

DOCENTE: DIANA SOFIA MUÑOZ Q.

COMPETENCIAS PLANEACION DEL PERIODO

Selecciono y utilizo eficientemente, en el ámbito personal y social, artefactos, productos, servicios, procesos y sistemas tecnológicos teniendo en cuenta su funcionamiento, potencialidades y limitaciones.

CONTENIDO TEMATICO

Las Tics y sus ventajas

ACTIVIDADES DE APRENDIZAJE



ACTIVIDAD 1:

Taller (en el cuaderno, para entregar) Después de haber leído el texto:

1. Haga una lista de palabras desconocidas.
2. Escriba una definición de pornografía infantil (REDACTE con sus propias palabras)
3. Como nos afecta.
4. Qué relación tiene la pornografía con internet.
5. Que recomendaciones daría para el uso adecuado de internet. Explique cada uno.
6. En donde podemos encontrar peligro o uso inadecuado de internet. Explique cada uno.
7. Explique las normas que se deben seguir para el uso de internet.
8. Qué tipo de sanciones hay para este tipo practicas o actos pornográficos.
9. Qué haría usted si se encontrara en una situación de estas. Explique
10. En una hoja haga una representación por medio de la técnica de VISUAL THINKING sobre la pornografía infantil en internet.
11. Haga una breve conclusión sobre el tema.

EXPLORACION SEXUAL INFANTIL

Es la situación en la cual una persona menor de edad es obligada o manipulada para ejecutar actos que involucran su cuerpo, para satisfacer deseos sexuales de otras personas, con o sin remuneración por ello. Esto comprende: La prostitución, la pornografía infantil, el turismo sexual, la venta y tráfico de niños y niñas.

Un caso especial y el cual nos toca más directamente como usuarios de la Red es la “pornografía infantil por Internet”; que es la creación, reproducción o transmisión de imágenes de menores de edad involucrados en actividades sexuales.

¿CÓMO NOS AFECTA? ¿CÓMO SE RELACIONA CON INTERNET?

Estos actos violan los derechos fundamentales de los niños, manipulando o atropellando su voluntad y dignidad. El daño que el abuso sexual puede causar en un niño es de extrema gravedad. Si, además, el abuso ha sido captado mediante una imagen pornográfica, el abuso original se ve a la vez agravado y magnificado. La tecnología permite que las imágenes sean digitalizadas y almacenadas en computadoras con gran facilidad. El hecho es que dichas imágenes se convierten entonces en registros imborrables de abusos. Por esto, la pornografía infantil es una de las principales y más aberrantes violaciones de los derechos de los niños. La llegada de Internet, unida a otros avances tecnológicos, ha facilitado un salto enorme tanto en el volumen como en la naturaleza de la pornografía infantil disponible. Internet no sólo actúa como mecanismo para crear, exhibir, comercializar y distribuir pornografía infantil, sino que también sirve de vehículo para que pornógrafos infantiles establezcan contacto con nuevas víctimas y las engañen. Cada día más y más niños acceden a Internet, una herramienta que debe ser supervisada por los padres, ya que les ofrece diversión y educación, pero que también los expone a información peligrosa. La mayoría de los padres advierten a sus hijos que no hablen con extraños, que no abran la puerta a un desconocido y que no den información a cualquiera que llame por teléfono, controlan adónde van a jugar, cuáles programas de televisión deben de ver y los libros y revistas que ellos leen. Sin embargo, frecuentemente no se dan cuenta de que el mismo nivel de supervisión y orientación se debe tener para el uso de Internet. En la red es fácil tener acceso a páginas que no son apropiadas para niños, la mejor forma de evitar que ellos las consulten, más allá de la tecnología, es brindándoles una correcta orientación. Estas son algunas recomendaciones que se pueden dar a los niños cuando naveguen en Internet:

- No dar información personal ni enviar fotografías.
- No responder a mensajes que sean agresivos, obscenos o amenazantes.
- Tener cuidado cuando alguien les ofrezca algo en Internet y/o les dé una dirección para reclamarlo.
- Recordar que la gente que navega por Internet no siempre es lo que parece, porque no puede ser vista ni oída.
- Usar buenas palabras y ser decente en chats y conversaciones en línea.

Hay que recordar que depende de los padres de familia y los mayores de edad que los niños puedan crecer felices y tener una infancia tranquila, para que en un futuro sean las personas de bien que construyan una mejor sociedad. Advértalos para que tengan cuidado, no para que tengan miedo. La escuela debe ser una buena influencia para los niños, lo que se consigue con una buena relación de los educadores con sus alumnos, entendiendo lo que están viviendo, aceptándolos con todas sus características sin condenarlos ni rechazarlos y con un buen dialogo regular.

¿A qué puede conducir, el uso inadecuado del Internet a niños(a) y jóvenes?

El uso inadecuado del Internet, puede conducir a los niños(a) y jóvenes, a ser víctimas de la explotación sexual, de la pornografía, del proxenetismo, del turismo sexual, del abuso sexual y físico, y del tráfico de personas. “Que hieren y lastiman la dignidad de los niños(a) y jóvenes de nuestra sociedad, causándoles daños sicológicos y físicos irreparables o difíciles de reparar”.

¿En dónde se pueden encontrar actos abusivos en el uso y aprovechamiento de las redes globales de información?

Ejemplos de actos abusivos cuya comisión se realiza mediante utilización de diversas tecnologías y herramientas informáticas:

- Páginas Web o páginas electrónicas a través de las cuales se divulga material pornográfico o en las que se alojan imágenes, textos, documentos o archivos audiovisuales que implican directa o indirectamente actividades sexuales con menores de edad. Se presentan en servicios de alojamiento (hosting), tanto contratados como gratuitos.
- Correo Electrónico: Se emplea para distribuir contenidos de pornografía infantil y para divulgar contenidos pornográficos de cualquier tipo, que pueden recibir menores de edad. Frecuentemente son utilizados como medio para la comisión de crímenes sexuales con menores.
- Salas de Encuentro o “Chat rooms”: Se utilizan para divulgar pornografía infantil u obtener información de contenido sexual explícito. Constituye además medio para obtener datos de menores (nombres, direcciones, teléfonos, fotografías) con el fin de lograr contacto personal que permita la comisión de actos abusivos.
- Grupo de Noticias (newsgroups): En ellos se puede obtener y compartir información sobre intereses particulares. Son propicios para distribuir pornografía infantil y divulgar direcciones de páginas web de contenido pornográfico.
- Videos: Archivos o cámaras web con escenas y fotografías de pornografía infantil, obtenidas a través de Internet.
- Telefonía: Ofrecimiento de servicios sexuales o distribución de material pornográfico infantil por medio de líneas telefónicas publicitarias mediante periódicos o revistas de amplia circulación.
- Redes Privadas de Información: Se emplean para distribuir material pornográfico con menores.

En Colombia, el Ministerio de Comunicaciones ha publicado una página en Internet llamada “dignidad infantil” (<http://www.conekto.com.co/dignidad-infantil/>), la cual busca informar y orientar a menores de edad, padres de familia y educadores acerca de la explotación sexual infantil, también ahí se podrán hacer las denuncias de casos de explotación sexual infantil, ya sea a través de esa misma página o en el teléfono que el ministerio a puesto a disposición para ello: 01800 09 12667

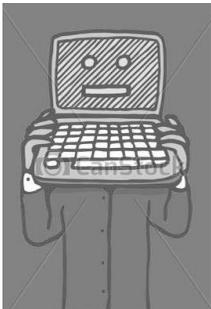
NORMAS BÁSICAS A SEGUIR POR PARTE DE LOS USUARIOS DE INTERNET.

Padres y Educadores:

- Aprender el funcionamiento básico de computadores e Internet.
- Conocer siempre lo que hijos y alumnos hacen en el computador.
- Ubicar el computador con conexión a Internet en lugares o habitaciones donde suela haber otras personas.
- No situarlos en las habitaciones de los menores, donde no es fácil saber qué están haciendo.
- Vigilar el tiempo que menores y alumnos pasan conectados y establecer tiempos.
- Limitar el acceso a áreas específicas con programas protectores o filtros.
- En el caso de niños pequeños, no debe permitírseles entrar en “Chats” o canales de conversación, sin la presencia de adultos.
- Leer los mensajes recibidos por hijos y alumnos de desconocidos.
- Controlar las facturas de teléfono y de otros medios de acceso a Internet.
- No permitir citas, reuniones o entrevistas con personas conocidas por los menores a través de Internet, especialmente si han recibido o enviado fotografías.
- Animar a los hijos y alumnos a contar cualquier información extraña o amenazadora enviada o encontrada a través de Internet.
- Denunciar a las autoridades cualquier información o conducta presumiblemente delictiva o peligrosa.
- El maestro responsable del aula de informática debe revisar periódicamente las paginas consultadas.
- La Institución Escolar debe llevar el registro de los usuarios de los equipos y el tiempo que le dedican.
- Se deben implementar controles que restrinjan el acceso a las páginas detectadas con contenidos de pornografía, violencia y en general temas que lesionen el desarrollo integral de los niños y niñas.
- Establecer las políticas de contenido de los exploradores (browsers) en nivel 0, para temas de sexo, violencia y desnudez.

Menores

- No suministrar nunca información personal ni de colegio o casa, a menos que reciba autorización expresa de padres o tutores.
- No enviar fotografías, detalles de tarjetas de crédito o datos bancarios de la familia.
- No revelar a nadie su clave de ingreso a la red
- No hacer arreglos para celebrar encuentros personales con nadie, sin consultarlo con los padres y lograr que éstos los acompañen y que sea siempre en lugares públicos.

	<p>☒ No responder nunca en los cuartos de Conversación en Internet (“Chat”) frases o anuncios en los que se incluyan mensajes agresivos, obscenos, amenazantes o que los hagan sentir mal y no responder mensajes de correo electrónico desagradables, sugestivos o groseros.</p> <p>☒ <i>No aceptar cosas por nada en Internet, ni asistir a direcciones para reclamar regalos, salvo que sea con la participación de los padres.</i></p> <p>☒ <i>Comentar a padres o maestros siempre que se reciba información o fotografías que generen incomodidad. Las personas que navegan por Internet no siempre son lo que parecen, ya que no se pueden ver ni oír.</i></p> <p>☒ <i>Conocer a los amigos de Internet en la misma forma que se conocen a los demás, y no permitirles nada que no les permitiría a los actuales amigos.</i></p> <p>Sanciones</p> <p>Actos Sexuales con menor de 14 años: (C.P. Art. 209). El que realizare actos sexuales diversos del acceso carnal con persona menor de catorce (14) años o en su presencia, o la induzca a prácticas sexuales, incurrirá en prisión de tres (3) a cinco (5) años.” “Si el agente realizare cualquiera de las conductas descritas en este artículo con personas menores de catorce (14) años por medios virtuales, utilizando redes globales de información, incurrirá en las penas correspondientes disminuidas en una tercera parte.” Utilización o facilitación de medios de comunicación para ofrecer servicios sexuales de menores: (C.P. Art. 219 A). El que utilice o facilite el correo tradicional, las redes globales de información o cualquier otro medio de comunicación para obtener contacto sexual con menores de dieciocho (18) años, o para ofrecer servicios sexuales con éstos, incurrirá en pena de prisión de cinco (5) a diez (10) años, y multa de cincuenta (50) a cien (100) salarios mínimos legales mensuales vigentes (SMLMV).” “Las penas señaladas en el inciso anterior aumentarán en la mitad (1/2) cuando las conductas se realizaren con menores de doce (12) años.”</p>										
 <p>ACTIVIDAD 2:</p> <ol style="list-style-type: none"> ¿Qué es lo que llamamos Usurpación de la identidad? ¿Cómo se produce? (Poniendo ejemplos concretos, si es posible con casos conocidos por tí) ¿Cómo se sentirán las personas a las que les ocurre? ¿Cómo se puede evitar? ¿Qué harías para ayudar a un compañero o compañera que lo sufre? ¿Qué les puedes ocurrir a las personas que lo hacen? 	<p style="text-align: center;">USURPACION DE LA IDENTIDAD</p> <p>La identidad es identificación. Mi identidad me "identifica", Mi identidad es la forma personal de ser único es el reconocimiento que socialmente tiene cada persona. Todos los individuos tenemos nuestra propia identidad A este concepto clásico y sabido de identidad en el siglo XXI le debemos unir la identidad en la sociedad digital. De esta unión resultan tres tipos de identidades en cualquier persona:</p> <p>La técnica (IP, user agent, geolocalización del dispositivo,) La identidad social (mail, nickname, teléfono virtual, perfiles en redes sociales...) La identidad analógica, la que aparece en el DNI (nombres, apellidos y número de identificación).</p> <p>La usurpación de la identidad es un riesgo cada vez más frecuente en Internet. Las dos formas principales de usurpación son: Entrar en la cuenta de otra persona para recabar información personal como fotos, desprestigiar a la otra persona (casos de ciberbullying), amenazas, robo de información, borrado de datos, etc... Este método se da con bastante frecuencia entre los adolescentes. Crear una cuenta haciéndose pasar por otra persona, es un caso muy frecuente para suplantar a gente famosa.</p> <p style="text-align: center;">ALGUNOS SENCILLOS CONSEJOS PARA PREVENIR LA SUPLANTACIÓN DE LA IDENTIDAD EN INTERNET</p> <ol style="list-style-type: none"> Nunca des tus contraseñas a NADIE. Y evita que cuando las introduces te miren. Utiliza contraseñas seguras. Ten cuenta lo que nos cuenta este artículo de 20minutos.es: Con contraseñas como "password", "123456", "qwerty" o "abc123", muchos "piratas" informáticos deben estar encantados de poder acceder a cuentas de correo, páginas privadas y contenidos poco protegidos. Éstas son las contraseñas más imprudentes que no deberíamos utilizar nunca: <table border="0" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding-right: 20px;">Password</td> <td style="padding-right: 20px;">123456</td> <td style="padding-right: 20px;">qwerty</td> <td style="padding-right: 20px;">abc123</td> <td>letmein</td> </tr> <tr> <td>Monkey</td> <td>myspace1</td> <td>password1</td> <td>blink182</td> <td>(tu nombre)</td> </tr> </table> <p><i>Fuente : http://www.20minutos.es/noticia/228488/0/claves/comunes/internet/</i></p> Gestiona correctamente las sesiones (sobre todo en ordenadores públicos): - No almacenes las contraseñas. - Cierra las sesiones. 	Password	123456	qwerty	abc123	letmein	Monkey	myspace1	password1	blink182	(tu nombre)
Password	123456	qwerty	abc123	letmein							
Monkey	myspace1	password1	blink182	(tu nombre)							

<p>7. ¿Qué es la Usurpación de identidad?</p> <p>8. Realice un folleto que promueva la prevención y cuidado hacia la usurpación y el robo de datos digitales.</p>	<p>4. Si descubres que han entrado a tu cuenta, cambia rápido la contraseña. Si ya no puedes, denúncialo.</p> <p>5. Si alguien se hace pasar por ti creando una cuenta similar a la tuya: denúncialo.</p> <p style="text-align: center;">CÓMO ACTUAR EN CASOS DE SUPLANTACIÓN DE IDENTIDAD:</p> <p>Si detectas que te han entrado a tu cuenta, lo primero que tienes que hacer es cambiar la contraseña y, en la medida de lo posible, tratar de deshacer todo lo que ha realizado el agresor en nuestro nombre.</p> <p>Una vez detectada la usurpación, hay que denunciarlo ante la red o las autoridades.</p> <p>Si la persona que ha realizado la usurpación puede haber actuado o usado fraudulentamente el nombre y los datos del afectado poniendo a éste en situaciones legales muy peligrosas; en esos casos es prioritario denunciar los hechos ante las Fuerzas y Cuerpos de Seguridad del Estado con el fin de que quede constancia de que la identidad ha sido suplantada y no puedan atribuirle a él los hechos cometidos por el infractor.</p> <p>Es recomendable ponerse en contacto con el administrador de la página web o red social para que elimine de forma inmediata el perfil infractor o devuelva su control al verdadero titular. En algunos casos, ponerse en contacto con el suplantador para terminar la suplantación de una forma menos agresiva también puede acelerar el proceso.</p> <p>En caso de que la vía judicial sea necesaria u oportuna, es recomendable levantar acta de presencia notarial de los contenidos infractores antes de solicitar su retirada.</p> <p>Si alguien se hace pasar por otra persona o por una empresa mediante perfiles falsos en redes sociales o servicios de internet está suplantando su identidad. En este caso, el delincuente busca crear un daño permanente en la imagen de su víctima, robar información personal de sus contactos o ganar la confianza de sus amigos o socios de negocios para realizar estafas y robos.</p> <p style="text-align: center;">SPOOFING</p> <p>Este término hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.</p> <ul style="list-style-type: none"> • No dé información personal o comercial en encuestas telefónicas o electrónicas. • Evite ingresar su nombre de usuario y contraseñas en vínculos que reciba por correo electrónico. Podría ser víctima de phishing. • Recuerde que sus contraseñas son privadas, no las comparta con nadie y cámbielas frecuentemente. • Antes de hacer transacciones en línea, asegúrese de que la página en que se encuentra es segura: revise que la dirección inicie con https:// y termine con un candado pequeño. • Cierre siempre las sesiones (de correos, redes sociales o transacciones), sin importar si usó un computador personal o computadores compartidos. • Recuerde que, si tiene archivos o información privada en su computador o teléfono celular, puede proteger su acceso (para visibilización o copia) por medio de contraseñas. • Cuide los documentos que tengan su firma, tanto en tinta como digital. Si tiene firma digital, evite que otros tengan acceso a ella. <p style="text-align: center;">TIPS</p> <p>Si descubre que alguien está suplantando su identidad Denuncie este hecho en la red social donde sucede, a través de sus canales de denuncia. Ellos desactivarán los perfiles falsos.</p> <p>Denuncie el hecho a través del CAI Virtual de la Policía Nacional.</p> <p>En lo posible, cuénteles lo que pasa a su red de contactos y amigos para evitar que sean estafados.</p>
<p>PRODUCTOS A ENTREGAR</p>	<p>Deben consignar la información en el cuaderno. Tomar fotografía y enviarla para ser evaluada en google classrom https://classroom.google.com/h con el código dpg54my o envía la evidencia como fotografía al correo de la docente: sofiagurtecnologia@gmail.com, si tienes alguna duda puedes preguntar en el grupo de whatsapp del curso. LOS CRITERIOS DE EVALUACION ESTAN EN LA PAGINA WEB DEL COLEGIO. EN EL LINK Guías de trabajo en el área de Informática.</p>
<p>EVALUACIÓN</p>	<p>Se evaluará el desempeño, la creatividad, organización y presentación de la información, la autenticidad, la puntualidad, la presentación de la actividad.</p>
<p>RECURSOS</p>	<p>Guía didáctica, cuaderno, computadores, internet, blog de tecnología: Nota: Esta guía también la encontrarás publicada en la página del colegio www.iedgur.edu.co</p>
<p>REFERENCIAS</p>	<p>http://www.dignidadinfantil.gov.co http://www.funrestrepobarco.org.co/ http://www.anesvad.org/nuestros_retos/explotacion_sexual/america/e_am_co.htm http://www.elamoresmasfuerte.com/2acciones/0denuncias.htm http://www.fundacionrenacer.org/explotacion.html</p>