MATERIALES DIDÁCTICOS CRFP

EXPERIENCIA DE AULA

SEGURIDAD EN REDES SOCIALES EN EL MARCO EDUCATIVO

GUÍA PARA TUTORES

Centro Regional de Formación del Profesorado
Castilla-La Mancha

MATERIALES DIDÁCTICOS CRFP

Cristina Alba Peinado (ed.)

Antonio Quintanilla Rodríguez (coord.)

Vicente Núñez Armero
Pedro Antonio Ortega Palazón
Miguel Ángel Rodríguez Cubas
Isabel Valverde López

ISBN **978-84-16077-20-5**

Descripción

ESTA GUÍA PARA TUTORES ofrece propuestas de tareas que puedan ser llevadas a cabo en las aulas en sesiones de tutoría, con el fin de abordar de manera clara y práctica aspectos relacionados con la SEGURIDAD EN LAS REDES SOCIALES.

No obstante, esta guía también va dirigida a todos aquellos docentes, de cualquier materia, que deseen trabajar con sus alumnos este tipo de cuestiones, bien sea de manera puntual o como parte de un proyecto de concienciación en los peligros de las Redes Sociales.

Consideramos que es un tema fundamental que debe ser abordado con la importancia que se merece, dada la relevancia que su uso está adquiriendo entre los alumnos y las consecuencias que, cada vez más, estamos observando en el ámbito educativo, a nivel social y personal.

Por ello, tras analizar y seleccionar material de calidad, desde el Grupo Colaborativo ***Seguridad en Redes Sociales en el ámbito educativo,*** hemos querido elaborar esta guía como un herramienta útil para la tarea de sensibilizar y concienciar al alumnado, con el fin de poner medidas a los posibles problemas que puedan surgir.

¡CONÉCTATE!

Visita la web

Centro Regional de Formación del Profesorado Castilla-La Mancha

Objetivos

SEÑALAMOS DIFERENTES OBJETIVOS que pretendemos alcanzar con las tareas que proponemos:

- Adoptar medidas preventivas en el uso de las redes sociales.
- Conocer qué hacer ante vulnerabilidades en la privacidad en el uso de las redes sociales.
- Concienciar al alumnado en la idea de que, al subir fotos a la red, dejan de ser los propietarios de las mismas.
- Transmitir al alumnado el conocimiento de que, al darse de baja de una red social, los datos e imágenes siguen existiendo y el poseedor de la información es la propia red social.
- Conocer cómo cambiar las opciones de privacidad en redes sociales.
- Conocer en qué consiste el *Grooming*.
- Estar al tanto del *Sexting*.
- Adoptar medidas preventivas en el uso de las redes sociales.
- Conocer qué hacer ante vulnerabilidades en la privacidad en el uso de las redes sociales

- Detectar el Ciberbulliying y sus tipos:

  El bloqueo social

  Hostigamiento

  Manipulación Social

  Coacción

  Exclusión social

  Intimidación

  Amenaza a la integridad

- Conocer la reacción de la sociedad ante la ciberdelincuencia.
- Adoptar medidas que los cuerpos de seguridad del estado nos proporcionan.
- Saber clasificar los delitos tecnológicos.
- Comprender la figura del "investigador tecnológico".
- Distinguir páginas pseudofalsas.
- Sospechar sobre aplicaciones presuntamente maliciosas.
- Aplicar medidas preventivas en la instalación de aplicaciones y en el uso del correo electrónico

Competencias

NUESTRO PROPÓSITO fundamental en este proyecto es afianzar la seguridad de los alumnos ante las Redes Sociales, es decir, crear pautas de trabajo y hábitos que hagan a los alumnos competentes en su uso y, por lo tanto, capaces de defenderse y dar respuesta a los problemas que pudieran producirse.

Por ello, destacamos las siguientes COMPETENCIAS BÁSICAS que pretendemos desarrollar en los alumnos:

La **competencia en comunicación lingüística**, necesaria tanto para comprender de manera adecuada los mensajes que le llegan al alumno a través de las Redes Sociales y su correcta interpretación, como para producir una respuesta adecuada a esos mensajes.

Trabajamos esta competencia, además, a través de las fórmulas que proponemos al alumno para poder comunicar a los demás sus inquietudes y temores ante los peligros que las Redes Sociales pueden ocasionar, como puede ser el *ciberacoso* o *bullying*.

Parte de las actividades que proponemos implican la participación de los alumnos como ponentes y, por lo tanto, como comunicadores, desarrollando claramente la expresión oral y la utilización e interpretación correcta del código lingüístico.

La **competencia digital** se desarrolla de una manera particular en este proyecto, ya que pretendemos formar al alumno en habilidades prácticas en su uso de las redes sociales, donde la seguridad juega un papel fundamental.

Cuanto más competente sea el alumno en materia digital, más herramientas tendrá para defenderse y para evitar peligros derivados de su mal uso por parte de otros usuarios. El conocimiento en materia digital supone un arma básica para el alumno del siglo XXI.

Unido a este conocimiento y, fundamentado en el interés de **aprender por aprender**, se pretende dotar al alumno de estrategias básicas para trabajar de forma autónoma y eficaz, motivándole en su aprendizaje de las nuevas tecnologías.

Las **competencias sociales y cívicas** las trabajamos constantemente, ya que muchos de los problemas que tratamos surgen de una baja autoestima del alumno y su intento por ser aceptado por los demás. Ante esto, tratamos de inculcar la seguridad y la valoración de la propia persona, así como la aceptación de los otros, tanto en el contexto escolar, como en dimensión social y cívica.

Proponemos el debate como una forma abierta y positiva de intercambiar diferentes puntos de vista, expresando con tolerancia y tolerancia la propia opinión y valorando la de los demás.

Desarrollamos el **sentido de la iniciativa y el espíritu emprendedor** de los alumnos, ofreciéndoles pautas de trabajo que les permitan adquirir una visión estratégica de las opciones que las Redes Sociales pueden proporcionar para su desarrollo, de manera que sean capaces de tomar decisiones ante estos retos, adoptando criterios de seguridad y confianza.

Finalmente, proponemos el desarrollo de la **conciencia y expresión cultural** no sólo a través de debates y vídeos donde pueden adquirir conocimientos de culturas distintas, sino también a través de creaciones propias de carácter cultural, favoreciendo la transmisión de valores de tolerancia y respeto ante la diversidad.

Contenidos

LOS CONTENIDOS que pretendemos abordar a través de las tareas propuestas son los siguientes:

Técnicas preventivas en redes sociales.

Técnicas correctivas en redes sociales.

Configuración de la privacidad en redes sociales.

Menores en la red. Los tres peligros y sus responsabilidades.

Grooming.

Sexting.

Ciberbullying y sus tipos:

- El bloqueo social
- Hostigamiento
- Manipulación Social
- Coacción
- Exclusión social
- Intimidación
- Amenaza a la integridad

Menores responsables penalmente.

Relevancia de las nuevas tecnologías y la ciberdelincuencia.

Reacción de la sociedad ante la ciberdelincuencia.

Respuesta de las fuerzas de seguridad del estado ante la ciberdelincuencia

Clasificación de los delitos tecnológicos:

Delitos de falsificación documental

Delitos de injurias y calumnias

Delitos de amenazas y coacciones

Delitos contra la integridad moral

Delitos de apología o incitación a la discriminación

La figura del "Investigador Tecnológico"

Páginas falsas *clickhaking*

Dispositivos móviles y aplicaciones maliciosas.

Consejos preventivos al instalar aplicaciones y con el correo electrónico.

Tareas

PROPONEMOS una serie de tareas que pueden ser llevadas a cabo por los tutores, especialmente entre alumnos de Secundaria.

Uno de los principales objetivos en la planificación de estas tareas es que sean los propios alumnos los que adopten el papel protagonista, ocupando el tutor una posición de orientador. No obstante, para ello es fundamental que el tutor (o el profesor) tenga un amplio conocimiento de la materia a tratar y no se vean "pillados" por los alumnos, quienes, en ocasiones, están más actualizados en este tipo de asuntos. Un buena formación por parte del tutor o docente es un requisito imprescindible para el éxito de estas tareas.

Creemos importante esta metodología, ya que unas de las funciones del tutor será precisamente intentar identificar algún tipo de problema específico sobre estas materias entre los alumnos, y facilitar un lenguaje abierto y coloquial entre compañeros es una buena opción para que los alumnos se sientan cómodos, más abiertos y, por lo tanto, más comunicativos.

TAREA 1.

CÓMO CONFIGURAR LA PRIVACIDAD DE LAS REDES SOCIALES

Objetivos:

1. Adoptar medidas preventivas en el uso de las redes sociales.
2. Conocer qué hacer ante vulnerabilidades en la privacidad en el uso de las redes sociales.
3. Concienciar al alumnado de que, al subir fotos a la red, dejan de ser los propietarios de las mismas.
4. Transmitir al alumnado que al darse de baja de una red social, los datos e imágenes siguen existiendo y el poseedor de la información es la propia red social.
5. Conocer cómo cambiar las opciones de privacidad en redes sociales.

Recursos:

El Tutor proporciona:

→***PPT de medidas preventivas y correctivas en redes sociales.***

→***PPT con las opciones de configuración de la privacidad en redes sociales.*** (No se expone, sólo se utiliza para indicar a los alumnos ponentes cómo deben realizar la configuración).

→ ***VÍDEOS*** correspondientes a campañas de difusión sobre redes sociales realizadas en televisión.

Contenidos

Técnicas preventivas en redes sociales.
Técnicas correctivas en redes sociales.
Configuración de la privacidad en redes sociales.

Destinarios de la actividad:

Descripción:

Esta tarea consiste en dar a conocer la configuración de los parámetros de seguridad y confidencialidad en redes sociales, y para ello serán los propios alumnos los que elaboren el material principal y, además, participen como ponentes, ya que tienen un lenguaje propio, con una mayor capacidad de llegar a los receptores, teniendo en cuenta el tema a tratar.

El tutor estará muy pendiente de las reacciones y comentarios de los alumnos, con el fin de detectar alguna problemática concreta entre los alumnos.

Metodología:

Se dividirá la clase en 3 grupos, correspondientes a las tres Redes Sociales más habituales entre los alumnos: FACEBOOK, TWITTER y TUENTI (se pueden hacer más grupos, en función del número de alumnos y de las Redes sociales con las que se quiera trabajar).

Cada uno de estos grupos se encargará de establecer unas pautas de configuración de la red social concreta con la que trabajan. Para ello, el tutor les proporciona un documento de ***Resumen de las condiciones de uso y privacidad*** de cada red social, que deberán leer en el grupo y analizar este tipo de cuestiones:

¿Se puede aceptar a cualquier tipo de contacto?.

¿Todos los contactos pueden escribir en su muro?.

¿Cómo se puede bloquear un contacto?

¿Qué puede ver un contacto que he agregado, aunque no lo conozco?

Si doy de baja mi perfil ¿el perfil sigue existiendo?

¿Estamos de acuerdo con las condiciones que aparecen al darnos de alta?.

¿Podemos subir cualquier tipo de imagen a esta red social?

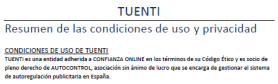
→***Resumen de las condiciones de uso y privacidad de FACEBOOK***:


FACEBOOK
Resumen de las condiciones de uso y privacidad

Declaración de derechos y responsabilidades
Fecha de la última revisión: 15 de noviembre de 2013

2. Compartir el contenido y la información

→***Resumen de las condiciones de uso y privacidad de TUENTI***:


TUENTI
Resumen de las condiciones de uso y privacidad

CONDICIONES DE USO DE TUENTI
TUENTI es una entidad adherida a CONFIANZA ONLINE en los términos de su Código Ético y es socio de pleno derecho de AUTOCONTROL, asociación sin ánimo de lucro que se encarga de gestionar el sistema de autorregulación publicitaria en España.

→***Resumen de las condiciones de uso y privacidad de TWITTER***:

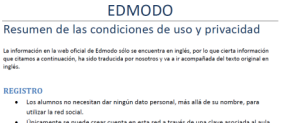

TWITTER
Resumen de las condiciones de uso y privacidad

Actualmente Twitter cuenta, entre otras, con estas tres páginas de información sobre su servicio y funcionalidad:

- CONDICIONES DE SERVICIO

https://twitter.com/tos

→***Resumen de las condiciones de uso y privacidad de EDMODO***:


EDMODO
Resumen de las condiciones de uso y privacidad

La información en la web oficial de Edmodo sólo se encuentra en inglés, por lo que cierta información que citamos a continuación, ha sido traducida por nosotros y va a ir acompañada del texto original en inglés.

REGISTRO

- Los alumnos no necesitan dar ningún dato personal, más allá de su nombre, para utilizar la red social.

Una vez analizados los parámetros de seguridad de cada una de las redes, cada grupo nombrará un ponente que se encargará de explicar al resto del grupo las condiciones de uso y configuración de la red social.

El tutor expone el ***PPT sobre las medidas preventivas***.

Se procede a poner el ***primer vídeo***. (El orden de los vídeos lo decide el alumno, en cualquier caso todos los vídeos tratan sobre lo mismo: vulnerabilidad de la privacidad en redes sociales).

Se pide un voluntario para acceder a su red social concreta. Si no hay ningún alumno voluntario el ponente utiliza su red social.

El ponente muestra como cambiar las opciones de seguridad y restringir el acceso a la red social.

Pasa el turno a su compañero quien se presenta de nuevo y repite la secuencia detallada desde el punto 4, pero en este caso con el ***segundo vídeo***.

Se culmina pasando el turno al tercer ponente.

Se procede a las preguntas por parte de los asistentes.

El tutor culmina la exposición con el ***PPT con las medidas correctivas.***

→¿Por qué hacerlo en internet 1?

→¿Por qué hacerlo en internet 2?

→Piensa antes de colgar tu imagen:

El tutor debe tratar de detectar posibles situaciones de:

Suplantación de identidad de contactos en redes de los alumnos.

Situaciones de acoso escolar.

Tipo de imágenes que suben los alumnos (es importante recordarle según se ha expuesto en la metodología en dos ocasiones que pierden todos los derechos sobre el contenido en la red social (lo publicado), en especial sobre las imágenes.

Grado de dificultad: Baja.

Tiempo destinado al desarrollo: 2 sesiones de 55 minutos.

Tiempo de preparación: 2 Horas.

El tiempo de preparación consiste en visualizar los ppt. Seleccionar a los alumnos en el caso de ser ellos los ponentes y que estos se lean los ppt. Visualizar previamente los vídeos por si se estima que alguno de ellos no es adecuado.

Experiencia previa en el desarrollo:

Esta tarea se ha realizado durante 4 cursos escolares hasta el 2013-14 y la experiencia ha sido muy positiva. Los asistentes se han sentido muy cómodos, interesados por el tema y muy participativos.

La participación del tutor en la exposición final sobre las medidas correctivas permite detectar alumnos que de algún modo se han sentido acosados y cuya problemática podrá ser abordada posteriormente; en cualquier caso, el alumnado debe conocer las actuaciones a realizar tras la ponencia.

Observaciones:

En las materias de Tecnología y de Informática se abordan el tema de creación de blog, y cuestiones referentes a la privacidad y seguridad en redes sociales.

TAREA 2.

CIBERACOSO HACIA MENORES

Descripción:

Esta tarea consiste en dar a conocer qué es el *grooming*, cómo detectarlo y, en consecuencia, cómo adoptar medidas preventivas y correctivas.

Debe quedar perfectamente claro que el *Grooming* es acosar sexualmente al menor pero ***"siempre cometida por un adulto hacia un menor"***, ayudándose de las nuevas tecnologías.

Tres son los conceptos básicos: *Grooming, sexting y ciberbulliying.*

Destinarios de la actividad:

Alumnos de secundaria

Metodología:

El tutor analiza el documento ***PPT Acoso a menores*** donde se expone claramente en qué consiste.

El tutor debe tener presente en todo momento que la ***pedofilia no es el riesgo más frecuente, sino el SextING y el CiberbullyING***

Recursos:

→***PPT de medidas preventivas y correctivas en redes sociales.***

→***PPT ciberacoso en la red a menores.***

→Documento maestro que se ha utilizado como fuente de información el libro de Pedro Pablo Avilés "x1red+segura informando y educando" de 323 páginas y elaborado con el visto bueno de la sección de la Guardia Civil dedicada al acoso de jóvenes en la red.

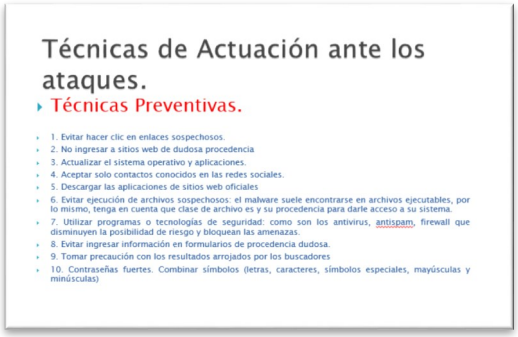
Pautas de desarrollo:

Previamente a la exposición del ciberacoso, el profesor preguntará si algún alumno ha recibido:

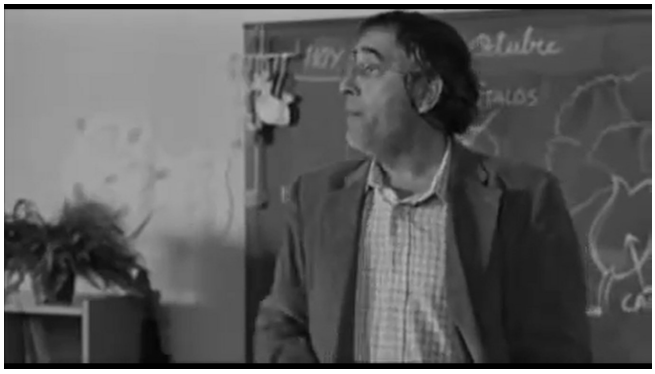
- SMS de índole sexual de una fuente desconocida.
- Email de índole sexual.

El tutor incidirá en que, aunque un alumno se excuse a través del anonimato para realizar ciberacoso a sus compañeros, penalmente es un delito. En la red siempre quedan rastros.

El tutor analiza el PPT con las ***Medidas preventivas y correctivas en el uso de las redes sociales*** (pincha en la imagen para acceder):



Se procede a poner ***El encargado: corto sobre el acoso escolar*** (pincha en la imagen para verlo):



Se procede a poner los **tres vídeos de campañas de difusión** sobre *grooming, sexting y ciberbullying.*

A continuación, el tutor expone el PPT ***Ciberacoso en la red a menores*** (pincha en la imagen para acceder):

Grado de dificultad: Media. Se requiere la colaboración del departamento de orientación.

Tiempo destinado al desarrollo: 2 sesiones de tutoría.

Tiempo de preparación: 4 Horas.

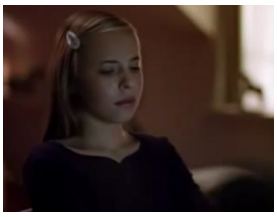
El tiempo de preparación consiste en leer aquellas secciones destinadas al ciberacoso del documento maestro que se ha utilizado como fuente de información: el libro de Pedro Pablo Avilés "***x1red+segura informando y educando***".

Es importante también visualizar previamente tanto el cortometraje como los vídeos publicitarios de información sobre acoso a menores, así como revisar los PPT que se van a utilizar.

→Campaña de buen uso de internet. Grooming:

→Sexting. Qué es:

→Spot Cyberbullying: bloquea el acoso en línea:



→PEDRO PABLO AVILÉS ***"x1red+segura informando y educando".***

Experiencia previa en el desarrollo:

Esta tarea se ha llevado a cabo durante los dos últimos cursos escolares, hay que ser muy muy prudentes. Es muy difícil detectar qué alumnos son acosados.

Afortunadamente todos los centros cuentas con unidades de orientación a quienes se derivarán aquellos alumnos ante la más mínima sospecha de que son ciberacosados.

Observaciones:

Hay que ser muy muy prudentes ya que pueden darse casos de falsos positivos.

Tenemos que dejar muy claro que lo que para unos es un juego para otros es acoso y que hay un desarrollo legal que penaliza, dicho desarrollo está expuesto en el PPT correspondiente al ciberacoso en jóvenes.

TAREA 3.

CIBERDELINCUENCIA

Objetivos:

Conocer la reacción de la sociedad ante la ciberdelincuencia.

Adoptar medidas que los cuerpos de seguridad del estado nos proporcionan.

Saber clasificar los delitos tecnológicos.

Comprender la figura del "investigador tecnológico.

Distinguir páginas peudofalsas.

Sospechar sobre aplicaciones presuntamente maliciosas.

Aplicar medidas preventivas en la instalación de aplicaciones y en el uso del correo electrónico

Contenidos:

Relevancia de las nuevas tecnologías y la ciberdelincuencia.

Reacción de la sociedad ante la ciberdelincuencia.

Respuesta de las fuerzas de seguridad del estado ante la ciberdelincuencia

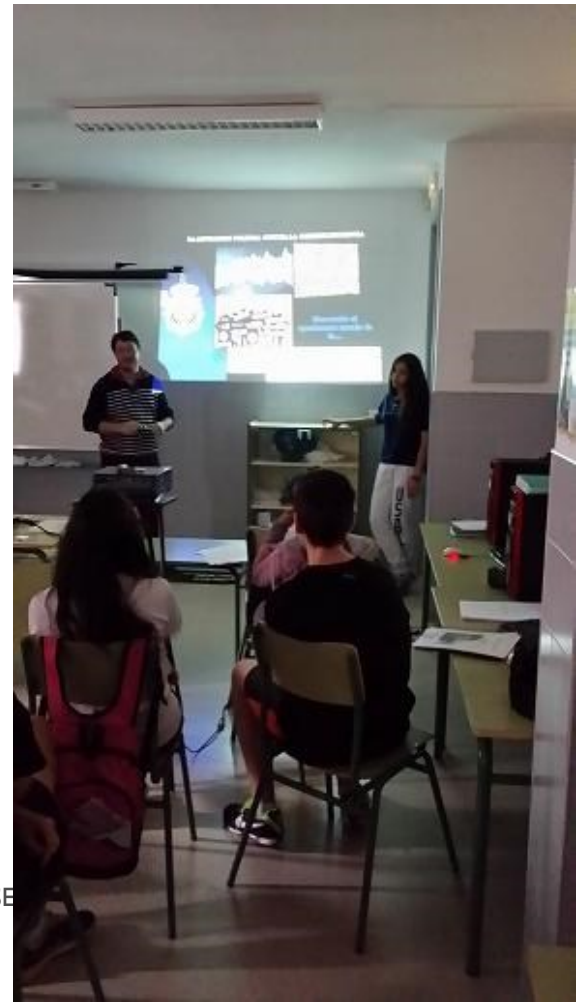
Clasificación de los delitos tecnológicos:

Recursos:

El Tutor dispondrá:

→PPT "***Ponencia CIBERDELINCUENCIA cuerpos y seguridad del estado***".

→Vídeo "***La ciberdelincuencia se pasa a los dispositivos móviles***"



Delitos de falsificación documental

Delitos de injurias y calumnias

Delitos de amenazas y coacciones

Delitos contra la integridad moral

Delitos de apología o incitación a la discriminación

La figura del "Investigador Tecnológico"

Páginas falsas *clickhaking*

Dispositivos móviles y aplicaciones maliciosas.

Consejos preventivos al instalar aplicaciones y con el correo electrónico.

Descripción:

Esta tarea consiste en dar a conocer qué es la ciberdelincuencia y los mecanismos utilizados por los Cuerpos de Seguridad del Estado en esta materia para tratarla.

Destinarios de la actividad:

Alumnos de Secundaria, Bachillerato y ciclos formativos.

Metodología:

El tutor analiza el documento PPT ***Ponencia CIBERDELINCUENCIA cuerpos y seguridad del estado*** (pincha en la imagen para acceder):

→***PPT Ponencia CIBERDELINCUENCIA cuerpos y seguridad del estado***

Pautas de desarrollo:

El tutor iniciará la sesión haciendo un sondeo sobre la reacción de la sociedad ante lo que es la ciberdelincuencia.

No expondrá lo que es, ya que pretendemos saber cuáles son los conocimientos previos de los alumnos; es importante hacer llegar al alumnado que suele haber:

→ rechazo,

→ Desconocimiento

→ conocimiento real o irreal de lo que es.

El tutor tratará de hacer llegar al alumno que hay dos tipos de delitos: contra las personas y contra el patrimonio.

Se proporcionará los siguientes ejemplos para que los alumnos marquen con una x según crean que es un delito contra las personas o contra el patrimonio.

	Delitos contra las personas	Delitos contra el patrimonio
PHISING. *PHARMING.* *SCAM.*		
USO FRAUDULENTO DE TARJETAS *CARDING.* COMPRAS EN INTERNET.		
INJURIAS, CALUMNIAS (ENTRE CONOCIDOS, POLÍTICOS)		
USURPACIÓN ESTADO CIVIL (E-MAIL, BLOGS)		
OTROS: Fraudes Telefonía Cheques falsos Fraudes inmobiliarios…		
DE SECRETOS (ROBOS DATOS, CUENTAS, PERFILES)		
GROOMING Y DELITOS RELATIVOS A LA CORRUPCIÓN Y PROSTITUCIÓN DE MENORES.		

El tutor procederá a poner el PPT de los Cuerpos y Seguridad del Estado "***Ponencia CIBERDELINCUENCIA cuerpos y seguridad del estado***".

Se procederá a reclasificar la tabla anterior sobre los ataques sobre el patrimonio y sobre las personas.

Se prestará especial atención a los consejos que dan las fuerzas de seguridad del estado como medidas preventivas.

Aunque en el PPT está perfectamente definido la nueva tendencia sobre la ciberdelincuencia a través del móvil se procederá al visionado "***La ciberdelincuencia se pasa a los dispositivos móviles***".

El tutor abrirá un debate entre el alumnado sobre la tendencia de lo que está ocurriendo a raíz de lo expuesto en la ponencia.

El alumno indicará la forma de protegerse ante los siguientes supuestos (todas las medidas de protección están expuestas en el PPT).

Delito	Protección preventiva
PHISING PHARMING SCAM.	
DE SECRETOS (ROBOS DATOS, CUENTAS, PERFILES).	
OTROS: Fraudes Telefonía Cheques falsos Fraudes inmobiliarios…	
USO FRAUDULENTO DE TARJETAS. CARDING. COMPRAS EN INTERNET.	
INJURIAS, CALUMNIAS (ENTRE CONOCIDOS, POLÍTICOS).	
GROOMING Y DELITOS RELATIVOS A LA CORRUPCIÓN Y PROSTITUCIÓN DE MENORES	
USURPACIÓN ESTADO CIVIL (E-MAIL, BLOGS)	

Se formarán grupos de tres o cuatro alumnos de forma que se centren en un tipo de delito y que busquen a través de la red (*Youtube* vídeos, webs de información, etc.).

Las webs deben ser determinadas por los alumnos; en el caso de no encontrar nada podemos sugerirles algunos de los enlaces que encontramos en la parte derecha.

Grado de dificultad: Media.

Tiempo destinado al desarrollo: 4 sesiones de tutoría. En ciclos formativos se determinará el módulo más conveniente para hacerlo, por ejemplo, en Sistemas Microinformáticos y Redes el módulo de Seguridad informática.

La última sesión será para que los alumnos realicen **un trabajo de investigación.**

Tiempo de preparación: 2 Horas.

El tiempo de preparación consiste en el visionado del vídeo y del PPT.

→http://staysafeonline.mediaroom.com/index.php?s=43&item=72

→http://www.bbb.org/us/Storage/113/Documents/Cox_BBB_Presentation%20_11_May_10.pdf

→http://ct.bbb.org/article/connecticut-bbb-issues-alert-about-cyber-criminalstargeting-small-businesses-with-malware-attacks-25028

→http://www.nacsonline.com/NACS/News/Daily/Pages/ND0113112.aspx

Experiencia previa en el desarrollo:

Esta tarea se ha llevado a cabo durante los cuatro últimos cursos escolares en la materia de Informática en la ESO, en *Tecnología de la información* en Bachillerato y en el ciclo de grado medio Sistemas Microinformáticos y redes.

Hay que ser muy muy prudentes con lo que se expone que no esté dentro del propio ppt ya que podemos caer en introducir conceptos erróneos. Por ejemplo, hace años les comenté a los alumnos que una forma de garantizar la protección ante búsquedas de acosadores mediante motores en las redes sociales era ponerse una edad de 99 años, nosotros como docentes no podemos decir que los alumnos falseen datos, además es un delito.

Observaciones:

Al alumno no hay que transmitirle que:

No todo lo que hay en la red es malo,

Siempre que hacen clic en una web en me gusta les va a traer consigo un ciberataque,

Es fundamental que las webs a las que accedan sean seguras,

Una web jamás pedirá contraseñas sobre nuestro código de seguridad de nuestra cuenta bancaria,

Una web nunca pedirá contraseñas sobre nuestra red social/mail.

Hay que tratar no llegar a ser extremista, realista sí, pero no rozar límites que lleguen a desconfiar de todo lo que hay en la red.

→http://www.tripwire.com/ponemon-cost-of-compliance/pressKit/True_Cost_of_Compliance_Report.pdf

→http://www.informationweek.com/news/smb/services/showArticle.jhtml?articleID=229219131

→http://www.crn.com/news/cloud/226700149/smb-cloud-spending-to-approach-100-billion-by-2014.htm?itc=refresh

→http://www.eweek.com/c/a/Security/IT-Security-Spending-Expected-to-Increasefor-Enterprises-SMBs-532369/

Evaluación

PARA VALORAR si se ha alcanzado los objetivos a través de las tareas propuestas, se realiza un proceso de autoevaluación, valorando de 1 (poco) a 5 (mucho) los siguientes indicadores:

Indicadores de autoevaluación	Valoración
Entiendo que al publicar contenidos en una red social dejo de ser el propietario de los mismos.	
He analizado las técnicas preventivas y correctivas en el uso de las redes sociales y sabría aplicarlas.	
Concibo qué es el *grooming* y el procedimiento ante estas situaciones.	
He comprendido qué es *sexting* y conozco mecanismos para solventarlo.	
He aprendido qué es el *ciberbullying*.	
Reconozco y diferencio entre el bloqueo social, hostigamiento, manipulación social, coacción, exclusión social, intimidación, y amenazas a la integridad	
Aprecio la responsabilidad de los menores en el uso de las redes sociales	
Conozco la reacción de la sociedad ante la ciberdelincuencia	
He comprendido los principales delitos tecnológicos y páginas pseudofalsas.	
Soy capaz de diversificar entre delitos de falsificación documental, delitos de injurias y calumnias, delitos de amenazas y coacciones, delitos contra la integridad moral y delitos de apología o incitación a la discriminación.	
Me he informado cómo reaccionar ante aplicaciones presuntamente maliciosas *clickhaking*	
He aprendido aplicar mecanismos de prevención en la instalación de aplicaciones y en el uso del correo electrónico.	
Interpreto la respuesta de las fuerzas de seguridad del estado ante la ciberdelincuencia	

Webgrafía

SELECCIONAMOS algunos espacios webs interesantes y muy útiles para los tutores que quieran preparar las sesiones y mantenerse al día en todo lo relativo a las Redes Sociales y su seguridad:

PABLO AVILÉS, Pedro (2014) "***x1red+segura informando y educando***" : http://enocasionesveoreos.blogspot.com.es/2013/05/recension-x1redsegura-informando-y.html

BRIGADA DE INVESTIGACIÓN TECNOLÓGICA DE LA POLICÍA NACIONAL (28/04/2014), "***BIT-Consejos de Seguridad***": http://www.policia.es/org_central/judicial/udef/bit_conse_segurid.html

GRUPO DE DELITOS TELEMÁTICOS, UNIDAD CENTRAL OPERATIVA, GUARDIA CIVIL (28/04/2014), "***Decálogo de navegación segura***": https://www.gdt.guardiacivil.es/webgdt/cusuarios.php

CENTRO REGIONAL DE FORMACIÓN DEL PROFESORADO (01/04/2014), "Escuela de seguridad en Red": http://centroformacionprofesorado.castillalamancha.es/es/web/guest/seguridad

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN (01/04/2014), "INTECO": http://www.inteco.es/

Recursos

ESCUELA DE SEGURIDAD EN LA RED

Dentro de la web del Centro de Formación Regional del Profesorado, encontramos una plataforma dirigida a los docentes de Castilla La Mancha, cuya finalidad es responder de forma rápida y eficaz a los conflictos que surgen en los centros educativos en la aplicación de las nuevas tecnologías.

Tiene un blog donde Carlos Represa (abogado y experto en el tema) pone información sobre la seguridad en Internet, y un foro donde los maestros y profesores exponen sus dudas que Carlos Represa contesta desde el punto de vista legal.

KIDDIA.ORG

Tiene como finalidad responder a necesidades en cuanto a juegos relacionados con las TIC para niños. Contiene recursos para que los profesores usen en sus clases y promuevan un uso seguro de las TIC entre sus alumnos. Su principal objetivo es educar y proteger a los menores en el uso de las nuevas tecnologías.

Tiene distintos apartados diferenciados para adultos y niños/as, además de ofrecer noticias interesantes sobre el uso de las TIC y un apartado dónde profundizar más sobre aspectos concretos. También dispone de un foro con temas diferenciados dependiendo del tipo de usuario (niños/as, padres, madres y profesores).

MATERIALES DIDÁCTICOS CRFP