En este documento se pretende realizar una revisión a las estrategias educativas desarrolladas en el IES Alyanub, desde las que se pretende dar respuesta a algunas de las prácticas nocivas que se pueden presentar en el uso de la tecnología. ***Estas prácticas educativas pretenden insistir en el modelo preventivo*** *.*
Por otro lado se describen actuaciones que el centro tiene definidas para atender un posible caso. Las conductas que se van a tener en cuenta son: Suplantación de personalidad, Ciberacoso, Páginas con contenidos potencialmente peligrosos y Grooming

1. Planes y proyectos que promueven el buen uso de las TIC y la actitud reflexiva ante el uso de la tecnología.
2. Suplantación de personalidad: acciones preventivas. Actuaciones ante un posible caso
3. Ciberacoso: acciones preventivas y actuaciones ante un posible caso
4. Páginas con contenidos peligrosos: acciones preventivas. Actuaciones ante un posible caso.
5. Grooming: acciones preventivas. Actuaciones ante un posible caso.

PLANES Y PROYECTOS QUE PROMUEVEN EL BUEN USO DE LAS TIC Y LA ACTITUD REFLEXIVA ANTE LAS REDES SOCIALES

- **Programa Cibermanagers:** este programa tiene como objetivo específico "Promover entre el alumnado del centro una cultura de autoprotección en la red" (M.ª Ángeles Moreno)

- **Plan Director**: la Guardia Civil viene a charlar con el alumnado sobre seguridad informática. Comenta con ellos casos que han debido atender y tratan de que el alumnado adopte una posición reflexiva respecto a la tecnología (Isabel Parra)

- **POAT:** Plan de Orientación y Acción Tutorial. Incluye, para cuarto de la ESO, una sesión de reflexión sobre la importancia de la figura del Cibermanager en un centro educativo (Isabel Parra)

- **Materias de programación y TIC**. Buena parte del alumnado tiene estas optativas y desde ellas el profesorado de informática tiene la vocación de promover la actitud crítica del alumnado frente a las tecnologías. Además se realizan varias actividades del **INCIBE: In**stituto **N**acional de la **Cibe**rseguridad (Ana Cervantes, Javier Martos, M.ª Ángeles Moreno)

- **Departamento de convivencia**: a través de sus actuaciones promueve la actitud de apertura frente al otro, trabajando específicamente la capacidad de empatía (Ángeles López)

- **Proyecto TIC:** este proyecto se centra en el mantenimiento del Hardware de las diferentes aulas de informática que existen en el centro. Establece relaciones de

colaboración con el alumnado, intentando que entiendan la importancia del cuidado de los materiales (Mariano Romero, Francisco Baraza)

- **Proyecto Formajoven:** tiene como objetivo promover una cultura de la salud entre el alumnado (Marco Ruíz)

SUPLANTACIÓN DE PERSONALIDAD:

La suplantación de identidad es aquella acción por la que una persona se hace pasar por otra para llevar a cabo actividades en su propio beneficio: cometer fraudes, dar de alta servicios, ciberacosar a alguien, difamarle, vender productos falsos...

ACTUACIONES PREVENTIVAS

Trabajamos con el alumnado los siguientes conceptos:

- Utilizar contraseñas robustas.
- Proteger adecuadamente los dispositivos para evitar que se infecten e malware.
- Evitar responder a mensajes de remitentes desconocidos y, en ningún caso, proporcionar datos sensibles: DNI, datos bancarios, contraseñas...
- Realizar compras seguras.
- Usa las redes WiFi públicas o abiertas solo para consultar información, no para proporcionarla.

Actuación del centro ante un posible caso de Suplantación de Personalidad

1. Recomendar que se conserven las evidencias de dicha suplantación como capturas de pantalla o testimonios de otro usuarios de la Red Social utilizada.

2. En función de la gravedad, poner en conocimiento los hechos y solicitar las oportunas medidas cautelares de protección a la Fiscalía, los Cuerpos y Fuerzas de Seguridad del Estado, la Policía Local o las diferentes instancias de seguimiento y control de un buen uso de las tecnologías de la información y la comunicación puestas a disposición de la ciudadanía.

3. Comunicación con terceras personas (amigos/as) que pudieran ser objeto de la confusión en la suplantación del perfil.

4. Implicación, en su caso, de alumnado ciberayudante para proporcionar apoyo, ayuda y seguridad al alumno o alumna.

CIBERACOSO

Se puede definir como una agresión intencional, que puede ser puntual o repetida, por parte de un individuo o un grupo, a través de medios tecnológicos como el correo electrónico, páginas web, redes sociales, juegos online o mensajes en teléfonos móviles, que pueden tener una alta difusión y mantener su impacto en el tiempo sin que la víctima pueda defenderse por sí misma, dañando su imagen social y su autoestima, hasta el punto de llegar a provocar grave daño o perjuicio en su desarrollo psicosocial.

TRABAJO EN PREVENCIÓN:

El trabajo en prevención promueve las siguientes **actuaciones con el alumnado**:

- Hablar con los menores sobre la existencia del grooming. Dependiendo de la edad, pueden utilizarse noticias sobre ciberacoso sexual para abrir el debate.
- Deben ser conscientes de que, cuanta más información sensible o comprometedora compartan (sobre todo gráfica), más expuestos estarán.
- Recomendarles agregar solo a personas que realmente conozcan, no a amigos de amigos.
- Estar atento al uso que otras personas hacen de las imágenes o información del menor.
- Por norma general, los menores de 14 años no deben tener redes sociales y si las tienen deben usarse bajo estricto control de un adulto responsable.
- Seguir las normas de uso del móvil que marca el centro.

*Existe en Andalucía un **Protocolo para casos de Ciberacoso** diseñado por la **Consejería de Educación**. En caso de encontrarse con un caso, el centro deberá realizar las acciones que allí se describen, algunas de las cuales son las siguientes:*

Actuación del centro ante un posible caso de Ciberacoso

1. Recomendar a la alumna o al alumno acosados la disminución del uso del teléfono móvil e Internet, o incluso la suspensión temporal de su utilización, en función del caso y tipo de ciberacoso, que mantenga la información personal que pueda ser sensible en privado y evite responder a posibles provocaciones.

2. Recomendar que se conserven las evidencias del acoso o ataque recibido, y proceda a bloquear al acosador o acosadora, denunciando a los servicios de la red el comportamiento inapropiado.

3. En función de la gravedad, poner en conocimiento los hechos y solicitar las oportunas medidas cautelares de protección a la Fiscalía, los Cuerpos y Fuerzas de Seguridad del Estado, la Policía Local o las diferentes instancias de seguimiento y control de un buen uso de las tecnologías de la información y la comunicación puestas a disposición de la ciudadanía.

4. Implicación, en su caso, de alumnado ciberayudante para proporcionar apoyo, ayuda y seguridad al alumno o alumna objeto del ciberacoso.

5. Incluir el apoyo emocional adulto. Contar con un profesor o profesora que pueda ofrecer al alumno o la alumna víctima del acoso apoyo emocional. Puede ser su tutor o tutora, algún profesional de la orientación o cualquier otro profesor o profesora que pueda cumplir esta función.

6. Establecer medidas cautelares dirigidas al alumno, la alumna, o al grupo de alumnos y alumnas presuntamente acosadores, incluyendo la supervisión o privación temporal del uso del teléfono móvil e Internet, en función del caso y tipo de ciberacoso, que deberán incluirse en el Reglamento de Organización y Funcionamiento y en el Plan de convivencia del centro.

CONTENIDOS POTENCIALMENTE PELIGROSOS

Entendemos por páginas con contenidos potencialmente dañinos aquellos que podrían incentivar conductas problemáticas en quien los ve como aquellos que promueven el consumo de drogas, las autolesiones o lesiones a terceros, los desórdenes alimentarios, las pseudoterapias, la discriminación, la violencia y el odio hacia ciertos colectivos...

TRABAJO EN PREVENCIÓN:

El centro promueve las siguientes **capacidades del alumnado**:

- Desarrollar la capacidad crítica y la alfabetización informacional del menor: debe aprender a contrastar información y a buscar fuentes fiables.
- Evitar compartir este tipo de contenidos ni siquiera cuando nuestro fin sea denunciarlos
- Los tutores/as y el profesorado en general, tratará de establecer con los menores un clima de confianza y diálogo que facilite que, ante posibles incidentes, acudan a nosotros.
- Promover proactivamente que el alumnado conozca las normas de uso del móvil en el centro educativo.

Actuación del centro ante un posible caso de Contenidos Potencialmente Peligrosos

1. Los educadores deberán comunicar de manera inmediata la situación a los padres que serán quienes encaucen la situación del menor.
2. El centro y la familia mantendrán un espacio de colaboración conjunta en el que se seguirán las siguientes recomendaciones:
    i. Vigilar y/o retirar al menor del contacto con los dispositivos, haciéndole ver que no es un castigo.
    ii. Efectuar una revisión total de las páginas que ha estado visitando y de los posibles contactos que haya podido establecer a través de ellas.
    iii. Si la situación es considerada avanzada, buscar ayuda especializada

3. El coordinador TIC del centro asesorará a la familia para que se lleven a cabo las siguientes actuaciones.
    i. Si existe la posibilidad, marcar los contenidos como inapropiados.
    ii. Pedir a la empresa que los aloja que los retire.
    iii. Reportar los contenidos en línea peligrosos a través un formulario que IS4K ha habilitado.

4. El propio centro sopesará poner en conocimiento de asociaciones y ONGs especializadas la existencia de webs que albergan contenidos potencialmente dañinos. Por ejemplo:
    Asociación Contra la Anorexia y la Bulimia de Cataluña
    SOSracismo
    Observatorio español contra la LGBTfobia

GROOMING:

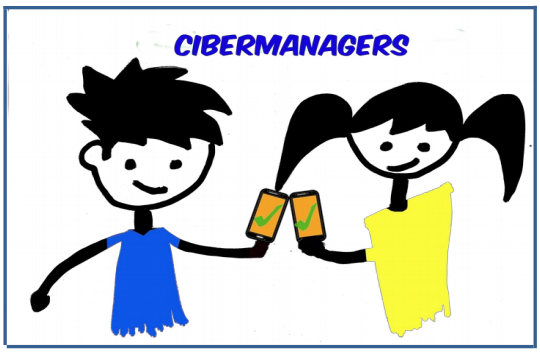
Denominamos grooming al acercamiento por parte de un adulto a un menor con fines

TRABAJO EN PREVENCIÓN:

El centro promueve las siguientes actuaciones con el alumnado:

- Hablar con los menores sobre la existencia del grooming. Dependiendo de la edad, pueden utilizarse noticias sobre ciberacoso sexual para abrir el debate.
- Deben ser conscientes de que, cuanta más información sensible o comprometedora compartan (sobre todo gráfica), más expuestos estarán.
- Recomendarles agregar solo a personas que realmente conozcan, no a amigos de amigos.
- Estar atento al uso que otras personas hacen de las imágenes o información del menor.
- Por norma general, los menores de 14 años no deben tener redes sociales y si las tienen deben usarse bajo estricto control de un adulto responsable.
- Seguir las normas de uso del móvil que marca el centro.

Plan de Orientación y Acción Tutorial



Actuación del centro ante un posible caso de Grooming

Si se sospecha una situación de ciberacoso sexual a un menor por parte de un adulto se debe:

1. Los educadores deberán comunicar de manera inmediata la situación a los padres que serán quienes deban denunciar ante las Fuerzas y Cuerpos de Seguridad del Estado los hechos. Ellos también te pueden ayudar con los siguientes pasos.
2. El centro y la familia mantendrán un espacio de colaboración conjunta en el que se seguirán las siguientes recomendaciones:
    i. Retirar inmediatamente al menor. Se debe evitar que siga manteniendo contacto con el acosador haciéndole entender que no se le está castigando.
    ii. Efectuar una revisión total de los dispositivos en busca de malware.
    iii. Cambiar a continuación todas las claves de acceso.
    iv. No ceder al chantaje en ningún caso.
    v. Buscar ayuda especializada y/o apoyo de otro adulto. Se trata de una situación nueva, delicada y estresante y es importante estar acompañado durante el proceso y tener una guía sobre qué hacer. Se puede encontrar ayuda en sitios como IS4K y la Fundación ANAR.
    vi. Evaluar la certeza de la posesión de material sensible por parte del acosador, la posibilidad de que lleve a cabo sus amenazas y las consecuencias.
    vii. Averiguar en qué situaciones ilícitas ha incurrido o incurre el acosador.
3. El coordinador TIC del centro podrá apoyar técnicamente a las familias en el trabajo de buscar y recopilar pruebas de la actividad delictiva, cuidando de no vulnerar la Ley.

FORMAJOVEN
Promueve Salud