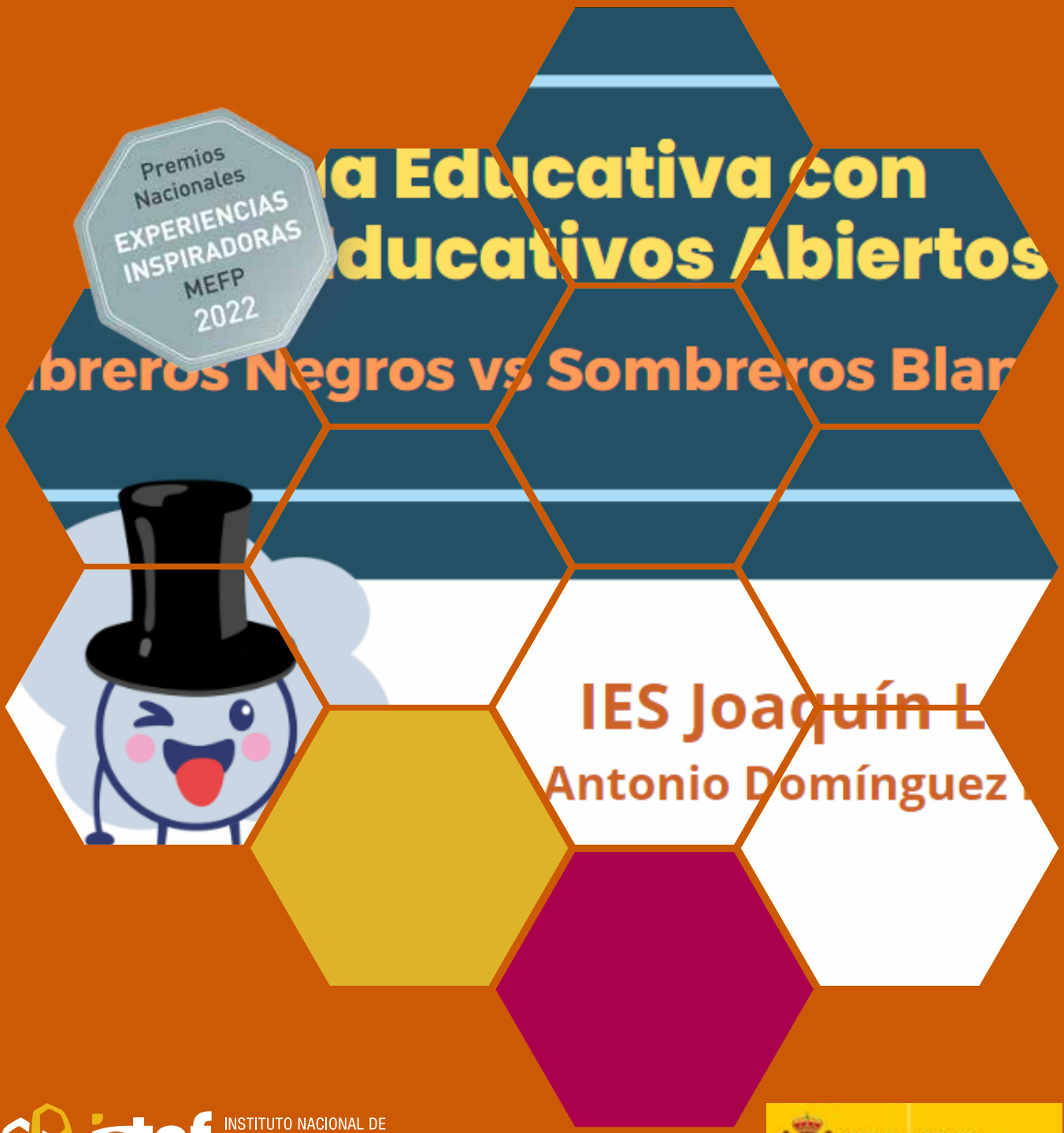
experiencias educativas inspiradoras

Nº 112

Sombreros negros vs Sombreros blancos

Integrando el DUA en el aprendizaje de la ciberseguridad



INSTITUTO NACIONAL DE TECNOLOGÍAS EDUCATIVAS Y DE FORMACIÓN DEL PROFESORADO

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

Dirección General de Evaluación y Cooperación Territorial

Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF)

Recursos Educativos Digitales

Junio 2023

NIPO (web) 847-22-067-6

ISSN (web) 2695-4184

DOI (web) 10.4438/2695-4184_EEI_2019_847-19-120-X

NIPO (formato html) 847-20-110-8

NIPO (formato pdf) 847-20-111-3

DOI (formato pdf) 10.4438/2695-4184_EEIpdf112_2020_847-19-133-8

“Sombreros negros vs Sombreros blancos. Integrando el DUA en el aprendizaje de la ciberseguridad” por Antonio Domínguez Peñuela para INTEF

<https://intef.es>

Experiencia galardonada con el 1º Premio en la categoría Secundaria modalidad A de los “Premios Nacionales a Experiencias Educativas Inspiradoras para el aprendizaje. Convocatoria 2022”.

Para cualquier asunto relacionado con esta publicación contactar con:

Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado

C/Torrelaguna, 58. 28027 Madrid.

Tfno.: 91-377 83 00. Fax: 91-368 07 09

Correo electrónico: cau.recursos.intef@educacion.gob.es

Entendiendo el proyecto...

El proyecto “Experiencias Educativas Inspiradoras” se encuadra dentro del Plan de Transformación Digital Educativa lanzado desde el INTEF en 2018.

A través de la realización de proyectos personales de los docentes, o proyectos de centro donde se busca mejorar algún aspecto del ámbito educativo, se encuentran experiencias asociadas a tecnología digital que consiguen efectos transformadores.

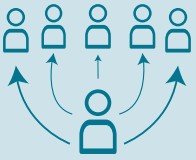
Son estas experiencias, las que este proyecto intenta localizar y darles visibilidad para conseguir que se extrapolen a otros entornos educativos reglados.

Dos son los OBJETIVOS claros que pretende alcanzar este proyecto:

CREACIÓN DE REPOSITORIO

Creación de un repositorio de experiencias didácticas asociadas a tecnología digital, ya aplicadas en el entorno educativo y que hayan demostrado tener un efecto transformador.

DIFUSIÓN ENTRE DOCENTES



Difundir estas experiencias con el fin de inspirar a otros docentes en su práctica diaria.

“Que las experiencias de unos sirvan de guía e inspiración para otros”.

Índice

Índice

1. Introducción

RESPONSABLE	Antonio Domínguez Peñuela
CENTRO ESCOLAR	IES Joaquín Lobato
DIRECCIÓN	Avenida Gerald Brenan 2
LOCALIDAD Y PROVINCIA	Torre del Mar - Málaga
WEB DEL CENTRO	IES Joaquín Lobato
EMAIL DE CONTACTO	profe.santi.tec@gmail.com

La ciberseguridad es una parte importante del currículo de la Educación Secundaria y de las Competencias Digitales que el alumnado debe tener al finalizar la educación obligatoria. Para tratar estos contenidos en la materia de Tecnología de la Información y Comunicación en 4.º ESO utilizamos un Recurso Educativo Abierto (REA) adaptado para 4.º ESO, el cual ha sido creado siguiendo los principios del Diseño Universal para el Aprendizaje (DUA).

Al alumnado se le presenta el reto de solucionar un ataque informático que ha recibido una empresa. Se pretende ir más allá de las típicas recomendaciones sobre contraseñas seguras y antivirus, adentrando al alumnado en el mundo de los *hackers* informáticos, sus métodos y estrategias. En este proceso se pretende despertar la curiosidad del alumnado sobre la ciberseguridad, desarrollar la competencia digital del alumnado integrando distintos recursos digitales y valorar la idoneidad de este tipo de recurso abierto para posteriormente compartirlo y difundirlo entre el profesorado.

Esta experiencia ha sido galardonada con el 1º Premio en la categoría Secundaria modalidad A de los “Premios Nacionales a Experiencias Educativas Inspiradoras para el aprendizaje. Convocatoria 2022”.

Portada del REA en la plataforma Moodle del centro

2. Punto de partida

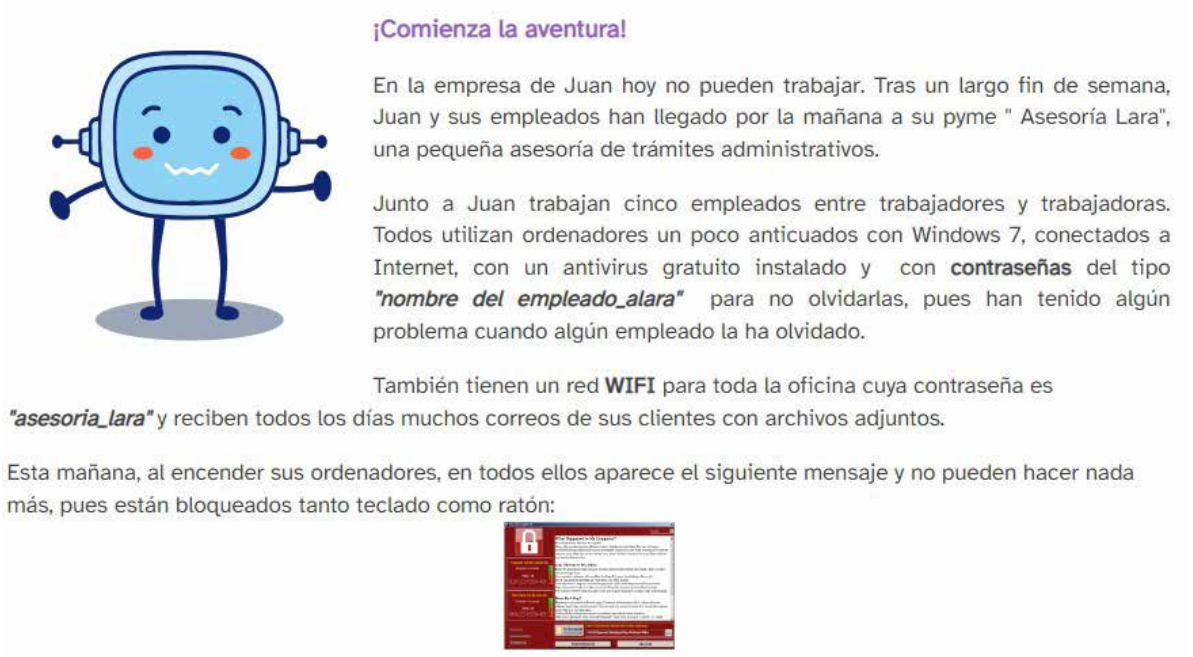
El I.E.S. Joaquín Lobato recibe únicamente alumnado de la ESO, proveniente de los tres colegios adscritos. Son alumnos que proceden de zonas muy diversas del municipio y de diversas nacionalidades, lo que en cierta medida dificulta la posibilidad de la elaboración de trabajos por grupos.

Esta experiencia educativa utiliza el REA *Sombreros Negros vs Sombreros Blancos*, recurso digital abierto publicado en los recursos del Proyecto REA/DUA de la Consejería de Desarrollo Educativo y Formación Profesional de la Junta de Andalucía.

Estos recursos están publicados como recursos gratuitos, con licencia abierta, creados con la herramienta de creación de contenidos eXeLearning, lo que permite su descarga y modificación para su adaptación al alumnado y a entornos educativos diferentes.

El profesor y elaborador de este REA (Recurso Educativo Abierto) se plantea la puesta en práctica de este tipo de recurso educativo, el cual ha sido creado siguiendo los principios del Diseño Universal para el Aprendizaje para 1.º de Bachillerato. Este REA es adaptado, de forma que se corresponde con el Bloque 4. Seguridad informática, de la materia de Tecnología de la Información y la Comunicación de 4.º ESO recogido en la programación de dicha materia para el curso 2021-2022 con el objetivo de iniciar al alumnado en la ciberseguridad.

Para la puesta en práctica, se ha descargado el archivo «.elp» de eXeLearning guardado en formato SCORM 1.2 de modo que permite su integración en la plataforma Moodle, lo que permite el seguimiento del alumnado durante su experiencia, proporcionando objetivos, seguimiento de notas, progreso del REA, utilización del calificador, generar informes...



Planteamiento inicial de la situación que da origen a ataque informático

3. Paso a paso

Paso 1. Movilizar

Se presenta el tema del REA de manera que el alumnado se sienta motivado y tenga interés en aprender.

Inicialmente y para movilizar al alumnado, se presenta el apartado "1. Presentación" del REA de forma grupal en el aula, de manera que el alumnado se sienta motivado.

La situación de aprendizaje se presenta como un reto que debe superar el alumnado para conseguir proteger a una empresa de unos *hackers*.

Se utiliza la PDI para mostrar el REA en la fase inicial de activación y que el alumnado conozca:

- Los criterios de evaluación.
- Instrumentos de evaluación, presentando la rúbrica.
- Instrumentos de reflexión, (diario de aprendizaje).
- Tareas que forman parte del reto.
- Agrupamientos.
- Producto final del reto.

Rétor es un personaje que propone retos o desafíos a lo largo de la actividad

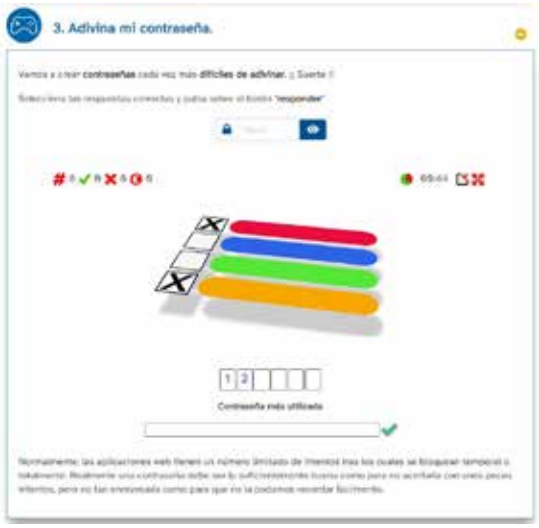
Presentación mediante pantalla en el aula de informática

Paso 2. Activar

Activar las ideas previas necesarias para la realización de la tarea.

A continuación, se activan los conocimientos previos que el alumnado pueda tener en los apartados 2 y 3 del REA. Se activan los conocimientos sobre contraseñas, virus, troyanos, gusanos, etc.

Las actividades están pensadas para su desarrollo en el aula intercalando actividades interactivas y de reflexión que permiten la personalización y adaptación a las características personales de cada alumno o alumna, a la vez que favorecen la creatividad e iniciativa personal. Las actividades interactivas se realizan tanto con los iDevices incluidos en eXeLearning como actividades creadas con H5P que se insertan en el REA.



Actividad interactiva creada con eXeLearning

Paso 3. Explorar

Se explora el mundo de los *hackers* y su forma de actuar. Para ello, el alumnado debe investigar respondiendo a las siguientes preguntas:

- ¿Son todos los *hackers* ciberdelincuentes?
- ¿Cuántos tipos de *hackers* hay?
- ¿Qué tipo de *hacker* te gustaría ser?
- ¿Qué es el *hacking* ético?
- Fases del *hacking*.
- ¿Cómo nos pueden atacar?
- Tipos de ataques más comunes

Actividad H5P para repasar los tipos de hackers y sus características

Paso 4. Estructurar

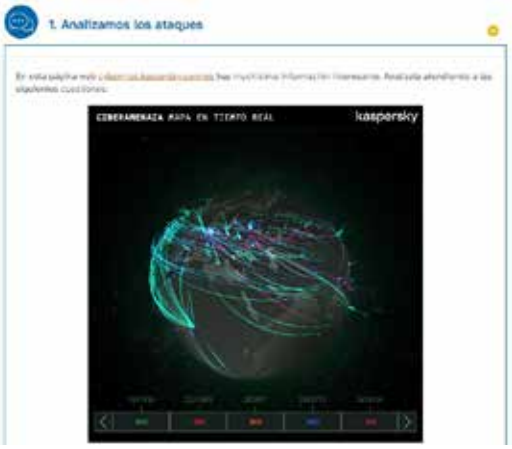
Mediante un proceso de reflexión y deducción, se va completando lo descubierto en la fase de exploración y adquiriendo los conocimientos necesarios para el reto final.

Es la fase más extensa de la actividad en la que se adquieren la mayoría de los nuevos conocimientos:

- Técnicas de *pentesting*.
- Técnicas de búsqueda de información.
- Pruebas de *pentesting*.
- Vulnerabilidades en sistemas.
- Ingeniería social.
- Herramientas de un *hacker* (Kali Linux).
- Los peligrosos *exploits*.
- Análisis forense.
- Ciberdelitos.

Lúmen y Klávis son otros dos personajes para prestar ayuda y aclarar ideas respectivamente

Alumna realizando una actividad de búsqueda de información



Mapa de ataques en tiempo real de Kaspersky

Paso 5. Aplicar y comprobar

En esta fase el alumnado lleva a cabo el reto planteado demostrando la asimilación de los aprendizajes adquiridos. Para ello debe redactar un informe a modo de plan de protección de la empresa con los siguientes puntos:

1. Portada.
2. Introducción.
3. Resultados del análisis.
4. Propuestas de medidas de seguridad.
5. Plan de información y formación.
6. Plan de prevención.

Diapositiva de una de las presentaciones del informe final del alumnado

Paso 6. Concluir

Presentamos y reflexionamos sobre los aprendizajes adquiridos.

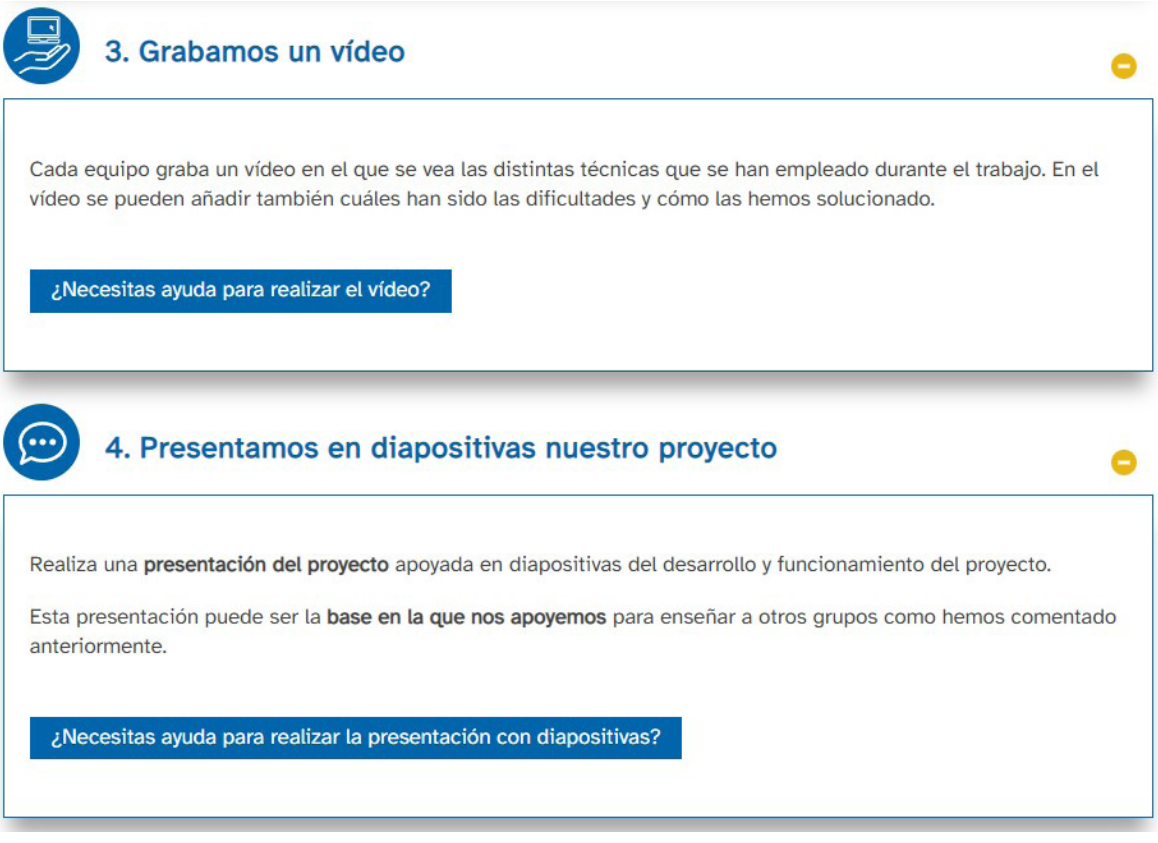
En este último paso, siguiendo uno de los principios del Diseño Universal del Aprendizaje, al alumnado se le ofrecen diversas formas de presentar el resultado final:

- Presentación con diversas herramientas digitales (PPT, Genially, etc.)
- Grabar un vídeo.
- Memoria escrita.

Finalmente realizamos una exposición en la clase enseñando y explicando nuestro trabajo a los demás compañeros y compañeras de otros cursos pues la ciberseguridad es un tema que seguro les interesa y les afecta.

La clase se divide en grupos de 3 o 4 alumnos y alumnas, con ayuda del profesor organizarán charlas informativas para los demás grupos de ESO o bachillerato.

Al final se realiza una actividad de reflexión en la que se responde a la pregunta «¿qué he aprendido?» en su diario de aprendizaje.



Para presentar los resultados hay diversas formas de hacerlo con sus ayudas correspondientes

4. Evaluamos

Se realiza una autoevaluación mediante un diario de aprendizaje que el alumnado ha ido completando a lo largo de toda la actividad. Además de incluye una rúbrica interactiva de autoevaluación del aprendizaje conseguido.

El profesorado realiza la evaluación del alumnado, por un lado, mediante la entrega de los documentos y evidencias de la realización de las distintas actividades que se realiza a través de la plataforma Moodle y, por otro, mediante una rúbrica interactiva que se incluye en la guía didáctica del REA.

En cuanto a la evaluación de la práctica docente, se consultó la opinión del alumnado sobre esta actividad con un resultado muy positivo. Además cabe destacar que este tipo de propuesta promueve un trabajo muy autónomo del alumnado, lo que permite al profesor prestar una atención más personalizada a aquellos alumnos y alumnas que necesiten más ayuda para adquirir las competencias correspondientes.

Rúbrica de autoevaluación del alumnado

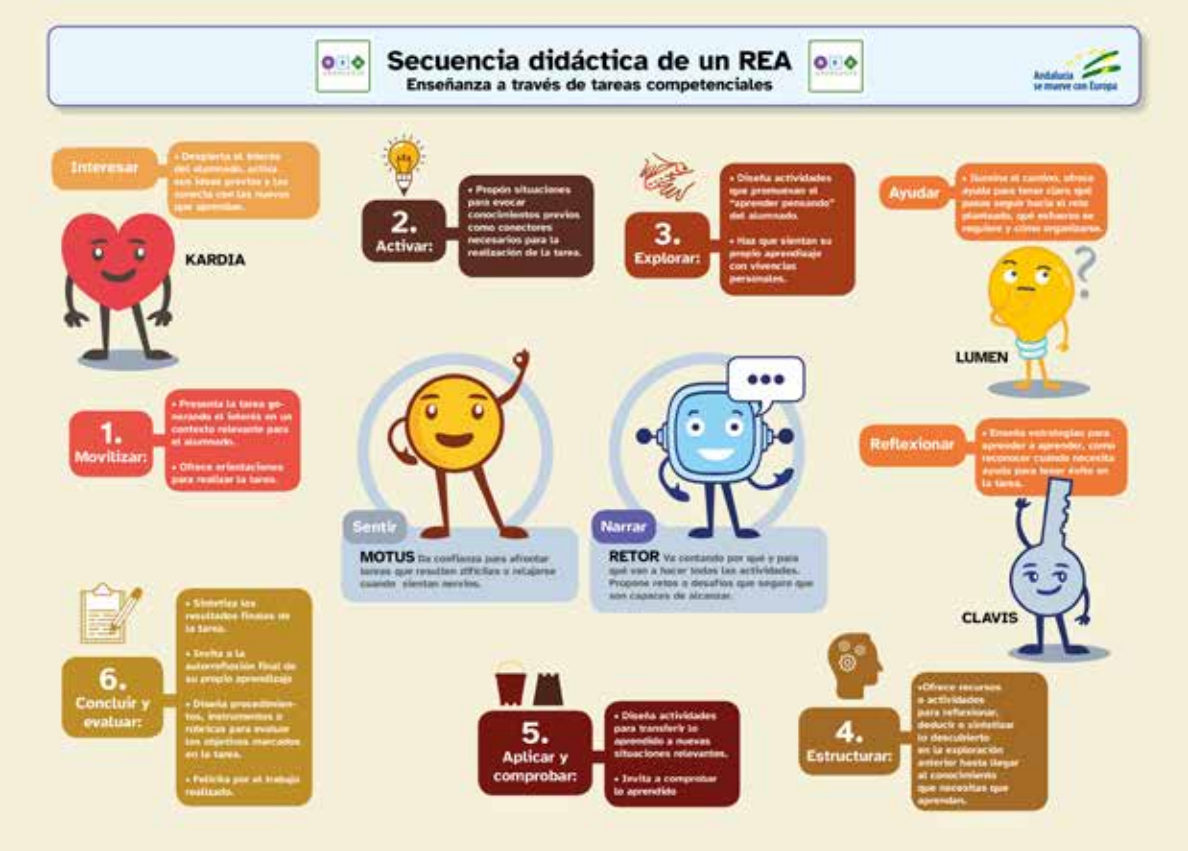
El diario de aprendizaje sirve de guía para el alumnado a lo largo del REA

5. Conclusiones

He de confesar que inicialmente no esperaba una diferencia significativa con otras metodologías que normalmente se vienen realizando en el aula, pues desde hace tiempo he trabajado el ABP o el aprendizaje por retos, pero tuve una agradable sorpresa y he de admitir que la conjunción del modelo de Diseño Universal para el Aprendizaje (DUA) y las actividades tipo Recurso Educativo Abierto (REA) funcionan muy bien.

No sé si es la secuencia de los recursos y actividades propuesta por el DUA, la inclusión de personajes que acompañan al alumnado durante el proceso, la novedad o el formato conjunto todos los factores, pero el resultado fue muy bueno tanto por la aceptación por parte del alumnado como por los resultados académicos.

Todo el alumnado llegó al final y su grado de satisfacción fue muy alto.



Secuencia didáctica de un REA con los personajes y las tareas competenciales

6. ¿Te animas?

Dado los resultados obtenidos, seguiré utilizando recursos educativos abiertos y te animo a probarlos. Puedes descargarlos de algunos de los repositorios que dejo en el material complementario.

Recomiendo aprender a utilizar eXeLearning, ello te permitirá modificar los REA adaptándolos a tu currículo y las características de tu alumnado. Además, si te animas puedes crear tus propios recursos educativos abiertos. Además, si utilizas Moodle podrás integrarlo perfectamente guardándolo en formato SCORM 1.2 de modo que permite su integración en la plataforma Moodle y realizar un seguimiento de las evidencias y realizar la evaluación de forma cómoda y rápida.

Los recursos educativos abiertos, siempre que se hayan creado con un nivel mínimo de calidad, constituyen en sí mismos experiencias de aprendizaje y si además incluyen la guía didáctica, su integración en la programación facilita la tarea al docente cumpliendo las exigencias de la LOMLOE.

La integración con Moodle permite el seguimiento y evaluación de las actividades

7. Material complementario

REA empleados en esta experiencia educativa:

- REA Sombreros Negros Vs Sombreros Blancos.
- Guía docente del REA.
- Proyecto REA/DUA de la Junta de Andalucía. Más de 250 recursos educativos abiertos (REA) de distintas materias de Primaria, Secundaria y Bachillerato organizados y creados por un equipo de 250 profesores y profesoras de acuerdo con los principios del diseño universal para el aprendizaje. Son situaciones de aprendizaje multiniveladas en las cuales el alumnado adquiere y desarrolla las competencias específicas de cada área o materia. Además incluyen sus guías didácticas.
- Proyecto EDIA del INTEF. Repositorio de recursos educativos abiertos en constante actualización. Organizado por materias y niveles educativos. Materiales creados y evaluados por equipos de docentes activos. Materiales adaptables, modificables y basados en la colaboración.
- Programa CREA de la Junta de Andalucía. Al igual que los anteriores son un conjunto de recursos educativos abiertos (REA) que dan respuesta a la diversidad de aprendizajes del aula, mediante la incorporación sistemática de metodologías activas, el diseño universal para el aprendizaje y la generación de materiales y recursos complementarios que contribuyan al éxito educativo de los estudiantes.
- eXeLearning. Programa libre y abierto para crear contenidos educativos de una manera sencilla. Descarga fácil y gratuita disponible para todos los sistemas operativos.
- Tutorial de eXeLearning. Herramienta de código abierto (*open source*) que facilita la creación de contenidos educativos sin necesidad de ser un experto.
- Moodle. Plataforma de aprendizaje de código abierto.
- H5P. Herramienta de código abierto, que permite crear y compartir contenido interactivo sin necesidad de conocimientos de javascript.
- Kali Linux. Distribución de Linux diseñada para realizar análisis de seguridad.

Página del proyecto REA/DUA de la Junta de Andalucía con los REA clasificados

Herramientas digitales empleadas:

Vídeos:

- Ciberseguridad. INCIBE (YouTube)
- INCIBE. La figura del ciberdelincuente (CC0)
- Prosegur. ¿Qué es el hacking ético? (CC BY-NC-SA)
- INCIBE. Ejemplo de fraude telefónico (CC BY-NC-SA)
- INCIBE. ¿Conoces los riesgos de tu empresa? (CC BY-NC-SA)
- ESET Latinoamérica. ¿Sabes qué es un Exploit y cómo protegerte de ellos? (CC BY-NC-SA)
- INCIBE. Ciberseguridad para la empresa (1/4) (CC BY-NC-SA)
- INCIBE. Ciberseguridad para la empresa (2/4) (CC BY-NC-SA)
- INCIBE. Ciberseguridad para la empresa (3/4) (CC BY-NC-SA)
- INCIBE. Ciberseguridad para la empresa (4/4) (CC BY-NC-SA)
- FIIAPP. ¿Qué es... Informática Forense? (INCIBE)
- INCIBE. Línea 017 de INCIBE (CC0)

Páginas web:

- Central Ops.net
- DonDominio
- Kaspersky. Ciberamenazas en tiempo real (CC BY-NC-SA)
- Kaspersky. Gráfica de ataques (CC BY-NC-SA)
- Proteger las contraseñas almacenadas mediante una contraseña maestra. Support Mozilla
- Keepass Password Safe
- LastPass Password Manager
- VirusTotal
- 8 tipos de hacker. The Bridge
- Conoce los tipos de hackers y su forma de operar. 24Horas
- decoder.link
- Qualys. SSL Server Test
- DigiCert® SSL Installation Diagnostics Tool
- Kali Linux
- Cuál es mi IP
- Agencia Española de Protección de Datos
- Observatorio Español de Delitos Informáticos. Ciberdelitos

Juegos:

- Google. Interland (CC0)

Herramientas de Google:

- Google Dorks o Google Hacking

Aplicaciones de escritorio:

- Tracert
- Terminal
- Libreoffice

Difusión de la experiencia:

Se ha dado publicidad a la experiencia educativa mediante intervenciones en grupos de redes sociales como Telegram y Whatsapp del profesorado, además de haberse dado a conocer en presentaciones y cursos.

Integrando el DUA en el aprendizaje de la ciberseguridad

Sombreros negros vs Sombreros blancos

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
intef
INSTITUTO NACIONAL DE TECNOLOGÍAS EDUCATIVAS Y DE FORMACIÓN DEL PROFESORADO