12.-PROTECCIÓN DE DATOS Y SEGURIDAD EN INTERNET

PLAN DE SEGURIDAD PARA HACER UN USO RESPONSABLE DE INTERNET			
OBJETIVOS	**ACTUACIONES**	**ENCARGADOS**	**EVALUACIÓN**
Proteger los dispositivos informáticos del Centro de programas maliciosos	1. Instalar sistemas de protección con cortafuegos y antivirus, manteniéndolos actualizados para evitar fallos de seguridad. 2. Bloquear sitios web y ventanas emergentes no deseados personalizando la configuración de seguridad del/de los navegador(es) que se utilizan en los ordenadores del centro. 3. Explicar al alumnado por qué se hace esto mencionando cómo se le protege. 4. Crear un protocolo estricto sobre uso de internet y comprobar automáticamente si hay programas maliciosos de correos electrónicos personales en los ordenadores escolares. 5. Formar al personal con conocimientos básicos para detectar archivos potencialmente infectados y con prácticas seguras en descarga de archivos y uso de dispositivos portátiles. 6. Enseñar a todo el mundo, personal y estudiantes, a realizar una búsqueda de programas maliciosos en	**EQUIPO DIRECTIVO** **TODO EL PROFESORADO**	**A FINAL DE CURSO**

	todos sus archivos antes de utilizarlos en dispositivos del centro. 7. Designar a una persona de contacto formada que trabaje todos los problemas relacionados con los programas maliciosos y poner en marcha procedimientos formales de resolución de incidencias.		
Proteger los datos más confidenciales en el centro	1. Establecer dos entornos de red informáticos separados, uno para estudiantes, personal y trato con las familias; el otro en un servidor más seguro para administración. 2. Mantener los sistemas de protección con cortafuegos y antivirus actualizados para evitar ser presa de crákers. 3. Cifrar y proteger con contraseña los datos confidenciales, así como no almacenar nunca información sin cifrar en dispositivos portátiles. 4. Formar al personal en protección de datos básica, para lo que puedes ponerte en contacto con la agencia de protección de datos u organismo similar de tu país. 5. Crear un protocolo estricto para la copia o descarga de datos confidenciales de los sistemas administrativos, evitando hacerlo siempre que sea posible. 6. Realizar copias de respaldo de los dispositivos necesarios con regularidad.	**EQUIPO DIRECTIVO** **TODO EL PROFESORADO**	**A FINAL DE CURSO**

Participar en diferentes talleres de prevención de uso de las redes sociales para alumnado, profesorado y familias.	• Talleres impartidos por PUNTO OMEGA sobre el uso responsable de las nuevas tecnologías para los alumnos de 5º y 6º curso.  • Talleres de prevención delas TIC impartidos por los alumnos del IES de la localidad para los alumnos de 6º curso. • Escuelas de padres organizadas por el departamento de Orientación del Centro. • Cursos de formación de profesorado.	**EQUIPO DIRECTIVO** **TODO EL PROFESORADO**	**A FINAL DE CURSO**

Crear contraseñas seguras	**1.** Una contraseña es una importante clave que desbloquea el acceso a tu sistema. Evita dar a los nuevos usuarios la misma contraseña «de primer uso». **2.** Asegura que tu sistema atribuye una contraseña diferente a cada nuevo usuario, y pídeles que generen la suya propia la primera vez que accedan al sistema informático del centro. **3.** Recuerda al personal y al alumnado las cuatro reglas doradas para crear una contraseña segura: **a.** Que sea larga y compleja, idealmente de 10 a 14 caracteres, pues la longitud de la contraseña es el aspecto más relevante de su seguridad. **b.** Que contenga una mezcla de números, símbolos, mayúsculas, minúsculas y puntuación. **c.** Que se pueda utilizar la mnemotecnia para ayudarnos a recordarla. **d.** Que la contraseña en ningún caso contenga información personal. Con esto nos referimos a nombres, fechas de nacimiento, mascotas, direcciones, nombre del colegio, números de teléfono, matrículas, etc. Si alguien quiere acceder a tu cuenta empezará adivinando primero a partir de este tipo de información. **4.** Incorporar las reglas esenciales de gestión de contraseñas en la política de seguridad digital (eSafety) del centro e invitar al cuerpo docente a revisar las normas con su clase regularmente como recordatorio de a qué nos hemos comprometido.	**EQUIPO DIRECTIVO** **TODO EL PROFESORADO**	**A FINAL DE CURSO**
Tener presencia en la plataforma de redes sociales de forma controlada	**1.** Desarrollo profesional en términos de herramientas técnicas y de redes sociales para docentes. **2.** Relación con el entorno social y las familias con grupos de Facebook, Remind, Twitter y otras herramientas. **3.** Fomento de la comunicación con las familias del alumnado	**EQUIPO DIRECTIVO** **TODO EL PROFESORADO**	**A FINAL DE CURSO**

	si siguen al centro, a la clase o a un proyecto en Facebook o similar. **4.** Comunicación intercultural con otros centros educativos. **5.** Aprendizaje de idiomas. **6.** Aprendizaje cooperativo y puesta en común con grupos de aprendizaje de compañeras y compañeros con enfoques similares. **7.** Contactos profesionales en el país o de todo el mundo. **8.** Integración de ejemplos de la realidad cotidiana en la enseñanza.		
Poner en marcha las normas de las NCOF del centro en caso de que los estudiantes sufran acoso digital	**Seguimiento del protocolo de actuación recogido en el Anexo I de las NCOF del Centro**	**EQUIPO DIRECTIVO** **TODO EL PROFESORADO**	**A FINAL DE CURSO**

CONSEJOS Y BUENAS PRÁCTICAS PARA LAS FAMILIAS

1. Hable siempre con sus hijos e hijas sobre lo que hacen y encuentran en Internet.

2. Acuerde con sus hijos e hijas que nunca proporcionen información personal familiar: edad, dirección, DNI, teléfono, su propia imagen en fotografía o video, etc.

3. Tenga cuidado con el e-mail y los archivos adjuntos, cuando no conoce quien lo envía, ya que podrían contener virus o códigos maliciosos. Nunca abra correos sospechosos.

4. Muéstrese interesado por las amistades que sus hijos e hijas hacen en línea, especialmente en los sistemas de «chats», de mensajería instantánea (Messenger) y redes sociales (Tuenti, Facebook,...).

5. Anime a sus hijos e hijas para que le informen de todo lo que les haga sentir incómodos, les desagrade u ofenda, o de aquello de lo que hayan tenido conocimiento en relación con los riesgos de Internet.

6. Hágales ver que acciones que para su hijo o hija puedan resultar de lo más normales, tienen su riesgo, como subir fotografías o videos propios a la red, que en cuanto a su difusión y por el número de personas que lo verían, podría ser algo similar a poner su foto pegada a todas las farolas de la ciudad o divulgar su video en todas las pantallas de publicidad.
7. Evite páginas con contenidos nocivos o falsos. No crea todo lo que encuentra, vea o lea en Internet. Circula por la Red mucha opinión o meros comentarios, más que verdadero conocimiento, por lo que se corre el riesgo de desinformarse más que de informarse.
8. Mantenga un contacto permanente con el Centro Educativo, en relación con el uso que sus hijos e hijas hacen de Internet.
9. No culpabilice a sus hijos e hijas sobre lo que ocurra en Internet, ni sea alarmista.

10. Acuerde un tiempo «generoso» para que sus hijos e hijas hagan uso de Internet, pero establezca un tiempo concreto de uso, así como un código familiar de uso de Internet. Es aconsejable que no se encierren en una habitación para navegar por Internet, sino que esto se haga en un lugar del hogar visible por todos.
La manera más directa de evitar los riesgos en el uso de Internet es la prevención.