ESO

Tecnologías de la Información y la Comunicación 4

Programación

Unidad 8

1. Presentación de la unidad
2. Temporalización
3. Objetivos didácticos
4. Contenidos de la unidad/Criterios de evaluación/Estándares de aprendizaje evaluables
5. Competencias/descriptores/desempeños
6. Recursos
7. Medidas para la inclusión y la atención a la diversidad

1. PRESENTACIÓN DE LA UNIDAD

Título

Seguridad y ética en la red

Descripción de la unidad

Es claro que el uso de las nuevas tecnologías está absolutamente integrado en multitud de actividades humanas en la sociedad actual. Su evolución es patente y nosotros somos testigos de que esta continúa de forma casi vertiginosa. Con ellas han aparecido muchísimas posibilidades de progreso que hasta hace tan solo unos pocos años parecían de ciencia ficción y, lamentablemente, también con ellas aparecen nuevos riesgos que tampoco fueron intuidos al principio y a los que hay que dar respuesta de forma permanente. Un tema relacionado con la seguridad y ética en la red se hace, pues, imprescindible si se desea abarcar todos los aspectos –buenos y malos– que rodean a las posibilidades casi ilimitadas de acceso a contenidos, recursos y datos que ofrece Internet. Por otra parte, este hecho es más acuciante en el momento en que muchos de los usuarios habituales de la red son menores de edad, que no siempre valoran con realismo el riesgo que suponen ciertas amenazas virtuales. Así, entendemos como una tarea ineludible la de no solo proporcionar información teórica acerca de los contenidos relacionados con la seguridad en la actividad cotidiana en Internet sino, en lo posible, concienciar de la relevancia crucial de este hecho a los alumnos y las alumnas en este contexto educativo.

La unidad parte de una descripción con cierto grado de detalle de las amenazas que están presentes en la red para comprender cuáles deben ser los objetos físicos y virtuales a proteger. Se analizan por ello las diferentes medidas de seguridad activa y pasiva que pueden ponerse en marcha y, en particular, se mencionan los virus informáticos como los agentes dañinos que pueden interferir de forma muy negativa sobre equipos y software.

Frente a este tipo de amenazas, se estudian a continuación algunas herramientas con las que combatirlas: antivirus, cortafuegos, antiespías y copias de seguridad, para continuar con el aspecto clave de la protección de datos de carácter personal en sus aspectos privado y público, es decir, tanto en la custodia personal de los mismos como en lo referente a los derechos que posee un usuario cuando voluntariamente cede a un tercero esa información valiosa.

Dados los hábitos de los adolescentes en la sociedad actual, es deseable mencionar el concepto de *huella digital*, y cómo es relativamente sencillo acceder a un registro de actividad que permita extraer conclusiones acertadas acerca de cuestiones privadas de los usuarios no precavidos de Internet. Como herramientas seguras de cesión de datos, se mencionan a continuación los procedimientos de identificación en la red, el DNI electrónico, los certificados electrónicos y la firma digital.

La última parte de la unidad está dedicada a las estrategias de protección de la información, algunas con mayor grado de aplicabilidad en el día a día que otras. Tal es el caso de la utilización de contraseñas seguras y la inclusión de los conceptos de criptografía y protocolos seguros. El análisis de los riesgos de seguridad en las comunicaciones cierra la presente unidad, poniendo en sobre aviso de los riesgos que aparecen con el correo electrónico, la suplantación de la personalidad, las descargas, el intercambio de archivos, los fraudes en Internet y las formas existentes de detección de los mismos.

2. TEMPORALIZACIÓN

Desde el 15 de mayo hasta el 15 de junio. 8 h.

3. OBJETIVOS DIDÁCTICOS

1. Adquirir conciencia responsable de la necesidad de hábitos seguros en la utilización de Internet.
2. Conocer los conceptos técnicos básicos que permitan identificar las amenazas más comunes en la red, las soluciones que pueden plantearse y los hábitos seguros que contribuyen a minimizar su efecto.
3. Identificar aquella información y aquellas prácticas que son especialmente sensibles en términos de seguridad y conocer los mecanismos que pueden emplearse para protegerlos de acciones externas dañinas.
4. Utilizar con autonomía y destreza los conceptos de seguridad en la red estudiados, empleando una expresión precisa y rigurosa tanto para amenazas, para riesgos de seguridad y para soluciones posibles.

4. CONTENIDOS DE LA UNIDAD / CRITERIOS DE EVALUACIÓN / ESTÁNDARES DE APRENDIZAJE EVALUABLES

Competencias clave (CC): comunicación lingüística (CCL), competencia matemática y competencias básicas en ciencia y tecnología (CMCT), competencia digital (CD), aprender a aprender (CAA), competencias sociales y cívicas (CSYC), sentido de iniciativa y espíritu emprendedor (SIEP) y conciencia y expresiones culturales (CEC).

Contenidos	Criterios de evaluación	Estándares de aprendizaje evaluables	CC
Seguridad y amenazas. - ¿Qué es la seguridad informática? - Proteger un sistema informático. - Ataques y amenazas. **Medidas de seguridad y tipos de malware.** - Seguridad activa y pasiva. - Virus y malware. **Herramientas de seguridad.** - Antivirus. - Cortafuegos. - Antiespías. - Copias de seguridad. **Protección de datos personales.** - Datos personales. - Información y consentimiento. - Tratamiento de los datos. - Derechos ARCO. **Identidad digital.** - La huella digital. - Reputación online. - Sistemas de identificación en la red. - El DNI electrónico. - Certificado electrónico. - La firma digital. **Protección de la información.** - Crear contraseñas	1. Conocer y exponer adecuadamente los conceptos de seguridad y amenazas en el contexto de la red.	1.1. Explica las características que deben ser preservadas gracias a la seguridad informática. 1.2. Conoce cuáles son los objetos de protección en un sistema informático. 1.3. Comprende cuáles son los agentes contra los que hay que proteger un sistema informático.	CCL, CD, CAA, CSYC
	2. Distinguir los distintos grupos en los que pueden clasificarse las medidas de seguridad y las posibles amenazas.	2.1. Diferencia entre prevención, detección y recuperación y emplea correctamente los diferentes conceptos. 2.2. Clasifica el malware de acuerdo a las acciones que ejecuta. 2.3. Define correctamente virus informático y lo caracteriza frente a otro tipo de malware.	CCL, CD, CSYC
	3. Estar al tanto de los diferentes tipos de herramientas de seguridad y las funciones específicas que desarrolla cada una.	3.1. Cita algunos tipos de antivirus y comprende algunos de los mecanismos que utilizan para cumplir su cometido. 3.2. Sabe la utilidad de los cortafuegos informáticos, pone ejemplos y nombra algunos. 3.3. Valora la funcionalidad de los antiespías y describe situaciones en las que estos actúan. 3.4. Adquiere hábitos para realizar copias de seguridad periódicas.	CCL, CMCT, CD, CAA, CSYC, SIEP

seguras. - Criptografía. - Protocolos seguros. - Verificar la legitimidad de un sitio web. **Riesgos de seguridad en las comunicaciones.** - Correo electrónico y mensajería instantánea. - Suplantación de identidad. - Descargas. - Intercambio de archivos. - Fraudes en Internet. - Detección del fraude.	4. Adquirir conciencia de la necesidad de proteger los datos personales en la utilización cotidiana de la red.	4.1. Explica con rigor los aspectos relativos a derechos y deberes en relación a los datos personales, su utilización y custodia. 4.2. Es consciente de la necesidad de ser informado de la utilización que vaya a hacerse de los datos personales y del consentimiento que puede otorgarse o no. 4.3. Conoce las características de seguridad que deben cumplir las entidades que custodian datos personales. 4.4. Maneja con soltura los aspectos que involucran los derechos ARCO.	CCL, CMCT, CD, CAA, CSYC, SIEP
	5. Valorar la huella digital que se deja en la utilización de Internet, cuantificarla en la medida de lo posible y controlarla de acuerdo a criterios objetivos de seguridad y privacidad.	5.1. Conoce el concepto de huella digital. 5.2. Interioriza la importancia de controlar la reputación online. 5.3. Enumera diferentes sistemas de identificación en la red. 5.4. Indica la utilidad y las posibilidades del DNI electrónico. 5.5. Valora la función que desempeñan los certificados electrónicos.	CCL, CMCT, CD, CAA, SIEP
	6. Asimilar diversas técnicas, activas y pasivas, para mejorar la protección de la información.	6.1. Adquiere el hábito de establecer contraseñas seguras en los diferentes dispositivos, plataformas o aplicaciones. 6.2. Comprende el término criptografía y lo utiliza con propiedad en el contexto de la seguridad informática. 6.3. Identifica cuándo se emplea un protocolo seguro en la transmisión de la información y entiende las prestaciones que proporciona.	CD, CSYC, SIEP

		6.4. Conoce el procedimiento para verificar la legitimidad de un sitio web.	
	7. Interiorizar los riesgos inherentes para la seguridad en la utilización de diversas aplicaciones informáticas que conlleven intercambio de información.	7.1. Sabe qué riesgos puede haber en la utilización del correo electrónico y en la mensajería instantánea. 7.2. Conoce qué es la suplantación de la personalidad, cómo se produce el robo y qué medios pueden ponerse para evitarlo. 7.3. Comprende las amenazas que pueden ocultarse en las descargas a través de Internet de vídeos, música, presentaciones, etc. 7.4. Es consciente del riesgo para la seguridad que puede esconderse en las comunicaciones para intercambiar archivos. 7.5. Identifica con criterio los fraudes que se muestran en diversos ámbitos en Internet.	CD, CAA, CSYC, SIEP, CEC

5. COMPETENCIAS / DESCRIPTORES / DESEMPEÑOS

Competencia	Descriptor	Desempeño
Competencia matemática y competencias básicas en ciencia y tecnología	- Analizar de forma crítica y sistemática los diferentes procesos que intervienen en el ámbito de la seguridad informática, para extraer patrones propios de comportamiento y estrategias personales para evitar las amenazas. - Conocer alguno de los aspectos científicos que sustentan la tarea de la encriptación de datos y de la detección de amenazas cibernéticas.	- Traza estrategias personales de resolución de problemas en base a las condiciones iniciales que se le proporcionen, la dificultad del proceso a seguir y la calidad de los objetivos a alcanzar. - Explica con cierto grado de detalle la base científica que soporta la seguridad informática en función del tipo de amenaza al que trata de dar solución.
Competencia en comunicación lingüística	- Utilizar con precisión y rigor el lenguaje técnico necesario para exponer oralmente y por escrito contenidos relacionados con la seguridad en Internet. - Describir sin ambigüedades los procedimientos precisos a seguir en la ejecución de procedimientos informáticos concretos.	- Mantiene una actitud crítica y de escucha ante los procesos comunicativos en los que se ve involucrado. - Domina los conceptos estudiados y los utiliza con propiedad oralmente y por escrito. - Enriquece el proceso comunicativo empleando diferentes elementos que acompañen al texto oral o escrito empleado. - Interviene oralmente en el desarrollo de la clase empleando construcciones gramaticales precisas que sustenten un razonamiento argumentado suficientemente elaborado.
Competencia digital	- Interiorizar alguno de los aspectos y dificultades técnicas que involucra la creación de sistemas seguros de transferencia de información. - Emplear de forma segura las distintas aplicaciones y plataformas en el uso cotidiano de Internet. - Incorporar mecanismos de control para hacer seguras las transferencias de datos personales en las diferentes interrelaciones establecidas a través de la red.	- Usa habitualmente la información incluida en la web de Anaya para afianzar la comprensión de conceptos. - Conoce y utiliza con corrección los términos relacionados con seguridad informática y amenazas digitales. - Identifica las situaciones de riesgo y pone los medios necesarios para minimizarlo. - Interioriza hábitos seguros en la utilización cotidiana de Internet.

	- Hacer uso de diferentes herramientas en la solución de problemas sobrevenidos al realizar un proyecto. - Emplear recursos de otras áreas de conocimiento informáticas para solucionar problemas o enriquecer los procedimientos que conducen a la ejecución de una tarea concreta.	- Valora los sistemas seguros de transmisión digital de la información DNIe, certificados electrónicos y firma digital.
Conciencia y expresiones culturales	- Elaborar con sentido estético la tarea encomendada, poniendo cuidado en los detalles. - Tomar conciencia de la necesidad de proteger la propiedad de datos personales y la intelectual de contenidos.	- Valora la realización de tareas visualmente atractivas y estéticas. - Comprende los riesgos asociados a ciertas actitudes deshonestas relacionadas con un uso inadecuado de Internet para obtener beneficio ilícito a costa del trabajo de otras personas.
Competencias sociales y cívicas	- Valorar la relevancia social que tienen los aspectos relacionados con la seguridad informática. - Asimilar procedimientos seguros de intercambio de información en las interrelaciones en la red. - Asumir una escala de valores personal y ética que se base en la probidad del propio trabajo y en la utilización responsable del ajeno.	- Respeta el trabajo ajeno, utilizándolo en función de la licencia de uso que tenga y, en su caso, citándolo convenientemente. - Asimila estrategias de resolución cooperativa de problemas, valora los beneficios que presenta y propicia el clima adecuado para llevar a buen término las tareas emprendidas. - Muestra una actitud de respeto hacia las opiniones ajenas, argumenta las propias de forma crítica y emplea un leguaje asertivo para exponerlas.
Sentido de iniciativa y espíritu emprendedor	- Proponer alternativas seguras a procedimientos habituales en la utilización de la red. - Promover actitudes que favorezcan hábitos seguros en la utilización de Internet.	- Propicia el trabajo colaborativo para la resolución de problemas planteados en el aula. - Es realista en la planificación de las tareas y pone en marcha las acciones precisas para llevarlas a cabo.
Aprender a aprender	- Extraer consecuencias de los propios errores y poner los medios adecuados para no volverlos a cometer, a la vez que utilizarlos para enriquecer el propio conocimiento.	- Proyecta el propio aprendizaje adecuándolo al tiempo disponible, a la dificultad previsible y a la capacidad de trabajo que pueda desarrollar.

	- Utilizar de forma personal el conocimiento extraído de fuentes externas para construir el propio aprendizaje. - Personalizar el texto a estudiar de forma que resulte significativo y eficaz en el objetivo de la construcción de conocimiento. - Realizar una constante autoevaluación de los procedimientos y de los logros en el aprendizaje.	- Evalúa el resultado de las actividades desarrolladas, analizando de forma crítica su adecuación a la realidad y a los requisitos del problema. - Personaliza el material de trabajo a través de esquemas, resúmenes y anotaciones propias. - Analiza el propio aprendizaje y toma consciencia de los logros conseguidos y de las carencias que aún haya que solventar. - Persevera ante las dificultades.

6. RECURSOS

Los siguientes materiales de apoyo servirán para reforzar y ampliar el estudio de los contenidos de la unidad:

- Cuaderno del alumno, en el que este tomará nota de los aspectos más relevantes de cada tema, añadirá la información complementaria que haya podido darse durante las clases y realizará las actividades del libro que lo requieran.
- Documentos online gratuitos sobre los contenidos estudiados.
- Recursos digitales Anaya del alumno, en los que se encontrará material de trabajo, de debate y análisis sobre los diferentes aspectos tratados en el tema.

Recursos digitales

En la web de Anaya, dispone de diferentes vídeos, presentaciones, simulaciones y actividades interactivas que constituyen un apoyo eficaz para el estudio de la unidad y, en muchos casos, para la ampliación de contenidos.

7. MEDIDAS PARA LA INCLUSIÓN Y LA ATENCIÓN A LA DIVERSIDAD

El profesorado dispone de una rúbrica en el anexo «Herramientas de evaluación» para evaluar las medidas para la inclusión y la atención a la diversidad individual y del grupo que el desarrollo de la unidad requiera.