N2M1

Alfabetización tecnológica y TIC

JUNTA DE EXTREMADURA

En el presente punto se incluyen materiales para trabajar los contenidos referentes a “Alfabetización tecnológica y TIC”. Los mismos deben ser utilizados de forma transversal al resto de los incluidos en este nivel y módulo, consiguiendo ser una herramienta global de comportamiento en la sociedad 2.0 en la que todos vivimos actualmente. Sociedad caracterizada por un incremento constante de la tecnología y las aplicaciones móviles, incremento constante que ha cambiado especialmente la forma en la que nos comunicamos.

Los contenidos de alfabetización tecnológica y TIC para este nivel y módulo se dividen en los siguientes apartados:

1. **Seguridad y amenazas. Instalación y configuración de antivirus, filtros y cortafuegos. Medidas de seguridad activa y pasiva.**
2. **Realización de copias de seguridad.**
3. **Creación y publicación en la web.**
4. **Diseño de diversos contenidos web. Concepto y uso de la nube.**

Apartados que pasan a detallarse a continuación.

1. Seguridad y amenazas. Instalación y configuración de antivirus, filtros y cortafuegos. Medidas de seguridad activa y pasiva.

Más que hablar de virus, sería conveniente utilizar el término malware o software malicioso. Por malware, según la página web www.malware.es, el nombre de malware se define como un software que tiene intención de dañar el dispositivo (PC, móvil u otro) para que el creador de este malware pueda obtener beneficios.

Serían softwares que tienen como objetivo infiltrarse, tomar el control, o dañar un ordenador o dispositivo informático, su sistema operativo, su sistema de información, o también sustraer información sin el consentimiento de su propietario, realizar ataques a otros ordenadores y redes…

Skull and crossbones.svg: SilsorComputer n screen.svg: Everaldo Coelho and YellowIconderivative work: Kizar [LGPL (http://www.gnu.org/licenses/lgpl.html)]

Aunque socialmente cada día existe un mayor nivel de concienciación con el malware en Internet, mucho queda por aún por hacer para conseguir un ecosistema seguro en esta materia.

Un estudio de 2017 sobre ciberseguridad en dispositivos realizado por El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de Red.es. y el Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO) en más de 3.000 hogares, arrojó unas seria de conclusiones bastante alarmantes. Entre los dispositivos analizados el 54,3% presentaba virus y sus usuarios no se habían percatado. Por otro lado, la mayoría de usuarios de smartphones (concretamente el 93,2%) declaró realizar descargas de aplicaciones desde los repositorios oficiales, sin embargo, en un tercio de los dispositivos analizados la configuración por defecto había sido modificada para permitir la instalación de aplicaciones desde fuentes desconocidas.

Este estudio pone de manifiesto el largo camino que aún queda por delante para alcanzar un nivel de seguridad suficiente en nuestro día a día digital.

1.1. Tipos de malware y cómo convatirlos

Se diferencian tipos de malware, los 2 más conocidos son:

- **Los gusanos informáticos:** es un malware que se propaga automáticamente sin necesidad de ayuda humana, ya sea ejecutándolos o compartiéndolos, ya que poseen capacidad de autorreplicación y de autoenviarse a otros ordenadores.
- **Un troyano informático:** no tiene apariencia de malware, más bien parece un programa normal e inofensivo. Lo que suele hacer es que al ser ejecutado y realizar las acciones previsibles de ese programa, en segundo plano abre una puerta de acceso remoto a nuestro ordenador, con el que una persona ajena puede controlar plenamente nuestro equipo.

No obstante, cada vez hay más y son de todo tipo. Clasificándose con nombres como rootkits, exploits, dialers, scareware, spyware, adware, crimeware...

¿Cómo saber que he sido infectado? Es importante detectar lo antes posible que hemos sido infectados y eliminarlo. Las razones principales de detección son:

1. El dispositivo va más lento de lo habitual.
2. Aparecen muchos mensajes/ventas de publicidad donde antes no había.
3. Hay aplicaciones (o todo el dispositivo) que están bloqueados.

¿Por qué me he infectado con un malware? Las razones más habituales son 3:

1. Descargar un programa de una fuente no recomendada.
2. Está escondido en otra programa de uso habitual.
3. Abriendo adjuntos por correo electrónico.

¿Cómo evitar que me infecten malwares? Las medidas de seguridad son principalmente 2:

1. Instalar un antivirus.
2. Aplicar el sentido común.

Por suerte, los ordenadores Windows (la mayoría del mercado y, en consecuencia, los más susceptibles a ataques) desde hace tiempo ya disponen de un antivirus preinstalado llamado **Windows Defender**. A su vez, también se pueden instalar adicionalmente otros antivirus como:

- Bitdefender
- Norton Security
- ESET
- Kaspersky
- BullGuard
- AVG

Everaldo Coelho (YellowIcon); [LGPL (http://www.gnu.org/licenses/lgpl.html)]

Todos antivirus dispone de una opción de “escanear”, con la que podemos detectar y eliminar todo malware, además se actualizan de forma recurrente incluyendo protocolos de acción ante nuevas amenazas. Además, suelen incluir un modo de “siempre activo”, que está escaneando de forma constante todo lo que hacemos para prevenir ataques.

Por otro lado, un antivirus no deja de ser un apoyo, un apoyo más, pero lo más importante es que el propio usuario aplique el sentido común para evitar ser infectado. Algunos hábitos importantes:

1. Sólo descargar información de fuentes fiables, preferiblemente de páginas web oficiales o tiendas online de confianza (Play Store, Apple Store…)
2. No hacer clic en enlaces sospechosos y menos todavía facilitar nuestros datos personales o credenciales de acceso.
3. No abrir correos electrónicos que desconozcamos su destinatario, mucho menos descargar adjuntos de dichos correos.

Sabías qué…

En el programa educativo Foro Nativos Digitales de la Junta de Extremadura, existen contenidos relacionados con protección ante virus y fraudes.

Incluyen materiales de formación básica para docentes, alumnos y familias que ayudan a desarrollar conductas que eviten estos riesgos. Son especialmente interesantes los manuales, ya que incluyen fichas para trabajar en clase. Ejemplo:

Actividad 1:

¿Por qué nos atacan los virus?

Objetivo: iniciar una aproximación a los virus y las distintas tipologías que permita disponer de un conocimiento básico sobre los mismos.

Tiempo previsto: 10 minutos.

Desarrollo: se comienza con la visualización del vídeo Los virus y se realiza un pequeño debate partiendo de la pregunta "¿Por qué nos atacan los virus?" El profesor recogerá en la pizarra tradicional o digital un resumen de las diferentes posiciones, concluyendo con la idea de que pese a la culpabilidad de los creadores de virus atacantes, **nosotros también somos responsables de lo que nos pase si realizamos conductas de riesgo**.

Ayuda para el docente

No se trata de extenderse mucho en esta parte, lo importante es que se constate el hecho de que si no somos cuidadosos podemos tener problemas o causar problemas a los demás.

Toda la información aquí: https://emtic.educarex.es/proteccion-frente-a-virus-y-fraudes

2. Realización de copias de seguridad.

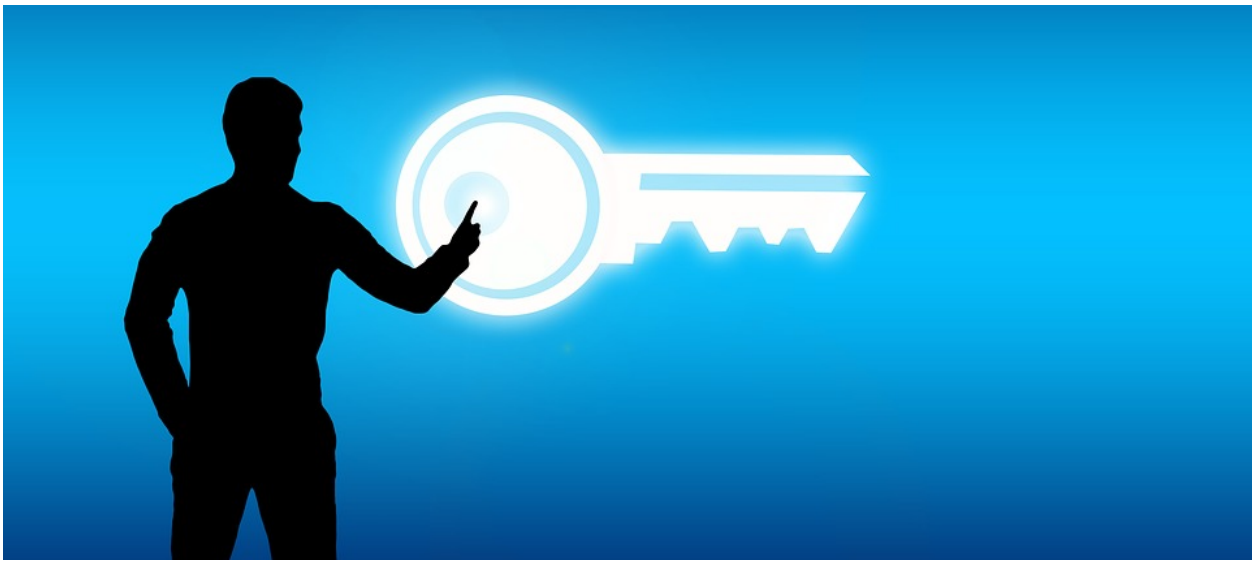
En la guía “Privacidad y seguridad en Internet”, elaborada por la Agencia Española de Protección de Datos, el INCIBE y la Oficina de Seguridad del Internauta, se incluye una interesante ficha para trabajar todo lo referente a copias de seguridad. Gran parte de la información incluida en la misma se reproduce a continuación.

Pensemos en la siguiente situación:

> *“El otro día, al conectar el disco duro externo al equipo, me saltó un mensaje que decía algo de formatear el disco, y sin querer acepté. ¡Vaya disgusto! He borrado toda la información que contenía el disco y me he quedado sin las fotos de los últimos 3 años porque era el único sitio donde las almacenaba…”*

Si te ves envuelto en una situación similar a la planteada y no habías realizado previamente copias de seguridad, desaparecerá tu información, con lo que ello supone:

- Perder recuerdos y momentos personales
- Repetir trabajos a los que habías dedicado tiempo y esfuerzo
- Etc.



https://pixabay.com/es/illustrations/seguridad-backup-de-datos-3994239/

La única forma segura de recuperar la información con ciertas garantías es disponiendo de una copia de seguridad.

Muchas de las veces estos problemas pueden ser accidentales, de hecho, es más habitual que perder información se deba a errores del usuario que a la acción de algún virus capaz de cifrar o borrar la información, por la pérdida, accidente o robo del dispositivo que contiene la información: smartphone, tablet, portátil, disco duro externo, pendrive, DVD…

2.1. Copias de seguridad en 4 pasos

La mencionada guía “Privacidad y seguridad en Internet” plantea un proceso en 4 pasos:

1. **Selecciona la información que bajo ningún concepto te gustaría perder:** un filtro tanto por contenido como por formato. Ejemplos de formatos de archivos a guardar en una copia de seguridad: imágenes, vídeos, documentos PDF, conversaciones de whatsapp, audios...

2. **Elige el soporte donde almacenarás la información:** desde un dispositivo USB a carpetas compartidas en la nube (Google Drive, Dropbox...), pasando por discos duros externos hasta un simple DVD regrabable. Siempre se recomienda guardar en más de un soporte. Antiguamente esta operación era costosa, pero ya podemos encontrar discos duros externos por precios muy asequibles, así como herramientas en la nube gratuitas como Google Drive.

3. **Haz la copia de seguridad:** hacer la copia de seguridad no es más que copiar en otro dispositivo, duplica la información en dos o más soportes. Por ejemplo, una copia podría estar en un disco duro externo y la otra en el disco duro del portátil o incluso en un servicio de la nube (Drive, Dropbox, etc.)

4. **Repite tus copias periódicamente:** con cierta periodicidad actualiza tus copias para comprobar que sigue, por un lado la información disponible, y por otro para incluir en dichas copias la nueva información que hayas generado. Es importante generar un hábito de realización de copias de seguridad.

¿No se pueden hacer de forma automática? El proceso de realización de copias de seguridad suele ser lento (muchos archivos a copiar requiere su tiempo). Es por ello que este

hábito se puede automatizar a través de algún tipo de herramienta. De hecho, algunas aplicaciones (como whatsapp) directamente te ofrecen esa posibilidad.

En el siguiente enlace del blog esgeeks.com se recomiendan 10 aplicaciones muy útiles para esta labor: https://esgeeks.com/mejores-software-backup-gratis/

Sabías qué…

Un lugar muy útil y cómodo para hacer copias de seguridad es Google Drive, herramienta a la que se tiene acceso si se dispone de cualquier cuenta de correo electrónico de Google (Gmail)

La Junta de Extremadura dispone de un acuerdo con Google por el cual se puede solicitar cuentas de correo electrónico Google especiales y específicas para Educación. Entre otras funcionalidades, incluyen la posibilidad de utilizar Google Drive **sin límite de capacidad**. Sin duda una gran lugar sin limitaciones para nuestras copias de seguridad.

Toda la información aquí: https://emtic.educarex.es/recursos/comunicate/google-para-educacion

3. Creación y publicación en la web

Hay muchas formas de crear un recurso y publicarlo en la web, todo lo que un usuario cree se considera recurso. Entendiendo por recurso cualquier creación desarrollada por un autor.

Tan fácil es definir un recurso, como complejo acotarlo. Por ejemplo, pensemos en un libro ilustrado:

- Un libro ilustrado será un recurso.
- No obstante, como su propio nombre indica, será una mezcla de texto e imágenes, cada una de las imágenes también será un recurso como tal, así como el texto fragmentado por capítulos, apartados, párrafos o cualquier otra medida que se nos ocurra.

Un recurso es en sí un conjunto de recursos. Si este ejemplo lo trasladamos a un recurso 2.0, un recurso integrará información textual, numérica, sonora y gráfica dentro de una estructura web.

Desde un punto de vista educativo, es imposible hablar de crear y publicar en la web sin hablar de la corriente educativa cada vez más activa de los **Recursos Educativos Abiertos o REA** (en inglés, Open Educational Resources, OER).

3.1. Creación de REA

¿Qué entendemos por REA? Pues qué mejor que conocerlo a través del siguiente vídeo de la miniserie “Hay que ver…” creada por Centro Nacional de Desarrollo Curricular en Sistemas No Propietarios (CEDEC): https://www.youtube.com/watch?v=5wE1I-ZCNBs

La definición formal aprobada por la UNESCO de REA es:

> *"Materiales de enseñanza, formativos o de investigación en cualquier soporte, digital o de cualquier otro tipo, que sean de dominio público o que hayan sido publicados bajo una licencia abierta que permita el acceso gratuito, así como el uso, modificación y redistribución por otros sin ninguna restricción o con restricciones limitadas"*

Para el desarrollo de un REA, lo habitual es utilizar una herramienta de autor. Las herramientas de autor son aplicaciones informáticas que facilitan la creación, publicación y gestión de los materiales educativos en formato digital a utilizar en procesos de enseñanza-aprendizaje 2.0. Son herramientas de carácter multimedia que permiten combinar documentos digitales, imágenes, sonidos, videos y actividades interactivas desde la misma herramienta, para crear contenidos digitales.

Hay diferencias entre unas herramientas de autor y otras, no obstante, de forma general una herramienta de autor cumple 3 características, características que marcan su potente utilidad:

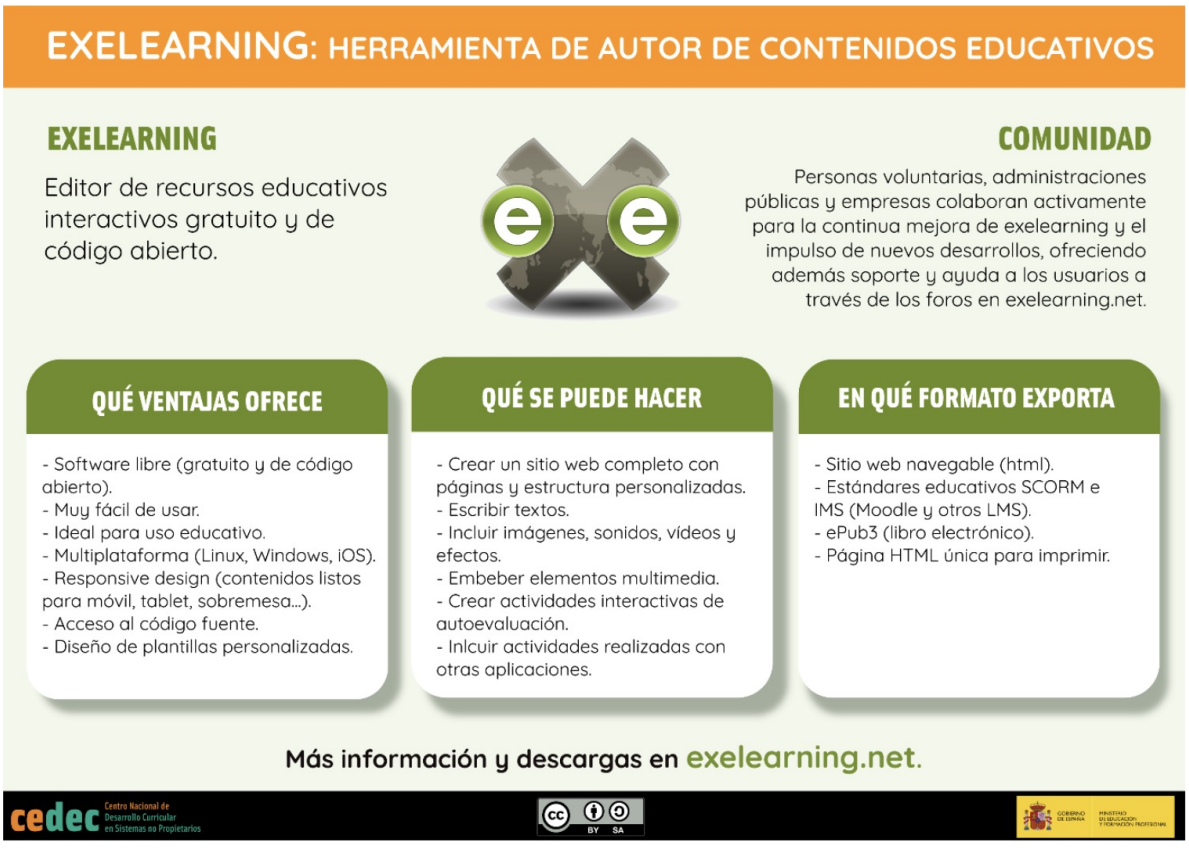
- **Entorno de trabajo sencillo:** para que no haya que ser un experto informático para poderlas utilizar.
- **Conexión siguiendo estándares:** para que todo sea lo más conectable y reutilizable posible.

- **Trabajo a través de plantillas:** unir con flechas, multi-respuesta…

La herramienta de autor más conocida en el ámbito educativo es eXe Learning. Es un programa libre y abierto para crear contenidos educativos de una manera sencilla. Puedes descargarse libremente en http://exelearning.net/, estando disponible para todos los sistemas operativos.

Una de las funcionalidades más potentes y particulares de eXeLearning, es que no sólo es una herramienta para crear contenidos, sino que permite también adaptar y modificar contenidos existentes desarrollados por otros compañeros.

Algo que la diferencia de otras herramientas de autor, es que incluso archivos exportadas en SCORM y creados con eXeLearning, pueden abrirse de nuevo de forma ágil y dinámica, modificarlos y volver a exportar una versión mejorada.



Sabías qué...

Algunas comunidades autónomas, a través de las Consejerías de Educación u otras instituciones públicas, fomentan la creación de recursos educativos abiertos. En Extremadura, por ejemplo, existe el programa CREA del proyecto INNOVATED.

El programa CREA (Creación de Recursos Educativos Abiertos) es una iniciativa de la Consejería de Educación y Empleo de la Junta de Extremadura que tiene como objetivo proporcionar a la comunidad educativa (y a los diferentes agentes del sector educativo que puedan estar interesados en ellos) un conjunto de recursos educativos abiertos (REA) que den 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 mejoren el rendimiento del de nuestro alumnado.

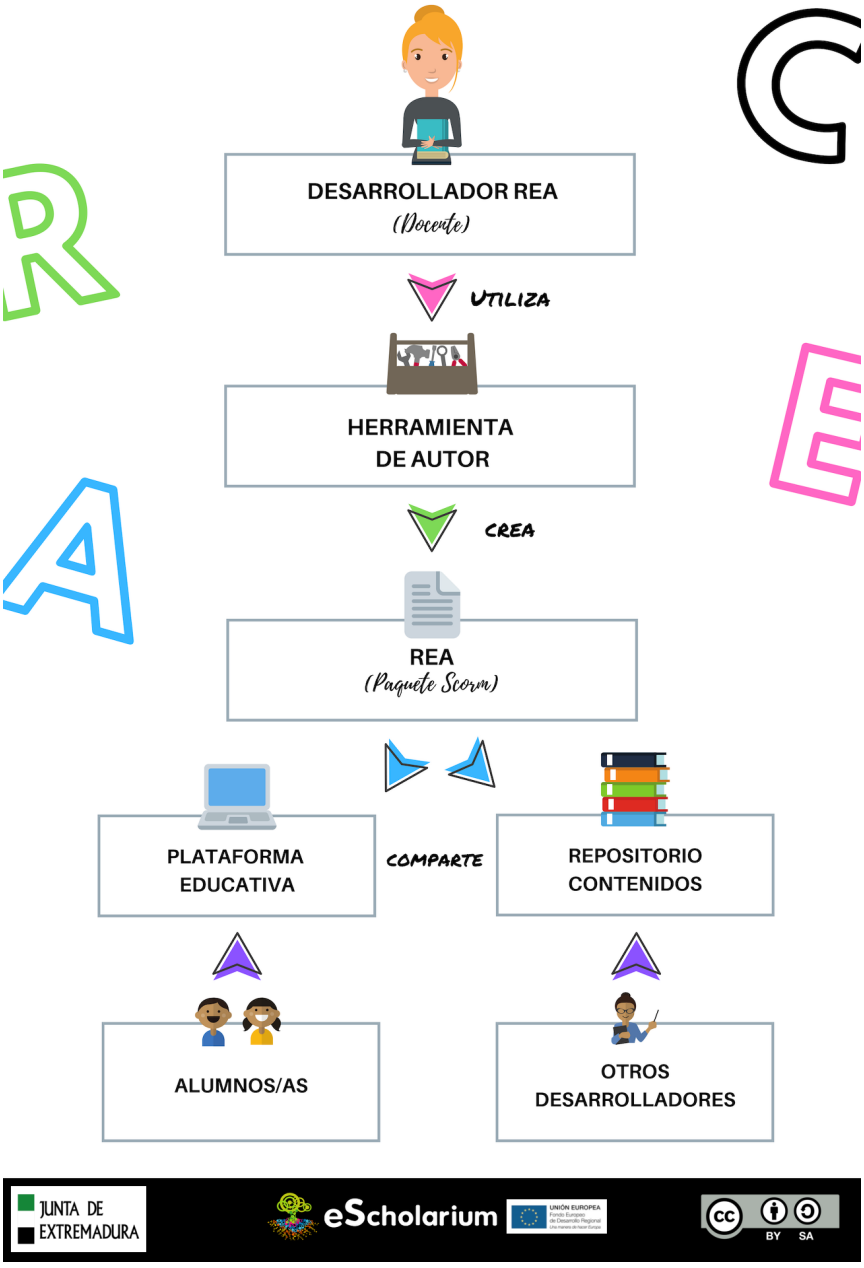
Las herramienta de autor que se utilizan en CREA son 2:

- eXeLearning
- Herramienta de autor eScholarium

Puedes conocer más de él (y sus recursos) en su página web: crea.educarex.es

4. Diseño de diversos contenidos web. Concepto y uso de la nube.

La publicación de contenidos web desde un punto de vista educativo se resume en el siguiente proceso:



Básicamente un desarrollado de Recursos Educativos Abiertos (o de cualquier otro tipo de recurso), lo crea utilizando una herramienta de autor. Esta herramienta de autor genera el

contenido en un formato compatible que puede subirse a Internet a diferentes fuentes, siendo las más habituales desde un punto de vista educativo las plataformas educativas y los repositorios educativos. No obstante, también podría subirse a un blog o incluso a las redes sociales directamente.

4.1. Conceptos básicos

En la infografía anterior hemos visto varios elementos importantes que forman parte de la publicación en la nube. Es importante definir los mismos para tener una visión detallada de todo el proceso. Conceptos como:

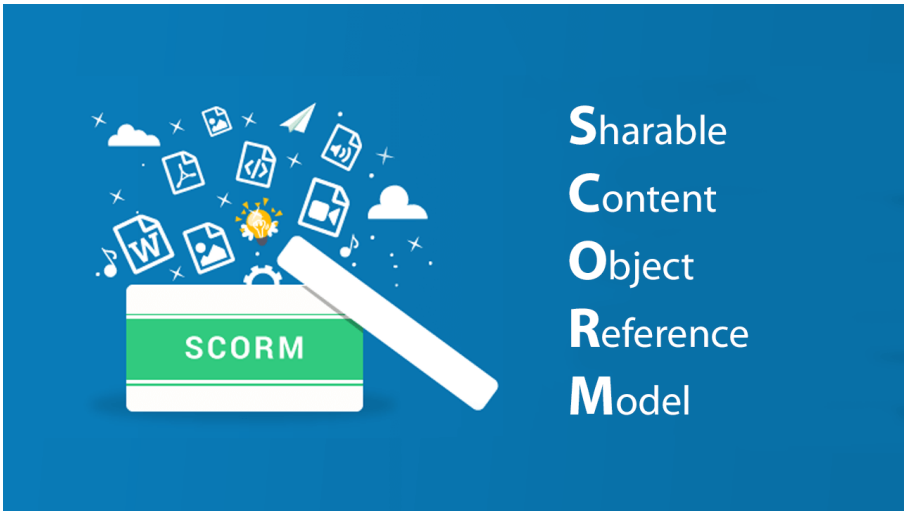
- Paquete SCORM
- Plataforma educativa
- Repositorio de contenidos

¿Qué es un paquete SCORM?

Las herramientas de autor permiten exportar los contenidos digitales creados en diferentes formatos estándar, siendo el formato SCORM el más habitual entre dichos formatos.

SCORM son las siglas del inglés del inglés Sharable Content Object Reference Model. Los contenidos digitales se empaquetan siguiendo el formato SCORM. Un paquete SCORM puede entenderse como un archivo comprimido que contiene todo el contenido digital desarrollado (webs enlazadas, imágenes, vídeos…) así como una serie de archivos de configuración que permiten subir el contenido a la plataforma educativa manteniendo su estructura, navegación e interactividad.

SCORM es un estándar que ya utilizan prácticamente todas las herramientas de autor y plataformas educativas del mercado, lo cual permite que un contenido educativo pueda ser accesible en muchos más lugares diferentes.



¿Qué es una plataforma educativa?

Una plataforma educativa es el mejor lugar para compartir un contenido digital y que el mismo pueda ser utilizado colaborativamente entre alumnos y docentes. Las plataformas educativas son conocidas habitualmente por las siglas en inglés LMS (Learning Management System) y también por su equivalente en castellano EVA (Entorno Virtual de Aprendizaje).

Las funciones más habituales son:

- Gestión y registro de usuarios:
- Seguimiento de alumnos
- Administración y programación de contenidos digitales
- Gestión de evaluaciones
- Herramientas de comunicación y colaborativas
- Informes

El ejemplo más conocido de plataforma educativa es Moodle (moodle.org)

¿Qué es un repositorio de contenidos?

Un repositorio de contenidos digitales es un sistema de gestión de contenidos donde se albergan, correctamente clasificados, contenidos digitales. Los diseñadores de REA (docentes) accederán al mismo y podrán descargar REAs que sean de su interés. Así como compartir los suyos.

Los repositorios de contenidos suelen ser conocidos por las siglas **CMS (Content Management System)**

4.2. Subir recurso a un repositorio de contenidos

Subir un recurso a un repositorio de contenidos no es un proceso complicado. No obstante, es muy importante facilitar todo lo posible para que el mismo sea encontrado por otros usuarios. No hemos de obviar que compartir un recursos sólo será útil si otro lo puede aprovechar, si no lo pudiera encontrar porque el mismo está perdido entre un número amplio y desordenado de recursos, no habrá servido de nada compartirlo.

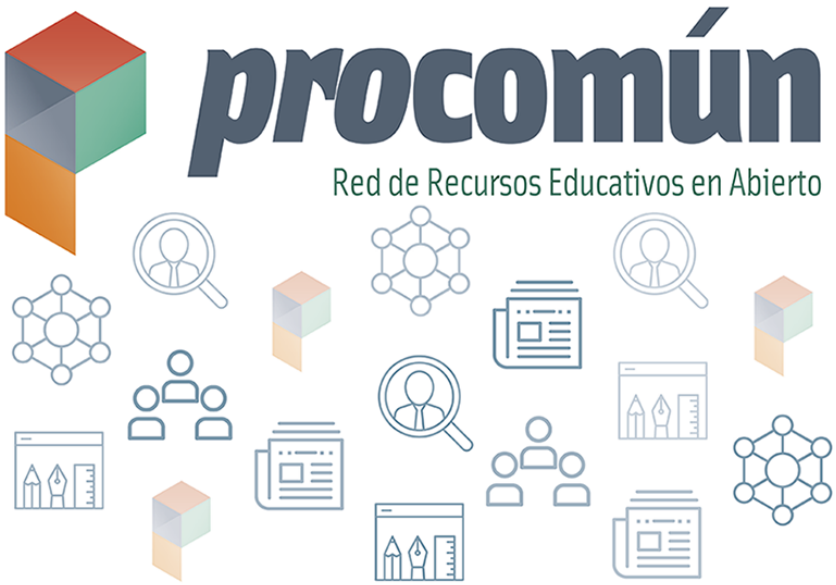
Existe un estándar que facilita esta tarea, el estándar LOM-ES V1.0. Tal y como se explica en la página web del INTEF (www.intef.es)

> *El perfil de aplicación de metadatos LOM-ES V1.0 ha sido realizado en el marco de los trabajos llevados a cabo por parte del Ministerio de Educación (Instituto Nacional de Tecnologías Educativas y Formación del Profesorado (INTEF), anteriormente Instituto Superior de Formación y Recursos en Red para el Profesorado), Ministerio de Industria, Turismo y Comercio (Entidad Pública Empresarial. red.es) y todas las Comunidades Autónomas en relación a los Programas institucionales para el desarrollo de la Sociedad de la Información y el Conocimiento (Convenio Marco del Programa Internet en el Aula). El objetivo general del perfil es servir como marco de referencia y punto de partida a iniciativas de desarrollo de Bancos/Repositorios de Recursos y Materiales Educativos basados en Objetos Digitales normalizados, fácilmente reutilizables y transferibles.*
>
> *Las Administraciones Educativas han elaborado este perfil de aplicación o esquema de metadatos específico de LOM con el objetivo de contemplar y satisfacer las necesidades específicas de la comunidad educativa española. El trabajo se ha desarrollado, tras un análisis pormenorizado del estándar de base original LOM v.1.0 propuesto por IEEE-LTSC, en el seno del Subcomité 36 "Tecnologías de la Información para el Aprendizaje" dependiente del Comité Técnico de Normalización 71 de AENOR.*

Es muy importante que a los recursos educativos les incluyamos los metadatos necesarios, metadatos que facilitarán su búsqueda posterior en los repositorios. Por suerte, herramientas de autor como eXe Learning ya permiten incluirlos, de esta forma los paquetes SCORM generados los incluirán también. Si el paquete los incluye cuando se suba al repositorio, ya quedará todo perfectamente etiquetado para su búsqueda.

¿Cómo subir un recurso a un repositorio?

Desde un punto de vista educativo, el repositorio de referencia es Procomún: https://procomun.educalab.es. El mismo reúne material didáctico catalogado de forma estandarizada a través de metadatos (LOM-ES), coherente con el currículo de enseñanzas anteriores a la Universidad (Educación Infantil, Primaria y Secundaria) y preparado para ser utilizado directamente en el aula o bien para ser modificado y adaptado a diferentes contextos o necesidades.



Visualizando los 2 vídeos siguientes puedes conocer más de Procomún de forma ágil y directa:

https://www.youtube.com/watch?v=sXy1C53MhIE

https://www.youtube.com/watch?v=YjtW69eNf10

Uno de los mayores potenciales de Procomún es que cualquiera puede registrarse en Procomún y empezar a utilizar REA o compartir los suyos propios. En el siguiente vídeo se explican los pasos para tal fin:

https://www.youtube.com/watch?v=uCSXVaoz7e4

Si el registro en Procomún es sencillo, el proceso para compartir tus REA en este repositorio de contenidos es incluso más fácil. En el siguiente vídeo puedes conocer este proceso:

https://www.youtube.com/watch?v=CIlJXnRfw-Q