GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

red.es

"Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad"

[Red.es]

UNIDADES DIDÁCTICAS PROTECCIÓN ANTE VIRUS Y FRAUDES

SECUNDARIA (13-17 años)

UNIDADES DIDÁCTICAS PROTECCIÓN VIRUS Y FRAUDES SECUNDARIA

1. UNIDAD DIDÁCTICA I: FRAUDE ELECTRÓNICO

1.1. FICHA RESUMEN

Objetivos didácticos

- Conceptualizar el fraude electrónico: ¿Qué es el fraude electrónico?
- Trabajar la prevención y actuación frente al fraude electrónico.

Competencias

- **Competencias digitales:** de información, en comunicación, de seguridad.
- **Competencias básicas:** en comunicación lingüística, en el conocimiento y la interacción con el mundo físico, de autonomía e iniciativa personal, social y ciudadana y para aprender a aprender.

Contenidos

- **Conceptuales:**
  - Concepto de fraude electrónico.
  - Principales riesgos de los fraudes electrónicos y la ingeniería social.
  - Casos reales de fraude electrónico.
  - Mecanismos de prevención ante fraudes electrónicos.
- **Procedimentales:**
  - Analizar las causas por las que se puede ser víctima de un fraude electrónico.
  - Concienciar al alumnado con casos reales de fraude electrónico.
  - Elaborar un listado de buenas prácticas y mecanismos de prevención ante los fraudes en Internet.
- **Actitudinales:**
  - Despertar el interés del alumnado por conocer los riesgos de los fraudes electrónicos.
  - Sensibilizar sobre los riesgos y la problemática asociada a la cesión de datos personales bajo engaños (ingeniería social) y otros problemas derivados como contraseñas robadas y suplantación de identidad en redes sociales.
  - Alertar al alumnado sobre las consecuencias personales, sociales y económicas que puede causar ser víctima de un fraude en Internet.

Metodología

- Temporalización: 2 sesiones (de 45 minutos cada una).
- Metodología basada en conocimiento previo, activa, reflexiva y participativa.
- Recursos didácticos: debate, estudio de casos y video.

Actividades

- Sesión 1: Conocer el fraude electrónico.
- Sesión 2: Mecanismos de prevención del fraude electrónico.
- Sesión 3: Evaluación.

Evaluación

- Métodos de evaluación: participación, observación y actividad de evaluación.
- Criterios de evaluación:
  - Conocimiento del concepto de *fraude electrónico* (uso adecuado de las redes sociales), las características del *fraude electrónico,* los recursos para la prevención.
  - Adquisición de los mecanismos de prevención del *fraude electrónico y* las herramientas de detección de un uso inadecuado de las redes sociales.
  - Desarrollo de actitudes responsables para el uso apropiado de las redes.

Documentación de apoyo

- Monográfico de protección ante virus y fraudes.
- Curso en línea Seguridad TIC y Menores.

1.2. OBJETIVOS DIDÁCTICOS

En la presente unidad didáctica se abordarán los siguientes objetivos didácticos:

- Conceptualizar el fraude electrónico: ¿Qué es el fraude electrónico?
  - Conocer los principales riesgos.
  - Distinguir los principales métodos de estafa.
- Trabajar la prevención y los mecanismos de respuesta frene al *fraude electrónico:*
  - Conseguir que los/as alumnos/as sean precavidos.
  - Identificar los canales por los que se produce.
  - Destacar la importancia de la prevención.
  - Conocer mecanismos de respuesta frente al fraude electrónico.

1.3. COMPETENCIAS

Esta unidad didáctica permite al alumnado participante trabajar las **competencias digitales** tomando como referencia las del "Marco Común de la Competencia Digital Docente" (INTEF: Ministerio de Educación, Cultura y Deporte):

a. Competencia de información: el alumnado será capaz de navegar y buscar información en Internet sobre *fraude electrónico*, aplicando un criterio de filtrado, y comparando diferentes fuentes de información y el alumnado desarrolla una visión crítica en cuanto a la información encontrada en las redes.

b. Competencia en comunicación: el alumnado desarrollará habilidades de interacción a través de diversos dispositivos y aplicaciones digitales, con el objetivo de entender cómo se distribuye, presenta y gestiona la comunicación digital, siendo crítico con la información que encuentre sobre *fraude electrónico*.

c. Competencia de seguridad: el alumnado será capaz de protegerse de los riesgos que supone el *fraude electrónico*, tanto de los riesgos relacionados con la protección de la información, datos personales, protección de la identidad digital, estableciendo medidas de seguridad, desarrollo de estrategias activas para la identificación de las conductas inadecuadas y métodos de engaño en materia de ingeniería social.

Esta unidad didáctica permite trabajar con el alumnado participante las siguientes **competencias básicas** establecidas en la Ley Orgánica 2/2006, de 3 de mayo, de Educación:

a. Competencia en comunicación lingüística: el alumnado conocerá el lenguaje específico relacionado con *fraude electrónico* como nuevo medio de engaño. Incluyendo el uso del lenguaje no sólo para describir, sino interpretar, representar, comprender, construir conocimiento, así como autorregulando pensamiento, emociones y conducta.

b. Competencia en el conocimiento y la interacción con el mundo físico: el alumnado tendrá la posibilidad de interactuar con el mundo físico, en los aspectos generados por la acción humana en relación con las diferentes formas de fraude, posibilitando la comprensión de diferentes formas de engaño, consecuencias, modos y medidas de prevención.

c. Competencia de autonomía e iniciativa personal: le permitirá al alumnado desenvolverse adecuadamente y de forma independiente ante la presencia de riesgos provocados por el *fraude electrónico*.

d. Competencia social y ciudadana: el alumnado comprenderá la realidad social en la que vivimos, empleando el juicio ético basado en valores y buenas prácticas. Se fomentará la actuación del alumnado bajo criterio propio, siempre orientado a la mejora de la convivencia.

e. Competencia para aprender a aprender: supone que el alumnado disponga de habilidades para iniciarse en su propio aprendizaje y que sea capaz de continuar aprendiendo de forma cada vez más eficaz y autónoma frente a nueva información relacionada con diferentes casos de *fraude electrónico*, sujetos intervinientes y formas de prevención.

1.4. CONTENIDOS

- **Conceptuales**:
  - Concepto de fraude electrónico.
  - Principales riesgos de los fraudes electrónicos y la ingeniería social.
  - Casos reales de fraude electrónico.
  - Mecanismos de prevención ante fraudes electrónicos.
- **Procedimentales**:
  - Pautas de prevención del fraude electrónico.

  - Analizar las causas por las que se puede ser víctima de un fraude electrónico.
  - Concienciar al alumnado con casos reales de fraude electrónico.
  - Elaborar un listado de buenas prácticas, mecanismos de prevención y de actuación ante los fraudes en Internet.
- **Actitudinales**:
  - Despertar el interés del alumnado por conocer los riesgos de los fraudes electrónicos.
  - Sensibilizar sobre los riesgos y la problemática asociada a la cesión de datos personales bajo engaños (ingeniería social) y otros problemas derivados como contraseñas robadas y suplantación de identidad en redes sociales.
  - Alertar al alumnado sobre las consecuencias personales, sociales y económicas que puede causar ser víctima de un fraude en Internet.

1.5. METODOLOGÍA

Esta unidad didáctica se compone de una serie de actividades programadas para realizar en dos sesiones, cada sesión tendrá una duración de 45 minutos y es conveniente que se realicen en el orden establecido.

La metodología utilizada será dinámica, solicitando una participación activa al alumnado en su propio aprendizaje y reflexiva. Basándose en el conocimiento previo del alumnado sobre fraude electrónico para que el aprendizaje sea significativo.

Teniendo en cuenta las características propias de la edad que nos ocupa se utilizan recursos didácticos como el estudio de casos, el video y el debate.

En cuanto al material empleado para el desarrollo adecuado de esta unidad didáctica, se utilizará:

- El monográfico sobre *virus y fraudes,* del cual se pueden extraer los conceptos claves en forma de diapositivas para su uso en clase.
- Vídeos informativos sobre las distintas tácticas de fraude electrónico y sus consecuencias.
- Fichas de preguntas para trabajar los contenidos del vídeo.
- Pizarra o rotafolio.

- Equipos informáticos con conexión a Internet en el aula, con objeto de realizar búsquedas en la red para ampliar y afianzar conocimientos sobre el tema.

1.6. ACTIVIDADES

Las actividades que se van a realizar en esta unidad didáctica se estructuran en diferentes sesiones del siguiente modo:

1.6.1. Sesión 1: Conocer el fraude electrónico

Parte inicial: para sondear conocimientos previos del alumnado en materia del *fraude electrónico,* el docente solicitará al alumnado que escriban en un papel todo lo que sepan sobre *fraude electrónico:* ¿qué es?, ¿cómo se produce?, ¿cómo puede prevenirse? Sus aportaciones se guardarán en una caja y se recuperarán al final de la sesión.

A continuación contextualizará la actividad explicando el concepto de fraude electrónico, los métodos de engaño, y sus consecuencias.

Para ello contará con el siguiente cuadro de referencia:

Guía para el docente

Entendemos **fraude electrónico** como **"la actividad delictiva que se lleva a cabo a través de medios como Internet, ordenadores y dispositivos móviles"**.

Debilidades:

El fraude electrónico se basa en la ingenuidad y desconocimiento de los usuarios para llevar a cabo una estafa. En el caso de los menores, el riesgo es aún mayor, debido a su inocencia e ímpetu, y los cibercriminales se aprovechan de esta vulnerabilidad para llevar a cabo sus estafas poniendo el foco en puntos de atención del menor, como los videojuegos y las aplicaciones gratuitas:

Falta de prevención:

Otro de los aspectos que aprovechan los ciberdelincuentes es el hecho de que muchos menores utilizan la misma clave de acceso y contraseña para distintos servicios (correo electrónico, redes sociales, etc.) lo que aumenta aún más el riesgo de robo de información personal cuando se es víctima de una estafa.

Suscripciones ocultas y con coste

Incluir publicidad en los juegos gratuitos es una práctica habitual. Hay casos en los que al hacer clic en la publicidad de aplicaciones, el móvil envía el alta a servicios de pago sin que el usuario sea consciente de ello. De hecho, en algunos casos los SMS Premium no quedan registrados en el teléfono, pero sí que figuran en la factura.

Robo de datos del menor

La popularidad de los juegos (especialmente entre los menores) atrae a nuevos jugadores, y cómo no, también atrae a los ciberdelincuentes. Se han dado casos en los que se trataba de embaucar a los menores para que proporcionaran sus datos de acceso a Facebook, a cambio de "vidas infinitas".

Así, es fácil para los menores caer en la tentación de conseguir "trucos para pasar de pantalla" o "vidas infinitas" ofreciendo a cambio (y de forma ingenua) sus datos de acceso a redes sociales. Por eso, es aconsejable instruir correctamente a los menores para que no proporcionen ningún dato personal ni contraseña, a aplicaciones que estén fuera de la versión oficial del juego.

Fraude electrónico y consecuencias:

El fraude electrónico conlleva una serie de consecuencias que tienen impacto en los menores y en los adultos:

- **Robo de identidad**: principalmente se basa en robo de claves de acceso y contraseñas.
- **Robo de información**: el objetivo principal suele ser tarjetas de crédito y datos bancarios. También se roba información personal y confidencial (fotografías, documentos, etc.) con objetivos como chantaje y extorsión.
- **Suscripciones a servicios de mensajes SMS Premium**: consiste en suscribir al propietario del dispositivo (normalmente, los padres) a servicios de mensajería con alto coste. La suscripción se realiza de forma legal (pero de forma inmoral y poco ética) ocultando cláusulas y condiciones en la aceptación de la instalación de juegos y aplicaciones.

Parte principal: el docente explicará qué se pretende conseguir con el desarrollo de la unidad didáctica. Con el objetivo de abrir un debate sobre mecanismos de protección anti fraude con los menores, se visionarán los siguientes videos:

- "La gente no se da cuenta de que puede poner todos sus datos personales en riesgo" Enlace directo: https://www.youtube.com/watch?v=WY6g-KzeMNw
- “Las nuevas estafas de las redes sociales" Enlace directo: https://www.youtube.com/watch?v=k_8mM7fO2_g
- Las estafas en WhatsApp que deberías conocer. Enlace directo : https://www.youtube.com/watch?v=yZ3MjoeuDn8
- “Alertan de un nuevo fraude en Facebook para robar los datos de los usuarios”. Enlace directo: https://www.youtube.com/watch?v=jegLcvxAO1c
- “Seguridad informática: ingeniería social.© UPV”. Enlace directo: https://www.youtube.com/watch?v=iXxgZooYYBY

Tras la visualización de los vídeos, los jóvenes contestarán a las preguntas recogidas en la siguiente ficha, siendo el docente quién se encargará de moderar el debate y de que se respeten los turnos de palabra.

PREGUNTAS

- ¿Cuáles son los objetivos del fraude electrónico?
- ¿Qué tipos de fraude electrónico hay actualmente?
- ¿Existe una legislación que regule el uso de Internet a nivel global?
- ¿En qué se diferencia un Hacker de un cibercriminal?
- ¿Qué riesgos tiene conectarse a una red WIFI abierta (sin contraseña)?
- ¿Qué es la ingeniería social?
- ¿Cuáles son los métodos habituales de ingeniería social?
- En Seguridad Informática ¿Cuál es el eslabón más débil?
- ¿A quién puede afectar el fraude electrónico?
- ¿A qué sistemas operativos afectan los fraudes en Internet?
- ¿Los antivirus protegen del fraude electrónico?

- ¿Qué casos conocéis (familiares o amigos) que hayan sido víctima de un fraude electrónico?

Los/as alumnos/as ponen en común las respuestas para su corrección. El docente hará una llamada de atención sobre lo fácil que es que un estafador contacte con ellos/as a través de redes sociales y los peligros que puede tener. Reflexionará sobre el hecho de que al ser uno de los medios más utilizados por jóvenes es frecuente que los estafadores lo utilicen.

Parte final: el docente trasladará al alumnado una serie de recomendaciones y pautas en relación al debate generado sobre el *fraude electrónico* a través de redes sociales, juegos y aplicaciones de dispositivos móviles.

Guía para el docente

Recomendaciones para detectar el fraude electrónico: El docente explicará los principales métodos de detección de fraudes en Internet y los síntomas que pueden alertar al menor ante una situación de intento de estafa:

- Las plataformas de servicios de Internet (bancos, redes sociales, etc.) no solicitan las claves de acceso por correo electrónico.
- No te puede tocar un premio de lotería a la que no has jugado.
- Las herencias no se notifican por correo electrónico.
- La participación en evasión de capitales es un delito.
- Si alguien te ofrece mucho dinero, pero debes empezar pagando tú algo a cuenta, se trata de una estafa.
- Si una señorita extranjera muy atractiva te ofrece entablar amistad, y posteriormente te pide dinero para viajar a España y conocerte, probablemente se trate de una estafa.

Recomendaciones 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 cada 60 días 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 anti-virus con frecuencia, en ordenadores y dispositivos móviles.
- Ten cuidado con los correos electrónicos con un sentido de urgencia; que tratan de apresurarlo 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.
- 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 actividades potenciales de *phishing*. Para ello, lo mejor es enviar los correos con destinatarios ocultos.
- No utilices redes WIFI abiertas para conectar a tus servicios de redes sociales o correo electrónico.

Para concluir la actividad, el docente repasará brevemente las ideas previas del alumnado sobre *fraude electrónico*, incluidas al inicio de la sesión en una caja. Comparará y reforzará los conocimientos adquiridos con los previos.

1.6.2. Sesión 2: Prevención del fraude electrónico

Parte inicial: el/la profesor/a, expondrá la temática sobre los principales mecanismos de prevención ante una situación de *fraude electrónico.* Para ello se apoyará en el

material del monográfico, haciendo uso de diapositivas extraídas del mismo como material de apoyo en caso de considerarlo necesario, y de los siguientes videos:

- "*Cómo proteger tu red WiFi*" de la Oficina de Seguridad del Internauta. Enlace directo:

  https://www.youtube.com/watch?v=fFIYxd6L-uM

- "Diez consejos para proteger tu correo electrónico". Enlace directo:

  https://www.youtube.com/watch?v=LSzep2YN0r8)

Parte principal: Se presentan al alumnado las siguientes recomendaciones como mecanismo de prevención:

Guía para el docente

Recomendaciones para evitar ser víctima del fraude electrónico:

- No abras mensajes de correo electrónico de remitentes desconocidos.
- No accedas a sitios web desde un enlace en un correo electrónico, especialmente un correo electrónico que te pide información personal.
- 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 cada 60 días 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 anti-virus con frecuencia, en ordenadores y dispositivos móviles.
- Ten cuidado con los correos electrónicos con un sentido de urgencia; que tratan de apresurarlo 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.
- 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 actividades potenciales de *phishing.* Para ello, lo mejor es enviar los correos con destinatarios ocultos.
- No utilices redes WIFI abiertas para conectar a tus servicios de redes sociales o correo electrónico.

Parte final: Se pondrán en común las aportaciones de los participantes y el docente explicará cómo reaccionar ante un fraude online.

Guía para el docente

Cómo reaccionar ante un fraude online

Si sospechamos (o tenemos la evidencia) de que estamos siendo víctimas de un fraude electrónico, lo primero que hay que hacer es notificarlo a la autoridad competente.

- INCIBE (Instituto Nacional de Tecnologías de la comunicación) ha puesto en marcha a través de la Oficina de Seguridad del Internauta (OSI) un formulario de alta de incidentes (https://www.osi.es/es/reporte-de-fraude/formulario-de-alta-de-incidentes-generales), desde donde se puede indicar la información disponible sobre el caso de fraude o estafa online, o a través del teléfono 901110121.
- La Guardia Civil cuenta con el Grupo de Delitos Telemáticos (GDT) de la Unidad Central Operativa (UCO), con el que se puede contactar a través de la sección colabora de su página web https://www.gdt.guardiacivil.es/webgdt/pinformar.php, o incluso utilizar el formulario de denuncia que, una vez rellenado, generará un documento denuncia en formato PDF, que se puede presentar en un centro policial para interponer la denuncia.
- Por su parte, el Cuerpo Nacional de Policía, dispone de la Brigada de Investigación Tecnológica (BIT) para combatir la delincuencia que utiliza los medios que proporcionan las nuevas tecnologías de la información, y se puede contactar con ella a través del correo electrónico delitos.tecnologicos@policia.es

Finalmente, se visualizarán los siguientes vídeos:

- "*Consejos ciberseguridad con Leo Harlem*" proporcionado por INCIBE (Instituto Nacional de Ciberseguridad) Enlace:

  https://www.youtube.com/watch?v=LiFxQsJO4kk

- "Entrevista Juan y Damián de El Hormiguero sobre un "cibercrimen" proporcionado por INCIBE (Instituto Nacional de Ciberseguridad) Enlace:

  https://www.youtube.com/watch?v=VpR1QmPvC4A&feature=em-subs_digest

1.7. EVALUACIÓN

Esta evaluación se realizará mediante la observación por parte del docente de la participación e implicación del alumnado en el desarrollo de la sesión, y en la realización de actividades, así como con el planteamiento de tantas aclaraciones como fuera necesario ante las posibles dudas que se planteen sobre los contenidos abordados. Del mismo modo, se realizará un continuo feedback a través de preguntas de reiteración y repaso de conceptos e ideas claves.

Los criterios de evaluación que se pretenden conseguir son los siguientes:

- Los/as alumnos/as conocen:
  - El concepto de *fraude electrónico* asociado al uso adecuado/inadecuado de las redes sociales.
  - Las características que presenta los diferentes objetivos perseguidos por el *fraude electrónico*.
- Los/as alumnos/as adquieren:
  - Los mecanismos de prevención del fraude electrónico y en concreto los que derivan del buen uso de las redes sociales.
  - Las herramientas para detectar un mal uso de los dispositivos móviles.
  - Conciencia de los riesgos que entrañan los fraudes en Internet.
- Los/as alumnos/as desarrollan:
  - Actitudes responsables que favorecen el uso apropiado en las redes sociales.

- Mecanismos de prevención y estado de alerta frente a invitaciones con enlaces sospechosos, juegos con “vidas infinitas” y aplicaciones gratuitas.
- Métodos de prevención y actuación ante fraudes electrónicos, y que son conscientes de que deben estar alerta ante las distintas vías de engaño (correo electrónico, redes sociales, aplicaciones de mensajería tipo WhatsApp, etc.).

1.8. DOCUMENTACIÓN DE APOYO

Los siguientes recursos son de utilidad para ampliar el conocimiento sobre protección ante virus y fraudes:

Monográfico de protección ante virus y fraudes

Marco teórico de referencia para aprender herramientas, sistemas y pautas para proteger a los menores ante virus informáticos y situaciones de fraudes por Internet.

Disponible en: http://www.chaval.es/

Curso en línea Seguridad TIC y Menores

Curso de 30 horas de duración bajo metodología **MOOC** (*Massive Online Open Course* - Curso en línea masivo y abierto-) dirigido a padres y educadores. Sensibiliza sobre los riesgos a los que se enfrentan los menores en el uso de Internet y las nuevas tecnologías, ofreciendo estrategias, pautas y recomendaciones para su prevención y respuesta en caso de producirse un incidente. Contiene un módulo exclusivo sobre Protección ante virus y fraudes.

Disponible en: http://www.chaval.es

2. UNIDAD DIDÁCTICA II: VIRUS

2.1. FICHA RESUMEN

Objetivos didácticos

- Conocer en profundidad los riesgos de los virus informáticos.
- Mejorar la prevención en el uso de Internet y la protección de ordenadores y dispositivos móviles.
- Responder a la problemática actual y garantizar el uso adecuado de los menores de las TIC
- Observar el progreso de los alumnos en su adquisición de conocimientos sobre los mecanismos de protección ante los virus informáticos.
- Reforzar conocimientos en aspectos de prevención y mecanismos de actuación.

Competencias

- **Competencias digitales:** de información, en comunicación, de seguridad.
- **Competencias básicas:** en comunicación lingüística, en el conocimiento y la interacción con el mundo físico, de autonomía e iniciativa personal, social y ciudadana y para aprender a aprender.

Contenidos

- **Conceptuales:**
  - Concepto de virus. Principales riesgos de los virus. Casos reales de virus.
  - Mecanismos de prevención ante infecciones.
- **Procedimentales:**
  - Analizar las causas por las que se producen las infecciones de virus.
  - Concienciar al alumnado con casos reales de virus y elaborar un listado de buenas prácticas y mecanismos de prevención sobre los riesgos asociados a los virus.
- **Actitudinales:**
  - Despertar el interés del alumnado por conocer los riesgos de los virus y las consecuencias.
  - Sensibilizar sobre los riesgos y la problemática asociada a la cesión de datos personales bajo engaños (ingeniería social) y otros problemas derivados como contraseñas robadas y suplantación de identidad en redes sociales.

Metodología

- Temporalización: 2 sesiones (de 45 minutos cada una).
- Metodología basada en conocimiento previo, activa, reflexiva y participativa.
- Recursos didácticos: debate, estudio de casos y video.

Actividades

- Sesión 1. Métodos de infección de los virus.
- Sesión 2. Mecanismos de respuesta y prevención de *virus.*
- Sesión 3. Evaluación.

Evaluación

- Se evaluará con la participación, observación y actividad de evaluación. Criterios de evaluación:
  - Conocimiento del concepto, las características de los *virus, y* recursos para la prevención.
  - Adquisición de los mecanismos de prevención y detección de infecciones de *virus.*
  - Desarrollo de actitudes responsables para el uso apropiado de ordenadores y móviles.

Documentación de apoyo

- Monográfico de virus y fraude electrónico.
- Curso en línea Seguridad TIC y Menores.

2.2. OBJETIVOS DIDÁCTICOS

En la presente unidad didáctica se abordarán los siguientes objetivos didácticos:

- Conceptualizar los virus: ¿Qué son los virus?
  - Conocer en profundidad los riesgos de los virus informáticos.
  - Establecer la importancia de los riesgos que se derivan de las infecciones de virus y programas maliciosos.
  - Asegurar el aprendizaje significativo de los menores en los aspectos referentes a protección anti virus.
- Trabajar la prevención y actuación frente a los *virus:*
  - Activar mentalmente a los jóvenes y despertar su intuición para mejorar la prevención en su uso de Internet con ordenadores y dispositivos móviles.
  - Responder a la problemática actual y garantizar el uso adecuado de los menores en el entorno tecnológico.
  - Acercar a los menores a la realidad de los peligros de Internet.
  - Observar el progreso de los menores en su adquisición de conocimientos sobre los mecanismos de protección ante los virus informáticos.
  - Reforzar conocimientos en aspectos de prevención.
  - Conocer mecanismos de actuación frente a infecciones de virus informáticos.

2.3. COMPETENCIAS

Esta unidad didáctica permite al alumnado participante trabajar las **competencias digitales** tomando como referencia las del "Marco Común de la Competencia Digital Docente" (INTEF: Ministerio de Educación, Cultura y Deporte):

a. Competencia de información: el alumnado será capaz de navegar y buscar información en Internet sobre *virus*, aplicando un criterio de filtrado, y comparando diferentes fuentes de información y el alumnado desarrolla una visión crítica en cuanto a la información encontrada en las redes.

b. Competencia en comunicación: el alumnado desarrollará habilidades de interacción a través de diversos dispositivos y aplicaciones digitales, con el objetivo de entender cómo se distribuye, presenta y gestiona la comunicación digital, siendo crítico con la información que encuentre sobre *virus*.

c. Competencia de seguridad: el alumnado será capaz de protegerse de los riesgos que suponen los *virus*, tanto de los riesgos relacionados con la

protección de la información, datos personales, protección de la identidad digital, estableciendo medidas de seguridad, desarrollo de estrategias activas para la identificación de las conductas inadecuadas y métodos de engaño en materia de ingeniería social.

Esta unidad didáctica permite trabajar con el alumnado participante las siguientes **competencias básicas** establecidas en la Ley Orgánica 2/2006, de 3 de mayo, de Educación:

a. Competencia en comunicación lingüística: el alumnado conocerá el lenguaje específico relacionado con los *virus* como medios de infección. Incluyendo el uso del lenguaje no sólo para describir, sino interpretar, representar, comprender, construir conocimiento, así como autorregulando pensamiento, emociones y conducta.

b. Competencia en el conocimiento y la interacción con el mundo físico: el alumnado tendrá la posibilidad de interactuar con el mundo físico, en los aspectos generados por la acción humana en relación con las diferentes formas de virus, posibilitando la comprensión de diferentes formas de infección, consecuencias, modos y medidas de prevención.

c. Competencia de autonomía e iniciativa personal: le permitirá al alumnado desenvolverse adecuadamente y de forma independiente ante la presencia de riesgos provocados por los *virus*.

d. Competencia social y ciudadana: el alumnado comprenderá la realidad social en la que vivimos, empleando el juicio ético basado en valores y buenas prácticas. Se fomentará la actuación del alumnado bajo criterio propio, siempre orientado a la mejora de la convivencia.

e. Competencia para aprender a aprender: supone que el alumnado disponga de habilidades para iniciarse en su propio aprendizaje y que sea capaz de continuar aprendiendo de forma cada vez más eficaz y autónoma frente a nueva información relacionada con diferentes casos de *virus*, sujetos intervinientes y formas de prevención.

2.4. CONTENIDOS

- **Conceptuales**:
  - Concepto de virus.

  - Principales riesgos de los virus.
  - Casos reales de virus.
  - Mecanismos de prevención ante infecciones.
  - Mecanismos de respuesta ante infecciones de virus informáticos.
- **Procedimentales**:
  - Analizar las causas por las que se producen las infecciones de virus.
  - Concienciar a los alumnos sobre los riesgos potenciales de los virus con casos reales.
  - Elaborar un listado de buenas prácticas y mecanismos de prevención sobre los riesgos asociados a los virus.
- **Actitudinales**:
  - Despertar el interés del alumnado por conocer los riesgos de los virus.
  - Sensibilizar sobre los riesgos y la problemática asociada a la pérdida de información y otros problemas derivados como contraseñas robadas y suplantación de identidad en redes sociales.
  - Interesar al alumnado sobre las consecuencias de infecciones a terceros y propagación de programas maliciosos.

2.5. METODOLOGÍA

Esta unidad didáctica se compone de una serie de actividades programadas para realizar en dos sesiones, cada sesión tendrá una duración de 45 minutos y es conveniente que se realicen en el orden establecido.

La metodología utilizada será dinámica, solicitando una participación activa al alumnado en su propio aprendizaje y reflexiva. Basándose en el conocimiento previo del alumnado sobre *virus* para que el aprendizaje sea significativo.

Teniendo en cuenta las características propias de la edad que nos ocupa se utilizan recursos didácticos como el estudio de casos, el video y el debate.

En cuanto al material empleado para el desarrollo adecuado de esta unidad didáctica, se utilizará:

- El monográfico sobre virus y fraudes, del cual se pueden extraer los conceptos claves en forma de diapositivas para su uso en clase.
- Vídeos informativos sobre las distintas tácticas de virus y sus consecuencias.
- Fichas de preguntas para trabajar los contenidos del vídeo.

- Pizarra o rotafolio.
- Equipos informáticos con conexión a Internet en el aula, con objeto de realizar búsquedas en la red para ampliar y afianzar conocimientos sobre el tema.

2.6. ACTIVIDADES

Las actividades que se van a realizar en esta unidad didáctica se estructuran en diferentes sesiones del siguiente modo:

2.7. Sesión 1: Causas de infección y propagación de los virus

Parte inicial: para sondear conocimientos previos del alumnado en materia de *virus* el docente solicitará al alumnado que escriba en un papel todo lo que sepan sobre *virus:* ¿qué son?, ¿cómo se producen las infecciones?, ¿cómo puede prevenirse? Sus aportaciones se guardarán en una caja y se recuperarán al final de la sesión.

A continuación contextualizará la actividad explicando el concepto de virus, los métodos de infección, y sus consecuencias.

Para ello contará con el siguiente cuadro de referencia:

Guía para el docente

Entendemos **virus** como **"programas informáticos que buscan alterar el funcionamiento de los dispositivos (ordenadores, tabletas, teléfonos móviles, etc.) y en muchos casos, robar información del usuario"**.

Objetivos de los virus:

- La mayor parte de los virus actuales tienen un objetivo común: obtener información de los usuarios infectados:
- Datos bancarios.
- Números de tarjetas de crédito.
- Información personal.
- Fotografías.
- Contraseñas de acceso a correo electrónico y redes sociales.
- Uso de la webcam del usuario sin que éste sea consciente de que está siendo grabado.

Ataques a terceros

Muchos programas maliciosos permiten tomar el control absoluto del ordenador y realizar cualquier tipo de acción sin conocimiento del usuario, como por ejemplo:

- Suplantación de identidad y envío de correos electrónicos en nombre de la víctima.
- Utilizar el ordenador de la víctima para realizar ataques a otros ordenadores.
- Infectar a otros ordenadores para obtener información de sus usuarios.
- Realizar estafas en las que figurará el ordenador de la víctima (y su IP) como origen del delito.
- Enviar publicidad.

Virus en dispositivos móviles

El riesgo es aún mayor en los dispositivos móviles, ya que estos virus pueden:

- Escuchar y grabar llamadas realizadas y recibidas en los teléfonos móviles.
- Enviar mensajes SMS Premium que incrementarán el coste de la factura.
- Obtener información de la posición geográfica del dispositivo mediante GPS.
- Hacer grabaciones con la cámara y tomar fotos sin conocimiento del usuario.

Y también están a la orden del día otros complementos como las barras de navegación que se instalan por defecto al instalar un programa, y que sin ser virus, obtienen información no autorizada del usuario sobre sus hábitos de navegación, con el objetivo de mostrar publicidad relacionada.

Métodos de infección

Mientras que los primeros virus requerían la acción humana para su propagación (por ejemplo, ejecutando un programa infectado con imágenes), hoy día existen virus que no requieren de esta intervención. En algunos casos, la infección puede llevarse a cabo sin que el usuario sea consciente de ello, simplemente conectándose a una página web infectada, introduciendo un pen-drive USB, o abriendo un correo electrónico que contiene una imagen (aparentemente inocua), pero que realmente contiene código que se ejecuta de forma automática en el momento en que se visualiza dicha imagen.

Los virus informáticos se propagan de ordenador a ordenador, en muchas ocasiones sin la ayuda de una persona, aprovechando una vulnerabilidad del sistema operativo o del navegador para propagarse. Actualmente, los ciberdelincuentes aprovechan fallos de seguridad en *plugins* y aplicaciones que los usuarios utilizan habitualmente (por ejemplo, Adobe Flash Player, Java, Acrobat Reader, etc.). Otra estrategia muy habitual consiste en redirigir al usuario a páginas maliciosas a través de enlaces de chats y redes sociales, "invitando a ver un vídeo gracioso" o "fotos de famosas". Lo más peligroso de los virus informáticos es su capacidad para replicarse, por lo que el ordenador de la víctima podría enviar cientos o miles de copias de sí mismo, creando un efecto devastador enorme. Un ejemplo sería el envío de una copia de sí mismo a cada uno de los contactos de la libreta de direcciones del programa de e-mail.

Ingeniería social:

En los últimos tiempos ha tomado gran relevancia la Ingeniería Social, es decir, embaucar con engaños y manipulaciones a los usuarios para conseguir información que posteriormente será utilizada para llevar a cabo la infección y la sustracción de información (claves de acceso, contraseñas, etc.).

Hoy día son muy comunes las estrategias de engaño en las que se "invita" a la víctima a pulsar sobre un enlace que le llevará a una web fraudulenta en la que se intentará infectar su dispositivo (ordenador, tableta o teléfono), o se le solicitarán datos de acceso a sus cuentas bancarias a través de e-mail, o hasta se le pedirá que introduzca su clave de usuario y contraseña, alegando un falso mantenimiento del servicio.

Protección antivirus

Ningún antivirus es efectivo al 100%. El antivirus siempre va por detrás del código malicioso. Cada día surgen cientos de nuevos virus en Internet, y el tiempo que transcurre desde que el virus está activo hasta que un antivirus incorpora la información de cada nuevo virus en sus bases de datos, es un tiempo de riesgo y exposición al que todos los usuarios están expuestos.

Los laboratorios de los fabricantes de antivirus analizan cada día miles de patrones de código presuntamente malicioso. La detección de nuevos virus puede ser cuestión de horas o de días, y en ese periodo de tiempo se pueden infectar miles de ordenadores, tabletas y teléfonos.

Parte principal: el docente explicará qué se pretende conseguir con el desarrollo de la unidad didáctica. Con el objetivo de abrir un debate sobre las causas de infección y propagación de los virus con los menores, se visionarán los siguientes videos:

- *Los peores virus informáticos de todos los tiempos* (enlace directo: https://www.youtube.com/watch?v=7vqshsymVr4)
- ¿Qué sabemos sobre los virus informáticos? Enlace directo:

  https://www.youtube.com/watch?v=J0O3D-6kxLI
- *Cómo proteger tu dispositivo Android de virus y troyanos.* Enlace directo: http://electronica.practicopedia.lainformacion.com/android/como-proteger-tu-dispositivo-android-de-virus-y-troyanos-19657
- El vídeo de despedida de Robin Williams es un virus. Enlace directo:

  https://es.finance.yahoo.com/video/el-v%C3%ADdeo-despedida-robin-williams-091445513.html
- The phombies: Nadie está a salvo. Enlace directo:

  https://vimeo.com/98555722
- Cómo saber si tu teléfono móvil tiene un virus. Enlace directo:

  https://es.finance.yahoo.com/video/sabes-si-tu-tel%C3%A9fono-m%C3%B3vil-085818811.html
- Virus de la Policía. Enlace directo:

  http://www.rtve.es/alacarta/videos/telediario/policia-alerta-virus-para-estafar-usuarios-internet/1801970/

Tras la visualización de los vídeos, los jóvenes contestarán a las preguntas recogidas en la siguiente ficha, siendo el docente quién se encargará de moderar el debate y de que se respeten los turnos de palabra

PREGUNTAS

- ¿Por qué existen los virus?
- ¿Qué tipos de virus hay?
- ¿Qué daños puede causar un virus?

- ¿Cuáles son los métodos habituales de infección?
- ¿Cuáles son los métodos habituales de propagación?
- ¿A qué dispositivos afectan los virus?
- ¿A qué sistemas operativos afectan los virus?
- ¿Los anti virus son efectivos al 100%?
- ¿Cuántos de vosotros tiene *smartphone*?
- ¿Cuántos tenéis instalado un anti virus en el *smartphone*?
- ¿Qué casos conocéis (familiares o amigos) que hayan tenido infecciones de virus en algún dispositivo (ordenador, tableta o *smartphone*)?

A continuación, y con el fin de concienciar a los alumnos sobre la facilidad con la que un virus puede infectar un ordenador, se leerá el siguiente artículo:

El falso vídeo porno de Facebook que en realidad es un virus

Hace pocos días se ha descubierto la existencia de un falso vídeo porno que se propaga por Facebook para robar la información personal de los usuarios.

Según ESET (una prestigiosa empresa de productos antivirus), este virus se está propagando con rapidez por todo el globo.

Se trata de un falso vídeo porno que cada vez que se publica en el muro de un usuario, etiqueta de forma involuntaria a 20 amigos. Si el usuario etiquetado pulsa sobre el enlace, se le instalará un troyano en el ordenador que intentará robar información personal y datos de acceso y contraseñas.

Desde Facebook han anunciado que ya están tratando de eliminar este contenido.

Se abrirá un nuevo debate entre el alumnado sobre las infecciones de virus, y sobre las estrategias habituales de engaño que se utilizan para infectar a otros dispositivos (ordenadores, tabletas, y *smartphones*) a través de los medios de comunicación

utilizados por los menores como Facebook y otras redes sociales. Se insistirá en que la falta de prevención entraña riesgos y puede tener serias consecuencias. Los conceptos clave serán anotados por el docente en la pizarra o rota folio.

Parte final: el docente trasladará al alumnado una serie de recomendaciones y pautas en relación al debate generado sobre los virus, para evitar el riesgo de infecciones.

Guía para el docente

Recomendaciones evitar infecciones de virus: El docente explicará los principales métodos de detección de virus y los síntomas que pueden alertar al alumno ante una situación de infección.

- Mantener actualizado todo el software instalado, el sistema operativo, el navegador de Internet y antivirus. Es fundamental contar con un antivirus actualizado en todos los dispositivos (ordenadores, tabletas y teléfonos móviles).
- Utilizar cuentas de usuario limitadas. Es aconsejable utilizar un usuario con permisos restringidos que no pueda instalar programas. De ese modo, si se cuela un virus, será más difícil que pueda instalarse. Las cuentas de usuario con permisos de administración sólo deben utilizarse para instalar aplicaciones, o para cambiar la configuración del equipo.
- Verificar los enlaces cortos antes de acceder a ellos. Los enlaces cortos, empleados especialmente en pantallas móviles para ahorrar en caracteres, se configuran como un caldo de cultivo perfecto para ataques de *phishing*, ya que el usuario no sabe hacia dónde apunta el enlace. Para poder prevenir este tipo de riesgos, es interesante que conozcas algunos servicios que permiten previsualizar el enlace antes de acceder al mismo y saber así, previamente, si es el correcto.
- Evitar la navegación por páginas web sospechosas. (Programas gratis, juegos gratis, fotos de famosas, etc.).
- Descargar los programas solo de las páginas oficiales. Para evitar la instalación de programas manipulados maliciosamente se recomienda descargarlos únicamente de sus páginas oficiales.

- Ten cuidado con las preguntas de seguridad: Algunos servicios ofrecen la opción de utilizar preguntas de seguridad para que, en caso de olvido, sea posible recuperar la contraseña. No obstante, algunas respuestas a estas preguntas pueden ser conocidas por personas del entorno. Por ejemplo: ¿Cómo se llama tu mascota? Por esta razón, no es recomendable utilizar preguntas de seguridad con respuestas obvias. Es conveniente establecer respuestas complejas que no puedan ser averiguadas por personas cercanas.

- Evitar introducir en los equipos medios de almacenamiento extraíbles de dudosa procedencia. Estos dispositivos se conectan vía USB y pueden ser una puerta de entrada para los virus.

Prevención en el hogar:

- Descargar aplicaciones sólo desde fuentes confiables.
    - Play Store para Android.
    - Apple Store para IOS.
    - Marketplace para Windows Phone.
- Sospechar ante un número bajo de descargas.
- Desconfiar si los comentarios son excesivamente halagadores, pues pueden estar escritos por el propio desarrollador o personas de su entorno.
- Comprobar los permisos de acceso al teléfono que se solicitan antes de iniciar la instalación. Por ejemplo, una aplicación de linterna no tiene sentido que requiera permisos para acceder al registro de llamadas.
- Desactivar en los dispositivos móviles la opción Permitir Orígenes Desconocidos ubicada en Ajustes -> Seguridad -> Orígenes desconocidos.
- Instalar un antivirus para dispositivos móviles.
- No utilizar navegadores extraños, ya que pueden contener vulnerabilidades que permitan “a los malos” robar las contraseñas.

Para concluir la actividad el docente repasará brevemente las ideas previas del alumnado sobre los virus, incluidas al inicio de la sesión en una caja. Comparará y reforzará los conocimientos adquiridos con los previos.

2.8. Sesión 2: Métodos de respuesta ante la infección de virus

Parte inicial: el/la profesor/a, abrirá el debate para que cada menor comente cuáles de los métodos de prevención expuestos en la tabla siguiente utiliza habitualmente.

El docente irá tomando nota de las mismas en la pizarra o rota folio, e irá contabilizando cada método de prevención, con el objetivo de crear un *ranking* en el que se podrá observar qué métodos son los más utilizados por los/as alumnos/as, y cuáles son los que deben poner en práctica, o aquellos en los que se debe poner el foco en colaboración con padres, madres y tutores.

Métodos de prevención
Mis padres me han explicado las ventajas y los riesgos que tiene navegar por Internet y los delitos de los cuales puedo ser víctima.
Mis padres tienen información sobre mis amigos virtuales.
Mis padres saben lo que son las herramientas de Control Parental.
En los dispositivos de mi casa se utilizan herramientas de Control Parental.
En mi casa el ordenador está colocado en un área común, en la que un adulto puede echar un vistazo al monitor de vez en cuando.
Mis padres conocen la jerga de los chat, como acrónimos, emoticonos, etc.
En los dispositivos que utilizo para conectar a Internet tengo un anti virus instalado y actualizado.
En los dispositivos que utilizo para conectar a Internet tengo actualizado todo el software y el sistema operativo.
Tengo actualizado el navegador de Internet.
Nunca abro mensajes provenientes de una dirección electrónica desconocida.
Antes de abrir un archivo adjunto, lo reviso con mi anti virus.
Nunca navego por páginas web sospechosas (programas gratis, juegos gratis, fotos

de famosas, etc.)
No envío ni publico información personal por correo electrónico, mensajería instantánea, redes sociales o cualquier otro medio.
Tengo configurada adecuadamente la privacidad en mis redes sociales.
Siempre verifico los enlaces cortos antes de pulsar sobre ellos.
Nunca instalo software (ni juegos) "pirata", porque pueden contener virus.
Cuando no utilizo la webcam la desconecto, y si está empotrada en el portátil, la tapo con una pegatina.
Sólo descargo aplicaciones para mi *smartphone* de fuentes confiables (App Store para IOS, Play Store para Android y Marketplace para Windows Phone).
Antes de instalar una aplicación en mi *smartphone*, siempre compruebo los permisos de acceso al teléfono que se solicitan antes de iniciar la instalación. Por ejemplo, una aplicación de linterna no tiene sentido que requiera permisos para acceder al registro de llamadas.
En mi *smartphone*/tableta tengo desactivada la opción Permitir Orígenes Desconocidos ubicada en Ajustes -> Seguridad -> Orígenes desconocidos.

Parte principal: Se presentan al alumnado las siguientes recomendaciones como mecanismos de respuesta y soporte:

Consejos sobre la instalación de aplicaciones en dispositivos móviles

- Descargar aplicaciones sólo desde fuentes confiables.
  - Play Store para Android.
  - Apple Store para IOS.
  - Marketplace para Windows Phone.
- Sospechar ante un número bajo de descargas.
- Desconfiar si los comentarios son excesivamente halagadores, pues pueden estar escritos por el propio desarrollador o personas de su entorno.
- Comprobar los permisos de acceso al teléfono que se solicitan antes de iniciar la instalación. Por ejemplo, una aplicación de linterna no tiene sentido que requiera permisos para acceder al registro de llamadas.

- Desactivar en los dispositivos móviles la opción Permitir Orígenes Desconocidos ubicada en Ajustes -> Seguridad -> Orígenes desconocidos.
- Instalar un antivirus para dispositivos móviles.
- No utilizar navegadores extraños, ya que pueden contener vulnerabilidades que permitan “a los malos” robar las contraseñas.

¿Cómo saber si un dispositivo está infectado?

- Se abren páginas web que no se han solicitado.
- El dispositivo funciona más lento de lo normal, deja de responder o se bloquea con frecuencia.
- El dispositivo se apaga solo (aun teniendo batería).
- El dispositivo se reinicia cada pocos minutos.
- El dispositivo no se puede iniciar.
- Las aplicaciones no funcionan correctamente.
- No se puede obtener acceso a los discos o a las unidades de disco.
- Aparecen mensajes de error poco usuales.
- Los menús y los cuadros de diálogo aparecen distorsionados.
- La factura refleja llamadas que no se han realizado, mensajes SMS que no se han enviado.
- Alguien responde a un correo electrónico que no se ha enviado.
- Aparecen mensajes de publicidad constantemente.
- Se muestran mensajes o imágenes inesperados.
- Se reproducen sonidos o música inusuales de forma aleatoria.
- El lector de CD-ROM se abre y se cierra de forma misteriosa.
- El antivirus se desactiva solo.
- Los programas se inician de forma espontánea.
- El cortafuegos informa de que algunas aplicaciones intentan conectarse a Internet, sin que el usuario las haya puesto en marcha.
- Los archivos y carpetas han sido borrados o su contenido ha cambiado.

- El disco duro muestra más actividad de lo normal, aun cuando no hay programas funcionando, (por ejemplo, si la luz en su unidad principal parpadea de forma rápida).

¿Qué hacer si se tiene la certeza de que un dispositivo está infectado?

Ante la evidencia de que un ordenador o teléfono ha sido infectado por un virus, se debe reaccionar rápidamente y llevar a cabo las siguientes medidas siguiendo el orden recomendado:

1. Dejar de utilizar el dispositivo.
2. No realizar ninguna actividad que pueda suponer riesgo de pérdida de información, por ejemplo:
    a. No realizar compras por Internet con el dispositivo infectado.
    b. No acceder al correo electrónico, ni a redes sociales, ni a ningún otro servicio que requiera introducir datos de usuario y contraseña.
3. Desconectar el dispositivo de Internet, quitando el cable del router y desactivando la conexión WIFI.
4. Deshabilitar el envío de datos en tabletas y teléfonos.
5. Eliminar de los navegadores los certificados digitales instalados (por ejemplo, el certificado digital de la Fábrica Nacional de Moneda y Timbre que se utiliza para la declaración dela renta, y que identifica al usuario con la misma validez que el DNI).
6. Apagar el dispositivo. Si no es posible apagarlo (por ejemplo, porque es un teléfono y es necesario realizar llamadas) hay que asegurarse de que está desconectado de la red WIFI y del router.
7. Hacer una copia de seguridad de la información importante (fotos, documentos, archivos de trabajo, etc.) Se recomienda hacer la copia de seguridad con el dispositivo apagado, accediendo desde otro dispositivo, siempre que sea posible.
8. Verificar que los datos de la copia de seguridad no están infectados. Existe el riesgo de que al conectar una unidad externa (disco externo, pen drive) para guardar los datos de la copia, ésta también sea infectada.

9. En algunos casos existe la posibilidad de restaurar el dispositivo a los valores de fábrica. Esta opción borrará todos los datos personales y configuraciones, por lo que es altamente recomendable realizar previamente una copia de seguridad.
10. En caso de no poder restaurar el dispositivo a los valores de fábrica, llevarlo a un servicio técnico para que un experto haga una limpieza general, y si es necesario, formatear las unidades de almacenamiento (disco duro, tarjeta SD, etc.) y reinstalar el sistema operativo.

Parte final: Cada alumno/a dispondrá de unos minutos para realizar una reflexión individual en la que deberá reflejar por escrito qué medidas tomará a partir de ahora para prevenir la actuación de virus informáticos. A continuación cada uno/a leerá en voz alta sus conclusiones.

2.9. EVALUACIÓN

Esta evaluación se realizará mediante la observación por parte del docente de la participación e implicación del alumnado en el desarrollo de la sesión, y en la realización de actividades, así como con el planteamiento de tantas aclaraciones como fuera necesario ante las posibles dudas que se planteen sobre los contenidos abordados. Del mismo modo, se realizará un continuo feedback a través de preguntas de reiteración y repaso de conceptos e ideas claves. Los criterios de evaluación que se pretenden conseguir son los siguientes:

- Los/as alumnos/as conocen:
  - El concepto de *virus* asociado y los riesgos asociados de los virus actuales.
  - Las características que presentan los diferentes tipos de virus.
- Los/as alumnos/as adquieren:
  - Los mecanismos de prevención ante los virus.
  - Las herramientas para detectar un uso inadecuado de los dispositivos móviles.
- Los/as alumnos/as desarrollan:
  - Actitudes de precaución que favorecen el uso apropiado de internet.

- Mecanismos de prevención y estado de alerta frente a invitaciones con enlaces sospechosos, fotos de “famosas” y aplicaciones gratuitas.
- Son conscientes de que deben estar alerta ante las distintas vías de infección (correo electrónico, redes sociales, aplicaciones de mensajería tipo WhatsApp, etc.).
- Mecanismos de respuesta frente a infección de virus informáticos.

2.10. DOCUMENTACIÓN DE APOYO

Los siguientes recursos son de utilidad para ampliar el conocimiento sobre protección ante virus y fraudes:

Monográfico de protección ante virus y fraudes

Marco teórico de referencia para aprender herramientas, sistemas y pautas para proteger a los menores ante virus informáticos y situaciones de fraudes por Internet.

Disponible en: http://www.chaval.es/

Curso en línea Seguridad TIC y Menores

Curso de 30 horas de duración bajo metodología **MOOC** (*Massive Online Open Course* - Curso en línea masivo y abierto-) dirigido a padres y educadores. Sensibiliza sobre los riesgos a los que se enfrentan los menores en el uso de Internet y las nuevas tecnologías, ofreciendo estrategias, pautas y recomendaciones para su prevención y respuesta en caso de producirse un incidente. Contiene un módulo exclusivo sobre Protección ante virus y fraudes.

Disponible en: http://www.chaval.es