Junta de Castilla y León
Consejería de Educación

PLAN DE SEGURIDAD Y CONFIANZA DIGITAL

Curso 2025/2026

IES DOCTOR SANCHO DE MATIENZO

C/ Cadagua, 13

09580 – VILLASANA DE MENA

(BURGOS)

Tfno.: 947126242 Fax: 947141479

E-mail: 09008937@educa.jcyl.es

Web: http://iesdoctorsanchodematienzo.centros.educa.jcyl.es

Elaborado por:
Roberto Salazar Cabajon (responsable CompDigEdu)
M.ª José Rodríguez Herrero (directora)

ÍNDICE

1- JUSTIFICACIÓN DE LA NECESIDAD DEL PLAN

1.1 Análisis del contexto del centro

El Valle de Mena es un pequeño municipio del norte de la provincia de Burgos, colindante con Vizcaya, Cantabria y Álava. Está formado por 52 pueblos y cuenta en la actualidad con aproximadamente 4.000 habitantes.

El entorno físico es de incalculable belleza, sus paisajes y monumentos dignos de admiración y en el ambiente se respira la tranquilidad propia de un medio rural que se ve claramente influenciado por la cercanía a Vizcaya, pero que no olvida sus raíces castellanas.

En su capital, Villasana, está ubicado el IES “Doctor Sancho de Matienzo”, un centro cuya titularidad corresponde a la Junta de Castilla y León y que, en sus orígenes, fue una Sección de Formación Profesional, transformada en 1995 en Instituto de Educación Secundaria, el único de la localidad.

1.1.1. Contexto social y cultural

La población activa se dedica mayoritariamente a actividades de los sectores primario y terciario. En los últimos años, el incremento de la tasa de desempleo ha provocado diferencias socioeconómicas entre el alumnado, aunque éstas no influyen significativamente en el proceso educativo.

La oferta educativa del Valle de Mena se limita al CEIP “Nuestra Señora de las Altices” y al propio Instituto. Las características orográficas del municipio hacen que para algunos alumnos el centro educativo sea la única vía de comunicación y relación con otros jóvenes a lo largo de la semana.

1.1.2. Alumnos

La matrícula se ve afectada por la mayor oferta educativa de los centros de las localidades vizcaínas más cercanas.

También es cierto que se ha notado en los últimos años un incremento de matrícula de los alumnos que se matriculan debido a sus dificultades con el idioma euskera que deben cursar obligatoriamente en el País Vasco; estos alumnos proceden de localidades vizcaínas cercanas al Valle de Mena o bien alumnos del propio Valle que en su día empezaron a estudiar en el País Vasco.

Los resultados académicos son claramente mejorables. A ello hay que añadir que un considerable número de alumnos adolece de una preocupante desmotivación y falta de hábito de estudio.

1.1.3. Profesorado

El Claustro de Profesores está integrado por 32 docentes, 14 de los cuales tienen destino definitivo en el centro. La movilidad del profesorado dificulta el desarrollo de planes y proyectos y, dado que el CFIE de Miranda de Ebro se encuentra a 110 km. de distancia, la mayoría de los docentes optan por la formación online.

La totalidad del profesorado participa en actividades formativas tanto presenciales como online. Desde hace varios cursos, dentro del Plan de Formación del Centro se incluye un itinerario TICA.

1.1.4. Personal de administración y servicios

La plantilla está formada por un auxiliar administrativo, dos ordenanzas y dos limpiadoras, plantilla que también se ve afectada con mucha frecuencia por la movilidad del personal.

1.1.5. Familias

La Asociación de Madres y Padres de Alumnos es muy activa. Aunque la totalidad de las familias pertenece a esa asociación, a las reuniones acuden generalmente pocos padres, lo que dificulta la mejora del proceso educativo.

1.1.6. Espacios y recursos materiales

El instituto cuenta con unas instalaciones extraordinarias, aunque presenta algunas deficiencias de obra. Respecto a los recursos materiales, la dotación en general es buena, aunque es preciso señalar la necesidad de renovar algunos equipos informáticos debido a su obsolescencia.

1.2 Autoevaluación del centro

Con el fin de mejorar en la medida de lo posible el funcionamiento y los resultados del IES, desde el Equipo Directivo se propuso llevar a cabo durante el curso 2014-2015 una Autoevaluación del Centro siguiendo el "Modelo de Autoevaluación para organizaciones educativas de Castilla y León", sistema estructurado y homogéneo que posibilita la participación de todos los sectores de la comunidad educativa en el proceso de identificación de Puntos Fuertes y Áreas de Mejora encaminado al logro eficaz de los objetivos del proceso educativo y la mejora de la organización y gestión del centro.

Convencidos de que todo ello, sin duda alguna, redundaría en beneficio de nuestros resultados, es decir, de nuestros alumnos que son los destinatarios finales de nuestro trabajo, en octubre de 2014 se inició el proceso de Autoevaluación. Como datos significativos hay que señalar la escasa participación, especialmente por parte de las familias, así como el consenso a la hora de identificar las "Relaciones con el entorno" como una de las Áreas de Mejora prioritarias. Asimismo, también se ha detectado que muchas comunicaciones no llegan a su destino (familias), porque los alumnos no entregan los documentos (oficios, Agenda Escolar, etc.) y se ha constatado nuevamente una escasa motivación en un número considerable de alumnos. A todo ello hay que añadir que para algunas familias resulta realmente complicado conciliar la vida laboral y familiar, que las características orográficas del Valle de Mena no favorecen esa imprescindible comunicación entre todos los miembros de la comunidad educativa y que también constituyen un hándicap en la participación del profesorado en actividades formativas presenciales.

En este contexto, se hace imprescindible la utilización de las Tecnologías de la Información y Comunicación para conseguir el objetivo de mejora de la calidad de educativa, herramientas que favorecerán el aprendizaje cooperativo y el trabajo en grupo y que favorecerán la comunicación entre todos los integrantes de la comunidad educativa. Por ello, desde el curso 2016-2017 se desarrollan en el centro planes de formación con un itinerario TIC. Varios docentes participan también en el Plan TICA organizado por la Dirección Provincial de Burgos.

Lógicamente, en este contexto es necesaria la adopción de medidas de seguridad y confidencialidad, así como la inclusión de las mismas en un Plan de Seguridad y Confianza Digital que potencie el uso responsable de estas nuevas tecnologías.

La publicación por parte de la Agencia Española de Protección de Datos de la Guía con Orientaciones para centros educativos, así como la aplicación del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento y la libre circulación de datos personales, implican una adaptación del Plan TIC del Centro en materia de Seguridad y Confianza Digital, por lo que en septiembre de 2018 utilizamos la “Propuesta-Apoyo para la verificación de la Seguridad y Confianza Digital en los centros educativos” elaborada por el Grupo de Trabajo Provincial de Integración Didáctica de las TICA y REDXXI del Área de Programas Educativos de la Dirección Provincial de Burgos como Herramienta de Autoevaluación. Esta herramienta nos permitió definir las líneas de trabajo para los cursos, trabajo al que se está dando continuidad durante el 2025-2026.

2- OBJETIVOS

1. Impulsar la alfabetización digital de todos los miembros de la comunidad educativa.
2. Fomentar el uso seguro de internet.
3. Informar y sensibilizar sobre las situaciones de riesgo más habituales a las que deben hacer frente los menores cuando navegan por internet.
4. Promocionar y difundir el buen uso de las TIC en educación.
5. Ofrecer información y estrategias de actuación ante situaciones no deseadas (usurpaciones de identidad, comportamientos inadecuados, contenidos inadecuados, ciberacoso…)
6. Reflexionar y sensibilizar acerca del importante papel que pueden y deben jugar las familias en cuanto a la relación de sus hijos con las nuevas tecnologías.
7. Impulsar la participación del profesorado en actividades formativas relacionadas con el uso de las TIC y el aumento de la cultura digital.
8. Utilizar como una más de las herramientas de enseñanza-aprendizaje por los profesores del centro, las herramientas de Plataforma 365.

3- ACTUACIONES

3.1. Medidas de protección de equipos, redes y datos

3.1.1. Gestión de usuarios (permisos y contraseñas)

a) Registro de contraseñas de las aplicaciones de gestión del centro:
   - Se custodia en Dirección.
   - Personas autorizadas: directora y secretaria.

b) Contraseñas de las aplicaciones de gestión de centro:
   - Registro: en Dirección.
   - Cambio periódico de contraseñas:
     - IES2000 y GECE2000: No procede.
     - ABIES: Se modificará anualmente (en julio), encargándose de este proceso la secretaria y/o la directora.
     - Correo oficial: El cambio de la clave de acceso se realizará al final de cada trimestre, operación que llevará a cabo la directora.

Notas:

** La periodicidad con la que se realizarán los cambios de las claves de acceso es orientativa. Lógicamente, si surge algún problema de seguridad que aconseje un cambio urgente de las mismas, éste será realizado de manera inmediata.*

.

3.1.2. Realización de copias de respaldo de los datos sensibles

a) Información oficial del centro:

La directora realizará semanalmente copias de seguridad de las aplicaciones IES2000, GECE2000 y ABIES, así como de la documentación que sea incluida en las carpetas oficiales que se comparten con el profesorado e Inspección en OneDrive. Asimismo, mensualmente comprobará el funcionamiento de dichas copias.

b) Documentación de los Departamentos:

Los jefes de los distintos departamentos de coordinación didáctica serán los responsables de la realización periódica de copias de seguridad de la documentación oficial de los mismos.

* *Todas las copias serán realizadas en dispositivos del centro (disco duro externo o pendrive).*

3.1.3. Encriptación de información relevante

a) Documentación oficial del centro. Será responsabilidad de la secretaria y de la directora del centro.

b) Documentación de los departamentos de coordinación didáctica. Los jefes de departamento se encargarán de esta tarea.

3.1.4. Reforzado de la seguridad de las aplicaciones informáticas utilizadas

a) Utilizar las plataformas corporativas: Aula virtual, Teams, correo de educacyl y herramientas de Plataforma 365.

b) Usar el correo corporativo como instrumento de comunicación entre el profesorado, así como con los alumnos y sus familias.

c) Elaborar de un inventario de aplicaciones específicas utilizadas en las distintas materias.

d) Informar al profesorado de la obligatoriedad de solicitar la autorización al centro educativo para el uso de aplicaciones informáticas no corporativas. Para ello, se usará el documento elaborado al efecto.

e) Revisar de la política de privacidad de dichas aplicaciones con el fin de autorizar o denegar su uso previa evaluación desde el punto de vista de la seguridad de la información, lo que implicará que solamente se autorizará la utilización de aquellas aplicaciones que ofrezcan

información claramente definida sobre los tratamientos efectuados, las finalidades de los mismos y sus responsables, así como sobre la ubicación de los datos, el periodo de retención y las garantías con relación a su seguridad (Anexo II).

f) Comprobar que esas aplicaciones permiten el control, por parte de los tutores o profesores, de los contenidos subidos por los menores, en especial de los contenidos multimedia (fotos, vídeos y grabaciones de voz de los alumnos).

g) Ofrecer información a las familias sobre la utilización de la tecnología en las aulas, así como de aquellas aplicaciones que traten datos personales de los alumnos y su funcionalidad.

h) Facilitar al profesorado una Guía con recomendaciones sobre seguridad y privacidad según la AEPD y los consejos elaborados desde el propio IES Doctor Sancho de Matienzo (Anexo III).

3.2 Actuaciones ante incidencias relacionadas con la seguridad

3.2.1 Registro de incidencias

a) En caso de que un profesor detecte cualquier defecto o incidencia relacionada con el hardware o el software, deberá comunicarlo de forma inmediata al responsable CompDigEdu o, como máximo, al finalizar la sesión en la que se haya producido la incidencia.

b) Si la detección de la incidencia corresponde a un alumno, este deberá informar de manera inmediata al profesor responsable del grupo o asignatura en la que se haya producido la misma.

c) El responsable de CompDigEdu registrará todas las incidencias en la Plantilla de incidencias de los equipos informáticos y audiovisuales del centro (Anexo IV), a fin de proceder a su notificación a la directora y a la resolución correspondiente.

3.2.2 Procedimiento de actuación ante situaciones de riesgo e incidencias que afecten a la seguridad

El responsable CompDigEdu pondrá en conocimiento de la directora cualquier incidencia relacionada con la seguridad digital. Ambas profesoras actuarán de forma coordinada en pro de la rápida y eficaz solución de la misma. En función del tipo y gravedad de la incidencia, procederán:

a) Solucionar ellas mismas la incidencia, si es viable.
b) Solicitar ayuda, según proceda:
    a. CAU
    b. Coordinador SIGIE
    c. Consejería de Educación:

Delegado de Protección de Datos

Avda. Monasterio de Ntra. Sra. de Prado, s/n, CP 47014, Valladolid

Correo electrónico: dpd.educacion@jcyl.es

3.3 Utilización inadecuada de equipos y servicios u otras actuaciones que atenten a la convivencia en red

En el artículo 71 del Reglamento de Régimen Interior del centro se tipifican como conductas gravemente perjudiciales para la convivencia en el centro, entre otras, las siguientes:

- Ciberacoso.
- Suplantación de personalidad.
- Deterioro intencionado del material informático del centro o de otros alumnos.
- Manipulación de datos y/o archivos informáticos de compañeros.
- Grabación de datos (incluidos imágenes, vídeos y audios) dentro del recinto escolar que no formen parte de una actividad lectiva.
- Difusión de datos obtenidos en el entorno escolar (incluidas las actividades complementarias y extraescolares).

En caso de que se produzca alguna situación de las mencionadas anteriormente, se seguirá el procedimiento contemplado en el RRI (artículos 73-77) y se aplicará alguna de las sanciones recogidas en el artículo 72.

3.4 Formación e información en materia de seguridad

3.4.1 Profesores

a) “Plan de Acogida al Profesorado", en el que nos centraremos en los recursos informáticos que hay en el IES y su correcta utilización. Inicio de curso (responsable: responsable CompDigEdu).

b) Detección de necesidades de formación. Formulario diseñado al efecto, que se cumplimenta a comienzos del segundo trimestre (responsables: coordinadora de formación, responsable CompDigEdu, directora, otros docentes colaboradores).

c) Plan de Formación de Centro. En base a la información obtenida a través de los diferentes procedimientos de detección, entre los que se incluye el formulario al que se hace referencia en el párrafo anterior, se diseñan las actividades que formarán parte de este plan (responsables: responsable de formación y responsable CompDigEdu).

d) Información al profesorado sobre la autorización o denegación de la publicación de imágenes por parte de las familias en el caso de menores de 14 años, o de los propios alumnos en caso de mayores de 14 años (responsable: equipo directivo).

e) Puesta a disposición del profesorado de información sobre ciberseguridad a través la carpeta “Seguridad y Confianza Digital” compartida con todos los docentes: guías oficiales, orientaciones y consejos, Instrucción de la Consejería de Educación sobre el tratamiento de datos de imagen/voz de alumnos, Propiedad intelectual y derechos de autor, Licencias Creative Commons… Esta carpeta se va actualizando constantemente (responsable: directora).

f) Participación en actividades de formación organizadas por el CFIE de Miranda de Ebro y por el Equipo TICA de la Dirección Provincial de Educación de Burgos (responsable CompDigEdu y directora).

3.4.2 Alumnos

a) Detección de necesidades de formación. Formulario diseñado al efecto, que se cumplimenta a comienzos del segundo trimestre (Responsables: responsable de formación, responsable CompDigEdu, directora, otros docentes colaboradores).

b) Acciones del Plan Director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos: Charlas con el alumnado de ESO sobre “Riesgos de Internet”.

c) Actividades dirigidas a la prevención del ciberacoso:
   a. Espacio web existente en el Portal de Educación de la Junta de Castilla y León dedicado a la navegación segura y el ciberacoso.
   b. Material de “pantallas amigas” (www.pantallasamigas.net).
   c. Talleres sobre “Internet y Privacidad”.
   d. Actividades organizadas por el INCIBE.

   Responsables de las actuaciones b) y c): tutores, responsable CompDigEdu y equipo directivo.

d) Desarrollo de actividades promovidas por el Equipo TICA de la Dirección Provincial de Educación de Burgos (responsables: responsable CompDigEdu y directora).

e) Participación en eventos que promuevan el uso seguro y responsable de internet entre los menores (Gestión de la privacidad. Huella Digital. Taller de Creación de Contraseñas Seguras):
   a. Día Europeo de la Protección de datos (28 de enero)
   b. Día de Internet Segura (10 de febrero).
   c. Día de Internet (17 de mayo).

   Responsables: Departamentos de Tecnología y Orientación.

3.4.3 Familias

a) Acciones del Plan Director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos: Charlas con el alumnado de ESO sobre “Riesgos de Internet”.

b) Participación en actividades formativas organizadas por el Equipo TICA de la Dirección Provincial de Educación de Burgos.

c) Se proporcionará la documentación y la formación necesarias para el uso de la plataforma STILUS, con el fin de optimizar la transmisión de información y la comunicación entre el centro educativo y las familias.

Responsables en ambas actuaciones: directora y responsable CompDigEdu.

3.5 Difusión de la información en materia de seguridad

a) Página web del centro.
b) OneDrive.
c) Claustro de Profesores.
d) Consejo Escolar.
e) AMPA.
f) Redes sociales (Instagram).
g) Aulas.

Responsables: responsable CompDigEdu y directora.

3.6 Otras actuaciones

a) Inclusión de las TIC como elemento transversal en las programaciones didácticas de las diferentes materias.

b) Integración de las TIC secuencialmente a través del plan de acción tutorial por cursos.

c) Actualización del Plan Digital del centro.

d) Utilizar el aula Moodle y Teams como herramientas habituales de trabajo.

e) Usar y fomentar las herramientas de Plataforma 365.

4- RESPONSABLES DEL PLAN

a) Equipo directivo.

b) Responsable CompDigEdu.

Destinatarios:

- Todo el profesorado, los alumnos y sus familias.

5- ASESORAMIENTO Y APOYO EXTERNO

a) Área de Inspección Educativa.

b) Área de Programas Educativos de la Dirección Provincial de Burgos (Equipo TICA).

c) CFIE de Miranda de Ebro.

d) Guardia Civil (Plan Director).

6- SEGUIMIENTO Y EVALUACIÓN FINAL

A la finalización de cada una de las actividades, se realizará una valoración sobre el desarrollo de las mismas y se reflejará en un informe en el que se incluirá una valoración cualitativa. Las valoraciones serán analizadas por las responsables del plan.

Mensualmente se recogerán las aportaciones de los diferentes departamentos a través de las reuniones ordinarias de la Comisión de Coordinación Pedagógica (CCP). Trimestralmente, se hará lo propio en Claustro de Profesores y Consejo Escolar.

Esos informes, que se incluirán en la Memoria Final del centro, harán posible la detección de áreas de mejora para el próximo curso.

ANEXO I - HERRAMIENTA DE AUTOEVALUACIÓN

PROPUESTA-APOYO PARA LA VERIFICACIÓN SEGURIDAD Y CONFIANZA DIGITAL EN LOS CENTROS EDUCATIVOS. HERRAMIENTA DE AUTOEVALUACIÓN

DESCRIPTORES	No planteado	En desarrollo	Sistematizado

PROTECCIÓN DE DATOS Y CONFIDENCIALIDAD

1. El centro emplea o dispone de ficheros diferentes a los registrados por la Junta de Castilla y León en el Registro General de Protección de Datos.	☒	☐	☐
2. El centro dispone de medidas de registro de las personas que acceden a los ficheros de datos de carácter personal de nivel básico	☐	☐	☒
3. El centro dispone de medidas de registro, autentificación personalizada con límite de intentos para ficheros de carácter personal que contengan datos de características personales, penales, financieras, tributarias…	☒	☐	☐
4. El centro dispone de medidas de registro, autentificación con límite de intentos y cifrado para los datos referidos a ideología, religión, origen racial, salud, psicológicos, etc., de los miembros de la comunidad educativa.	☒	☐	☐
5. El centro dispone de un documento de planificación y organización de los procesos básicos de protección de datos.	☐	☒	☐
6. Existe un responsable de gestión de la protección de datos que aborda las incidencias relativas a la información y los datos.	☐	☐	☒
7. El centro tiene un plan de auditorías de seguridad para la protección de datos.	☒	☐	☐
8. Existe un reglamento claro con directrices específicas respecto a la disposición de imágenes y fotografías en la red.	☐	☐	☒
9. Tanto el profesorado como los padres y la comunidad escolar están informados y se les recuerda de forma regular dicho reglamento de centro sobre protección de datos.	☐	☐	☒
10. El centro solicita consentimiento en el uso de fotografía de los alumnos a los padres si es menor de 14 años y en el caso de mayores de 14 años al propio interesado. En todo caso se explicita el lugar de difusión y el tiempo de uso/fecha de retirada.	☐	☐	☒

ALMACENAMIENTO Y CUSTODIA DE DATOS

1.	El centro tiene un procedimiento sistematizado de la realización periódica de copias de respaldo y está documentado.	☐	☒	☐
2.	Las copias de seguridad se custodian en un lugar diferente a los equipos informáticos y están resguardados de incidencias (protección eléctrica, inundaciones,)	☐	☐	☒
3.	Se verifica periódicamente la lectura de copias anteriores.	☐	☐	☒
4.	Existe una relación e identificación de equipos y dispositivos en los que se encuentran datos protegidos.	☐	☐	☒
5.	Existe una relación de recursos compartidos en red con datos de carácter personal.	☐	☒	☐
6.	Existe una relación de usuarios con acceso físico a los equipos con datos.	☐	☐	☒
7.	Existe relación de personas ajenas al centro con acceso a equipos con datos de carácter personal, y mantienen acuerdos por escrito de confidencialidad.	☒	☐	☐
8.	Existen criterios establecidos para la eliminación segura/definitiva de datos de dispositivos de almacenamiento (borrado seguro, destrucción física, inutilización…)	☐	☐	☒
9.	La instalación de datos de carácter personal en otros equipos o dispositivos diferentes a los destinados a tal efecto se lleva a cabo con consentimiento del responsable e identificación del equipo	☒	☐	☐
10.	Los datos o información de carácter personal en dispositivos móviles o en la nube, se mueven encriptados o con las medidas de seguridad adecuadas al nivel del fichero.	☐	☒	☐

REDES LOCALES

1.	El centro tiene segmentadas las redes del centro en redes administrativas, redes educativas (de profesores y alumnos) y no son accesibles entre ellas.	☐	☐	☒
2.	Están establecidos los criterios de uso, perfiles de usuario, configuración y acceso a cada una de las redes.	☐	☐	☒
3.	Las redes tienen sistemas de filtrado de acceso y bloqueo de aplicaciones en función de los usuarios de la red.	☐	☐	☒
4.	En las distintas redes de alumnos existe algún sistema de control parental o protección de acceso a lugares inapropiados.	☐	☐	☒
5.	El centro dispone de un gráfico con el esquema de la estructura física de las redes de centro en la que se muestren la ubicación de dispositivos de red y asignación de IP.	☐	☐	☒
6.	Existen protocolos para el control de la descarga de materiales ilegales.	☐	☒	☐
7.	El centro tiene implementados cortafuegos de red.	☒	☐	☐

8.	Existe en el centro un protocolo sobre el acceso a las redes de centro de equipos o dispositivos personales por parte del personal docente, no docente y alumnos.	☐	☐	☒
9.	Existe un responsable para el mantenimiento de la seguridad de las redes locales de centro.	☐	☐	☒
10.	Existe un registro sobre incidencias relativas a la seguridad de la red	☐	☐	☒

REDES INALÁMBRICAS

1.	Los dispositivos de red (*router*, *wifis*, *plc*,…) tienen claves de acceso a la gestión registradas y suficientemente seguras, y son solamente accesibles desde la red local del centro.	☐	☐	☒
2.	Los puntos *wifi* y *routers* de aulas se apagan en periodos no lectivos.	☐	☐	☒
3.	Los dispositivos *wifi* disponen de un cifrado del tipo WPA2 con AES como mínimo.	☐	☐	☒
4.	El centro realiza un control periódico de los dispositivos que incorporan *wifis* virtuales.	☒	☐	☐
5.	Se realizan revisiones periódicas de configuración de *wifis* cobertura, claves de acceso y protocolo.	☐	☐	☒
6.	La potencia de los puntos *wifi*es adecuada al espacio que se desea utilizar (en el caso de *wifis* de aula o de administración).	☐	☒	☐
7.	En los periodos vacacionales se cierran los dispositivos de red prescindibles.	☐	☐	☒
8.	Existen limitaciones al acceso a los puntos *wifi* en función de la red de centro (filtrado de MAC, portales cautivos, claves de uso restringido…).	☐	☐	☒
9.	Se realizan revisiones periódicas de configuración de *wifis* cobertura, claves de acceso y protocolo.	☐	☒	☐
10.	El centro dispone de documentación sobre la organización tecnológica de las redes y servicios.	☐	☐	☒

SEGURIDAD DE EQUIPOS Y DISPOSITIVOS

1.	El centro tiene asignadas contraseñas de administrador y usuario con perfil de administración, y profesor y alumno con perfil estándar en los ordenadores y dispositivos de centro.	☐	☐	☒
2.	Existe un registro y criterios de centro para el uso de equipos personales y/o privados que acceden las redes del centro.	☒	☐	☐
3.	Se revisa la seguridad y uso de los equipos con periodicidad.	☐	☐	☒
4.	Los ordenadores del centro están inventariados, registrados, identificados y localizados.	☐	☐	☒

5.	Se dispone de inventario de software básico de los equipos, en general, con las licencias pertinentes	☐	☒	☐
6.	Se dispone de estrategias para la restauración de los equipos a estados anteriores (congeladores, recuperadores) o clonación de los mismos.	☐	☐	☒
7.	Todos los equipos disponen de programas de antivirus y control de malware adecuados a las características de los dispositivos.	☐	☐	☒
8.	En los dispositivos móviles del centro se tienen activadas las opciones de geolocalización antirrobo.	☐	☒	☐
9.	Los equipos y dispositivos de centro tienen activados los cortafuegos.	☐	☒	☐
10.	Las contraseñas de los usuarios son siempre de al menos 8 caracteres alfanuméricos	☐	☐	☒
11.	El software es instalado únicamente por responsables específicos, teniendo en cuenta las licencias disponibles y de seguridad para equipos y datos.	☐	☐	☒
12.	El alumno firma el compromiso de uso adecuado y seguro de los dispositivos de centro y de las redes del mismo.	☐	☐	☒
13.	Existen normas de buen uso de los equipos y dispositivos en los espacios en los que se utilizan.	☐	☐	☒
14.	Los navegadores están configurados para eliminar los datos al cerrar la sesión.	☒	☐	☐
15.	En los momentos de uso de los equipos y dispositivos en el centro por parte de los alumnos, siempre hay personal responsable.	☐	☐	☒

SERVICIOS DE INTRANET

1.	Existe un registro con indicación de características, definición de funciones y usuarios de servicios de intranet de centro (NAS, servidores de centro, nubes privadas de centro,…).	☒	☐	☐
2.	El centro tiene establecidos perfiles de usuario protegidos con contraseñas de seguridad en los servicios de intranet de centro: Administrador, profesorado, alumnado e invitados.	☐	☐	☒
3.	Se realizan copias de seguridad de datos con periodicidad de los documentos depositados en la intranet.	☐	☐	☒
4.	Los servicios de intranet están separados de los servicios de internet.	☐	☐	☒
5.	Se realiza un seguimiento del uso y la seguridad de los servicios de intranet.			

SERVICIOS DE INTERNET Y REDES SOCIALES

1.	Se analizan los datos antes de almacenarlos o subirlos a servicios de internet.	☐	☐	☒

2.	El centro tiene registrados todos los servicios de internet que utiliza, e identificado el responsable de cada servicio, así como registro de las cuentas y contraseñas del centro.	☐	☐	☒
3.	Se conocen los contratos y las condiciones de los servicios que se utilizan el centro y es aplicable en la legislación española.	☐	☒	☐
4.	El centro tiene registrados todos los servicios de internet que utiliza, e identificado el responsable de cada servicio, así como registro de las cuentas y contraseñas del centro.	☐	☒	☐
5.	La localización del almacenamiento físico de los datos se encuentra preferentemente en el Espacio Económico Europeo, o en empresas que han subscrito los principios del Puerto Seguro.	☐	☐	☒
6.	Los servicios de internet garantizan la integridad de los datos**,** y evitan el acceso de personal no autorizado.	☐	☐	☒
7.	Se ha comprobado que datos proporcionados a un servicio de internet no son cedidos a terceros proveedores.	☐	☒	☐
8.	Los servicios de internet permiten recuperar toda la totalidad de los datos en caso de que se produzcan incidencias de seguridad.	☐	☒	☐
9.	Los servicios de internet garantizan el borrado seguro de datos.	☐	☒	☐
10.	Las plataformas de aprendizaje que utiliza el centro permiten controlar los datos que se visualizan de los alumnos y en caso contrario se ha solicitado el consentimiento de los usuarios.	☐	☐	☒
11.	Se han solicitado permiso a los alumnos o padres para proporcionar los datos de carácter personal que permiten el acceso a las plataformas de aprendizaje o servicios de internet de terceros	☐	☒	☐
12.	En períodos vacacionales se revisan los perfiles, se eliminan permisos y servicios que no se utilicen.	☐	☐	☒
13.	Se hace un seguimiento de los servicios de internet en momentos vacacionales para controlar las posibles incidencias.	☐	☒	☐
14.	Los datos de carácter personal dispuestos en servicios de internet se suben encriptados.	☐	☐	☒
15.	El centro controla los materiales depositados en servicios de internet, y se respetan los derechos de autor y de distribución.	☐	☒	☐
16.	El centro tiene documentados los criterios de uso y los perfiles de los usuarios de los distintos servicios, así como las funciones de cada una de ellos.	☐	☐	☒

FORMACIÓN Y CONCIENCIACIÓN

1.	El centro desarrolla planes de formación y concienciación sobre el uso seguro de los equipos, redes y servicios de internet para el profesorado y personal no docente.	☐	☐	☒
2.	El centro integra objetivos y procesos de aprendizaje sobre el uso seguro de las tecnologías en el currículo escolar.	☐	☐	☒

3.	El Reglamento de Régimen Interior recoge los procesos y actuaciones a aplicar en el caso de uso inadecuado e incidencia en dispositivos y servicios.	☐	☐	☒
4.	El Reglamento de Régimen Interior contempla protocolos de actuación para hacer frente a las incidencias de seguridad.	☐	☒	☐
5.	El centro dispone de un Plan TIC de centro coordinado, evaluado, actualizado y aplicado actualmente en el centro.	☐	☐	☒
6.	El Plan TIC de centro hace referencia a la incorporación de la seguridad digital en el currículum. De este modo, el profesorado toma conciencia de su responsabilidad compartida.	☐	☐	☒
7.	Se informa anualmente a todo el profesorado sobre las novedades en seguridad digital.	☐	☐	☒
8.	Se insta a los padres a adoptar un papel activo en materia de seguridad digital y a reforzar los mensajes clave.	☐	☐	☒
9.	En caso de duda sobre seguridad, el profesorado sabe dónde solicitar orientación.	☐	☐	☒
10.	El centro cuenta con un profesor de referencia al que los alumnos pueden consultar sobre temas relacionados con Internet.	☐	☐	☒

ANEXO II - EVALUACIÓN DE APLICACIONES

Sobre la información ofrecida por los responsables de la aplicación:

Lo primero que se realiza es la disponibilidad de esa aplicación en: Microsoft Store o Centro de software de Educa.jcyl, en ese caso ese programa o aplicación se podrá descargar.

Si no fuera éste el caso, se solicita permiso al CAU para proceder a la instalación de ese programa y son ellos los que dan la autorización o no.

Sobre la ubicación de los datos:

Los datos deben estar almacenados en un país del Espacio Económico Europeo o un país que ofrezca un nivel de protección equivalente (que haya sido así acordado por la Agencia Española de Protección de Datos por Decisión de la Comisión Europea).

Se puede consultar el listado de países con nivel adecuado de protección en la página web de la Agencia Española de Protección de Datos. Asimismo, los datos también pueden localizarse en empresas ubicadas en Estados Unidos siempre que éstas se hayan acogido a los principios del Escudo de Privacidad.

Actualmente, la AEPD incluye los siguientes países en su lista:

- *Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000*
- *Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos*
- *Argentina. Decisión 2003/490/CE de la Comisión, de 3 de junio de 2003*
- *Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003*
- *Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004*
- *Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008*
- *Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010*
- *Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010*
- *Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011*
- *Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012*

- *Estados Unidos. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016.*

Sobre la seguridad de los datos:

La aplicación debe proveer mecanismos que permitan la realización de copias de seguridad o la descarga de los datos, de tal forma que el centro educativo pueda cumplir con las obligaciones que le son exigibles al respecto. El responsable CompDigEdu se encargará de la realización de copias de seguridad de los datos tratados mediante estas aplicaciones, así como del cambio anual de las contraseñas.

Igualmente, la aplicación debe implementar un mecanismo de autentificación que permita la identificación inequívoca y personalizada de los usuarios, recomendándose que este mecanismo consista en códigos de usuario y contraseñas, evitando la identificación de menores mediante datos biométricos (reconocimiento facial o huella dactilar).

Prueba de la aplicación:

La directora del IES, la responsable CompDigEdu y el profesor o profesores que deseen usar una aplicación, deberán realizarán una prueba de la aplicación de forma previa a su definitiva utilización en el centro, comprobando la corrección de las informaciones que fueron facilitadas por el responsable de la aplicación. Para la realización de esa prueba no se introducirán datos personales reales de los alumnos, ni se les involucrará en su utilización.

Se dejará constancia documental de las pruebas realizadas, reflejando los aspectos que hayan sido analizados y los resultados obtenidos.

ANEXO III - RECOMENDACIONES SOBRE SEGURIDAD Y *PRIVACIDAD (AEPD)*

- Es imprescindible tener cuidado al publicar imágenes y vídeos mediante apps y herramientas en nube para no poner en riesgo la intimidad de las personas.
- Se recomienda leer la información sobre el servicio (política de privacidad y condiciones de uso) antes de empezar a utilizarlo.
- Al utilizar redes sociales se recomienda configurar las opciones de privacidad en el perfil de usuario para permitir el acceso a la información publicada a un grupo conocido y previamente definido de usuarios.
- Al facilitar datos en cualquier ámbito (en cualquier tipo de aplicación, en el registro de usuarios, en los contenidos) evitar incorporar datos del domicilio de los menores y otros datos personales que puedan poner en peligro su seguridad. Debe recomendarse no atender la demanda que puedan tener las aplicaciones para recabar datos personales, que pueda llevar al tratamiento de datos excesivos.
- Las contraseñas deben ser robustas, evitando las que sean fáciles de adivinar por otras personas, con suficientes caracteres y compuestas por mayúsculas, minúsculas, números y caracteres especiales. No se deben facilitar nunca a otras personas.
- Para el almacenamiento de datos en la nube, se utilizarán OneDrive, el Aula Virtual Moodle corporativa y Teams.

CONSEJOS DE SEGURIDAD PARA EL BUEN USO DE INTERNET ELABORADAS DESDE EL IES DOCTOR SANCHO DE MATIENZO

- Realiza periódicamente **copias de seguridad** del sistema que permitan restaurarlo.
- Utiliza siempre **contraseñas seguras** (mayúsculas, minúsculas, caracteres no aleatorios, rápida de teclear, sin datos personales, etc.) y no tengas la misma contraseña para todas tus cuentas.
- Publica (fotos, vídeos, opiniones, etc.) **con responsabilidad** y **de forma consciente**. Todo lo que publicas en Internet se queda en Internet.

- No intercambies datos privados en redes WIFI de confianza.
- Instala y actualiza el **antivirus**.
- Ten **actualizado** el sistema operativo.
- Revisa periódicamente todos los **dispositivos externos** (*pen drives, discos duros, etc.*) que conectes al ordenador personal.
- Cuidado con las **descargas** de archivos o programas, pueden contener virus.
- No entregues datos personales en páginas que no sean de confianza, ni guardes contraseñas.
- Cuidado con el **spam**, **apps autorizadas** y **privacidad en las redes sociales**.
- Abre **sesiones** seguras y ciérralas al terminar.
- No abras correos electrónicos que no vengan a tu nombre ni de direcciones sospechosas o desconocidas.
- **Para favorecer la navegación y las búsquedas privadas** se aconseja, entre otros: 1) activar los modos privados de los navegadores; 2) pedir a los buscadores principales (Google y similares) que borren nuestros datos (en Google se puede hacer mediante el panel de control); 3) avisar a las páginas visitadas de que no queremos ser rastreados (los navegadores incluyen opciones *Do not track*); 4) borrar y controlar el uso de las galletas en el navegador para que no se recuerden nuestras visitas ni nuestra actividad en los sitios web que hemos visitado.
- ¡Actúa con cabeza!

ANEXO IV- REGISTRO DE INCIDENCIAS EN EQUIPOS INFORMÁTICOS Y AUDIOVISUALES

FECHA	EQUIPO	LOCALIZACIÓN	INCIDENCIA	SOLUCIÓN ADOPTADA