2024-2025

PLAN DE SEGURIDAD Y CONFIANZA DIGITAL

IES MONTES OBARENES

I.E.S. Montes Obarenes Miranda de Ebro

INDICE

1. INTRODUCCIÓN, IDENTIFICACIÓN DE LA ACTIVIDAD Y SERVICIOS

1.1. Justificación y dimensión del Plan

En la actualidad el centro presenta un contexto tecnológico-educativo complejo, con la aparición de nuevas herramientas, metodologías y escenarios de actuación. Todo ello impulsa la creación de un documento como este, que complemente al *Plan Digital* de centro en materia de seguridad y confianza digital.

La adaptación a la situación educativa originada por la pandemia de COVID-19 obligó a acelerar el proceso de integración de las TIC en el instituto, revalorizando las plataformas y aulas virtuales, e intensificando el uso de todas aquellas herramientas de comunicación electrónica que se han puesto a disposición de la comunidad educativa.

Cabe destacar la variedad y diversidad de herramientas digitales que se han incorporado a la actividad docente, aumentando la complejidad del contexto educativo, a la exposición de alumnado y profesorado, y al almacenamiento indiscriminado de datos en servidores de los proveedores de servicios.

A lo anterior se han de sumar una serie de factores que han condicionado la creación de un documento como este.

El primero de esos factores fue la entrada en vigor el 25 de mayo de 2018 del "*Reglamento General de Protección de Datos* (*RGPD)*", que establece una serie de requerimientos en entornos en los que se produce una recogida, tratamiento, gestión y almacenamiento de datos personales, dentro del cual se encuentra la actividad que realiza el centro.

El segundo es la envergadura del entorno tecnológico, pues a las medidas y tecnologías en materia TIC localizadas en el entorno físico del centro, hemos de sumar todas aquellas aplicaciones y tecnologías que presentan una naturaleza deslocalizada, fuera del recinto, y que hay que acotar mediante una serie de normas y medidas de seguridad para garantizar su correcto empleo.

El tercero es el grado de cumplimiento de los indicadores relacionados con la seguridad y la confianza digital planteados en el área 8 de la certificación "*CoDiCe TIC*", que establece una serie de ítems para medir el nivel de competencia digital del centro de acuerdo a los principios que se detallan en el marco de desarrollo común "*Marco Europeo para Organizaciones Educativas Digitalmente Competentes (DigCompOrg)*".

El cuarto es la competencia digital en materia de seguridad de los profesionales, familias y alumnado. El fomento de buenas prácticas en materia de seguridad y desempeño con nuevas tecnologías entre estos lleva a un aumento de la seguridad

individual en el empleo de nuevas tecnologías, fomentando su empleo en la acción docente e interacción social, fomentando, en definitiva, la mejora de la competencia digital de todos los intervinientes.

Así se pretende sentar unos principios reguladores en materia de seguridad, explícitamente recogidos, totalmente sujetos a evaluación, que permitan crear una base sobre la que desarrollar todas aquellas actividades de centro, y en la que los profesionales, familias y alumnado se sientan protegidos y seguros durante el empleo de nuevas tecnologías.

1.2. Identificación de la actividad y servicios

Partiendo de lo dispuesto en el RGPD, se establece, en primer término, que el plan de seguridad y confianza digital deberá identificar la actividad realizada y los tipos de servicios que se prestan en el centro.

El centro "IES Montes Obarenes" es un centro de Educación Secundaria Obligatoria y Bachillerato. Geográficamente situado en calle Francia 28 en Miranda De Ebro (Burgos), con número de teléfono 947427669 y correo electrónico de contacto 09007787@educa.jcyl.es.

La descripción y detalle de los niveles educativos impartidos y de los servicios prestados por y para su comunidad educativa se encuentran recogidos en su sitio web oficial alojado en la dirección http://iesmontesobarenes.centros.educa.jcyl.es.

2. TRATAMIENTO DE DATOS Y RESPONSABLES

Como consecuencia de la actividad educativa del centro, la creación, recogida, tratamiento y almacenamiento de datos es un componente fundamental, que permite que la acción docente pueda ser un proceso continuo y supervisado, y dota a los profesionales de la información necesaria para la toma de decisiones y medidas de carácter didáctico, informativo y disciplinario.

Sobre el tratamiento de datos personales la normativa indica que:

Cuando se trate de centros educativos públicos, el responsable del tratamiento será normalmente la Administración pública correspondiente: la Consejería de la Comunidad Autónoma competente en materia educativa, salvo para los centros de Ceuta y Melilla o los centros en el exterior titularidad del Estado dependientes del Ministerio de Educación Cultura y Deporte.

Así, como se indica en el RGPD, ha de identificarse un responsable del tratamiento de los datos personales, que en este caso es la administración educativa de la Junta de Castilla y León, a través del responsable nombrado para tal fin.

Responsable del tratamiento	DIRECCIÓN GENERAL DE POLÍTICA EDUCATIVA ESCOLAR (Consejería de Educación).	Avda. Reyes Católicos N.º 2, CP 47006, Valladolid Teléfono: 983 41 48 77 Correo electrónico: protecciondatos.dgpee.educacion@jcyl.es
		Delegado de Protección de Datos: Avenida Monasterio de Nuestra Señora de Prado s/n C.P. 47014, Valladolid. Mail: dpd.educacion@jcyl.es

Los centros docentes están legitimados por la Ley Orgánica de Educación de 2006 (LOE) para el tratamiento de los datos en el ejercicio de la función educativa. También están legitimados para el desarrollo y ejecución de la relación jurídica que se produce con la matriculación del alumnado en un centro, así como por el consentimiento de los interesados, o de sus padres o tutores si son menores de 14 años.

La procedencia y contenido de estos datos permite su clasificación en los siguientes tipos:

① **Datos del alumnado**. La ley orgánica en materia educativa legitima a los centros a recabar datos de carácter personal para la función docente y orientadora del alumnado en referencia a:

- El origen y ambiente familiar y social.
- Las características o condiciones personales.
- El desarrollo y resultados de su escolarización.
- Las circunstancias cuyo conocimiento sea necesario para educar y orientar a los alumnos.

Incluyendo otras categorías especiales de datos, como son los de salud o de religión cuando fuesen necesarios para el desempeño de la función docente y orientadora.

Así, los datos del alumnado pueden ser diferenciados entre:

- ***Datos personales de los alumnos***. Datos procedentes de la aplicación *Stilus*. Estos proceden de los procesos de admisión, en el caso del alumnado nuevo, y de anteriores procesos de matrícula. En la actualidad el servidor que alberga el programa y la base de datos de GEIWin se encuentra virtualizado en un centro de procesado de datos

externo al cual se tiene acceso mediante sesiones de escritorio remoto. El acceso y consulta de datos puede ser realizada por el personal administrativo, el equipo directivo y el profesorado mediante el aplicativo online *Stilus Enseña* empleando sus cuentas corporativas.

Si como consecuencia del empleo de la aplicación se generasen tablas y listados para uno personal del profesorado, estos tendrán la obligación de salvaguardar y custodiar los datos descargados y almacenados en los dispositivos empleados.

- ***Expedientes académicos*:** creados en formato físico y digital, almacenados por la administración del centro. Estos incorporan tanto datos personales del alumnado, progenitores o tutores legales, que fueron recogidos durante el proceso de matrícula, como datos académicos, sanitarios y otros datos descriptores de alguna situación relevante del alumno.

  Al comienzo del curso los centros de origen de primaria envían en formato físico (papel) los informes del alumnado que se incorpora al centro. Estos informes son recibidos, supervisados y almacenados junto al resto de información personal del alumno cuyo conocimiento sea necesario para formar y orientar a los alumnos, como indica la ley.

② **Datos del personal docente:** datos personales y laborales del personal docente activo en el centro y de todos aquellos que en un momento determinado formaron parte de la plantilla. Esta información se encuentra en formato físico y digital, esta última, almacenada en la base de datos del aplicativo *Stilus*. Estos datos son recogidos y custodiados por el personal de administración en el momento de la incorporación al centro.

Los documentos y datos relativos a las solitudes de permisos, ausencias y sus correspondientes justificaciones, son recibidos y almacenados por jefatura de estudios, siendo posteriormente enviados a inspección educativa.

③ **Datos en documentos oficiales:** datos que forman parte de la documentación oficial del centro, que, entre otros, recogen nombres y apellidos de los participantes en los claustros, reuniones y otras actividades de centro que requieran de esta información. Se encuentran tanto en formato digital como físico en poder de dirección y la secretaria del centro.

En el caso de las programaciones didácticas y actas de reuniones de departamento, al contener los datos personales de los miembros de los departamentos, son consideradas en este apartado. Estas se encuentran en ambos formatos y custodiadas por los jefes de los departamentos docentes y por dirección. En el caso de las programaciones didácticas también estarán

alojadas en la web del instituto en el espacio "DOCUMENTOS INSTITUCIONALES".

④ **Datos de proveedores de servicios**: datos que identifican a empresas proveedoras de servicios a través de facturas, albaranes y cualquier otro de documento contable. Estos se encuentran disponibles en formato físico y digital, custodiados por la secretaria del centro.

⑤ **Datos de seguridad y credenciales**: datos que recogen los usuarios y contraseñas de los equipos de centro, de los perfiles de servicios y correos electrónicos oficiales, configuración de redes y accesos e información sensible relacionada con la seguridad informática del centro. Debido a su naturaleza se encuentra únicamente en formato digital. Se encuentra custodiada por la secretaria de centro y es únicamente accesible por la secretaria y el personal encargado del mantenimiento y supervisión de ese equipamiento.

En el caso de las credenciales personales necesarias del alumnado para el acceso a las plataformas digitales como *Moodle* u *Office 365*, una vez entregadas por el centro, será el alumno el responsable exclusivo de su custodia, actualización y empleo; y deberá informar al centro de cualquier percance que pudiera surgir. El centro no es responsable de almacenar tales credenciales, sí de solicitar unas nuevas en caso de pérdida tras haberse agotado los otros medios por los que el alumno o las familias pueden recuperarlas.

⑥ **Datos en pruebas escritas:** Los exámenes realizados por los distintos departamentos deberán ser almacenados y custodiados por los profesores que los realizan. Atendiendo a las indicaciones de la Agencia Española de Protección de Datos (AEPD) "*Los exámenes de los alumnos no deberían mantenerse más allá de la finalización del periodo de reclamaciones*", debiendo ser destruidos tras finalizado el citado periodo.

⑦ **Contenido multimedia (fotografía, vídeos, sonido).** Para que pueda registrarse sonora o gráficamente al alumnado durante las actividades realizadas por el centro, debe tenerse previamente la autorización expresa de las familias o tutores, autorizando la captura y difusión de tales contenidos para todos aquellos alumnos de edad inferior a 14 años. Para el alumnado de 14 años y mayores, bastará con su consentimiento expreso.

La autorización o negación directa de las familias o tutores es recogida al comienzo del curso mediante documento incluido en el sobre de matrícula (A*nexo A: documento informativo sobre protección de datos y tratamiento de imágenes*).

Si el profesorado dispone de la autorización expresa de los interesados, o de las familias o tutores en caso de ser menores de 14 años, todo el contenido gráfico obtenido durante las actividades deberá ser almacenado en los equipos de los departamentos encargados o del departamento de actividades complementarias y extraescolares si fueran de tal naturaleza, pasando estos a ser los custodios de tales datos y garantizando su seguridad y no difusión.

Como se indica en la normativa, los titulares podrán ejercer control sobre sus datos tratados. Estos derechos son los de **acceso, rectificación, cancelación y oposición**. Este control podrá ser ejecutado, previa información, con la finalidad de bloquear estos datos personales.

3. LÍNEAS DE ACTUACIÓN

3.1. Formación del alumnado, familias y profesorado

Como se indica en el *Plan Digital*, el contexto tecnológico del centro supera los límites físicos de este, llegando a los domicilios de nuestro alumnado y en consecuencia involucrando a las familias en este nuevo espacio. Estas han pasado a tener la necesidad de acceder a todas aquellas herramientas oficiales para consultar resultados académicos, acceder a información oficial y colaborar en las actividades programadas empleando las plataformas digitales.

Así, se programan líneas de actuación dentro del plan de seguridad, cuya misión es la de informar y formar sobre medidas de actuación y buenas prácticas en el empleo de recursos digitales, ya sean de carácter oficial o lúdico.

A. FORMACIÓN DEL ALUMNADO.

La atención formativa del alumnado en materia de seguridad se desarrolla en torno a las siguientes actividades:

1.- **Actividades dentro del contenido curricular de los departamentos**. Aquellos departamentos con contenidos curriculares en materia de TIC, planean y desarrollan unidades didácticas y actividades que se llevan al aula. Cabe la posibilidad de su inclusión en las programaciones didácticas como contenido transversal.

2.- **Sesiones de formación de la comisión TIC**. También como una actividad del *Plan de Acogida*, los integrantes de la comisión imparten sesiones a los distintos grupos en las horas de tutoría siempre que sea posible. El contenido aborda el tratamiento de las credenciales de acceso a las plataformas y herramientas oficiales. Aspectos como la creación de contraseñas seguras, custodia de las mismas y su recuperación tras olvido o pérdida de confianza.

3.- Actividades desarrolladas dentro del plan de Seguridad y confianza digital provincial.

Las actuaciones propuestas se apoyan en el Plan de seguridad y confianza digital en el ámbito educativo (Orden EDU/834/2015, de 2 de octubre).

Una de las actividades propuestas, como en cursos anteriores, consiste en la creación de un vídeo corto, de producción propia, que permita promocionar la privacidad, seguridad, confidencialidad e identidad digital.

En el caso de Educación Secundaria el contenido a desarrollar consiste en la elaboración de un corto y una campaña publicitaria.

4.- Actividades propuestas por el plan provincial de integración de las TIC en el aula.

Desde el grupo de trabajo provincial de integración de las TICA, se proponen actividades enmarcadas dentro de la semana de la seguridad en la red, llevada a cabo de forma anual la primera semana de febrero.

B. FORMACIÓN DE LAS FAMILIAS.

En lo referente a la formación a las familias sobre las tecnologías TICA, en el presente curso 2024-2025, desde el centro se difundirá y favorecerá el desarrollo de los talleres de formación propuestos por la administración educativa.

Para la difusión de esta información se cuenta con la colaboración del AMPA, además del sitio web y las redes sociales del centro.

C. FORMACIÓN DEL PROFESORADO.

En el plan de formación de centro se define un itinerario para el desarrollo de la competencia digital. Para cursos posteriores, se propone la planificación de acciones formativas del profesorado en materia de almacenamiento y custodia de datos. Esto permitirá dotar al profesorado de pautas y directrices que le permitan el tratamiento de datos personales con confianza.

3.2. Equipamiento informático

Los cambios en el contexto tecnológico de centro han obligado a una profunda revisión de las medidas de seguridad del equipamiento informático y de la red de centro.

A. MEDIDAS FÍSICAS DE SEGURIDAD.

- ***Higiene de los cableados*.** En todos los puestos informáticos de trabajo ubicados en aulas los cables se encuentran agrupados y anclados a los puestos mediante la utilización de bridas, canaletas o pasa-cables. En función de la disposición de los puestos de trabajo, si es posible, el cableado

no es accesible por el alumnado. Esto disminuye el desgaste del cableado por fricción con el suelo y evita que el profesorado tropiece o se arrastren los cables durante la limpieza del aula.

En el caso de las salas de informática el cableado se encuentra distribuido por canaletas, tanto en paredes como en las mesas, asegurado mediante bridas y con las tomas de corriente no accesibles por el alumnado.

- ***Acceso limitado a sala*.** Las oficinas, salas de informática, laboratorios y departamentos que contienen información, recursos o bienes de importancia tienen el acceso limitado al personal autorizado. Así, el acceso al equipamiento informático de los departamentos, oficinas de jefatura, dirección y administración, solo se permite al personal que los emplea y a otros en su presencia, además del personal o profesionales de mantenimiento. En horario no lectivo, o de no servicio, permanecen cerrados.

B. MEDIDAS LÓGICAS DE SEGURIDAD.

Criterios de acceso mediante usuarios registrados y permisos. Todos los equipos informáticos se encuentran integrados en el dominio de la red de centros, siendo su acceso exclusivo mediante el empleo de las credenciales de Educacyl.

Esta política de acceso es aplicable tanto al personal administrativo, como al equipo directivo, docentes y alumnado.

En lo referente al acceso de equipamiento de aula y dispositivos portátiles, al encontrarse dentro del dominio EducaCyL, atenderán a los mismos criterios anteriores. Profesorado y alumnado accederán mediante el empleo de sus credenciales de EducaCyL.

El acceso a estos equipos para su mantenimiento queda limitado en exclusiva a los técnicos del CAU.

C. MEDIDAS DE PUESTA EN MARCHA DE EQUIPAMIENTO NUEVO.

- ***Inventariado del equipo y catalogación***. Tras la recepción de los dispositivos la secretaria, en colaboración con los responsables de mantenimiento informático, los registrará en el inventario del centro.

  Durante el curso 2024-2025 se continuará la labor con la nueva dotación de equipamiento informático.

- ***Configuración* inicial del equipamiento nuevo**. Todo equipamiento de nueva adquisición se incorporará a la red de centro y su acceso estará regulado por el dominio EducaCyL. Esto implica que la puesta en marcha inicial, actualización, instalación de *drivers* y del todo aquel *software*

necesario para su empleo corra a cargo del CAU, que deberá ser informado mediante incidencia realizada al número de asistencia.

D. MEDIDAS DE MANTENIMIENTO.

- ***Registro de la incidencia***. Todas las incidencias de carácter informático se deberán registrar previamente en el formulario disponible a tal efecto en el "Espacio Profesorado" de la página web del instituto o en el registro habilitado en la conserjería del centro. En este registro se hará constar el nombre del solicitante, fecha de la incidencia, aula o zona donde se ubica el dispositivo y una descripción de la avería o mal funcionamiento. Los responsables de mantenimiento podrán solicitar más información, actualizar el estado de la reparación e indicar el tiempo invertido en la misma.

- ***Evaluación de la incidencia y respuesta***. En el Plan Digital ya se detalla el protocolo a seguir en caso de tener que hacer frente a la reparación por uno de los encargados del mantenimiento informático del centro. Este está detallado en el anexo B: *Protocolo de garantías de operatividad y continuidad de los servicios frente a incidencias*.

  En caso de que la incidencia sea consecuencia de un uso irresponsable por algún miembro de la comunidad educativa, el responsable informará a la secretaria para que, desde dirección, y conforme a lo establecido en el RRI, se tomen las medidas oportunas.

- ***Mantenimiento por empresa externa***. En el caso de incidencias relacionadas con la red de escuelas conectados o de imposible resolución por parte del centro, hay que ponerse en contacto con el "*Centro de Asistencia al Usuario" CAU* (983 – 41 87 45 – 6336), con objeto de que dicha incidencia quede registrada informando, tanto al personal de la asistencia técnica (*SATIC*), como a los técnicos de telecomunicaciones, o a los técnicos de informática (Servicios Centrales y/o Provincias), dependiendo del caso, para que puedan proceder a su resolución.

  Se indica de <u>forma explícita</u> que las empresas de mantenimiento ajenas al CAU, no pueden actuar ni sobre el equipamiento de los centros que esté en red, ni en la electrónica del centro, ni en el equipamiento de escuelas conectadas, ni en la instalación de software.

  Si la incidencia se encuentra en equipamiento informático que no se puede considerar dentro del supuesto anterior, y precisa ser trasladado del centro al SAT de una empresa externa, esta deberá responsabilizarse de la confidencialidad de los datos almacenados si los hubiera. Para ello, el encargado de retirarlos deberá firmar el documento de responsabilidad,

cuyo modelo se detalla en el anexo C: *Responsabilidad de custodia de datos por empresa externa.*

E. PRÉSTAMO DE EQUIPAMIENTO INFORMÁTICO.

Actualmente el centro posee equipamiento informático portátil, que puede ser cedido temporalmente para su empleo dentro y fuera del centro educativo. Este préstamo podrá realizarse tanto a miembros del alumnado como a docentes previa solicitud a la comisión TICA del centro, quien estudiará la concesión o no del préstamo.

Cuando este se produzca para ser empleado fuera del centro, el receptor, deberá leer y aceptar las condiciones indicadas en el documento anexo F: *Préstamo de equipamiento informático*. Se firmarán tres copias del mismo: una para el interesado, una para la secretaria del centro y la última para la persona responsable de medios.

F. MEDIDAS DE ELIMINACIÓN DE EQUIPAMIENTO OBSOLETO.

- ***Realización de copias de seguridad*.** Cuando el equipo sea dado de baja en el inventario del centro por quedar obsoleto o por avería irreparable, sobre este se deberá realizar copia de seguridad del contenido cuando sea haya empleado por el equipo directivo, administración o los departamentos didácticos. Los equipos de aula quedarán a decisión del encargado del mantenimiento con conocimiento de la secretaria.
- ***Borrado de seguridad*.** Previo al traslado al punto de reciclaje, aquellos medios magnéticos y de estado sólido que hayan podido albergar datos deberán ser sometidos a borrados de seguridad.

3.3. Red de centro

Uno de los activos más importantes dentro del contexto tecnológico-educativo es la red de centro. Como se detalla en el Plan Digital, es el eje vertebrador de las comunicaciones con el exterior, el soporte de la red interna y una herramienta didáctica que se ha ido convirtiendo en un recurso clave.

Esta importancia hace que se hayan desplegado una serie de medidas de protección, además de una serie de normas para el correcto uso y empleo de la red como recurso, las cuales son recogidas en el anexo D: *Normas generales sobre el acceso y empleo de la red de centro*.

A. MEDIDAS FÍSICAS.

- ***Acceso limitado a recintos de telecomunicaciones y racks de aula*.** Todas aquellas salas que alberguen exclusivamente equipamiento electrónico de red serán consideradas recintos de telecomunicaciones. Por lo que deberán

permanecer cerradas y solamente accesibles previa autorización por parte de la secretaria y/o responsables de mantenimiento del centro. El equipamiento de red que se encuentre instalado en aulas deberá estar contenido en armarios o *racks* homologados, cerrados bajo llave y accesibles bajo las condiciones anteriores.

La red de centro se encuentra estructurada en torno a una serie de *racks* centrales unidos entre sí mediante fibra óptica multimodo y cableado UTP Cat6. Estos armarios reciben el cableado de datos y de potencia mediante canaletas y accesos físicos habilitados en los mismos. Estos se encuentran cerrados bajo llave, que son custodiadas por la secretaria y las personas encargadas del mantenimiento de medios informáticos.

- ***Cableado estructurado canalizado***. La mayor parte de la instalación de la red está realizada mediante cable UTP Cat5, conducido a través de canaletas de plástico. Esto impide accesos directos al cable y a su manipulación. Además de ser una medida de seguridad frente a enganches y tropiezos.

  El cableado que discurre por falsos techos no se encuentra con esta disposición.

B. MEDIDAS DE ACCESO LÓGICO.

- ***Acceso a la electrónica de red***. La electrónica de red inteligente (*routers*, *switchs* y puntos de acceso) son dispositivos gestionados de forma remota por el servicio central de gestión. Tienen acceso a ellas los encargados de mantenimiento y personal del CAU.

  En el caso de la electrónica de red perteneciente a escuelas conectadas, el centro no dispone de registro ni modo de acceso a la configuración de este equipamiento.

- ***Hardware de seguridad***. Viene implementado por la red de escuelas conectadas y por la red educativa, por ello no gestionable por el centro.

- ***Líneas de red telefónica conmutada (RTC)***. Las comunicaciones para los servicios de mantenimiento del ascensor y alarma son encauzadas al exterior mediante líneas telefónicas analógicas (RTC) independientes. Estas son gestionadas y mantenidas por las empresas de servicios.

- ***Segmentación IP de la red* y *Virtualización de la red***. La implementada por escuelas conectadas y por la red educativa. Diferenciando redes independientes: administración, navegación, red inalámbrica y dispositivos.

- ***Red inalámbrica WiFi***. La red inalámbrica principal de centro ha sido sustituida por la red de escuelas conectadas, de forma que el centro no se encarga de su gestión.

C. MEDIDAS DE PUESTA EN MARCHA DE EQUIPAMIENTO DE RED NUEVO.

Como consecuencia de la integración total de la infraestructura de escuelas conectadas, **el centro no podrá incorporar equipamiento de red nuevo sin informar previamente al CAU**. Este será el encargado de evaluar el tipo de equipo a instalar, su configuración inicial, inventariado y puesta en marcha.

D. MEDIDAS DE MANTENIMIENTO.

Se siguen las mismas medidas que las indicadas en el equipamiento informático. En el documento del Plan Digital de centro, se detalla el protocolo a seguir en caso de incidencia y las medidas a realizar para garantizar el funcionamiento de centro, incluyendo las medidas de mantenimiento de la red.

A esto se añade la existencia de un protocolo de supervisión (anexo E: *Protocolo de supervisión de la red de centro*), donde se detallan los pasos del procedimiento, el testeo de funcionamiento y seguridad de la red.

E. MEDIDAS DE ELIMINACIÓN DE EQUIPAMIENTO OBSOLETO.

Se siguen las mismas medidas que las indicadas en el equipamiento informático.

3.4. Servicios de red online

En el Plan Digital se detallan una serie de normas que definen el protocolo de difusión de contenidos a través de redes y servicios externos.

- Sólo se permite el empleo de los servicios oficiales dados de alta y registrados por el centro para la divulgación de contenidos relacionados con cualquier actividad docente o de otra índole realizada en él.
- Si como consecuencia de la aplicación de la programación didáctica se necesitase el alta de un perfil de centro en un servicio concreto, se deberá informar, con antelación, a la comisión TICA para iniciar la activación del mismo a través del CAU.
- Antes de añadir cualquier tipo de contenido en el que aparezcan alumnos, el encargado de la publicación deberá cerciorarse que todos los alumnos (mayores de 13 años) o los familiares firmaron el consentimiento para la publicación de contenidos de imagen, vídeo o voz de los alumnos en cuestión.
- Al finalizar el curso se deberá cesar la actividad del perfil de centro en los servicios de terceros, siendo necesaria la copia de seguridad del contenido, si así se decidiese, y la eliminación de toda la información relacionada con el alumnado.

- El centro no se hace responsable de los comentarios publicados por los usuarios como respuesta a los contenidos en los servicios oficiales.

3.5. Destrucción de documentación en formato papel y óptico

Las disposiciones sobre protección de datos establecen que todo aquel soporte físico que posea datos identificativos, o cualquier otro que permita la identificación indirecta de un particular, en el caso de ser destinado a destrucción, deberá ser destruido garantizando la imposibilidad de acceder a los datos.

Para tal fin, el centro dispone de varias destructoras de papel que cumplen las funciones anteriormente citadas. Por lo que todo profesional del centro que se disponga a destruir cualquier prueba escrita o documento con datos identificativos deberá emplear ese medio para su eliminación.

En el caso de encontrarse almacenado en soportes ópticos CD, DVD y *BlueRay*, deberá consultarse si las destructoras de papel están equipadas para destruir ese tipo de soporte. En caso de no ser así, se consultará con la persona responsable de medios del centro.

3.6. Credenciales de acceso: Contraseñas

Para la creación de las credenciales de acceso a los servicios externos (redes sociales, registros web, etc.), se siguen las indicaciones del "*Instituto Nacional de Tecnología de la Comunicación (INTECO)*" en su documento "*Política de contraseñas y seguridad de la información*".

En él se establecen los criterios mínimos:

1. Se deben utilizar al menos 12 caracteres para crear la clave.

2. Se recomienda utilizar en una misma contraseña dígitos, letras y caracteres especiales.

3. Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas. Hay que recordar qué letras van en mayúscula y cuáles en minúscula. Según el mismo estudio, el 86% de los usuarios utilizan sólo letras.

4. Cambio regular de contraseña, evitando generar reglas secuenciales de cambio.

5. Utilizar signos de puntuación, si el sistema lo permite.

En el caso de las credenciales de acceso a las cuentas EducaCyL se seguirán las indicaciones de seguridad aportadas por la administración. Esta dará las pautas necesarias sobre la longitud, composición y periodicidad de actualización de las contraseñas asociadas.

El centro dispone de un registro digital de todas las contraseñas relacionadas con las cuentas de perfiles de servicios oficiales externos. Este registro se encuentra custodiado por la secretaria del centro y accesible por las personas encargadas del mantenimiento informático y de red.

En este registro ya no aparecen las credenciales de acceso a la electrónica de red, ya que esta ha pasado a formar parte de la infraestructura de escuelas conectadas.

Los accesos a perfiles de conexiones *wifi* o a las herramientas oficiales, al ser de carácter personal, no se albergarán en este registro.

En el momento que el personal docente de centro o externo necesite las credenciales para accesos a los servicios externos (redes sociales, web de centro, etc.), realizará una solicitud a la secretaria, quien concederá permiso tras evaluar las motivaciones y la seguridad.

3.7. Copias de seguridad

La política de copias de seguridad establece una serie de criterios que también se encuentran definidos en el Plan Digital de centro.

Las medidas de copias de seguridad dependerán del carácter de los datos tratados y de los profesionales que realizan el proceso.

A. ***Almacenamiento de datos personales y documentos institucionales***.
   Los documentos institucionales contenidos en los equipos de administración y dirección son albergados en el OneDrive corporativo y deberán ser respaldados mediante copia periódica en una unidad de disco duro externo, custodiada por la directora.

B. ***Almacenamiento de datos personales y recursos de aprendizaje y enseñanza en los departamentos***.

   Recae sobre los departamentos y los docentes a título individual. Actualmente el profesorado recurre a dispositivos de almacenamiento portátil (discos externos, DVDs y memorias USB), que tiene carácter personal no gestionado por el centro. Es altamente aconsejable el almacenamiento en servicios *cloud* como *OneDrive* para la deslocalización de los datos y favorecer la accesibilidad remota. En el caso de datos personales no se recomienda la utilización de otros proveedores de almacenamiento online, esto garantizará el cumplimiento del RGPD.

4. TRATAMIENTO DE DATOS POR EMPRESAS EXTERNAS

Como fija el RGPD, dentro de sus obligaciones como custodio de los datos, el centro en ningún momento cederá los datos personales o académicos a empresas externas o a terceros.

Cuando el acceso a datos se pueda producir de manera indirecta, como es el caso de los momentos en los que empresas de mantenimiento accedan a equipamiento informático que posea información sensible, se seguirá el proceso establecido en el punto anterior relacionado con el mantenimiento del equipamiento informático. Así se hace imprescindible que la empresa de mantenimiento, o sus representantes, firmen el documento cuyo contenido se encuentra en el anexo C: *Responsabilidad de custodia de datos por empresa externa.*

5. PUBLICACIÓN DE CONTENIDOS Y NORMAS DE SEGURIDAD

Este plan servirá como medio para la publicación de las normas, reglas, protocolos y derechos relacionados con la adquisición, almacenamiento y cancelación de datos.

Su publicación se realizará en las siguientes etapas:

- Presentación de una adaptación de este documento a las jefaturas de departamentos en CCP, para que sean difundidos y tratados en las reuniones de departamento. El soporte para esta documentación será el aplicativo WEB del profesorado.
- Creación de infografías para el alumnado. Tratamiento en las sesiones de formación.
- Comunicación a las familias y alumnado a través de modelos como el documento anexo A: *Documento informativo sobre protección de datos y tratamiento de imágenes*. Posibilidad de creación de infografías orientadas a las familias.

6. EVALUACIÓN DE LA EFICIENCIA DEL PLAN DE SEGURIDAD

Como ocurre con el resto de planes de centro, se determina una herramienta de supervisión del plan y evaluación de su impacto.

Para ello se establece la revisión trimestral del nivel de despliegue y efecto de las medidas al comienzo del primer y segundo trimestre. En el tercer trimestre se realizará al final del mismo y tendrá carácter final.

Los encargados serán los miembros de la comisión TIC seleccionados para tales funciones. Para ello se empleará la herramienta de autoevaluación que se muestra en la siguiente tabla:

EVALUACIÓN DEL PLAN DE SEGURIDAD Y CONFIANZA DIGITAL				
FECHA DE LA REVISIÓN				
TIPO DE REVISIÓN (TRIMESTRAL/FINAL)				
RESPONSABLE DE LA REVISIÓN				
1	**MEDIDAS EQUIPAMIENTO INFORMÁTICO**	**MEDIDAS FÍSICAS**		1 2 3 4 □□□□
2		**MEDIDAS LÓGICAS**		1 2 3 4 □□□□
3		**MEDIDAS PUESTA EN MARCHA EQUIPAMIENTO NUEVO**		1 2 3 4 □□□□
4		**MEDIDAS DE MANTENIMIENTO**		1 2 3 4 □□□□
5		**MEDIDAS DE ELIMINACIÓN DE EQUIPAMIENTO OBSOLETO**		1 2 3 4 □□□□
6	**MEDIDAS RED DE CENTRO**	**MEDIDAS FÍSICAS**		1 2 3 4 □□□□
7		**MEDIDAS DE ACCESO LÓGICO**		1 2 3 4 □□□□
8		**MEDIDAS PUESTA EN MARCHA EQUIPAMIENTO NUEVO**		1 2 3 4 □□□□
9		**MEDIDAS DE MANTENIMIENTO**		1 2 3 4 □□□□
10		**MEDIDAS DE ELIMINACIÓN DE EQUIPAMIENTO OBSOLETO**		1 2 3 4 □□□□
11	**SERVICIOS DE RED ONLINE**	**ACTUALIZACIÓN DEL DOCUMENTO TÉCNICO**		1 2 3 4 □□□□
12		**CUMPLIMIENTO NORMAS PROTOCOLO DE DIFUSIÓN DE CONTENIDOS**		1 2 3 4 □□□□
13	**MEDIDAS DOCUMENTACIÓN FORMATO PAPEL Y ÓPTICO**			1 2 3 4 □□□□
14	**MEDIDAS CREDENCIALES DE ACCESO.**			1 2 3 4 □□□□
15	**MEDIDAS COPIAS DE SEGURIDAD**			1 2 3 4 □□□□
16	**ACTUACIONES SEGURIDAD Y CONFIANZA DIGITAL**			1 2 3 4 □□□□
17	**MEDIDAS TRATAMIENTO DATOS POR EMPRESAS EXTERNAS**			1 2 3 4 □□□□
18	**ACTUALIZACIÓN INVENTARIO ACTIVOS INFORMÁTICOS CRÍTICOS**			1 2 3 4 □□□□
19	**DIFUSIÓN DE LAS MEDIDAS DEL PLAN DE SEGURIDAD**			1 2 3 4 □□□□
20	**IDENTIFICACIÓN DE LOS TIPOS DE DATOS PERSONALES Y RESPONSABILIDADES**			1 2 3 4 □□□□
21	**REVISIÓN DE INCLUSIÓN EN EL PLAN TIC DE CENTRO**			1 2 3 4 □□□□

VALORACION FINAL:	1 2 3 4 □□□□

IDENTIFICACIÓN DE LOS NIVELES DE VALORACIÓN:

[4]: Las medidas contempladas son actuales, perfectamente detalladas, identificando a los responsables de su aplicación.

[3]: Las medidas contempladas son actuales, perfectamente detalladas, pero no se identifican a los responsables de su aplicación.

[2]: Las medidas contempladas no son actuales o no están perfectamente detalladas o no se identifican a los responsables de su aplicación.

[1]: Las medidas contempladas no son actuales, ni están perfectamente detalladas y no se identifican a los responsables de su aplicación.

7. LÍNEAS Y ACTUALIZACIONES FUTURAS DEL PLAN DE SEGURIDAD

El presente plan define una estructura de seguridad de centro sometida a continuas revisiones, adaptaciones y actualizaciones. Para determinar una línea de actuación en futuras mejoras se establecen unos puntos orientadores.

1. Reafirmar el plan de seguridad y confianza digital como documento público que ha de ser conocido y sus reglas aplicadas para conseguir un entorno tecnológico estable y seguro.
2. Ampliar la formación del profesorado en materia de aplicación del reglamento general de protección de datos, definiendo entorno de aplicación, responsabilidades y adecuación de las medidas individuales para la custodia de datos.
3. Asegurar la presencia del plan de seguridad dentro del Plan Digital, y de sus medidas en todos los documentos oficiales de centro, reflejando con ello la importancia de la consideración de este, como documento base o parte de los restantes.

ANEXO A: Documento informativo sobre protección de datos y tratamiento de imágenes

Junta de Castilla y León
Consejería de Educación

INFORMACION SOBRE PROTECCIÓN DE DATOS TRATAMIENTO DE IMÁGENES/VOZ DE ALUMNOS EN CENTROS DE TITULADIDAD PÚBLICA DE LA COMUNIDAD DE CASTILLA Y LEÓN REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016.		
EPÍGRAFE	**INFORMACIÓN BÁSICA**	**INFORMACIÓN ADICIONAL**
Responsable del tratamiento	**DIRECCIÓN GENERAL DE POLÍTICA EDUCATIVA ESCOLAR (Consejería de Educación)**	Avda. Reyes Católicos nº 2, CP 47006, Valladolid Teléfono: 983 41 48 77 Correo electrónico: protecciondatos.dgpee.educacion@jcyl.es
		Delegado de Protección de Datos: Avenida Monasterio de Nuestra Señora de Prado s/n C.P. 47014, Valladolid. Mail: dpd.educacion@jcyl.es
Finalidad del tratamiento	Difusión de las actividades de los centros docentes de titularidad pública de Castilla y León.	Usamos los datos relativos a imágenes/ voz de los alumnos, con la finalidad de difundir las actividades de los centros docentes de titularidad pública de la Comunidad de Castilla y León a través de los medios de difusión del centro que se detallan en el documento que figura en el anverso de esta información por el que se otorga o deniega el consentimiento para este tratamiento.
		Las imágenes/voz almacenadas en sistemas de almacenamiento de la Consejería de Educación o contratados con terceros, serán conservadas durante el curso académico en el que sean tomadas.
Legitimación del Tratamiento	Consentimiento	**Artículo 6.1 a) del RGPD Consentimiento** de los padres o tutores para aquellos alumnos menores de 14 años, o de los propios alumnos, cuando tengan 14 o más años. El consentimiento se solicitará y deberá en su caso otorgarse para cada uno de los medios de difusión citados, siendo posible que se autorice el tratamiento de las imágenes/voz en unos medios de difusión y en otros no. Si se toman imágenes/voz a través de fotografía, vídeo o cualquier otro medio de captación, de alumnos que no han consentido el tratamiento, se procederá a distorsionar sus rasgos diferenciadores, especialmente cuando en una foto/vídeo concurran con otros compañeros que sí cuenten con la autorización para el tratamiento de sus imágenes/voz.
Destinatarios de cesiones o Transferencias Internacionales	No se cederán datos a terceros.	La difusión de datos de imagen/voz en redes sociales supondrá una comunicación de datos a terceros, atendiendo a la naturaleza y funcionamiento de estos servicios.
	No están previstas transferencias Internacionales de datos.	
Derechos de las personas interesadas	Derecho a acceder, rectificar, y suprimir los datos, así como otros derechos recogidos en la información adicional.	Tiene derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad, en los términos de los artículos 15 a 23 del RGPD.
		Tiene derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada.
		Puede ejercer estos derechos ante el responsable del tratamiento o ante el Delegado de Protección de datos
		Tiene derechos a reclamar ante Agencia Española de Protección de Datos www.aepd.es

Junta de Castilla y León
Consejería de Educación

CONSENTIMIENTO INFORMADO TRATAMIENTO DE IMÁGENES/VOZ DE ALUMNOS EN CENTROS DE TITULARIDAD PÚBLICA - CURSO 2018/2019.

La rápida evolución tecnológica, así como la proliferación de plataformas de difusión de la actividad de los centros implica el tratamiento de datos de carácter personal de alumnos con finalidades distintas a la estrictamente educativa, por lo que **es necesario contar con el consentimiento de padres y/o tutores de alumnos menores de 14 años o de los propios alumnos, si estos tienen 14 o más años**, para el tratamiento de estos datos.

La finalidad de este documento es:

- **Informar** a los padres/tutores de los alumnos menores de 14 años y a los alumnos mayores de 14 del centro, del tratamiento que éste realizará de las imágenes/ voz de los alumnos.
- **Recabar el consentimiento** de padres, tutores o alumnos como base jurídica que permitirá al centro el tratamiento de las imágenes/voz de los alumnos.

Con carácter previo a la firma del presente documento usted **deberá leer la información relativa a la protección de datos de carácter personal** sobre el tratamiento de imágenes/voz de los alumnos en centros docentes de titularidad pública, **que se detalla al dorso del presente documento.**

Si el Alumno/a es menor de 14 años:D/Dª _____con DNI _____,(padre/madre/tutor/a)
y D/Dª _____ con DNI _____, (padre/madre/tutor/a)
del alumno/a_____ o
Si el Alumno/a es de 14 o más años: El/la alumno/a _____
con DNI _____ en su propio nombre

☐ **CONSIENTE** ☐ **NO CONSIENTE**

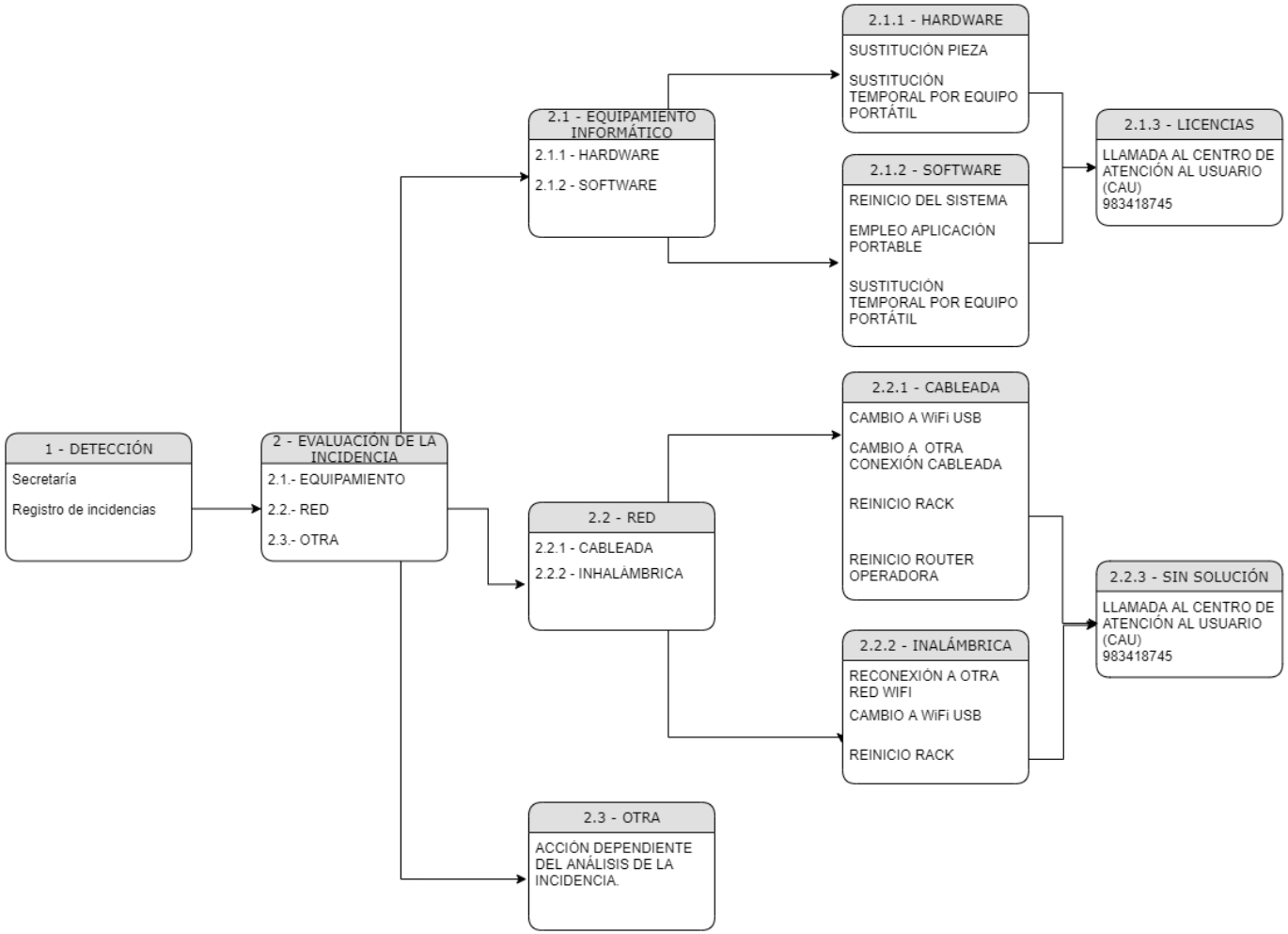
Al Centro_____**el tratamiento de la imagen/voz** de su hijo/a, o **de mi imagen/voz** (si el alumno tiene 14 años o más), especialmente mediante fotografías o vídeos, con **la finalidad de difundir las actividades del centro,** en los siguientes medios:
(Sólo se entenderá que consiente la difusión de imágenes/voz por los medios expresamente marcados a continuación):

☐ **Página Web del centro.**	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐

En _____, **a**____ **de**_____ **de 20**___.

Fdo.- _____	**Fdo.-** _____	**Fdo.-** _____
(Padre/madre/tutor-a del alumno/a Nombre, apellidos y firma)	(Padre/madre/tutor-a del alumno/a Nombre, apellidos y firma	(Alumno/a de 14 o más años Nombre, apellidos y firma)

ANEXO B: Protocolo de garantías de operatividad y continuidad de los servicios frente a incidencias



ANEXO C: Responsabilidad de custodia de datos por empresa externa

REGISTRO DE RETIRADA Y ACEPTACIÓN DE LAS CONDICIONES DE CUSTODIA Y PROTECCIÓN DE DATOS CONTENIDOS EN EL EQUIPAMIENTO TECNOLÓGICO.

D/Dª _____ con D.N.I._____

en calidad de (técnico, responsable, instalador, otro a indicar) _____ , procede a la retirada temporal o definitiva de equipo _____ con número de serie _____ registrado en el inventario de centro con referencia _____.

Así mismo, se compromete a custodiar y no difundir el o los contenidos de carácter personal o académico, tanto de alumnos, profesorado o de otro profesional del centro, que pudiesen estar almacenados en el interior de estos dispositivos.

De igual forma, se compromete a la inmediata notificación a la dirección del centro, en el caso que se produjese, la filtración parcial o total de datos personales de los sujetos anteriormente mencionados como consecuencia de la manipulación de los dispositivos de almacenamiento.

En Miranda de Ebro a _____ de _____ de 20_____.

Nombre y Firma del receptor.

Nombre y firma del responsable de centro.

Sello del centro.

ANEXO D: Normas generales sobre el acceso y empleo de la red de centro

NORMAS DE ACCESO A LA RED DE CENTRO

① El acceso a la red, ya sea empelando medios cableados o medios inalámbricos, habrá de realizarse bajo el conocimiento previo de los gestores de la misma y siempre con fines relacionados con la actividad docente o de gestión del centro.

② El acceso a la red cableada siempre será realizado empleando las tomas de red ubicadas en los recintos del centro. Se informará previamente a los gestores de la red para determinar la configuración de IP fija o DHCP que ha de tener el equipo a conectar.

③ Nunca se emplearán enrutadores o modems de tecnologías ADSL o modems de tecnologías móviles para los accesos a internet. Esto supone una vulneración de las medidas de seguridad pasiva y activa desplegadas en el centro.

④ En el caso de emplear dispositivos con conexión inalámbrica se emplearán exclusivamente las redes desplegadas por escuelas conectadas.

⑤ En caso de tener acceso a switchs no modificará el conexionado existente en los mismos para garantizarse el acceso a internet o a la red local.

NORMAS DE EMPLEO DE LA RED DE CENTRO

① El empleo de la red, independientemente del soporte, tendrá fines relacionados con la actividad de centro.

② Nunca se modificará la configuración de acceso a red e internet de los equipos existentes en cualquier reciento del centro. En caso de un funcionamiento no correcto se informará o se activará una incidencia. El usuario nunca modificará a título individual la configuración.

③ Nunca se emplearán programas de descarga P2P o descarga masiva de datos, esto limita el acceso al ancho de banda del resto de usuarios.

④ Será función del profesor la de supervisar el acceso a contenidos no adecuados mediante el empleo de equipamiento del centro.

⑤ Cuando se trate del empleo de dispositivos móviles de centro (tablets) estas se configurarán para su conexión exclusiva a los puntos de acceso de escuelas conectadas.

⑥ No se permite la compartición indiscriminada de recursos y carpetas en las distintas redes de centro. En caso de necesitar la compartición de un recurso se informará y solicitará asesoramiento técnico sobre tal medida o se emplearán sistemas de almacenamiento basados en la nube.

⑦El acceso a los dispositivos de reprografía está permitido tanto a personal docente como personal laboral mediante el empleo de las correspondientes cuentas de usuario.

ANEXO E: Préstamo de equipamiento informático

PRÉSTAMO DE EQUIPAMIENTO INFORMÁTICO.
COMPROMISO DEL ALUMNO/PROFESOR.

El alumno/profesor _____ perteneciente al grupo/departamento _____ del centro I.E.S. Montes Obarenes, recibe el equipamiento informático listado a continuación.

El profesor/alumno, al recibir dicho equipamiento, se compromete a:

- Mantenerlo en perfectas condiciones físicas e higiénicas.
- No manipular los componentes internos.
- Emplearlo exclusivamente para el desarrollo de su actividad académica.
- No instalar software sin consultarlo previamente con el centro.
- No prestar el equipamiento a terceros.
- Ponerse en contacto con el centro en caso de avería u otro tipo de incidencia.
- A devolver la totalidad de los componentes prestados, en idénticas condiciones a como fueron entregados, cuando así se solicite o al finalizar el curso escolar.

Con la siguiente firma asegura haber realizado la lectura de las condiciones del préstamo, y se compromete a su cumplimiento.

Fecha Entrega: Responsable de la entrega: Firma del docente responsable de la entrega: Responsable de la recogida: Firma del alumno/a, padre/madre/tutor.	Fecha Devolución: Responsable de la recogida: Firma del docente responsable de la recogida: Responsable de la devolución: Firma del alumno/a, padre/madre/tutor.