas, que han sido manipuladas por ciberdelincuentes, **redirigiendo a webs maliciosas o fraudulentas**. Una forma de llegar a éstas podría ser, por ejemplo, hacer clic en **enlaces acortados** en Twitter (u otras redes sociales) o en enlaces facilitados en correos electrónicos fraudulentos.
- **Redes sociales.** Utilizadas para infectar los dispositivos debido a la gran cantidad de usuarios que las frecuentan y el alto grado de propagación que facilitan. Hay que ser precavidos frente a publicaciones con enlaces a páginas web con mensajes o titulares llamativos que resulten "raros" o poco fiables, solicitudes para instalar programas para poder acceder o visualizar un contenido, o aplicaciones que solicitan autorización no justificada para el acceso a nuestra **información personal**.
- **Vulnerabilidades y fallos de seguridad** en los sistemas operativos, navegadores, aplicaciones, plugins o programas instalados en el dispositivo. Son aprovechadas por los ciberdelincuentes para infectar los equipos, a veces sin que el usuario tenga que realizar una acción que le haga consciente de ello. El ejemplo comentado en este caso por el formador puede ser el **Fallo de seguridad de Abobe Flash Player**. A través de este fallo de seguridad un atacante puede tomar el control remoto de un dispositivo y realizar cualquier acción, como por ejemplo instalar malware. Para evitarlos, es importante mantener actualizados nuestros dispositivos. El docente comentará que precisamente la actualización del programa

ante la vulnerabilidad detectada en Adobe Flash permitió que la incidencia se solventara con total rapidez.

A modo de resumen, se recogen en la siguiente tabla algunos de los principales **mecanismos de actuación** de diferentes tipologías de virus y las **consecuencias y riesgos** que pueden acarrear éstos:

MECANISMOS DE ACTUACIÓN	CONSECUENCIAS. RIESGOS
• Bloqueo o toma del control del ordenador infectado, en algunos casos solicitando un ingreso económico para desbloquearlo, previa suplantación de identidad, es decir haciéndose pasar generalmente por una organización, empresa o entidad conocida con cierta reputación y prestigio.  Ejemplo "**Virus de la Policía**" • Captura de pulsaciones del teclado para hacerse con claves y contraseñas de acceso a los servicios online. • Espionaje mientras permanece oculto el virus en el sistema y sin mostrar actividad aparente, escondiéndose del antivirus. • Aprovechamiento de fallos de seguridad en plugin y aplicaciones que los usuarios utilizan habitualmente (Adobe Flash Player, Java, Acrobat Reader, etc.). • Conectando un pen-drive USB o accediendo a una página web infectada. • Abriendo un archivo adjunto de imagen (aparentemente inocua) que contiene un código que se ejecuta de forma automática en el momento en que se visualiza ésta. • Activando la webcam del usuario sin que éste sea consciente de que está siendo grabado.	• Cifrado y/o borrado de la información almacenada en el dispositivo.  Ejemplo "**Falsa factura de Endesa**" • Ralentización o inutilización del dispositivo. • Espionaje y/o robo de información personal: fotografías, datos bancarios, números de tarjetas de crédito, documentación importante, etc. • Suplantación de identidad. Envío de correos electrónicos en nombre de la víctima, publicar en sus perfiles en redes sociales, realizar transferencias económicas a otras cuentas bancarias, realizar compras y pagos online, etc. • Robo y pérdidas económicas • Uso del ordenador de la víctima para realizar ataques a otros ordenadores, infectándolos para obtener información de sus usuarios, realizar estafas o el envío de publicidad. • Envío de SPAM desde el ordenador de la víctima sin que ésta sea consciente.

5.2. Principales medidas de protección frente a los virus

Ante el posible ataque de un virus informático hay que estar protegido aplicando **pautas y recomendaciones** de forma habitual en el uso de cualquier tipo de dispositivo o servicio online:

Genéricas

- ☐ Actualizar el software instalado: sistema operativo, navegador, plugin, complemento y cualquier otro programa que se utilice.
- ☐ Instalar y mantener actualizado el antivirus en todos los dispositivos (ordenadores, tabletas y teléfonos móviles).
- ☐ Configurar cuentas de usuario limitado. Permisos restringidos para la instalación de programas.
- ☐ Comprobar a qué sitio web nos redirige un enlace antes de abrirlo.
- ☐ Evitar navegar por páginas web de dudosa reputación o sospechosas.
- ☐ Descargar contenidos sólo desde páginas web oficiales y, antes de abrirlos, analizarlos con un antivirus.
- ☐ No utilizar medios de almacenamiento extraíbles que no sean de confianza.

Específicas de dispositivos móviles

- ☐ Descargar aplicaciones sólo desde fuentes seguras y confiables.
- ☐ Comprobar los permisos solicitados por cada aplicación antes de comenzar su descarga e instalación.
- ☐ Sospechar de las aplicaciones con bajo número de descargas y/o con pocos comentarios de usuarios que sean excesivamente halagadores.
- ☐ Desactivar la opción 'Permitir orígenes desconocidos' (a través de los Ajustes de Seguridad del dispositivo) para que no se instalen aplicaciones de tiendas no oficiales.
- ☐ Respetar las restricciones del fabricante del dispositivo móvil (no hacer un jailbreak o rootearlo).

5.3. Fraudes electrónicos

El fraude electrónico se puede definir como la actividad delictiva que se lleva a cabo a través de medios como Internet, ordenadores y dispositivos móviles. Generalmente se apoya en la ingeniería social para materializarse.

- **Ingeniería social**[9]: engaños y manipulaciones dirigidos a embaucar a los usuarios para conseguir información que posteriormente será utilizada para sustraerle claves de acceso, contraseñas, extorsión, etc. La característica esencial es que se trate un tema o situación que resulte atractivo o llamativo para el usuario, por ejemplo:
  - **Desastres naturales/accidentes.** Este tipo de situaciones son utilizadas por los ciberdelincuentes para aprovecharse de la sensibilidad y vulnerabilidad que estos hechos provocan en las personas para, por ejemplo, difundir páginas fraudulentas de donaciones.
  - **Celebración de olimpiadas, mundiales, festivales, congresos**... son una buena excusa para poner en circulación falsos sorteos, entradas, descuentos que todo el mundo querrá obtener. Para ello, solo tienen que introducir sus datos personales ¡Quién puede resistirse a conseguir algo gratis!
  - **Noticias sobre famosos**: escándalos, controversias o muertes captan la atención de los usuarios. Los ciberdelincuentes utilizan toda su imaginación para conseguir que se haga clic en vídeos o links que darán detalles escabrosos del suceso. El problema es que detrás de esa supuesta información se suele esconder algún virus.
  - **Situaciones que generan alarma:** multas, denuncias, notificaciones, problemas de seguridad... En este grupo estarían clasificados los ya más que conocidos Phishing, en los que, a través de un email, se le alerta al usuario de que debe realizar una acción de forma inmediata. Principal objetivo de esto: robar datos personales y bancarios de los usuarios e infectar dispositivos para obtener un beneficio económico. Ejemplos típicos:
    - **Problemas de seguridad en cuenta bancaria**
    - **Multas de Policía**
    - **Notificaciones de la Agencia Tributaria**
    - **Envío de facturas electrónicas**
  - **Lanzamiento de nuevos producto o servicios.** La presentación de un nuevo iPhone, actualizaciones en el sistema operativo o en cualquier otro producto o servicio de interés general pueden ayudar a propagar correos, mensajes, noticias, vídeos e imágenes con malware.
  - **Situación política del país.** Difundir bulos sobre los políticos y sus partidos es perfecto para recopilar direcciones de correo electrónico de usuarios así como otros posibles datos personales gracias al reenvío de los mensajes.

[9] Ambas definiciones han sido extraídas del Monográfico sobre Protección ante virus y fraudes, elaborado por RED.ES (recogido en el apartado Bibliografía / Documentación complementaria de esta Unidad Didáctica).

Basados en el engaño y aprovechando la ingenuidad y desconocimiento de los usuarios, los cibercriminales utilizan esta "vulnerabilidad humana" (especialmente entre los más jóvenes) para llevar a cabo sus estafas, propagándolas principalmente a través de servicios de juego online, redes sociales, correo electrónico y aplicaciones móviles gratuitas.

Existen **numerosos ejemplos** de fraudes electrónicos, que llegan al usuario en forma de falsas notificaciones, y facturas, tiendas online de venta de artículos falsificados, botones de descargas fraudulentos que llevan a sitios web maliciosos o que intentan que te suscribas a servicios Premium, alquileres falsos, falsos premios, cupones y loterías, fraudes en la venta de artículos de segunda mano, etc.

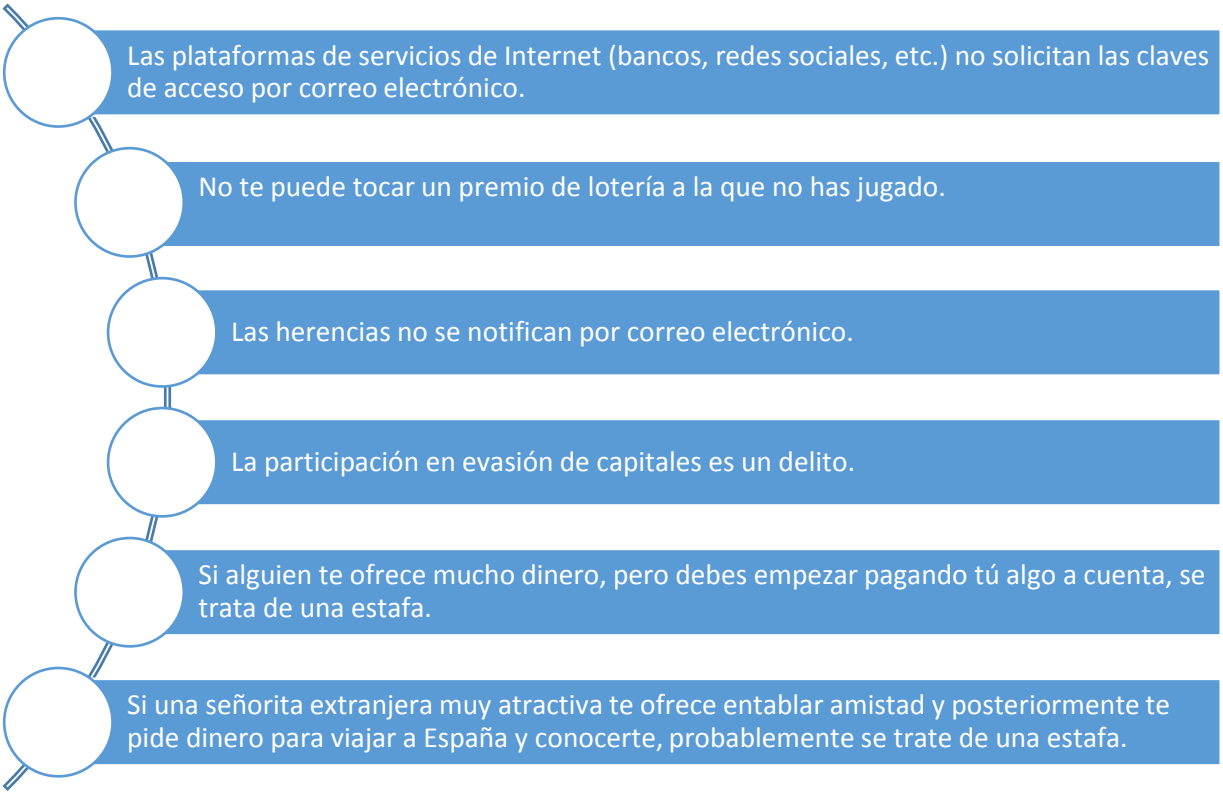
Algunos ejemplos:

- **Los Rogues (falsos antivirus),** que a través de un programa fraudulento genera en el ordenador falsas alertas en las que se advierte al usuario de que su sistema se encuentra infectado con un peligroso virus. Utilizan este engaño para invitar al usuario a descargar una supuesta versión completa de un programa de protección para supuestamente desinfectar el equipo, previo pago y generalmente haciendo uso de medios no recomendados para transacciones online.
- **Phishing:** Una actividad delictiva cuyo objetivo se basa en obtener de forma ilícita claves de acceso, contraseñas así como cualquier otra información sensible del usuario. A través de una falsa página web y utilizando estrategias de ingeniería social (normalmente por medio de correo electrónico, SMS y actualmente también por mensajería instantánea), hacen creer a la víctima que se está conectando a la web original de un banco o entidad conocida, robando sus datos y claves de acceso cuando los introducen en dicha web.
- **Aplicaciones fraudulentas** para dispositivos móviles que envían mensajes desde el teléfono, sin que la víctima se dé cuenta, suscribiéndoles a servicios de tarificación especial (*SMS Premium)* con un coste económico añadido para el usuario.
- **Robo de datos del menor** a través de juegos y redes sociales, que con el pretexto de 'conseguir vidas' o 'trucos para pasar de pantalla' embaucan a los menores para hacerse con sus datos personales.

En todo caso, el fraude electrónico conlleva importantes **consecuencias**, con gran impacto tanto en los menores como en los adultos:

- **Robo de identidad**: por causa del robo de claves de acceso y contraseñas.
- **Robo de información**: el objetivo principal suele ser tarjetas de crédito y datos bancarios, así como información personal y confidencial (fotografías, documentos, etc.) para obtener un beneficio económico con ellos, bien sea porque venden esa información en "mercados negros" o porque directamente esa información la pueden convertir en dinero. Por ejemplo, si consiguen directamente el acceso al servicio de banca online, o bien extorsionan con difundir los contenidos comprometidos si no se realiza el pago de una cantidad económica.
- **Suscripciones a servicios de mensajería de alto coste**: mediante la suscripción al propietario del dispositivo a servicios de mensajería *SMS Premium*. La suscripción se realiza de forma legal ocultando cláusulas y condiciones en la aceptación de la instalación de juegos y aplicaciones.

Una buena forma de prever estas consecuencias y minimizarlas es seguir las siguientes **recomendaciones**, de sentido común, **dirigidas a detectar el fraude electrónico**:



5.4. Recomendaciones básicas para evitar ser víctima del fraude electrónico

- Sospecha de los mensajes de correo electrónico de remitentes desconocidos.
- No accedas a sitios web desde enlaces en correos que te resulten sospechosos.
- Desconfía de correos o mensajes extraños aunque vengan de conocidos o amigos. Existen virus que tras infectar un sistema envían mensajes fraudulentos a los contactos del correo o de las redes del propietario del dispositivo.
- Desconfía de los correos electrónicos que te ofrecen un premio o un descuento.
- Cambia tus contraseñas periódicamente y asegúrate de que son robustas. No uses la misma para todos los servicios.
- Ten en cuenta que los correos electrónicos fraudulentos a menudo incluyen faltas de ortografía y mala gramática.
- Actualiza tu software antivirus con frecuencia, tanto en ordenadores como en dispositivos móviles.
- Ten cuidado con los correos electrónicos que tratan de apresurarte a la acción. Mensajes como "Actualizar ahora o vamos a cerrar su cuenta..." son comunes entre los correos fraudulentos.
- No incluyas datos personales o sensibles en respuesta a un correo electrónico cuyo remitente desconoces o que el mensaje te parezca raro o sospechoso aun procediendo de alguien conocido.

- Evita las cadenas de mensajes, ya que éstas son fuente de correo basura *(spam)* y un modo de recopilación de direcciones de correo electrónico que pueden ser utilizadas para enviar correos fraudulentos. Para ello, lo mejor es enviar los correos con destinatarios ocultos.
- No utilices redes wifi públicas para acceder a servicios de redes sociales, correo electrónico o realizar cualquier otro tipo de trámite que requiera de intercambio de información privada.

5.5. Principales medidas de protección frente a virus y fraudes electrónicos

De entre todas las recomendaciones y pautas facilitadas al alumnado a lo largo de la Unidad Didáctica, merece la pena destacar y trabajar específicamente las siguientes, dirigidas a prevenir y protegernos frente a virus y fraudes, fomentando el uso responsable de la tecnología:

- Llevar a cabo instalaciones seguras (que no comprometan los dispositivos) a través de sitios oficiales de descarga. Descargar programas y aplicaciones sólo desde páginas oficiales.
- Instalación y correcta actualización de programas antivirus, tanto en ordenadores como en tabletas y smartphones, descargándolos desde la web oficial del fabricante.
- Activación de cortafuegos (integrado en el sistema operativo) que bloquea el acceso no autorizado a nuestros dispositivos, permitiendo las comunicaciones autorizadas.
- Actualizaciones: sistema operativo, navegadores, plugins y programas.
- Realización de copias de seguridad: para impedir que la acción de algún virus suponga su pérdida.
- Cifrado de la información como medida de protección para que sólo puedan acceder a ésta las personas autorizadas que dispongan de la clave de descifrado.
- Gestionar el acceso a dispositivos compartidos con cuentas de usuario limitado, que permiten la instalación de aplicaciones o modificaciones en la configuración sólo a través del perfil “administrador”.
- Llevar a cabo una buena gestión de contraseñas (secretas, robustas y no repetidas).
- Cambiar periódicamente la contraseña de la clave wifi del router.
- Tomar precauciones al utilizar dispositivos públicos y conectarse a redes wifi públicas.
- Tener precaución con los enlaces cortos (tipo bit.ly; goo.gl;) antes de acceder a ellos – sobre todo desde Twitter y otras redes sociales, donde se usan para ahorrar caracteres – ya que pueden dirigir a páginas web fraudulentas que contienen malware.
- Evitar la navegación por páginas web sospechosas.
- Configurar adecuadamente los ajustes de privacidad en las redes sociales.
- Evitar conectar a los dispositivos medios de almacenamiento extraíbles (USB) de dudosa procedencia, que pueden ser una puerta de entrada para los virus.

Una buena recomendación, en la prevención frente a virus y fraudes electrónicos es permanecer atentos a las últimas novedades en seguridad informática a través de la **página web de la Oficina de Seguridad del Internauta** (OSI)

- Comprender que la tecnología evoluciona constantemente y con ella la elaboración de nuevas formas de infectar dispositivos electrónicos y engañar a sus usuarios. Esto nos obliga a permanecer en alerta y permanentemente informados a través de **entidades y servicios de referencia** como por ejemplo:

Grupo de Delitos Telemáticos (Guardia Civil):

- Web sección **Colabora**
- **Formulario web de denuncia**
- Canal **Twitter**

Brigada Investigación tecnológica (Policía Nacional):

- **Web**
- **delitos.tecnologicos@policia.es**
- 902.102.112
- Canal **Twitter**

INCIBE:

- **Web Incibe**
- **Web OSI**
- **Web Internet Segura for Kids**
- Formulario alta incidentes: **incidencias@certsi.es**
- 901.111.121

OSI ofrece también la interesante opción de suscribirse a las últimas novedades en seguridad informática, **a través de sus boletines**, facilitando tan sólo una dirección de correo electrónico

---

6. Bibliografía / Documentación complementaria.

- Monográfico sobre protección ante virus y fraudes. Red.es
- Ponte al día con los virus informáticos. Oficina de Seguridad del Internauta
- Infografía "Fauna y flora de los virus". Oficina de Seguridad del Internauta
- El phishing versión gráfica. Oficina de Seguridad del Internauta
- Vídeo: Usa un escudo e impide el avance de los virus. Oficina de Seguridad del Internauta
- Herramientas gratuitas para proteger nuestros dispositivos
- Sección de avisos de la Oficina de Seguridad del Internauta

- Vídeo: Cómo proteger nuestros dispositivos móviles de los ataques de los virus. Radio Televisión Española
- Vídeo: La principal puerta de entrada del malware para teléfonos es la descarga de aplicaciones. Radio Televisión Española
- Fraude Online. Oficina de Seguridad del Internauta
- Sección de "Reporte de fraude" de la Oficina de Seguridad del Internauta

Internet Segura for Kids http://www.is4k.es

Página web del Centro de Seguridad en Internet para menores en España. Incluye:

- La información que "**necesitas saber**" sobre privacidad, ciberacoso escolar, sexting, contenido inapropiado, uso y configuración segura, mediación parental.
- Artículos de interés y actualidad en el "**blog**".
- Guías, juegos, herramientas de control parental y otros recursos "**de utilidad**".
- Información de "**programas**" de sensibilización para un uso seguro y responsable de Internet por los menores.
- Una "**línea de ayuda**" con una serie de preguntas frecuentes y un contacto para resolver dudas.

7. Anexo 1. Test de autoevaluación

1.- Un virus es un programa informático que busca alterar el funcionamiento de dispositivos electrónicos, como ordenadores, teléfonos móviles o tabletas.
❑ Verdadero
❑ Falso

2.- ¿Cuál de los siguientes términos corresponde a un tipo de fraude electrónico?
❑ a) *Phishing.*
❑ b) *Rogues* o falsos antivirus.
❑ c) SMS Premium.
❑ d) Todas las anteriores.

3.- Una red zombi es aquella que de forma engañosa, suscribe al usuario a servicios de envío de mensajes de pago, a través de su teléfono móvil.
❑ Verdadero
❑ Falso

4.- Cuál de las siguientes opciones NO es un riesgo relacionado con los dispositivos móviles (teléfonos, tablet):
❑ a) El escaso volumen de datos que guardamos a través de este tipo de dispositivos.
❑ b) Las aplicaciones maliciosas que puedes encontrar en sitios de descarga no oficiales.
❑ c) El uso de aplicaciones como *Facebook*, *Twitter*, *WhatsApp*, *Line* o *Snapchat* para extender virus y fraudes de forma rápida.
❑ d) La falta de un antivirus instalado en este tipo de dispositivos.

5.- ¿A cuál de los dos términos se refiere esta definición: '*actividad delictiva que se lleva a cabo a través de medios como Internet, ordenadores y dispositivos móviles*'?
❑ Ingeniería social.
❑ Fraude electrónico.

6.- Señala la opción incorrecta. Cuál de las siguientes medidas NO es una buena estrategia de prevención ante el fraude electrónico:
❑ a) Actualizar el software antivirus en nuestros dispositivos con frecuencia.
❑ b) Desconfiar de los mensajes que ofrecen premios o descuentos de forma gratuita.
❑ c) No acceder a sitios web desde enlaces que resulten sospechosos o enlaces Web acortados.
❑ d) Utilizar la misma contraseña de acceso para todos nuestros servicios (correo, redes sociales, etc.)

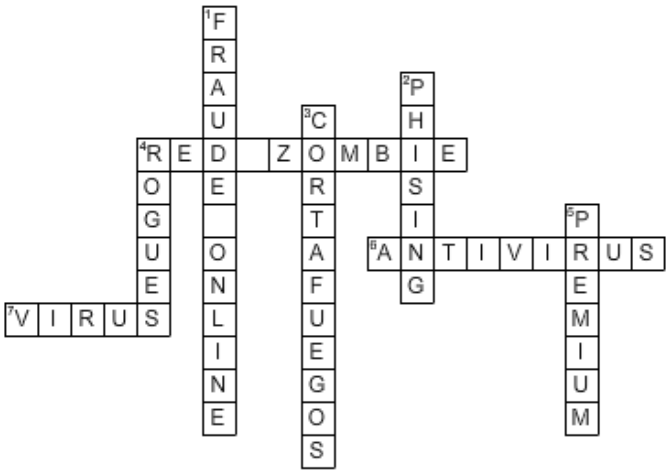
7.- Enumera al menos 3 recomendaciones técnicas, que es oportuno tener en cuenta, como medida de prevención, ante virus y fraudes electrónicos en nuestros dispositivos electrónicos.

8. Anexo 2. Respuestas al test de autoevaluación

1. **Verdadero**. Efectivamente, entendemos por **virus informáticos** aquellos programas que buscan alterar el funcionamiento de los dispositivos (ordenadores, tabletas, teléfonos móviles, etc.) y en muchos casos, robar información del usuario.
2. **Opción D**. Todas las anteriores afirmaciones son correctas.
3. **Falso**. Una red zombi es una red de ordenadores infectados que, sin el conocimiento de sus propietarios legítimos, están siendo controlados por un grupo de ciberdelincuentes de forma remota.
4. **Opción A**. Hoy en día, en un teléfono móvil se almacenan gran cantidad de datos: contactos, fotos personales, contraseñas de acceso a múltiples aplicaciones, documentos, grabaciones, y todo tipo de información personal, que aumentan la vulnerabilidad y riesgo de este tipo de dispositivos móviles, a sufrir ataques e malware o fraudes electrónicos.
5. **Opción B.** Aunque ambos términos están relacionados, la descripción expuesta corresponde a la definición de "fraude electrónico", entendiendo por "Ingeniería social" aquellos engaños y manipulaciones que – aprovechando la ingenuidad y desconocimiento del usuario – aprovechan su vulnerabilidad para realizar la estafa o fraude, a través de herramientas como videojuegos, redes sociales, correo electrónico y aplicaciones móviles gratuitas.
6. **Opción D**. Sigue todas las indicaciones recogidas en esta pregunta… incluido el ¡cuidado y precaución con tus contraseñas! Utilizar la misma clave de acceso y contraseña para distintos servicios aumenta aún más el riesgo de robo de información personal cuando se es víctima de una estafa.
7. **Respuesta correcta**: Sería correcta cualquier respuesta que incluya alguna de las siguientes recomendaciones, trabajadas en el aula:
   - Acudir a sitios oficiales para la descarga e instalación de programas y aplicaciones.
   - Instalar y mantener actualizado el antivirus en todos nuestros dispositivos electrónicos.
   - Instalar un **cortafuegos**.
   - Actualizar periódicamente el sistema operativo, navegadores y programas instalados en nuestros dispositivos.
   - Realizar periódicamente copias de seguridad.
   - Limitar los permisos de instalación en nuestros dispositivos.
   - Verificar la legitimidad de las páginas Web a las que accedemos, especialmente de aquellas que nos parecen sospechosas.
   - Instalar en nuestros dispositivos el **Servicio Antibotnet.**
   - Revisar nuestras contraseñas, modificándolas periódicamente, no utilizando en ningún caso la misma contraseña para todos los servicios a los que accedemos a través de ella.
   - Tener precaución y rechazar el uso de wifi no confiables.

9. Anexo 3. Respuestas al crucigrama propuesto

VIRUS Y FRAUDES



Horizontal

4. Red de ordenadores infectados que, sin saberlo, estan siendo controlados de forma remota
6. Programa que detecta la presencia de un virus informatico y generalmente, lo elimina
7. Programa informatico que busca alterar el funcionamiento de dispositivos electronicos

Vertical

1. Actividad delictiva orientada a tener un beneficio economico ilicito, a traves de dispositivos electronicos
2. Actividad delictiva que busca obtener de forma ilicita nuestras claves de acceso
3. Sistema que previene el uso y acceso desautorizados a tu ordenador
4. Falsos antivirus que infectan nuestros dispositivos
5. Servicios que utilizan la red de telefonia para enviar contenido a tu telefono, previo pago por este servicio

10. Anexo 4. Recursos asociados

Recursos asociados a esta Unidad Didáctica disponibles para su futura utilización por los docentes:

- Presentación charla sensibilización dirigida al alumnado.
- Guía de preparación. Charla sensibilización dirigida al alumnado.

Toda la información del programa de Jornadas Escolares está disponible en la sección **programas** del portal **IS4K**.