



**UNIDAD
DIDÁCTICA
INTERNET
SEGURO PARA
*ALUMNOS***



UNIDAD DIDÁCTICA: INTERNET SEGURO **PARA ALUMNOS**

Objetivos:

- Promover el uso responsable y seguro de las nuevas tecnologías.
- Comprender los procesos elementales del flujo de información en la red.
- Potenciar la actitud responsable y desarrollar espíritu crítico ante los mensajes que reciben y elaboran.
- Conocer las normas de comportamiento en la red, los riesgos del uso de las tecnologías de la información y la comunicación.
- Utilizar de forma creativa las TIC.
- Adquirir hábitos orientados a la protección de la intimidad y seguridad personal en la interacción en entornos virtuales.
- Conocer páginas de referencia con respecto al ciberacoso y su denuncia.

Contenidos:

- Posibles Riesgos:
 - Amenaza personal a través del ciberacoso: grooming, sexting...
 - Amenazas digitales: virus, troyanos, spyware...
 - Mensajería instantánea y redes sociales
 - Privacidad



- 
- Acceso a contenidos inapropiados
 - Compartir archivos
 - Seguridad en el teléfono móvil
 - Huella digital
 - Herramientas de seguridad
 - Antivirus
 - Actualizaciones
 - Firewall
 - Copias de seguridad
 - Wi-fi seguro
 - Contraseñas seguras
 - Medidas de seguridad
 - Control parental
 - Creación de usuario sin permisos de administrador
 - Historial
 - No permitir detectar ubicación
 - Páginas de confianza: phishing, suplantación de identidad, páginas seguras...
 - Navegación de incógnito
 - Sitios de referencia: www.protegeles.com, www.educa.jcyl.es/es/webs-tematicas/ciberacoso

Metodología:

La organización del proceso de enseñanza debe basarse en una serie de principios metodológicos tales como:

- ✓ Conocimientos previos del alumno
- ✓ Aspectos esenciales que se tratan de enseñar.
- ✓ Interrelación de los contenidos.



- ✓ Aprendizaje personalizado
- ✓ Creatividad
- ✓ Funcionalidad de los aprendizajes.

Estos principios, implican una línea metodológica flexible que debe ser adaptada tanto a la realidad diversa del alumnado, como a los condicionantes de recursos y medios disponibles.

Temporalización:

1. Presentación : “Plan de seguridad y confianza digital en el ámbito educativo”: Día de internet seguro
2. Posibles Riesgos:
 - Amenaza personal a través del ciberacoso: grooming, sexting...
 - Amenazas digitales: virus, troyanos, spyware...
 - Correo electrónico, mensajería instantánea y redes sociales
 - Privacidad
 - Acceso a contenidos inapropiados
 - Compartir archivos
 - Seguridad en el teléfono móvil
 - Huella digital
3. Herramientas de seguridad
 - Antivirus
 - Actualizaciones
 - Firewall
 - Copias de seguridad
 - Wi-fi seguro



- Contraseñas seguras

4. Medidas de seguridad

- Utilización de usuario sin permisos de administrador
- No permitir detectar ubicación
- Páginas de confianza: phishing, suplantación de identidad, páginas seguras...
- En ordenadores no personales: Navegación de incógnito y cerrar sesión
- Sitios de referencia: www.protegeles.com, www.educa.jcyl.es/es/webs-tematicas/ciberacoso

5. Conclusión: uso positivo y creativo de la Red

Actividades:

1. Posibles Riesgos:

- Lluvia de ideas acerca del uso que hacen en casa de internet y de los diferentes dispositivos móviles: teléfono móvil, tablets...
- Qué sabemos acerca del grooming, ciberacoso, sexting...
- A través de una presentación y diferentes videos analizaremos:
 - Amenazas personales a través del ciberacoso: grooming, sexting...
 - Amenazas digitales: virus, troyanos, spyware...
 - Correo electrónico, mensajería instantánea y redes sociales



- Privacidad
- Acceso a contenidos inapropiados
- Compartir archivos
- Seguridad en el teléfono móvil
- Huella digital

2. Herramientas de seguridad

- Propondremos distintas herramientas que propician la seguridad en las TIC:
 - Antivirus
 - Actualizaciones
 - Firewall
 - Copias de seguridad
- Analizaremos cómo fomentar la seguridad en los Wi-fi
- Realizaremos una práctica para crear contraseñas seguras

3. Medidas de seguridad

- Ejemplificaremos:
 - Utilización de usuario sin permisos de administrador
 - Cómo no permitir detectar ubicación
 - Cómo comprobar que navegamos en páginas de confianza
 - En ordenadores no personales: Cómo navegar de incógnito y cerrar sesión
 - Visitar las páginas www.protegeles.com, www.educa.jcyl.es/es/webs-tematicas/ciberacoso y realizar el test de Protégete.



4. Conclusión: uso positivo y creativo de la Red: creación de un muro colaborativo con la herramienta Padlet

Organización tecnológica:

La sesión se realizará en el aula de informática o en aula digital. Dicha aula debe contar, al menos, con ordenadores o minipc con acceso a internet y un videoprojector.

Recursos:

- PDI y videoprojector
- Aula con conexión a internet
- Ordenadores o minipc

Evaluación:

Grado de participación de los asistentes.

Cuestionario sobre los contenidos trabajados.