Marzo 2021

PLAN DE ACTUACIÓN DIGITAL

PROTOCOLO PARA EL BUEN USO DE LAS TIC Y TAC

Junta de Andalucía

C.E.I.P. SAN JOSÉ ARTESANO | TORREBLASCOPEDRO

PROTOCOLO PARA EL BUEN USO DE LAS TIC Y TAC

INDICE:

I. INTRODUCCIÓN.

El uso de las Tecnologías de la información y comunicación (TIC) y de internet, son hoy día un instrumento esencial para el desarrollo de nuestro Proyecto Educativo.

Por tanto facilitar el acceso a internet al alumnado como medio educativo en un contexto de seguridad, poniendo las medidas necesarias de prevención y fomentando el acceso a la información y cultura es una responsabilidad de profesores y familias. Pues la buena formación de los menores dependerá de saber desenvolverse con fluidez aprovechando las virtudes de las tic pero también conociendo y previniendo y peligros que pueden tener.

II.- FINES DEL PROTOCOLO

1. Concienciar al alumnado, familias y profesorado en el uso adecuado de internet y las TIC.
2. Prevenir los riesgos que implica el acceso indiscriminado a contenidos inapropiados, ilícitos o lesivos.
3. Promover el acceso seguro a Internet y las Tic.
4. Aprovechar los recursos de internet para el acceso al conocimiento, desarrollo social y divertimento personal como complemento a su formación académica, cultural.

III.- MEDIDAS GENERALES PARA PROMOVER EL BUEN USO DE INTERNET EN CENTROS EDUCATIVOS.

Todas las medidas que se tomen en el centro irán encauzadas a preservar los derechos del menor a la intimidad, confidencialidad y protección de datos.

Siendo las personas responsables en la atención de la educativa del menor (familia o profesorado) en ese momento las que deberán orientar, educar y acorar con ellos los un uso responsable de internet y tic aspectos como el tiempo de utilización, páginas que se pueden o no visitar o información que no deben proporcionar, con el objeto de protegerles de mensajes y situaciones perjudiciales

1. Dar a conocer a todos los miembros este protocolo.
2. La información y diálogo continuo con el alumnado y las familias.
3. Elegir un delegado de protección de datos.
4. Pedir autorización a familias para la publicación de imágenes del alumnado con fines educativos.

5. Diseñar desde los diferentes programas educativos actividades, talleres, folletos… que sirvan de sensibilización sobre la responsabilidad del buen uso de internet y tic y desarrollo de valores positivos.
6. Teniendo claros los rolles que cada uno (tutores o profesor. a) tiene en el proceso de enseñanza aprendizaje del alumnado.
7. Promoviendo el uso de sistemas de seguridad y filtrado de contenidos inapropiados para proteger al menor.
8. Colaborando con otras Administraciones manteniendo comunicación fluida y aprovechando actividades, guías, talleres… que nos puedan ofertar (programa director…).

IV.- NORMAS DE USO DE LAS TIC PARA TODOS LOS MIEMBROS DE LA COMUNIDAD EDUCATIVA.

4.1-Alumnado:

1. Hacer caso de las indicaciones de uso que haga el profesorado.
2. Cuidado y mantenimiento de los dispositivos que utilizan en el centro.
3. Comunicar cualquier anomalía en el funcionamiento del tic.
4. Usar la red con una finalidad formativa evitando páginas de **contenido inapropiados e ilícitos*.**
5. No suplantar la identidad de nadie en la red.
6. Controlar el tiempo que se conecta a cualquier dispositivo (ordenador, tablet, móvil...)
7. Ser prudentes y no dar datos personales (información, contraseñas, claves…) ni concertar citas con personas desconocidas a través de internet.
8. Sólo se podrán utilizar en horario escolar dispositivos autorizados por el centro. Siendo esto motivo de sanción.
9. No realizar difusión de información, audios, videos, ni fotografías de alumnado, profesorado o personal laboral dentro del recinto escolar o en actividades extraescolares sin autorización.
10. Saber que existe el derecho a la privacidad personal y que no pueden publicar sus datos sin su consentimiento o de su familia al ser menores.
11. Saber que pueden pedir ayuda al profesorado y familias si algo consideran peligroso, para su seguridad, para poder denunciarlo a las autoridades.

4.2.- Familia:

1. Estar al día en el uso de internet y nuevas tecnologías, a fin de ayudar a sus hijos.as, estableciendo unas normas claras de uso, horario para tareas escolares y ocio adecuado.

2. Controlar que el menor haga una navegación en red adecuada y saludable.
3. Enseñar a usar motores de búsqueda y contrastar varia fuentes de información.
4. Instalar si es necesario filtros de contenidos.
5. Coordinarse y colaborar en la realización de tareas con el profesorado.
6. Favorecer el diálogo con los hijos.as sobre su vida digital, páginas que visita, redes… y sus riesgos .Es importante que el menor sienta confianza plena para contarles cuando sienta algo extraño o alguien le incomode en las redes.
7. Mantener entrevistas periódicas con el tutor. a para estar informados del proceso enseñanza aprendizaje.
8. En caso de incidencias o conductas inadecuadas, colaborar con el centro.
9. Cuidar los dispositivos que puedan dejárseles desde el centro, evitando peligros físicos, ponerlos en lugares peligrosos o instalándole software no oficial distinto del que tiene.
10. Transmitir valores de respeto hacia todos los miembros de la Comunidad Educativa, transmitiendo a sus hijos e hijas que las faltas de respeto a través de cualquier medio de internet tiene el mismo valor y consecuencias que la vida real.
11. Enseñarle en qué consiste la privacidad, que los datos personales son información sensible y que antes de registrarse en cualquier página o aplicación deben consultarlo con la familia.
12. Cuidar de la postura respecto al ordenador siguiendo las siguiente pautas:
    - Los ojos deben estar situados enfrente de la pantalla, a una distancia mínima del doble de la pantalla.
    - La espalda recta, y reposada en zona lumbar contra el respaldo de la silla.
    - El ángulo de rodillas y codo ha de ser de 90 grados.
    - Descansar de mirar a la pantalla cada 15 o 20 minutos.

4.3.-Profesorado.

4.3.1.-Profesorado respecto al alumnado:

1. Informar al alumnado de las normas de este protocolo para su cumplimiento.
2. Controlar el tiempo que el alumnado se conecta a internet en clase.

3. Colaborar en el mantenimiento del dispositivo tecnológico que estén utilizando en el aula. Evitando peligros físicos, ponerlos en lugares peligrosos o instalándole software no oficial distinto del que tiene sin autorización.
4. Fomentar la navegación segura por internet, para que accedan a contenidos adecuados a su edad.
5. Transmitir valores de respeto hacia todos los miembros de la Comunidad Educativa, transmitiendo al alumnado que las faltas de respeto a través de cualquier medio de internet tienen el mismo valor y consecuencias que la vida real.
6. Crear un espíritu crítico en la búsqueda de información que aparece en red, valorando y evaluando la calidad de los contenidos. Evitando el corta y pega, así como plagios de trabajos.
7. Informar sobre el derecho a la privacidad personal y de los demás, enseñándoles a no compartir datos personales propios o de otras personas sin su consentimiento (imágenes, datos, perfiles, números de teléfono...)
8. Enseñarle en qué consiste la privacidad, que los datos personales son información sensible y que antes de registrarse en cualquier página o aplicación deben consultarlo con la familia.
9. Fomentar el uso de una apostura correcta frente al ordenador:
    - Los ojos deben estar situados enfrente de la pantalla, a una distancia mínima del doble de la pantalla.
    - La espalda recta, y reposada en zona lumbar contra el respaldo de la silla.
    - El ángulo de rodillas y codo ha de ser de 90 grados.
    - Descansar de mirar a la pantalla cada 15 o 20 minutos.

4.3.2.- Profesorado respecto a su uso profesional:

Teniendo como referencia la resolución de 22 de octubre de 2020 de la Secretaria de Administración Pública por el que se acuerda el código de conducta e el uso de las tecnologías de la información y Comunicación para profesionales de la Administración de la Junta de Andalucía.

1. El profesorado realizará uso del equipamiento tic compatible con el desempeño de sus funciones.
2. El profesorado no podrá permitir el uso del equipamientos del centro tic a terceros nos autorizados.
3. El profesorado cuidará y conservará en buen estado el equipamiento tic.

4. El profesorado no alterará el software ni se instalará nuevo sin previa autorización aunque sea libre y gratuito.
5. En todo momento se seguirán protocolos y mecanismos establecidos por la Consejería de Educación y el propio centro para incidencias, permisos, equipamientos tic y software.
6. El profesorado usará las herramientas, aplicaciones y sistemas oficiales para desarrollo del desempeño de sus funciones profesionales, cerrando las sesiones una vez finalizado el uso de las mismas.

- **Uso de la Información**

1. El profesorado está obligado a proteger la información a la que tiene acceso y hacer uso exclusivamente profesional de la misma, y así mismo prevenir y evitar el mal uso de la misma.
2. En todo momento se velará para que la información en formato papel que se incorpore a sistemas de información no pueda ser conocida por personal no autorizado. No dejando documentos en impresoras, escáneres… o almacenar en lugar poco seguro.
3. No se utilizaran cuentas particulares en servicios externos de almacenamiento en la nube, para guardar de documentos oficiales y realización de sus funciones.

- **Tratamiento de datos:**

1. El profesorado está obligado a cumplir el deber de confidencialidad sobre datos personales en cuyo tratamiento participen.
2. Los datos personales no serán tratados fuera de los medios oficialmente establecidos.
3. El centro nombrará un delegado de protección de datos.

- **Internet, correo electrónico, herramientas colaborativas y redes sociales.**

1. El uso de internet por el profesorado tendrá una finalidad adecuada a su ámbito profesional, quedando estrictamente prohibido el acceso a páginas que no tenga un contenido ético, sea ofensivo o atentatorio contra la dignidad humana.
2. Se evitará el visitar páginas no fiables o seguras para evitar incidentes de seguridad.
3. Se tendrá en consideración que la navegación que se realice por internet podrá se monitorizada y registrada en su totalidad (direcciones, tiempo, ficheros descargados.

- **Correo electrónico**

1. La cuenta de correo electrónico corporativa es una herramienta de servicio, productividad y comunicación habilitado bajo las directrices de la Consejería de Educación a la que se accederá por una credencial personal e intransferible.
2. El uso del correo corporativo debe ser de uso exclusivamente profesional, no como medio de contacto personal o registro para otros propósitos.
3. Se gastará precaución de acceder a mensajes de correo sospechosos de tener propósito dañino. Y queda prohibido enviar deliberadamente programas o códigos dañinos o maliciosos que puedan causar daños en los equipos.

- **Herramientas de colaboración**

1. El profesorado utilizará solo para funciones profesionales las plataformas y herramientas oficiales de la Consejería de educación para la realización de reuniones virtuales, mensajería instantánea y compartición de ficheros como herramientas de servicio y colaboración entre profesionales.

- **Redes sociales.**

1. Los profesionales podrá utilizar en el desempeño de sus funciones las redes sociales como herramientas de comunicación, transparencia…siempre bajo el cumplimiento de la normativa en materia de protección de datos.

V.- RIESGOS EN EL MAL USO TIC Y TAC

Cuando nos referimos a las tic no es exclusivamente el uso del ordenador, se refiere al mal uso de las diferentes herramientas electrónicas de comunicación que existen y que el alumnado tiene acceso: Mal uso del Móvil, videoconsolas, tablet, televisión…

Posibles problemas:

- Problemas psicológicos y académicos.
- Trastornos del sueño.
- Bajada de rendimientos escolares.
- Déficit de atención.
- Forma de escape de realidad y aislamiento.
- Falta de autocontrol y adicciones.
- Irritabilidad al ser interrumpido. a.
- Exigencias hacia los padres.
- Desinformación.
- Problemas físicos posturales y dolores articulares.
- Sobrepeso o anorexia.
- Problemas oculares.

VI.-OTROS PROBLEMAS: CIBERDELITOS

6.1.- Violación de la Privacidad, del derecho a la imagen y a la intimidad:

Todo el mundo tiene derecho a la protección de datos, así como tenemos la obligación de respetar la privacidad de la de los demás. Ser menor no excluye el cumplimiento de las leyes.

Algunos casos de violación del derecho a la privacidad son:

- Suplantación de identidad accediendo a cuentas, perfiles o roles sociales ajenos.
- La Estafa.
- Spam.
- Etiquetado de fotos con mal intención o ensañamiento a la víctima.
- Distribución, sin querer de imágenes, videos… de pornografía infantil.

6.2.- Ciberacoso o Ciberbulling:

Se trata de un tipo de acoso entre iguales en un entorno TIC (móvil, foros, chat, correos...), que se repite en el tiempo (insultos, chantaje, coacción, injurias, vejaciones…)

Cómo Prevenirlo:

- Usar seudónimos y no nombre verdadero en registros.
- No dar datos personales ni familiares a extraños.
- Poner filtros en perfiles para que no accedan a nuestros datos personales.
- No aceptar invitaciones, ni establecer relaciones en redes sociales de perfiles desconocidos.
- Cuidar las publicaciones de imágenes, videos y comentarios que se realicen en redes sociales, tanto personales como ajenas.
- No responder a provocaciones.
- Comunicar rápidamente a padres y profesores cualquier cosa extraña que detecten y que le hagan sentir mal.

*En el caso de ser detectado en el entorno escolar se procederá como establece el protocolo: ► Protocolo de actuación ante situaciones de ciberacoso

6.3.- Acoso sexual o Grooming:

Se trata de un tipo de acoso realizado entre un adulto hacia un menor con intenciones sexuales.

En estos caso el adulto establece relaciones a través de las tic (redes sociales, foros…) con perfiles falsos a fin de ganar la confianza del menor y conseguir que este le mande fotos o videos comprometidos, con la intención de chantajearlo si no cumple los deseos del acosador.

Cómo prevenirlo:

- Usar perfiles privados en redes sociales.
- No aceptar invitaciones de perfiles desconocidos o sospechosos.
- No compartir ni datos personales, ni imágenes y videos íntimos a través de las redes.
- No aceptar mensajes de contenido sexual.
- No borrar pruebas
- Comunicar rápidamente a padres y profesores cualquier cosa extraña que detecten y que le hagan sentir mal.

*En el caso de ser detectado en el entorno escolar se procederá como establece el protocolo:► Protocolo de actuación ante situaciones de ciberacoso

6.4.- Ciberbaiting:

Consiste en el acoso del alumnado hacia un profesor. a.

Cómo prevenirlo:

- Extremar filtrado de privacidad en redes sociales.
- No aceptar invitaciones de perfiles desconocidos o sospechosos.
- No compartir ni datos personales, ni imágenes y videos íntimos a través de las redes.
- No aceptar mensajes de contenido inapropiado o sospechoso.
- No borrar pruebas.
- Comunicar rápidamente al centro

*En el caso de ser detectado en el entorno escolar se procederá como establece el protocolo:► Protocolo de actuación ante situaciones de ciberacoso

6.5.- Sexting:

Consiste en el envío a través de móvil de imágenes y videos pornográficos de menores tomadas por ellos mismos.

La falta de autoestima, la necesidad de pertenencia al grupo o de notoriedad y el exceso de confianza, a veces son razones que llevan al menor a actuar inadecuadamente enviando imágenes íntimas sin prever las consecuencias sobre quién y cómo puedan ser pueda difundirlas.

Cómo prevenirlo:

- No enviar contenidos sexuales propios a través del móvil
- Si recibe en el móvil contenidos multimedia de pornografía infantil borrarla inmediatamente, es delito tanto el hacer, el tener y o el distribuir imágenes de pornografía infantil.
- No confiar en estos contenidos provengan de desconocidos o de personas cercanas.
- Tener claro que hacer un video o una foto no da derecho a que se pueda compartir.
- No ceder ante presiones o chantajes.
- Comunicar rápidamente a padres y profesores cualquier cosa extraña que detecten y que le hagan sentir mal.

*En el caso de ser detectado en el entorno escolar se procederá como establece el protocolo:► Protocolo de actuación ante situaciones de ciberacoso

6.6.-Phishing:

Consiste en el envío masivo de correos electrónicos que suplantan la identidad de bancos, empresas…, para pedirnos datos, contraseñas, número de tarjetas…con la intención de robarnos.

Cómo prevenirlo:

- No abrir correos sospechosos
- No compartir datos ni información personal.
- Comprobar que la página a la que entramos es la auténtica ante introducir contraseñas o datos.

6.7.- Correos falso (spam) Virus, malware y spyware.

A veces en nuestro correo llegan cadenas de mensajes falsos cuya intención es recopilar nuestros datos y difundir nuestra información.

Otras veces son virus, gusanos o troyanos los que nos llegan a través del correo, cuyo objetivo es alterar el buen funcionamiento de nuestro PC. Son programas malintencionados o software malicioso, que roban información usando nuestro equipo para cometer delitos o para realizar chantajes.

Cómo prevenirlo.

- No abriendo correos de destinatario desconocidos o sospechosos.
- Poniendo un antivirus y manteniéndolo actualizado.
- Actualizando el sistema operativo de nuestro equipo.
- No instalando software pirata.
- Analizar los medios extraíbles antes de abrirlo en nuestro equipo (USB, CD…

Aclaración:

***Contenidos inapropiados e ilícitos:**

- Son contenidos susceptibles de atentar o que induzcan a atentar contra la dignidad humana, la seguridad y derechos de protección especialmente de menores.
- Contenidos violentos, degradantes o favorecedores a la corrupción de menores, así como relativos a prostitución, pornografía…
- Contenidos xenófobos, sexistas, relativos a sectas y los que hagan apología al crimen, terrorismo o ideas totalitarias o extremas.
- Contenidos que dañen identidad y autoestima, por la condición física o psíquica.
- Contenido que fomenten la ludopatía y consumos abusivos.

VII.- SANCIONES

Las sanciones derivadas del incumplimiento de estas normas, así como del mal uso intencionado o reiterado de internet o de los dispositivos electrónicos del centro podrán ser:

- Aplicación de medidas del Plan de Convivencia.
- Acciones tutoriales de alumnado y familias.

- Recogida en dirección de dispositivos personales que traigan al centro y entrega a tutores. Legales.
- Retirada temporal o definitiva del acceso a dispositivos del centro.
- Reparación de desperfectos o reposición del material dañado por el mal uso.
- Aplicación de protocolos de ciberacoso.
- En cualquier momento el centro podrá informar a las autoridades competentes de cualquier actividad, ilegal detectada o situaciones que atenten contra la integridad de cualquier miembro de la Comunidad Escolar.

VIII.- ANEXOS:

1. Boletín de seguridad tic de la Junta de Andalucía:

   file:///C:/Users/34671/Desktop/DIRECCI%C3%93N/carteleria%20riesgos%20internet%20junta%20andalucia.pdf

CARTELERÍA:

Descargar cartel: Ciberseguridad para niños: 10 comportamientos que debes evitar (aesdigital.es)


NAVEGA Y APRENDE CON SEGURIDAD
No digas en la Red tus datos personales
Chatea con tus amigos y amigas, nunca con desconocidos
Tus contraseñas deben ser secretas, solo pueden saberlas tus padres
Enseñale a tus padres las páginas que usas
Pide ayuda a tus padres o profes para descargarte los programas que necesites
Los correos de desconocidos pueden ser virus, no los abras
No hagas bromas pesadas por la Red
Usa Internet para mejorar en tus asignaturas favoritas

IX.-FUENTES CONSULTADAS.

Normativa:

- RESOLUCIÓN de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía (BOJA 27-10-2020)
- LEY ORGÁNICA 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 06-12-2018). (Modifica artículos de LOE, LPA, EBEP y otras leyes).
- DECRETO 25/2007, de 6 de febrero, por el que se establecen medidas para el fomento, la prevención de riesgos y la seguridad en el uso de Internet y las tecnologías de la información y la comunicación (TIC) por parte de las personas menores de edad. (BOJA 22-2-2007)
- ► Protocolo de actuación ante situaciones de ciberacoso

Otras fuentes de interés consultadas:

2. Boletín de seguridad tic de la Junta de Andalucía:

   file:///C:/Users/34671/Desktop/DIRECCI%C3%93N/carteleria%20riesgos%20internet%20junta%20andalucia.pdf

3. Instituto nacional de ciberseguridad:
   https://www.incibe.es/cibercovid19

4. Ciberacoso y ciberbulling: https://ciberacoso.wordpress.com/

5. Centro de seguridad en internet http:
   https://www.bienestaryproteccioninfantil.es/fuentes1.asp?sec=18&cod=2203
6. Guía del buen uso de internet de Extremadura:
   file:///C:/Users/34671/Desktop/DIRECCI%C3%93N/uso%20informacion%20tic/guia_buen%20uso%20internet%20extremadura.pdf

7. Grupo de delitos telemáticos. Guardia Civil :
   https://www.gdt.guardiacivil.es/webgdt/home_alerta.php