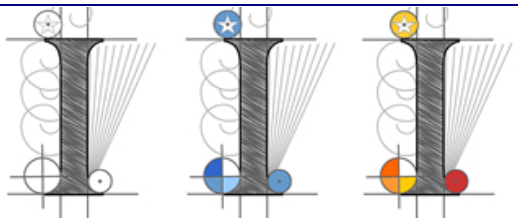
GOBIERNO DEL PRINCIPADO DE ASTURIAS

CONSEJERÍA DE EDUCACIÓN Y CULTURA

Informe sobre utilización por parte de profesorado y alumnado de aplicaciones que almacenan datos en nube con sistemas ajenos a la plataforma educativa institucional del Gobierno del Principado de Asturias



Servicio de Inspección Educativa

Índice

INTRODUCCIÓN 3

ESTUDIO DE LA AEPD 4

SUGERENCIAS Y ORIENTACIONES 5

APPS QUE ALMACENAN DATOS EN NUBE 6

APPS MÓVILES 6
ENTORNOS DE APRENDIZAJE 7
HERRAMIENTAS DE ALMACENAMIENTO EN NUBE 7
REDES SOCIALES 7
CORREO ELECTRÓNICO 8
MENSAJERÍA INSTANTÁNEA 9

EVALUACIÓN DE APLICACIÓN QUE ALMACENA DATOS EN NUBE 10

DATOS DE LA APLICACIÓN 10
INFORMACIÓN BÁSICA SOBRE EL TRATAMIENTO DE DATOS 10
PERMISOS DE LA APLICACIÓN 11
SOBRE LA UBICACIÓN DE LOS DATOS 12
OBSERVACIONES 12
PRUEBA DE LA APLICACIÓN 12
SOBRE LA SEGURIDAD DE LOS DATOS 12

Introducción

El Reglamento General de Protección de Datos (RGPD) es la nueva normativa que regula la protección de datos de los ciudadanos que vivan en la Unión Europea. El reglamento entró en vigor el 24 de mayo de 2016, pero es de obligado cumplimiento desde el 25 de mayo de 2018. Conserva parte de la regulación existente -conceptos, principios y derechos de los interesados- pero modifica algunos otros y contiene nuevas obligaciones que habrán de ser cumplidas por los sujetos obligados según sus circunstancias, en este caso, los centros educativos.

El nuevo reglamento recoge nuevos derechos a los ciudadanos, información clara, olvido y derecho a la portabilidad.

Los equipos directivos, profesorado, personal administrativo y auxiliar de los centros educativos en el ejercicio de sus funciones y tareas necesitan tratar datos de carácter personal del alumnado y de sus familiares, lo que deberán realizar con la debida diligencia y respeto a su privacidad e intimidad, teniendo presente el interés y la protección de los menores.

Las Administraciones y los centros educativos son los responsables del tratamiento de los datos y deben formar sobre sus principios básicos y cómo hacerlo correctamente.

Con objeto de adecuar el tratamiento de datos de carácter personal a la nueva ley, desde los centros educativos deberán realizarse una serie de actuaciones:

- Revisión de los protocolos internos de autorización de las familias para el uso de los datos personales, autorización de uso de imágenes, etc.
- Revisión de las páginas web y otros servicios en línea, en especial de los protocolos de publicación de información de datos de carácter personal y de recogida de estos en esos medios
- Revisión de los protocolos de comunicación entre los miembros de la comunidad educativa
- En especial se revisarán todas aquellas apps que registren datos personales, con almacenamiento en la nube, correo electrónico o redes sociales ajenas a la plataforma institucional -Educastur y Office 365 de Educastur- utilizadas en el entorno escolar por parte de profesorado y alumnado.

En todo caso, para la revisión de los protocolos y servicios utilizados en el centro educativo, deberán seguirse las sugerencias y orientaciones que aporta la Agencia Española de Protección de Datos (AEPD).

Este informe sobre utilización por parte de profesorado y alumnado de aplicaciones que almacenan datos en nube con sistemas ajenos a la plataforma educativa institucional del Gobierno del Principado de Asturias, las recomendaciones que se derivan del mismo y el ejemplo que se incluye de análisis de una aplicación que guarda datos en nube, se fundamenta en el informe publicado por la Agencia Española de Protección de Datos, cuya consulta es complementaria y recomendable:

Informe sobre la utilización por parte de profesorado y alumnado de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas
Orientaciones para centros educativos

AEPD (Agencia Española de Protección de Datos)
https://www.aepd.es/media/guias/guia-orientaciones-apps-datos-alumnos.pdf

También como lecturas complementarias se incluyen las referencias a la Guía sectorial para el ámbito educativo de la propia AEPD y al texto del Reglamento general de protección de datos.

Guía para centros educativos
Guías sectoriales AEPD
AEPD (Agencia Española de Protección de Datos)
http://www.tudecideseninternet.es/agpd1/images/guias/GuiaCentros/GuiaCentrosEducativos.pdf

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
https://www.boe.es/doue/2016/119/L00001-00088.pdf

Estudio de la AEPD

El estudio de la AEPD tiene su origen en el fuerte incremento del uso de apps en el entorno escolar por parte de profesorado y alumnado, así como el gran volumen de datos personales que se manejan.

- El informe destaca que se utilizan apps, almacenamiento en nube, correo electrónico o redes sociales ajenas a las plataformas de los centros (institucionales) y que, en muchos casos, podría existir un riesgo de pérdida de control sobre los datos personales que se aportan
- El documento incluye orientaciones y un decálogo de recomendaciones para fomentar la protección de datos a través del buen uso de las aplicaciones en los centros docentes

El cuestionario online en el que se basó el informe recababa información sobre los siguientes aspectos relativos al uso de las apps tanto por el alumnado a instancias del profesorado, como por el propio profesorado:

- Aplicaciones para el aula en dispositivos tales como móviles, tabletas o portátiles.
- Herramientas de almacenamiento en nube (tipo Dropbox, Google Drive, etc.)
- Redes sociales (Facebook, Instagram, etc.), para trabajos colaborativos u otro tipo de trabajos en el aula.
- Correo electrónico para el intercambio de información entre alumnado, familias y profesorado
- Existencia en los centros de normas internas y procedimientos con relación al uso de estas aplicaciones.

Sugerencias y orientaciones

Del citado estudio, la AEPD ha elaborado un decálogo de sugerencias y orientaciones.

1. Los centros educativos deben velar por que la incorporación de las tecnologías en las aulas se realice respetando el derecho a la protección de datos de aquellos cuya información personal se trata.
2. Los centros deben utilizar únicamente aquellas aplicaciones que ofrezcan información claramente definida sobre quién trata los datos, para qué y con qué finalidad, así como dónde se almacenan, el tiempo que se guardan y las medidas de seguridad.
3. La política de seguridad de los centros debe incluir a las aplicaciones utilizadas y el profesorado debe solicitar autorización para su uso al centro, el cual debe hacer una evaluación de la aplicación en materia de seguridad de la información. Deben establecerse procedimientos que obliguen a solicitar la autorización del Centro para el uso de estas aplicaciones.
4. Los centros deben informar de manera sencilla y transparente a las familias o tutores sobre la utilización de la tecnología en las aulas, así como de las apps que utilicen para tratar datos personales del alumnado.
5. Las aplicaciones utilizadas deben permitir el control por parte de los tutores y las tutoras o profesorado de los contenidos subidos por los y las menores, y en especial de los contenidos multimedia.
6. Debe tenerse especial cuidado con la publicación de fotografías o vídeos de alumnado facilitados por terceros, tales como otro alumnado o profesorado.
7. Deben establecerse programas informativos de concienciación para profesorado y alumnado sobre protección de datos y la importancia del uso correcto de aplicaciones, sobre todo en lo concerniente a la publicación de imágenes y vídeos, configuración de opciones de privacidad o uso de contraseñas robustas, entre otros.
8. Al utilizar sistemas de almacenamiento en nube se debe evitar incluir especialmente datos de salud, contraseñas, datos bancarios o material audiovisual de contenido sensible.
9. Cuando exista en el centro una plataforma educativa que permita la interacción entre el alumnado, y entre este y el profesorado, se aconseja que se prime su utilización para este fin, sin establecer mecanismos de comunicación adicionales.
10. Para los casos de tratamientos especiales de datos que puedan suponer un mayor riesgo, tal como el reconocimiento facial de menores de edad, el centro docente debe obtener el consentimiento expreso del alumnado (si son mayores de 14 años) o de las familias o tutores (si son menores de 14 años) y asegurarse de la finalidad para la que se utilizan.

En ningún caso se prohíbe directamente el uso de este tipo de aplicaciones. Cada una de ellas debe ser analizada bajo las premisas indicadas y actuar en consecuencia.

Parte de las acciones que se deben tomar están dentro de la autonomía de los centros. Es previsible que la situación que se plantea tras la publicación de este informe, y ante el proceso de adaptación a la nueva ley, provoque desconcierto en los centros educativos.

Con todo ello, desde el Servicio de Inspección Educativa se ha considerado conveniente estudiar algunas de las herramientas más populares en nuestros centros entre profesorado y alumnado, analizando su uso, posibles alternativas corporativas y acciones recomendadas en

el nuevo contexto que se plantea dentro del ámbito de la protección de datos, especialmente a partir del 25 de mayo de 2018 al pasar a ser de obligado cumplimiento el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Se incluye como anexo un ejemplo de análisis de aplicación que guarda datos en nube.

Apps que almacenan datos en nube

Apps móviles

Aplicación	Tipo	Alternativa corporativa	Acciones recomendadas
Additio	Organizador docente	No existe	Evaluar
iDoceo	Organizador docente	No existe	Evaluar
Evernote	Bloc de notas	OneNote Office 365 educación	Sustituir
Apple Notas	Bloc de notas	OneNote Office 365 educación	Sustituir
Google Keep	Bloc de notas	OneNote Office 365 educación	Sustituir
SlideShare	Presentaciones	Sway Office 365 educación	Sustituir
Kahoot	Gamificación	No existe como tal. Parcialmente cubierta con Forms Office 365 educación	Evaluar
Mindomo	Mapas conceptuales	No existe	Evaluar
Pixton	Cómics	No existe	Evaluar

Nota: este listado no pretende ser exhaustivo. Existe un número muy elevado de aplicaciones que hace imposible recogerlas todas. Las citadas aparecen como ejemplos.

En este apartado se incluyen no solo las apps para dispositivos móviles sino también las herramientas propias de la web 2.0. Debido su elevado número y a que todas ellas son herramientas con finalidad muy específica, no suelen existir alternativas corporativas que las puedan sustituir. Por ello deberán evaluarse y someterse al proceso de autorización y, en la medida de lo posible, utilizar cuentas genéricas (sin incluir datos reales de alumnado) para su uso.

Acciones recomendadas

- Evaluar siguiendo el guion sugerido en el informe
- Autorizar a nivel de centro si la aplicación supera la evaluación
- Incluir en la política de seguridad
- Informar al claustro, indicando que, independientemente de la superación de la evaluación, se debe evitar incluir datos personales sensibles
- Informar a las familias de su uso

Las aplicaciones que más datos personales del alumnado pueden llegar a tratar son los cuadernos de notas del personal docente, que mantienen el progreso, calificaciones y

observaciones del alumnado. Dadas las funcionalidades que ofrecen estas aplicaciones y la tipología de los datos que tratan, los tratamientos efectuados podrían incluir la elaboración de perfiles de aprendizaje, preferencias o comportamiento de menores de edad por parte de los responsables de las aplicaciones.

Entornos de aprendizaje

Aplicación	Tipo	Alternativa corporativa	Acciones recomendadas
Moodle	LMS	Educastur Aulas Virtuales Teams Office 365 educación	Sustituir
Edmodo	LMS	Educastur Aulas Virtuales Teams Office 365 educación	Sustituir
Google Classroom	LMS	Educastur Aulas Virtuales Teams Office 365 educación	Sustituir

Herramientas de almacenamiento en nube

Aplicación	Tipo	Alternativa corporativa	Acciones recomendadas
Dropbox	Almacenamiento archivos	OneDrive Office 365 educación	Sustituir
Google Drive	Almacenamiento archivos	OneDrive Office 365 educación	Sustituir
iCloud	Almacenamiento archivos	OneDrive Office 365 educación	Sustituir
Google Fotos	Almacenamiento fotografías	OneDrive/Sway Office 365 educación	Sustituir
iCloud Fotos	Almacenamiento fotografías	OneDrive/Sway Office 365 educación	Sustituir
Flickr	Almacenamiento fotografías	OneDrive/Sway Office 365 educación	Sustituir
Instagram	Almacenamiento fotografías	OneDrive/Sway Office 365 educación	Sustituir
YouTube	Almacenamiento vídeos	Stream Office 365 educación (aún no disponible)	Evaluar

Son utilizadas tanto por el profesorado como por el alumnado con la finalidad fundamental de compartir documentos, normalmente apuntes de clase y materiales didácticos en general, así como trabajos del alumnado. Pero también se da la utilización de estas herramientas para almacenar datos personales tales como listas de asistencia, calificaciones, fotos y vídeos.

Redes sociales

Aplicación	Tipo	Alternativa corporativa	Acciones recomendadas
Facebook	Red social	No existe como entorno abierto	Evaluar
Twitter	Red social	No existe como entorno abierto	Evaluar

Instagram	Red social	No existe como entorno abierto. También ofrece almacenamiento de fotografías (ver más arriba)	Evaluar

El uso de las redes sociales suele satisfacer dos necesidades en los centros educativos.

1. Divulgación de las actividades de los centros. La gran entrada de estas redes sociales entre los usuarios finales, especialmente Facebook, contando entre ellos a las familias del alumnado, las hace una excelente plataforma para ese fin. La comunicación y difusión, en algunos casos, no es solo de un solo sentido, al permitir interactuar con las familias.
2. Uso didáctico, en forma de proyectos educativos donde el factor motivador de la herramienta tiene un gran peso.

Correo electrónico

Aplicación	Tipo	Alternativa corporativa	Acciones recomendadas
gmail.com	Correo electrónico	Outlook Office 365 educación	Sustituir
outlook.es **outlook.com** **hotmail.com**	Correo electrónico	Outlook Office 365 educación	Sustituir
icloud.com **me.com**	Correo electrónico	Outlook Office 365 educación	Sustituir
yahoo.com **yahoo.es**	Correo electrónico	Outlook Office 365 educación	Sustituir

El uso del servicio de correo electrónico en los centros está generalizado, especialmente entre el profesorado. Sin embargo, la introducción de la cuenta institucional de educastur.org, aunque ya está en su segundo año, es desigual.

Hay pocos centros donde se exija el uso del correo de Educastur para cualquier comunicación con la comunidad docente, permitiendo el uso de servicios públicos y comerciales como los reseñados en la tabla. Debería separarse el correo electrónico personal del corporativo.

Más allá de redirecciones, se recomienda el uso de la configuración directa de la cuenta en el cliente preferido por el usuario o, aún mejor, la instalación de un segundo cliente de correo electrónico, preferiblemente Outlook, para atender el correo corporativo.

En ocasiones se utiliza el correo electrónico para mandar informes tutoriales entre el profesorado. En este caso ambos docentes deberían estar usando la plataforma corporativa.

Cuentas válidas
educastur.org (profesorado)
educastur.es (alumnado)

Mensajería instantánea

Aplicación	Tipo	Alternativa corporativa	Acciones sugeridas
WhatsApp	Mensajería	Teams Office 365 educación	Sustituir
Telegram	Mensajería	Teams Office 365 educación	Sustituir
Hangouts	Mensajería	Teams Office 365 educación	Sustituir en lo posible
Skype	Mensajería	Teams Office 365 educación	Sustituir en lo posible
TokApp School	Notificación escolar	No existe	Evaluar
EdVoice	Notificación escolar	No existe	Evaluar

El tipo de uso de este tipo de aplicaciones es variado. Suele cubrir la comunicación entre profesorado, entre profesorado y alumnado y, en algunos casos, entre profesorado y familias. El uso entre familias no se analiza aquí.

La única limitación de Teams dentro de Office 365 educación se daría para encuentros con profesorado/alumnado de fuera de la comunidad/país, necesidad que se da frecuentemente en proyectos europeos, asociaciones escolares, etc. En estos casos tanto **Hangouts** como **Skype** suelen ser las plataformas escogidas para establecer estas comunicaciones. Es de destacar aquí el esfuerzo de Microsoft por ofrecer el acceso a Invitados, usuarios externos a la organización, pero estos usuarios invitados deben contar con una cuenta de Microsoft profesional o educativa.

Mención especial merecen TokApp School https://www.tokappschool.com y Additio EdVoice http://www.additioapp.com/es/edvoice como soluciones globales de comunicación con las familias, llegando incluso a integrar los organizadores docentes comentados en el primer apartado. En este mismo tipo de aplicaciones se encuentran Smart Schools https://www.smart-schools.com, Alexia http://www.alexiaeducacion.com, Click Edu https://clickartedu.com/ y otras. Todos ellas requerirían una evaluación exhaustiva para determinar el alcance de datos implicados en la interacción con las familias y la forma de disponer el contacto con las mismas, debiendo considerarse en este último caso la provisión de los datos y el necesario consentimiento para ella.

Evaluación de aplicación que almacena datos en nube

Centro educativo	
Fecha de la evaluación	
Resultado de la evaluación	
Apartados no superados	

Datos de la aplicación

Nombre	**Additio App**
Sitio web	http://www.additioapp.com/es/
Política de privacidad	http://www.additioapp.com/es/seguridad-y-privacidad/
Nota Legal	http://www.additioapp.com/es/nota-legal/

Información básica sobre el tratamiento de datos

Se debe comprobar si el responsable de la aplicación informa claramente de:

Apartado	**Informa**	**Información**
Identidad del responsable	Sí	DIDACTIC LABS S.L. NIF: B55240162
Dirección del responsable	Sí	C/ Bescanó, 10. 17007 Girona. España Teléfono: +34 972 39 32 40 Email: info@additioapp.com
Finalidades de los datos	Sí	Ofrecer y gestionar nuestros servicios y productos para el sector educativo.
Comunicaciones de datos a terceros	Sí	A las administraciones públicas, siempre que lo exija la legislación vigente, y a todas aquellas entidades cuando sea necesario
Identidad de terceros	Sí	Administraciones públicas Otras entidades cuando sea necesario
Finalidad de la cesión a terceros	Sí	Cumplir con la legislación vigente. Cumplir con la finalidad del tratamiento.
Derechos que asisten a los titulares de los datos	Sí	Cualquier persona tiene derecho a obtener confirmación sobre si en Additio App están tratando datos personales que les conciernan, o no. Las personas interesadas tienen derecho a acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos. En determinadas circunstancias, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservarán para el ejercicio o la defensa de reclamaciones. En determinadas circunstancias y por motivos relacionados con su situación particular, los interesados podrán oponerse al tratamiento de sus datos. Additio App dejará de tratar los datos, salvo por motivos legítimos

		imperiosos, o el ejercicio o la defensa de posibles reclamaciones. Los interesados tienen derecho a la portabilidad de sus datos. Finalmente, los interesados pueden dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.
Periodos de conservación de los datos	Sí	Mientras los interesados usen Additio App. El no uso de la aplicación durante un largo periodo de tiempo (12 meses) hace que pierda su finalidad y se procede a eliminar la cuenta y los datos asociados a ella.
Medidas de seguridad facilitadas	Sí	Aplica las medidas de seguridad exigidas por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, teniendo los mecanismos necesarios para salvaguardar la confidencialidad, integridad y disponibilidad de los datos y prevenir, en la medida que sea posible, el acceso no autorizado, robo, modificaciones ilícitas y la pérdida de datos.

Nota: *Esta información debería estar fácilmente accesible en la política de seguridad y nota legal de la aplicación. En caso de que falte alguno de estos aspectos, o que la información facilitada no ofrezca las garantías adecuadas, se recomienda no utilizar la aplicación.*

Permisos de la aplicación

Informa de posibles accesos a los datos del dispositivo o a sus sensores	Sí

Detalle de los accesos

Apartado	Información
Identidad	buscar cuentas en el dispositivo añadir o eliminar cuentas
Calendario	leer eventos de calendario e información confidencial añadir o modificar eventos de calendario y enviar mensajes a los invitados sin el consentimiento de los propietarios
Contactos	buscar cuentas en el dispositivo
Teléfono	consultar la identidad y el estado del teléfono
Fotos/multimedia/archivos	leer el contenido de tu almacenamiento USB modificar o eliminar contenido del almacenamiento USB
Almacenamiento	leer el contenido de tu almacenamiento USB modificar o eliminar contenido del almacenamiento USB
Micrófono	grabar sonido
Información sobre la conexión Wi-Fi	ver conexiones Wi-Fi
ID de dispositivo y datos de llamada	consultar la identidad y el estado del teléfono
Otros	recibir datos de Internet

	ver conexiones de red crear cuentas y establecer contraseñas acceso completo a red usar cuentas del dispositivo

Nota: *Esta información debería estar accesible en las correspondientes tiendas de aplicaciones o en su web. En caso de que la información facilitada no ofrezca las garantías adecuadas, se recomienda no utilizar la aplicación.*

Sobre la ubicación de los datos

País y/o empresa	EU	EQ	EU-US EP
Hetzner Online GmbH (Alemania)	Sí		
Amazon Web Services			Sí
Google Firebase			Sí

EU: *País del Espacio Económico Europeo*
EQ: *País con nivel de protección equivalente (que haya sido así acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea). Puede consultar la lista de países con nivel adecuado de protección en el siguiente enlace.*
https://www.aqpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php#paises
EU-US EP: *Los datos también pueden localizarse en empresas ubicadas en Estados Unidos siempre que estas se hayan acogido a los principios del Escudo de Privacidad. Si desea saber si una empresa de Estados Unidos forma parte del Escudo de Privacidad, puede consultar la Lista empresas adheridas: https://www.privacyshield.gov/welcome*

En cualquier otro caso, se recomienda solicitar información sobre las posibles transferencias internacionales de datos y las garantías de su licitud, en particular sobre las que necesitan autorización por parte de la Agencia Española de Protección de Datos.

Observaciones

Additio App se integra con Google Classroom y G Suite.
Additio App tiene una funcionalidad aparte llamada EdVoice.
En ambos casos habría que evaluar cada una de esas funcionalidades como aplicación independiente ya que Additio App puede funcionar sin hacer uso de ambas.

Prueba de la aplicación

Se considera conveniente poner a prueba la aplicación de forma previa a su definitiva utilización en el Centro, realizando la prueba sin introducir datos personales reales del alumnado ni involucrarlo en su utilización. En esta fase de prueba se debería comprobar la corrección de las informaciones que fueron facilitadas por el responsable de la aplicación.

Sobre la seguridad de los datos

La responsabilidad del cumplimiento de las medidas de seguridad debe entenderse siempre compartida entre los diferentes actores intervinientes (responsable de la aplicación, Centro Educativo y usuarios), debiendo en todo caso el responsable de la aplicación facilitar las medidas técnicas adecuadas para garantizar la seguridad de los datos

tratados, y el Centro aplicarlas o utilizarlas correctamente, además de implementar las medidas organizativas apropiadas.

Así, por ejemplo, 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 pueda cumplir con las obligaciones que le son exigibles al respecto, introduciendo en su política de seguridad la realización de copias de seguridad de los datos tratados mediante estas aplicaciones, y realizando efectivamente la realización de dichas copias.

La responsabilidad de las medidas de identificación de usuarios también es compartida. Por un lado, la aplicación debe implementar un mecanismo de autenticación 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).

Si se utilizan contraseñas, el Centro debe incluir en su política el cambio periódico de las mismas, por lo que las aplicaciones que se vayan a utilizar deben incluir mecanismos para permitir dichos cambios. A los usuarios les corresponde la obligación de utilizar contraseñas fuertes y custodiarlas sin desvelarlas a terceros.