93683

"Año del buen servicio al ciudadano"

Vitarte, 17 OCT 2017

OFICIO MÚLTIPLE Nº 428 **– 2017 – DIR.UGEL06/J.AGEBRE**

Señor (a):
DIRECTOR(A) DE LAS INSTITUCIONES EDUCATIVAS PÚBLICAS Y PRIVADAS DE LA UGEL 06

Presente.-

ASUNTO : **MEDIDAS DE PREVENCIÓN Y PROTECCIÓN**

REFERENCIA : Reglamento de la Ley Nº 28119, modificada por la Ley Nº 29139
Ley que prohíbe el acceso de menores de edad a páginas web de contenido pornográfico y a cualquier otra forma de comunicación en Red de Igual contenido.

Es grato dirigirme a Usted para expresarle mi cordial saludo y a la vez solicitarles que adopten las medidas de prevención y protección; sobre el acceso de menores de edad a páginas web de contenido pornográfico y a cualquier otra forma de comunicación en red de igual contenido; que puedan dañar la integridad de los estudiantes; teniendo en cuenta que los niños y adolescentes son los más vulnerables a ser víctimas de delitos y agresiones por internet.

En tal sentido resulta de suma urgencia utilizar estrategias adecuadas que permitan que los estudiantes desarrollen habilidades para identificar, evitar y defenderse de los peligros y amenazas que se les puedan presentar cuando navegan por Internet y cuando interactúan a través de las redes sociales.

Por lo tanto debe:

- Encargar al docente del aula AIP/CRT/CIST; desarrollar un Plan de acción frente a los peligros que pueden estar expuestos los estudiantes con el uso inapropiado y sin control de las páginas de Internet tanto dentro como fuera de la Institución Educativa.
- Instalar y/o actualizar, en todos los equipos de cómputo de su institución educativa, un software especial de filtro; que tenga como efecto impedir la visualización de páginas Web de contenido y/o información pornográfica.

Se adjunta al presente en anexo las recomendaciones a los docentes, estudiantes y a padres de familia que puede utilizar y difundir.

Sin otro particular, le reitero las muestras de mi especial consideración y deferencia personal.

Atentamente,

MINISTERIO DE EDUCACIÓN – Unidad de Gestión Educativa Local N° 06 – DIRECCIÓN – ATE

Dra. MARIA ALEJANDRINA MILAGROS RAMIREZ BACA
DIRECTORA DE LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL N° 06 – VITARTE

MINISTERIO DE EDUCACIÓN – AGEBRE – UGEL N° 06 – JEFATURA – ATE VITARTE

MAMRB/DIR UGEL 06
AMRB/J AGEBRE
FDMAC/E. AGEBRE.

"Año del buen servicio al ciudadano"

ANEXO

RECOMENDACIONES PARA DOCENTES

- Informe a los estudiantes el reglamento del uso de las salas de informática, de la red escolar y del acceso a Internet. Si no existe reglamento en la Institución Educativa, es de mayor urgencia establecer uno y divulgarlo.
- 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 sean 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.
- 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.
- Asegúrese que los estudiantes comprenden que no deben invadir la privacidad de otras personas cuando interactúan con ellas por medio de redes sociales.
- 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.
- 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.
- Y otros que Ud. crea conveniente.

MINISTERIO DE EDUCACIÓN AGEBRE FATURA VITARTE

"Año del buen servicio al ciudadano"

RECOMENDACIONES PARA ESTUDIANTES

- No dar nunca, a personas que no conozca de manera presencial, su información personal (dirección particular, número de teléfono, etc), de la Institución Educativa (nombre, ubicación, etc) o de su familia (nombres de padres y hermanos, etc).
- Respetar la información que se tiene de los compañeros de clase y no publicarla en Internet sin su autorización.
- No revelar nunca a nadie, que no sean sus padres (ni siquiera a sus mejores amigos), claves de acceso al correo electrónico y a las redes sociales . Esto evitará que sean suplantados.
- Utilizar contraseñas fuertes, difíciles de adivinar, con longitud de al menos 8 caracteres, que incluyan la combinación de números y letras.
- Cerrar completamente tanto cuentas de correo electrónico como de redes sociales cuando termine de utilizar el computador.
- No enviar nunca sus fotografías o de familiares, sin el permiso de los padres.
- Informar a sus padres y profesores cuando encuentren información que me les haga sentir incómodo(a) y/o amenazado(a).
- No realizar procedimientos en Internet que cuesten dinero, sin el permiso de sus padres.
- Nunca contestar a mensajes que sean agresivos, obscenos, amenazantes o que le hagan sentir mal o amenazado.
- No responder correos electrónicos de personas que no conozcas personalmente.
- Avisar a tus padres y profesores cuando alguien te ofrezca un regalo y te dé una dirección a la que debas ir para recibirlo.
- No aceptar citas de desconocidos y avisar inmediatamente a tus padres y profesores. Siempre recuerda que hay personas que no siempre son lo que dicen ser.
- Desconfiar de aquellas personas que recién conozcas y que quieren verte por medio de la cámara Web del computador o que encienden su cámara sin que lo hayan solicitado.
- Cuídate en los ambientes tecnológicos como lo harías cuando sales a la calle.
- Aceptar solicitudes de amistad en redes sociales que provengan únicamente de personas conocidas.
- No utilizar, en las redes sociales en las que participas, identidades falsas para suplantar personas.
- Nunca descargar, instalar o copiar nada de Internet sin el permiso previo de padres o docentes.
- Y otras que Ud. Crea por conveniente.

MINISTERIO DE EDUCACIÓN AGEBRE UGEL N.06 JEFATURA ATE VITARTE

"Año del buen servicio al ciudadano"

RECOMENDACIONES PARA PADRES

- De a sus hijos buen ejemplo cuando navegue por Internet y cuando se relacione en redes sociales con otras personas.
- Hable frecuente y abiertamente con sus hijos sobre posibles riesgos que existen en Internet.
- Acompañe a sus hijos a navegar en Internet; conozca y evalúe cuáles son sus sitios favoritos y las redes sociales en las que participan.
- Ubique el computador en áreas comunes del hogar (estudio, sala, etc). Para un delincuente resulta más difícil comunicarse con un menor cuando el computador está en un lugar a la vista de todos los que habitan el hogar.
- Cuando sus hijos utilicen en casa un computador con cámara Web, adviértales que dicha cámara solo se debe usar en comunicaciones con personas conocidas.
- Tenga en cuenta que cuando los menores son objeto de ciberacoso, "cyberbullying" o de Grooming, casi nunca lo manifiestan voluntariamente. Por lo regular guardan silencio sobre este problema, haciendo que esta práctica sea muy difícil de detectar y eliminar.
- Muestre a sus hijos cómo respetar a los demás cuando se usa Internet y asegúrese de que comprendan que las reglas del buen comportamiento no cambian respecto a las presenciales, sólo porque estén frente a un computador.
- Elabore un reglamento con normas claras para el uso de Internet en el hogar (horario, duración de la conexión, forma de uso) y comuníquelo a sus hijos. Además, vigile su cumplimiento. Recomendamos consultar el "Contrato de código de conducta en línea" propuesto por Microsoft.
- Asegúrese que la conexión a Internet de su hogar es segura, especialmente si es inalámbrica. Protéjala siempre con una contraseña fuerte; de lo contrario, cualquier vecino se puede conectar a través de ella, restándole velocidad de navegación.
- Si instala un router inalámbrico para tener acceso a Internet en el hogar, ubíquelo en un sitio al cual tengan acceso en todo momento personas adultas. De esta forma es más fácil controlar los horarios de acceso a la red ya que con solo desconectar el aparato de la fuente de energía, cesa el acceso a Internet.
- Si sus hijos visitan salas de chat, utilizan programas de mensajería instantánea (como Messenger), videojuegos en línea u otras actividades en Internet que requieran un nombre de usuario para identificarse, ayúdeles a elegirlo y asegúrese de que dicho nombre no revela ninguna información personal.
- Manténgase informado tanto de las últimas amenazas como de las herramientas informáticas para contrarrestarlas.
- Enseñe a sus hijos, desde pequeños, a usar las TIC con responsabilidad.
- Y otras que Ud. Crea por conveniente.

MINISTERIO DE EDUCACIÓN AGEBRE UGEL N° 06 JEFATURA ATE VITARTE