SITUACIÓN DE APRENDIZAJE

IDENTIFICACIÓN

TÍTULO	NAVEGACIÓN SEGURA EN INTERNET. PROTECCIÓN ANTE VIRUS Y FRAUDES				
ÁREA/MATERIA/ÁMBITO	TRDR	NIVEL	1º ESO	TEMPORIZACIÓN	8 sesiones
DESCRIPCIÓN	Esta situación de aprendizaje tiene el objetivo de informar y capacitar al alumnado para actuar de manera proactiva frente a los riesgos asociados a virus y fraudes informáticos extendidos a través de Internet, ofreciéndole recomendaciones, pautas y herramientas para su prevención y/o actuación en caso de verse afectados por ellos.				
RETO, PREGUNTA, PROBLEMA, NOTICIA, NECESIDAD...	En su día a día, el alumnado se expone a la amenaza de virus y fraudes cuando navega por internet y/o redes sociales. Por ejemplo, cuando buscan ropa de una determinada marca, en ocasiones pueden acceder a páginas falsas e intentar comprar productos que ellos piensan que es el que están buscando pero realmente es un fraude y realizan la compra de un producto que no recibirán nunca, además de exponer datos como tarjetas bancarias o números de cuenta. Reto: Conocer los conceptos de ingeniería social, fraude y virus informáticos, sus características, medios y métodos de actuación, así como los riesgos que ambos – virus y fraudes – suponen para el usuario, analizando éstos mediante ejemplos y casos reales. Abordaremos también los mecanismos y pautas de prevención y actuación frente a virus y fraudes electrónicos, así como las entidades de referencia que pueden darnos soporte y ayuda ante éstos.				
PRODUCTO INTERMEDIO/S O FINAL	Elaborar una infografía que informe sobre los distintos tipos de virus y fraudes, cómo protegernos de ellos y cómo actuar en caso de ser víctima de un virus informático o un fraude. Las infografías serán colgadas en los paneles del centro para que el resto de estudiantes puedan informarse.				

CONCRECIÓN CURRICULAR	COMPETENCIAS CLAVE	COMPETENCIAS ESPECÍFICAS	CRITERIOS DE EVALUACIÓN		SABERES BÁSICOS Y OTROS SABERES
			Código	Descripción y concreción	
	☒CCL ☒CP ☒STEM / CMCT ☒CD ☒CPSAA ☒CC ☐CE ☒CCEC	CE1: Utilizar dispositivos digitales de uso personal en el entorno domestico y educativo de manera saludable, segura y sostenible. CE2: Buscar y seleccionar críticamente información digital de diferentes fuentes, interpretarla, organizarla en el entorno personal de aprendizaje y crear contenidos digitales. CE4: Mostrar hábitos básicos que fomenten el bienestar en las relaciones a través de entornos digitales.	1.3 1.5 2.1 2.5 2.6 4.4	Conectar dispositivos digitales a Internet de manera segura. Mostrar hábitos básicos de seguridad para proteger los dispositivos. Buscar, seleccionar y interpretar información de acuerdo con las necesidades a partir de diversas fuentes con sentido crítico, contrastando la veracidad. Organizar y gestionar el entorno personal de aprendizaje mediante la integración de recursos digitales. Crear, integrar y editar contenidos digitales con sentido estético de manera creativa y respetando los derechos de autor. Identificar y saber reaccionar de manera básica ante situaciones que representen comportamientos abusivos o amenazas a través de dispositivos digitales valorando el bienestar personal y colectivo.	• Hábitos básicos de seguridad para proteger los dispositivos. • La brecha digital. • Selección de información en medios digitales a través de buscadores web contrastando su veracidad. • Lectura y interpretación de información de • medios digitales. • Creación básica de contenidos con herramientas digitales. • Estética y lenguaje audiovisual. • Exposición personal en la red. La huella digital • La privacidad en la red. La protección de datos de carácter personal. Información y consentimiento. • Riesgos y amenazas del uso de dispositivos y relaciones en red: ciberacoso y fraudes

CCL: Competencia en comunicación lingüística	**CP**: Competencia plurilingüe	**STEM**: Competencia matemática y competencia en ciencia, tecnología y ingeniería	**CD**: Competencia digital
CPSAA: Competencia personal, social y de aprender a aprender	**CC**: Competencia ciudadana	**CCEC**: Competencia en conciencia y expresión cultural	**CE**: Competencia emprendedora

Autoría: Lorena Marco Armero

GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura i Esport
cefire

DISEÑO DE LA SITUACIÓN DE APRENDIZAJE

ACTIVIDADES / TAREAS

DESCRIPCIÓN ACTIVIDAD/TAREA 1

Nombre: ¿Qué sabes a cerca de los virus y los fraudes informáticos?
Objetivos: Conocer qué son y cómo funcionan los virus informáticos y los fraudes informáticos para poder prevenirse ante ellos.

Temporalización:
Primeros 10', visualización del vídeo: **'Cómo proteger nuestros dispositivos de ataques de virus'** (1:01)**,** en el que se presenta una acción conjunta de Policía Nacional y empresas desarrolladoras de antivirus. Exposición de los principales términos de los que se habla en el vídeo.
Visualización y análisis de la web de amenazas en tiempo real de karpesky, para darse cuenta de la realidad de ataques informáticos constantes.
Resto de la clase: trabajo sobre la terminología relacionada con los distintos tipos de virus y ataques informáticos. De manera que después el alumnado pueda profundizar en cada uno de los términos para ir recopilando información para poder realizar la tarea expositiva final.

MEDIDAS DE RESPUESTA (I,II)		MEDIDAS DE RESPUESTA (IIII, IV)	CÓDIGO CRITERIOS DE EVALUACIÓN	EVALUACIÓN
METODOLOGÍA/ AGRUPAMIENTO	RECURSOS MATERIALES, PERSONALES Y ESPACIALES			
- Primera parte: En grupo- - Segunda parte: individual	- Aula de informática - Cañón proyector - Ordenador con conexión a Internet - Plataforma Aules	-Dossier en papel con los términos y sus definiciones primer, y actividades que los relacionen. -Herramientas del SO de accesibilidad: teclado en pantalla, lector de pantalla... -Portátil adaptado para diversidad funcional	2.1 2.6	-Primera parte: Observación de la actitud y participación del alumnado. -Segunda parte: Observación del trabajo realizado durante la clase.

DESCRIPCIÓN ACTIVIDAD/TAREA 2

Nombre: Virus. Mecanismos y vías de infección
Objetivos: Aplicar medidas y pautas para la protección de ordenadores y dispositivos móviles ante la amenaza de éstos.

APRENDIZAJE ACCESIBLE

- ❑ Accesibilidad
  - ❑ Física
  - ❑ Sensorial
  - ❑ Cognitiva
  - ❑ Emocional
- ❑ Considera la perspectiva cultural, de género y socioeconómica.
- ❑ Considera la conexión con los desafíos, ODS y favorece el rol activo del alumnado.
- ❑ Consigue la máxima implicación y participación de todo el alumnado.
- ❑ Lleva un seguimiento continuo proporcionando feedback.
- ❑ Presenta la información al alumnado utilizando diferentes formatos.
- ❑ Favorece la reflexión y el procesamiento de la información a diferentes niveles.
- ❑ Ofrece al alumnado

Temporalización
Primeros 15', debate planteando la siguientes cuestiones: Teniendo en cuenta el trabajo realizado en la clase anterior, ¿Qué tipos de virus conocéis? ¿Os habéis visto amenazados en alguna ocasión por alguno de ellos? ¿Cuáles creéis que son los métodos más habituales de infección? ¿Qué crees que se podría haber hecho para evitarlos? ¿Afectan sólo a ordenadores? ¿Habéis detectado algún virus en vuestros dispositivos móviles? ¿Tenéis instalado y configurado un antivirus en vuestro Smartphone o Tableta?
Resto de la clase: investigación a cerca de los principales mecanismos y vías de infección para seguir completando la infografía a finalizar en la siguiente actividad.

MEDIDAS DE RESPUESTA (I,II)		MEDIDAS DE RESPUESTA (IIII, IV)	CÓDIGO CRITERIOS DE EVALUACIÓN	EVALUACIÓN
METODOLOGÍA/ AGRUPAMIENTO	RECURSOS MATERIALES, PERSONALES Y ESPACIALES	-Dossier en papel con los términos y sus definiciones primer, y actividades que los relacionen. -Herramientas del SO de accesibilidad: teclado en pantalla, lector de pantalla... -Portátil adaptado para diversidad funcional	1.5 2.1 2.6	-Primera parte: Observación de la actitud y participación del alumnado. -Segunda parte: Observación del trabajo realizado durante la clase.
- Primera parte: En grupo- - Segunda parte: individual	- Aula de informática - Cañón proyector - Ordenador con conexión a Internet - Plataforma Aules			

diferentes maneras de expresión del conocimiento.

DESCRIPCIÓN
ACTIVIDAD/TAREA 3

Nombre: Ingeniería Social y fraude electrónico
Objetivos: Conocer en qué consiste la ingeniería social y los tipos de fraudes electrónicos existentes para evitar ser manipulados por los delincuentes y no ser víctimas de un fraude en Internet

Temporalización
Primera parte: Se tratarán ejemplos de situaciones reales de fraudes electrónicos conocidos y denunciados en medios de comunicación mediante vídeos y/o noticias.
Segunda parte: Finalización de la infografía que se comenzó a realizar en la primera actividad, recopilando la información de todas las tareas.

MEDIDAS DE RESPUESTA (I,II)	MEDIDAS DE RESPUESTA (IIII, IV)	CÓDIGO CRITERIOS DE EVALUACIÓN	EVALUACIÓN

	METODOLOGÍA/ AGRUPAMIENTO	RECURSOS MATERIALES, PERSONALES Y ESPACIALES	- Dossier en papel con los términos y sus definiciones primer, y actividades que los relacionen. - Herramientas del SO de accesibilidad: teclado en pantalla, lector de pantalla... - Portátil adaptado para diversidad funcional	2.1 2.2 2.5 2.6	-Primera parte: Observación de la actitud y participación del alumnado. -Segunda parte: Evaluación por parte del profesorado de la infografía realizada por el alumnado en las sesiones anteriores mediante una rúbrica. Autoevaluación por parte del alumnado utilizando una rúbrica que facilitará el profesorado.	
	- Primera parte: En grupo- - Segunda parte: individual	- Aula de informática - Cañón proyector - Ordenador con conexión a Internet - Plataforma Aules				