



**Junta de
Castilla y León**

DIRECCIÓN PROVINCIAL DE EDUCACIÓN
DE SALAMANCA



**UNIDAD
DIDÁCTICA
INTERNET
SEGURO PARA
*FAMILIAS***



UNIDAD DIDÁCTICA: INTERNET SEGURO PARA FAMILIAS

Objetivos:

- Fomentar el uso responsable y seguro de las Tecnologías de la Información y la Comunicación.
- Conocer los riesgos a los que se pueden enfrentar los menores en la Red.
- Conocer puntos de orientación e información sobre seguridad en la red.
- Establecer estrategias para proteger a los menores ante los posibles riesgos derivados del uso de las Tecnologías de la Información y la Comunicación.
- Difundir y fomentar usos, contenidos, aplicaciones y servicios tecnológicos que garanticen una navegación segura.
- Conocer páginas de referencia con respecto al ciberacoso y su denuncia.

Contenidos:

- 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
 - 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 sesión se basará en el tratamiento de aspectos teóricos combinados con ejercicios prácticos.



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...
 - 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
 - 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
5. Conclusión: uso positivo y creativo de la Red

Actividades:

1. Posibles Riesgos:

- Lluvia de ideas acerca del uso que sus hijos hacen en casa de internet y de los diferentes dispositivos móviles: teléfono móvil, tablets...
- Qué sabemos acerca del ciberacoso: grooming, sexting...
- A través de una presentación y diferentes videos analizaremos:
 - Amenazas personales 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

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:
 - Creación de un control parental
 - Creación de usuario sin permisos de administrador
 - Borrar el historial periódicamente
 - Cómo no permitir detectar ubicación
 - Cómo comprobar que navegamos en páginas de confianza
 - Cómo navegar de incógnito
 - Navegación de incógnito
 - Visitar las páginas: www.protegeles.com,
www.educa.jcyl.es/es/webs-tematicas/ciberacoso

4. Conclusión: uso positivo y creativo de la Red

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.

