INTERNET SEGURO
RECOMENDACIONES PARA EDUCADORES

A continuación, ofrecemos una serie de recomendaciones a tener en cuenta por parte de los docentes, cuando realizan actividades educativas enriquecidas con Internet:

- Informe a los estudiantes que el *reglamento de uso de las salas de informática*, de la red escolar y del acceso a Internet, prohíbe expresamente navegar por páginas con contenido inapropiado para menores; explique que no atender esta norma acarreará sanciones. Si no existe reglamento en la Institución Educativa, es de la mayor urgencia establecer uno y divulgarlo. Recomendamos consultar un modelo de reglamento publicado en Eduteka.
- Comunique claramente a los estudiantes que está prohibido descargar cualquier software de Internet, sin la debida autorización y sin la presencia de un(a) docente.
- Cuando sea necesario, permita que se descarguen aplicaciones únicamente desde sitios Web oficiales. Muchos sitios simulan ofrecer programas populares que se alteran, modifican o suplantan por versiones que contienen algún tipo de virus o software malintencionado (malware) y que infectan el computador cuando el usuario lo instala en el sistema.
- Indique a sus estudiantes que eviten hacer clic en enlaces sospechosos. Los enlaces son uno de los medios más utilizados para direccionarlos a páginas Web que tienen amenazas capaces de infectar el computador del usuario con virus o software malintencionado/espía.
- Informe a los estudiantes sobre las responsabilidades civiles, penales o administrativas que existen cuando se vulneran derechos propios o de terceros en la red.
- Asegúrese que los estudiantes son conscientes de que la distribución de contenidos prohibidos por la Ley (en especial la pornografía infantil), el acoso (en especial el acoso sexual), la discriminación, la promoción del odio racial, la difamación y la violencia, entre otros, son ilegales en Internet y en las redes sociales. Estas conductas se castigan con cárcel en la mayoría de los países.
- Evite que los estudiantes ingresen información personal en formularios Web de dudosa procedencia. Cuando un formulario contiene campos con información *sensible* (por ejemplo, usuario y contraseña), es recomendable verificar la legitimidad del sitio.
- Notifique a los estudiantes que se requiere tanto la autorización como la presencia de un(a) docente en la sala de informática para que ellos puedan utilizar Chats, IRC, servicios en línea de comunicación en tiempo real y redes sociales.
- Asegúrese que los estudiantes comprenden que no deben invadir la privacidad de otras personas cuando interactúan con ellas por medio de redes sociales.
- Muchas de las "riñas virtuales" que se convierten en "cyberbullying", se inician porque una de las partes no observa buenas maneras al comunicarse por Internet.

Explique a sus estudiantes las normas básicas de "Netiqueta" y asegúrese que las cumplen cuando se comunican con otras personas.

- Esté atento al comportamiento de los estudiantes cuando utilicen redes sociales en Internet, con el fin de detectar y evitar situaciones de ciberacoso (responsable: menor/adulto; víctima: adulto), de "cyberbullying" (responsable: menor; víctima: menor) o de Grooming (responsable: adulto; víctima: menor).
- Antes de que los estudiantes envíen información a otras personas a través del correo electrónico, mensajería instantánea o redes sociales, promueva el hábito de reflexionar y evaluar la conveniencia de que esas personas conozcan dicha información y los riesgos que esto puede representar para su seguridad personal o familiar.
- Asegúrese que los estudiantes entienden que al participar en redes sociales, existe la posibilidad de encontrarse con personas que no son quienes dicen ser y que desean aprovecharse de otras personas.
- Reflexione con los estudiantes sobre los aspectos positivos del uso de pseudónimos como medio de protección en las redes sociales, mensajería instantánea, chats y foros. Además, sobre el uso responsable de estos pseudónimos que, entre otras cosas, implica no utilizarlos para engañar o confundir a otros.
- Tenga en cuenta que la legislación de algunos países requiere autorización expresa de los padres o acudientes antes de permitir a menores de 13 años participar en actividades educativas en las que se utilice correo electrónico, blogs, wikis, servicios de mensajería instantánea, redes sociales, etc. También hay que solicitar autorización cuando se utilizan servicios en línea que pueden almacenar alguna información sensible acerca de los estudiantes.
- Diseñe y realice un taller para padres en el que se informe a estos los riesgos que corren sus hijos cuando, sin control alguno, navegan en Internet o se comunican con otras personas. Comparta y discuta con ellos la sección "Recomendaciones para padres" (pdf) que encontrará más abajo en este mismo documento.
- Destine un espacio en el currículo de las asignaturas que tiene a su cargo para socializar con los estudiantes las "Recomendaciones para estudiantes" que encontrará más abajo en este documento. Puede descargar el pacto "Me Comprometo a..." (pdf) y realizar una actividad de aula en la que los estudiantes se comprometan a cumplir con todos los puntos del pacto estampando en el documento su firma y pidiéndole a su acudiente que también lo haga. Póngase de acuerdo con otros docentes que también utilizan/integran las TIC en sus procesos educativos para hacerle seguimiento al cumplimiento de este pacto.
- Promueva la inclusión del pacto "Me comprometo a..." (doc), para que haga parte del "Manual de convivencia de la Institución Educativa".
- Conozca y tenga a mano los números telefónicos y las páginas Web de las autoridades de su país, ante las cuales denunciar delitos informáticos.
- Consulte con frecuencia sitios especializados en Internet Seguro para mantenerse al tanto de las últimas amenazas (spam, phishing, fraude electrónico, robo de identidad, etc) y de la forma de prevenirlas.

CRÉDITOS:
Documento producido por el equipo de EDUTEKA con información proveniente de Internet.
Publicación de este documento en EDUTEKA: Octubre 01 de 2010.
Última actualización de este documento: Octubre 01 de 2010.