SEGURIDAD Y CONFIANZA DIGITAL

1. El software usado en el Centro es el proporcionado por la Junta de Castilla y León a través de las cuentas institucionales, dada la seguridad que esta ofrece. Todo software utilizado diferente del institucional será bajo la responsabilidad del profesorado.

2. El Centro tiene establecidos acuerdos, procedimientos y mecanismos de protección del contexto tecnológico con la finalidad de prevenir accesos no autorizados, difusión no permitida, alteración de datos, accesos a entornos inapropiados, prevención de ac. Todos los ordenadores del centro tienen una clave de acceso. El usuario se hace responsable del mal uso de los recursos del IES.

3. El Equipo de Convivencia junto con el responsable de TIC son los encargados del uso correcto de las TIC en el centro. En caso de que hubiese un incidente de acceso no autorizado se podría realizar una auditoría en la WIFI.

4. El centro tiene identificados los equipos, dispositivos y servicios donde se almacenan datos sensibles de carácter personal. Existen medidas estrictas de control de acceso a los equipos, dispositivos y servicios según la tipología de los datos almacenados. El Reglamento de Régimen Interior recoge los procesos y actuaciones en caso de alteración del servicio o el acceso a la información.

5. El Reglamento de Régimen Interior recoge normas relativas al buen uso de los equipos, dispositivos y los espacios en los que se utilizan (se resumen estos aspectos en el punto 8.1.). El Centro contempla periódicamente procesos de evaluación y de auditoría en lo que se refiere a la seguridad y a las normativas de protección de datos. De forma periódica se analiza la seguridad en las redes locales cableadas e inalámbricas y se modifican las claves de acceso. El centro tiene implementadas normas claras sobre el tratamiento de datos de imagen/voz de alumnos conforme a la instrucción de la DG de Política Educativa o equivalente. El IES reestructuró la secretaría para que personas no autorizadas no usen los ordenadores con información sensible. Tan sólo el equipo directivo, el personal administrativo y algunas personales colaboradoras a modo de excepción tienen acceso a esa información Las contraseñas de acceso al Ordenador Central, así como las utilizadas para el acceso a diferentes aplicaciones, son absolutamente confidenciales y solo son conocidas por el Equipo directivo y el personal autorizado que se señala en el Plan de confidencialidad del IES.

6. El centro contempla periódicamente procesos de evaluación y de auditoría en lo que se refiere a la seguridad y a las normativas de protección de datos aunque no se ha realizado ninguna hasta la fecha.

7. Se tienen en cuenta estructuras organizativas y de actuación relativas a la protección de la confidencialidad y de los datos.

8. Se tienen establecidos criterios de almacenamiento, de replicación de seguridad y custodia de los datos confidenciales, documentos y recursos didácticos digitales. En cuanto a los elementos de seguridad y protección de los datos del servidor, está programado para hacer una copia de seguridad todos los días a las 17:00 de manera remota; además existe un protocolo para realizar una copia de seguridad en cinta de la unidad E y de la unidad F una vez por semana. El servidor está protegido además con un S.A.I. para proteger los datos del mismo en caso de alteración eléctrica. Los datos se almacenan en un disco duro externo para mayor seguridad, evitando así el acceso a ellos a través de internet y periódicamente se comprueba la bondad de la copia.

9. El centro tiene establecidos procedimientos para informar sobre las normas de propiedad intelectual, derecho de autor y propiedad industrial. El IES protege la propiedad intelectual y condena el plagio. Estas normas se explicarán a los alumnos en tutorías y por los profesores en el momento de la realización de los trabajos.

10. El centro desarrolla actuaciones de formación y concienciación sobre el uso seguro de los equipos, redes y servicios de internet para el alumnado, el profesorado y el personal no docente. El centro, dentro de su programación educativa y didáctica, integra resultados de aprendizaje (contenidos, criterios de evaluación, estándares de aprendizaje evaluables…) relativos al uso seguro de equipos, redes y servicios para todo el alumnado. El centro cuenta con un responsable de referencia al que el alumnado puede consultar sobre temas relacionados con los servicios en red, seguridad, protección de datos, que es el responsable de TIC.

11. El centro considera actuaciones de formación y concienciación de los usuarios externos de su entorno tecnológico del centro (familias, usuarios,…). Para ello, utilizamos los recursos del Portal de Educación de la Junta de Castilla y León y las posibilidades que nos ofrece nuestra participación en el PLAN DE APOYO TICA de la Dirección Provincial que este año ha realizado un plan de formación a familias. Además, se utiliza el apoyo externo del CEAS, la Guardia Civil y otras instituciones para realizar actividades tanto para alumnos como para familias.