ANEXO II PROTOCOLO DE PROTECCIÓN DE DATOS

PROTOCOLO DE PROTECCIÓN DE DATOS EN EL IES NUESTRA SEÑORA DE AL-HARILLA

ÍNDICE

1. Introducción y justificación..... LXXXII

2. Identificación del responsable del tratamiento y del Delegado de Protección de Datos (DPD) LXXXIII

3. Inventario y registro de actividades de tratamiento (RAT) LXXXIV

4. Bases jurídicas y legitimación del tratamiento LXXXVI

5. Medidas de seguridad técnicas y organizativas LXXXVIII

6. Deber de confidencialidad y obligaciones del personal XC

7. Cesiones y comunicaciones de datos a terceros y encargados del tratamiento XCII

8. Derechos de las personas interesadas y procedimiento para su ejercicio XCIV

9. Gestión de la imagen del alumnado, web institucional y redes sociales del IES XCVI

10. Protocolo de actuación y notificación ante brechas de seguridad XCVII

1. Introducción y justificación

La Dirección del IES Nuestra Señora de Alharilla de Porcuna (Jaén) presenta el presente **Protocolo de Protección de Datos y Garantía de Derechos Digitales**, un documento institucional de obligado cumplimiento que articula el compromiso firme de nuestro centro con la privacidad, la seguridad de la información y el uso responsable de la tecnología en el entorno educativo.

Como centro educativo público dependiente de la **Consejería de Desarrollo Educativo y Formación Profesional de la Junta de Andalucía**, el IES gestiona diariamente un volumen elevado de información de carácter personal. La naturaleza de nuestra labor pedagógica y administrativa exige recopilar, procesar y custodiar datos relativos a nuestro alumnado —en su gran mayoría menor de edad—, sus familias o representantes legales, el claustro de profesorado y el personal de administración y servicios (PAS).

1.1. Marco Normativo de Referencia

Este protocolo se fundamenta en el cumplimiento de la legislación vigente en materia de protección de datos, garantizando la cobertura legal de todas las actuaciones del centro:

- **Reglamento (UE) 2016/679 (RGPD):** Marco normativo europeo 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.
- **Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD):** Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.
- **Disposición Adicional Vigesimotercera** de la Ley Orgánica 2/2006, de 3 de mayo, de Educación
- **Ley 17/2007, de 10 de diciembre, de Educación de Andalucía (LEA):** Marco autonómico que regula la gestión del sistema educativo andaluz.
- **Decreto 327/2010, de 13 de julio:** Reglamento Orgánico de los Institutos de Educación Secundaria en la Comunidad Autónoma de Andalucía.
- **Guía de la Agencia Española de Protección de Datos** para centros educativos**.**
- **Guía del Consejo de Transparencia y Protección de Datos de Andalucía** sobre protección de datos personales para centros educativos de Andalucía**.**
- **Instrucciones de la Viceconsejería de Desarrollo Educativo y Formación Profesional:** Directrices anuales sobre la utilización de recursos digitales, la gestión de la imagen en los centros educativos y la ciberseguridad en las aulas.

1.2. Necesidad y Oportunidad del Protocolo

La implantación de este protocolo responde a una necesidad operativa, ética y legal imperiosa, motivada por los siguientes factores:

1. **Protección reforzada del menor:** El alumnado de Educación Secundaria Obligatoria, Bachillerato y Formación Profesional requiere una tutela especial de sus derechos fundamentales. La información manejada abarca datos de especial protección, tales como informes psicopedagógicos, necesidades específicas de apoyo educativo (NEAE), situaciones sociofamiliares y datos de salud (alergias, adaptaciones médicas o partes de accidentes).

2. **Transformación digital y entornos virtuales:** El uso cotidiano del sistema de gestión corporativo **Séneca** y la comunicación mediante **iPasen**, sumado al despliegue del Plan Digital de Centro, las Aulas Virtuales y herramientas de trabajo colaborativo, exige un control riguroso sobre las credenciales de acceso, la custodia de calificaciones y el tratamiento de información en entornos en la nube.

3. **Gestión de la imagen y difusión institucional:** Las actividades complementarias, extraescolares, proyectos de innovación y eventos de la comunidad educativa generan material audiovisual. Es imprescindible regular la recogida de consentimientos explícitos para la publicación de fotografías o vídeos en la página web del centro, revistas escolares o canales oficiales en redes sociales, protegiendo el derecho al honor, a la intimidad y a la propia imagen.

4. **Prevención de brechas de seguridad:** Se requiere establecer pautas claras de actuación para prevenir incidentes de seguridad involuntarios, como el uso desinformado de copias ocultas en correos masivos, el almacenamiento de datos sensibles en dispositivos personales no cifrados o la difusión no autorizada de listados con datos personales.

5. **Delimitación de responsabilidades:** Es necesario que todos los integrantes del centro (equipo directivo, docentes, personal no docente, familias y alumnado) conozcan con precisión sus derechos, deberes y pautas de actuación en el tratamiento diario de la información.

1.3. Objetivos Generales

A través del presente protocolo, el centro garantiza que todo tratamiento de datos personales se realice bajo los principios de **licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, confidencialidad e integridad**. Asimismo, se promueve entre el alumnado una competencia digital crítica y respetuosa con la privacidad propia y ajena.

2. Identificación del responsable del tratamiento y del Delegado de Protección de Datos (DPD)

2.1. Responsable del Tratamiento de Datos

En el ámbito de los centros educativos públicos de Andalucía, el **Responsable del Tratamiento** de los datos de carácter personal es la **Consejería de Desarrollo Educativo y Formación Profesional de la Junta de Andalucía**.

Como centro docente, el IES Nuestra Señora de Alharilla actúa bajo el principio de atribución funcional: la Dirección del centro, en representación de la Consejería, gestionara y custodiara localmente las actividades de tratamiento necesarias para la prestación de la función docente y la organización de la vida escolar, de acuerdo con las instrucciones normativas de la administración educativa.

2.2. Delegado de Protección de Datos (DPD)

De conformidad con el artículo 37.1.a del RGPD y el artículo 34 de la LOPDGDD, la Administración Educativa andaluza cuenta con la figura designada del **Delegado de Protección de Datos (DPD)** para todo el ámbito de la enseñanza pública no universitaria.

- **Identificación y canal de contacto:**

- **Entidad:** Consejería de Desarrollo Educativo y Formación Profesional - Junta de Andalucía.
- **Correo electrónico de contacto:** dpd.ced@juntadeandalucia.es

- **Funciones principales del DPD respecto al centro y la comunidad educativa:**

1. **Asesoramiento e información:** Asesorar al centro educativo y a sus profesionales sobre el cumplimiento de las obligaciones legales en materia de privacidad.
2. **Supervisión:** Velar por el cumplimiento de la normativa en el uso de las aplicaciones corporativas y procedimientos administrativos.
3. **Interlocución con las familias y el personal:** Atender las consultas, reclamaciones o solicitudes presentadas por el alumnado, sus familias o los trabajadores del IES en relación con el tratamiento de sus datos.
4. **Enlace con la autoridad de control:** Actuar como punto de contacto con el **Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA)** y la Agencia Española de Protección de Datos (AEPD).

2.3. Rol y Funciones del Equipo Directivo

Dentro de la gestión cotidiana del centro, la **Dirección del Instituto** asume las siguientes competencias operativas:

- **Implementación y difusión:** Garantizar el conocimiento y aplicación del presente protocolo entre el claustro de profesorado y el Personal de Administración y Servicios (PAS)-
- **Control de accesos:** Velar por que el acceso a la información confidencial (expedientes académicos, informes NEAE, datos de salud, partes de faltas) se restrinja estrictamente al personal que lo requiera para el desempeño de sus funciones pedagógicas o administrativas.
- **Gestión del ejercicio de derechos:** Recibir, tramitar y canalizar hacia la Consejería/DPD las solicitudes presentadas por las familias o el alumnado para ejercer sus derechos de acceso, rectificación, supresión o limitación.
- **Notificación de incidencias:** Comunicar de forma inmediata al DPD de la Consejería cualquier quiebra de la seguridad o brecha de datos que pueda producirse en el instituto.

2.4. Encargados del Tratamiento (Proveedores y Servicios Externos)

Tienen la consideración de **Encargados del Tratamiento** aquellas personas físicas o jurídicas, empresas o entidades externas que prestan servicios al instituto y que, para su ejecución, requieren acceder a datos personales de la comunidad educativa.

- **Requisito de contratación:** Ningún proveedor externo podrá tratar datos del alumnado o del personal del centro sin la firma previa de un **Contrato de Encargo del Tratamiento** (conforme al art. 28 del RGPD), que garantice el uso de los datos estrictamente para la finalidad contratada y la aplicación de las medidas de seguridad adecuadas.

3. Inventario y registro de actividades de tratamiento (RAT)

En cumplimiento de lo dispuesto en el artículo 30 del Reglamento General de Protección de Datos (RGPD) y el artículo 31 de la Ley Orgánica 3/2018 (LOPDGDD), este Instituto mantiene un **Registro de Actividades de Tratamiento (RAT)** actualizado que refleja las operaciones con datos personales realizadas en el ámbito de nuestras competencias educativas y administrativas.

Aunque el inventario oficial consolidado forma parte del RAT de la **Consejería de Desarrollo Educativo y Formación Profesional**, el centro gestiona de forma operativa las siguientes Actividades de Tratamiento dentro de su ámbito competencial:

3.1. Fichas de las Actividades de Tratamiento del Centro

RAT-01: Gestión Académica, Administrativa y Orientación Educativa del Alumnado

- **Finalidad del tratamiento:** Tramitación de matrículas, gestión del expediente académico, registro de calificaciones, control de asistencia, gestión de faltas, atención a la diversidad, emisión de títulos, tramitación de becas, gestión del transporte escolar y servicios complementarios, y comunicación continua con las familias.
- **Base jurídica:**
  - Cumplimiento de una obligación legal (Art. 6.1.c RGPD) en aplicación de la *Ley Orgánica 2/2006, de Educación (LOE)* y la *Ley 17/2007, de Educación de Andalucía (LEA)*.
  - Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos (Art. 6.1.e RGPD).
  - Para datos de especial categoría (salud/NEAE): Art. 9.2.g del RGPD y disposición adicional vigesimosegunda de la LOE.
- **Categorías de datos procesados:**
  - *Datos identificativos y de contacto:* Nombre, apellidos, DNI/NIE, fecha de nacimiento, domicilio, teléfono, correo electrónico, firma del alumnado y de los progenitores/tutores legales.
  - *Datos académicos y disciplinarios:* Expediente académico, calificaciones, medidas correctoras, informes de orientación.
  - *Datos de especial protección:* Datos de salud (alergias, enfermedades crónicas, partes de accidentes, adaptación de educación física) e informes psicopedagógicos.
- **Categorías de interesados:** Alumnado matriculado en el centro y sus padres, madres o representantes legales.
- **Destinatarios/Cesiones:** Consejería de Desarrollo Educativo y Formación Profesional, Ministerio de Educación, Inspección Educativa, centros sanitarios en caso de urgencia médica o accidente escolar, y entidades aseguradoras del seguro escolar.
- **Plataformas tecnológicas empleadas:** Sistema corporativo **Séneca**, aplicación **iPasen** y archivo físico del centro.

RAT-02: Gestión del Personal Docente y de Administración y Servicios (PAS)

- **Finalidad del tratamiento:** Organización de la labor docente y administrativa del centro, elaboración de horarios, control de asistencia y permanencia, gestión de guardias, tramitación de licencias y permisos, prevención de riesgos laborales y asignación de tutorías y órganos colegiados.
- **Base jurídica:** Ejecución de la relación laboral o estatutaria (Art. 6.1.b RGPD) y cumplimiento de obligaciones legales derivadas del *Estatuto Básico del Empleado Público* y la normativa autonómica de función pública (Art. 6.1.c RGPD).
- **Categorías de datos:** Datos identificativos (DNI, NIF, cuerpo docente, especialidad), datos de contacto, horario lectivo y no lectivo, firma (digital o física), control horario y partes de baja médica (IT).
- **Categorías de interesados:** Profesorado del claustro y Personal de Administración y Servicios (PAS) asignado al instituto.
- **Sistemas de soporte:** Sistema de gestión **Séneca** y registro de control de presencia del centro.

RAT-03: Difusión Institucional, Imagen y Eventos Escolares

- **Finalidad del tratamiento:** Documentar y difundir las actividades lectivas, complementarias, extraescolares, proyectos de innovación educativa (Erasmus+, Escuela Espacio de Paz, etc.), graduaciones y vida escolar a través de los medios de comunicación oficiales del centro (página web institucional, tableros de información y perfiles oficiales en redes sociales).
- **Base jurídica:** Consentimiento explícito e informado del interesado o de sus representantes legales (Art. 6.1.a RGPD). En caso de menores de 14 años, prestado obligatoriamente por los padres/tutores; en mayores de 14 años, prestado por el propio alumno/a.
- **Categorías de datos:** Imagen (fotografías y vídeos), voz, nombre y curso académico.
- **Destinatarios:** Comunidad educativa y público general accediendo a los canales oficiales del IES.
- **Garantías especiales:** El consentimiento es revocable en cualquier momento sin carácter retroactivo. Se prohíbe la captura y difusión no autorizada de imágenes por parte de particulares.

RAT-04: Entornos Virtuales de Aprendizaje y Herramientas Digitales

- **Finalidad del tratamiento:** Facilitar la docencia presencial y a distancia, la entrega de trabajos, la realización de actividades interactivas y el uso de herramientas colaborativas educativas.
- **Base jurídica:** Ejercicio de la función docente e interacciones pedagógicas previstas en el Plan Digital de Centro (Art. 6.1.e RGPD).
- **Categorías de datos:** Identificador de usuario corporativo (@g.educaand.es o iANDE), correo electrónico corporativo, registros de conexión (logs), contenido de tareas y calificaciones.
- **Plataformas autorizadas: Moodle Centros** (plataforma institucional de la Junta de Andalucía) y servicios de la suite corporativa educativa homologada por la Consejería (*Google Workspace for Education* bajo dominio corporativo).

RAT-05: Videovigilancia y Control de Accesos

- **Finalidad del tratamiento:** Garantizar la seguridad de las personas (alumnado, personal y visitantes), de los bienes e instalaciones del centro educativo.
- **Base jurídica:** Interés público (Art. 6.1.e RGPD) y artículo 22 de la LOPDGDD.
- **Categorías de datos:** Imágenes captadas por el sistema de cámaras en accesos y zonas comunes exteriores e interiores.
- **Garantías y límites:**
  - No se instalarán cámaras en aulas, salas de profesores, aseos, vestuarios o zonas de descanso.
  - Existencia de carteles informativos en los accesos a las zonas videovigiladas.
  - **Plazo de conservación:** Las imágenes se destruirán o sobreescribirán en un plazo máximo de **30 días**, salvo que deban ser puestas a disposición de las Fuerzas y Cuerpos de Seguridad o de los Tribunales.

3.2. Plazos Generales de Conservación de la Información

Los datos personales gestionados por el centro se conservarán conforme a los siguientes criterios:

1. **Expediente académico e historial escolar:** Se conservarán de forma permanente en la plataforma **Séneca** y en el archivo histórico del centro, de acuerdo con la regulación de archivos públicos de la Comunidad Autónoma de Andalucía.
2. **Datos de contacto y gestión anual:** Se mantendrán durante la estancia del alumno/a en el centro y se cancelarán una vez finalizada la relación educativa y transcurridos los plazos legales de prescripción de responsabilidades.
3. **Autorizaciones de imagen:** Permanecerán vigentes durante el curso lectivo para el que fueron recabadas, o hasta que se ejerza el derecho de revocación del consentimiento.
4. **Registros de control de acceso y videovigilancia:** Máximo de 1 mes desde su captura.

3.3. Medidas de Seguridad Aplicables

El tratamiento de los datos contenidos en este registro está sujeto a las medidas de seguridad organizativas, técnicas y jurídicas establecidas por el **Esquema Nacional de Seguridad (ENS)** en el ámbito de la administración electrónica de la Junta de Andalucía, garantizando los niveles de confidencialidad, integridad, disponibilidad y trazabilidad requeridos.

4. Bases jurídicas y legitimación del tratamiento

Todo tratamiento de datos de carácter personal en el centro debe contar con una base jurídica que lo legitime expresamente, de conformidad con los artículos 6 y 9 del Reglamento General de Protección de Datos (RGPD) y los artículos 6 a 10 de la LOPDGDD.

Las actividades de tratamiento desarrolladas en el instituto no responden al libre arbitrio del centro, sino que se fundamentan en las siguientes bases legales:

4.1. Principales Bases de Legitimación (Art. 6.1 RGPD)

1. **Cumplimiento de una obligación legal (Art. 6.1.c RGPD):**

   Es la base principal que ampara la mayor parte del tratamiento de datos en el centro. La función docente y la gestión administrativa están obligadas por ley a recoger y tratar datos del alumnado y de sus familias.

   - *Normativa habilitante:* Ley Orgánica 2/2006, de 3 de Mayo, de Educación (LOE); Ley 17/2007, de 10 de diciembre, de Educación de Andalucía (LEA); y Decreto 327/2010 por el que se aprueba el Reglamento Orgánico de los IES en Andalucía.
   - *Aplica a:* Matrícula, expediente académico, gestión de calificaciones, control de asistencia, partes de faltas y expedientes disciplinarios, emisión de certificaciones y comunicación de datos a la Consejería de Desarrollo Educativo y Formación Profesional.

2. **Misión en interés público o ejercicio de poderes públicos (Art. 6.1.e RGPD):**

   El instituto, como centro público de titularidad de la Junta de Andalucía, ejerce la función regulada de la enseñanza y la orientación escolar.

   - *Aplica a:* La acción tutorial, la atención a la diversidad, la evaluación psicopedagógica, el seguimiento de la convivencia escolar y la impartición de las materias del currículo oficial mediante entornos virtuales homologados.

3. **Consentimiento libre, específico, informado e inequívoco (Art. 6.1.a RGPD):**

   Se requiere para aquellos tratamientos de datos que no sean estrictamente imprescindibles para la función educativa regulada por ley.

   - *Aplica a:* Publicación de fotografías y vídeos del alumnado en la página web o redes sociales oficiales; participación en actividades complementarias no obligatorias con cesión de datos a terceros; u orlas de graduación.
   - *Garantía:* El consentimiento puede ser retirado en cualquier momento por el interesado o sus representantes legales sin que ello afecte a la prestación de la función educativa principal.

4. **Ejecución de un contrato o relación jurídica (Art. 6.1.b RGPD):**

   Aplica a la relación laboral y administrativa del personal docente y no docente del centro, así como a las relaciones vinculantes con proveedores y empresas externas de servicios (transporte, cafetería, actividades extraescolares).

5. **Protección de intereses vitales (Art. 6.1.d RGPD):**

   Permite el tratamiento y cesión puntual de datos personales o de salud en situaciones de emergencia o fuerza mayor.

   - *Aplica a:* Situaciones de urgencia médica en el centro, accidentes escolares o atención prioritaria por parte de los servicios sanitarios o Fuerzas y Cuerpos de Seguridad.

4.2. Tratamiento de Datos de Categorías Especiales (Art. 9 RGPD)

En la actividad escolar diaria se manejan datos de especial protección, como datos relativos a la **salud** (alergias, enfermedades crónicas, partes de lesiones), la **orientación psicopedagógica y diversidad (NEAE)**, o las **convicciones religiosas**.

Su tratamiento no requiere el consentimiento de las familias cuando responde al cumplimiento de la función educativa, amparándose en:

- **Disposición Adicional Vigésima Tercera de la LOE (en relación con el Art. 9.2.g del RGPD - Interés público esencial):** Autoriza expresamente a los centros docentes a recabar los datos personales necesarios para el ejercicio de la función docente y orientadora, incluidos los relativos a la salud y la atención a la diversidad, sin necesidad de solicitar consentimiento previo a los progenitores.
- **Protección de la salud y prevención médica (Art. 9.2.h RGPD):** Permite la custodia de datos de salud en el centro para la exención de contenidos en Educación Física por prescripción médica o la aplicación de protocolos de actuación ante crisis sanitarias o anafilácticas.

4.3. Régimen de Edad y Regulación del Consentimiento del Alumnado

De acuerdo con el artículo 7 de la LOPDGDD y las directrices del marco normativo español y andaluz:

- **Menores de 14 años:** La autorización, el otorgamiento del consentimiento y la firma de documentos (autorizaciones de imagen, salidas extraescolares, etc.) corresponden **exclusivamente a los padres, madres o tutores legales**.
- **Mayores de 14 años:** Tienen capacidad legal para otorgar su propio consentimiento en relación con el tratamiento de sus datos de carácter personal (por ejemplo, autorizar el uso de su propia imagen en la web del centro o gestionar sus credenciales de acceso digitales). Sin embargo, la información académica de su proceso evaluativo seguirá manteniéndose a disposición de sus progenitores o representantes legales mientras dependan económicamente de ellos y sean menores de edad.

5. Medidas de seguridad técnicas y organizativas

De conformidad con el artículo 32 del RGPD y los principios del **Esquema Nacional de Seguridad (ENS)** aplicables a la Administración Pública andaluza, nuestro centro docente aplica un conjunto de medidas técnicas, organizativas y físicas destinadas a garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales manejados en el ejercicio de la función educativa.

5.1. Medidas Organizativas y Normas de Conducta del Personal

El factor humano es crucial en la gestión de la privacidad. Todo el personal del IES (docentes, personal de administración y servicios y personal externo) debe cumplir con las siguientes directrices organizativas:

- **Deber de confidencialidad y secreto profesional:**
  - Todo el personal que tenga acceso a datos personales del alumnado o de sus familias mantiene la obligación de guardar secreto profesional, compromiso que perdura de forma indefinida incluso tras la finalización de su relación laboral o administrativa con el instituto.
  - Queda estrictamente prohibido comentar o divulgar información sobre el alumnado, su rendimiento académico, situaciones familiares, de salud o medidas disciplinarias en espacios públicos dentro o fuera del centro (pasillos, cafetería, salas de profesores compartidas o redes personales).
- **Principio de acceso de necesidad de conocer:**

    - El acceso a expedientes, informes psicopedagógicos o datos de salud está restringido exclusivamente a las personas que lo requieran para el ejercicio de sus funciones docentes u orientadoras (tutores/as, equipo de orientación, equipo directivo o profesorado de la materia en su ámbito de actuación).
- **Formación y concienciación:**
    - El centro impulsará acciones informativas periódicas dentro del Plan de Formación del Profesorado para actualizar al claustro y al PAS sobre buenas prácticas en ciberseguridad, prevención de *phishing* y gestión segura de datos escolares.

5.2. Medidas Técnicas y Ciberseguridad

Las actuaciones en el entorno digital deben sujetarse a las pautas marco establecidas por la Consejería de Desarrollo Educativo y Formación Profesional:

- **Uso de plataformas corporativas oficiales:**
    - Toda gestión académica, de evaluación, de asistencia y de comunicación con las familias debe canalizarse obligatoriamente a través de las herramientas oficiales de la Junta de Andalucía: **Séneca**, **iPasen** y **Moodle Centros**.
    - Queda prohibido el uso de plataformas o aplicaciones privadas de terceros que no hayan sido homologadas por la administración educativa o que almacenen datos personales en servidores situados fuera del Espacio Económico Europeo sin las debidas garantías.
- **Gestión de credenciales y cuentas corporativas:**
    - Las credenciales de acceso al sistema Séneca y las cuentas del dominio corporativo (@g.educaand.es o de identidad digital) son **personales e intransferibles**.
    - Se exige el uso de contraseñas robustas (combinación de letras, números y símbolos) y su renovación periódica. Está prohibido compartir contraseñas o anotarlas en lugares visibles.
    - Es obligatorio el cierre de sesión explícito en ordenadores compartidos (aulas, sala de profesores, secretaría) al finalizar cualquier tarea.
- **Uso de dispositivos portátiles y soportes extraíbles:**
    - Se desaconseja el almacenamiento de listas con datos de salud, informes NEAE o datos identificativos del alumnado en carpetas locales de ordenadores personales o memorias USB sin cifrar.
    - En caso de requerirse el traslado de información fuera del centro por motivos docentes, los archivos deberán estar protegidos mediante contraseña o cifrado.
- **Redes y conectividad:**
    - El personal docente y administrativo utilizará la red de comunicaciones oficial del centro para fines profesionales.
    - No se gestionará información confidencial ni se accederá a Séneca desde redes Wi-Fi públicas o abiertas no seguras.

5.3. Medidas de Seguridad Física y Gestión Documental en Papel

Aunque la gestión se encamina progresivamente hacia el entorno digital, el soporte físico en papel exige el mismo nivel de exigencia de custodia:

- **Custodia de archivos en papel:**
    - Los expedientes académicos históricos, libros de escolaridad, boletines de matrícula, autorizaciones firmadas e informes psicopedagógicos se conservarán en los armarios o dependencias del archivo de Secretaría.
    - Dichos espacios permanecerán cerrados con llave cuando no se encuentre en ellos el personal autorizado.
- **Política de «pantallas y mesas limpias»:**
    - Durante las ausencias de las dependencias u oficinas (Secretaría, Dirección, Jefatura), ningún documento que contenga datos personales deberá quedar visible sobre las mesas.
    - Las pantallas de los ordenadores deberán bloquearse automáticamente mediante salvapantallas con contraseña tras un breve periodo de inactividad.
- **Destrucción segura de documentos:**

- Todos los borradores, exenciones, listados provisionales de notas, exámenes o documentos en papel desechables con datos personales deberán eliminarse utilizando las **destructoras de papel en corte cruzado** disponibles en el centro o mediante contenedores seguros de reciclaje confidencial.
- En ningún caso se depositarán documentos con datos personales en papeleras comunes.

5.4. Resumen de Obligaciones Diarias para el Personal

DECÁLOGO DE BUENAS PRÁCTICAS

1. Usa exclusivamente Séneca o IPasen para gestionar datos.
2. Mantén tus claves de acceso en secreto; nunca las compartas.
3. Cierra la sesión en el ordenador del aula antes de salir.
4. No utilices correos personales para comunicaciones oficiales.
5. Bloquea tu pantalla cuando te ausentes de tu puesto de trabajo.
6. No dejes exámenes, actas o listados con notas a la vista sobre las mesas.
7. Destruye la documentación en papel obsoleta en las destructoras del IES.
8. No difundas datos de salud o situaciones del alumnado en zonas comunes.
9. Verifica los destinatarios (uso de CCO) al enviar correos masivos.
10. Notifica a la Dirección cualquier pérdida de dispositivos o brecha de seguridad.

6. Deber de confidencialidad y obligaciones del personal

El **deber de secreto y confidencialidad** constituye uno de los pilares fundamentales en la gestión de un centro educativo público. Todo el personal que presta sus servicios en el instituto —ya sea docente, de administración y servicios, o de personal laboral y contratado externo— está sujeto a la obligación estricta de confidencialidad respecto a cualquier dato de carácter personal al que tenga acceso en el desarrollo de sus funciones.

6.1. Alcance y Naturaleza del Deber de Secreto

De conformidad con el artículo 5.1.f del RGPD y el artículo 5 de la Ley Orgánica 3/2018 (LOPDGDD):

1. **Permanencia indefinida:** La obligación de reserva y confidencialidad **no finaliza cuando concluye la relación laboral, estatutaria o contractual** de la persona con el centro docente. Perdura de forma indefinida en el tiempo, extendiéndose tras traslados, jubilaciones, cese de contratos o cambios de destino.
2. **Acceso exclusivo por necesidad de servicio:** El acceso a la información personal (expedientes, calificaciones, datos familiares o informes de salud) queda reservado únicamente a quienes lo requieran de forma imprescindible para el cumplimiento de sus funciones docentes u organizativas.
3. **Prohibición absoluta de divulgación informal:** Queda terminantemente prohibido comentar, trasladar o divulgar datos del alumnado, sus familias o el personal del centro fuera de los cauces oficiales o en entornos donde la privacidad pueda verse comprometida (salas comunes no reservadas, pasillos, cafetería del centro o redes sociales personales).

6.2. Obligaciones Específicas del Personal Docente

El profesorado del claustro, en el ejercicio de su función pedagógica, tutoría y orientación, manejará la información con arreglo a las siguientes pautas de obligado cumplimiento:

- **Información académica y de evaluación:**
  - Las calificaciones, partes de faltas, medidas correctoras e informes individuales solo se comunicarán a los propios alumnos/as e interesados o a sus padres, madres o tutores legales a través de **Séneca/iPasen** o entrevistas personales concertadas.

    - Se evitará la publicación de listados con nombres, apellidos y notas en tableros de anuncios públicos de los pasillos salvo cuando la normativa aplicable lo exija expresamente (y, en tal caso, se anonimizarán o limitarán los datos conforme a las instrucciones de la administración).
- **Atención a la diversidad e informes sensibles:**
    - Los informes psicopedagógicos, dictámenes de escolarización y datos sobre Necesidades Específicas de Apoyo Educativo (NEAE) gozan de una **protección reforzada**. Solo tendrán acceso a ellos el equipo directivo, el departamento de orientación, las/los tutoras/es directos y el profesorado especialista directamente implicado.
    - Dichos informes no se dejarán impresos sobre las mesas ni en carpetas compartidas de acceso general.
- **Comunicaciones con familias y alumnado:**
    - Toda comunicación oficial se canalizará preferentemente a través de la plataforma **iPasen** o el correo corporativo del dominio @g.educaand.es.
    - Se prohíbe el uso de canales de mensajería instantánea no corporativos (grupos personales de WhatsApp, Telegram, etc.) para tratar temas individuales del alumnado con las familias o con los propios estudiantes.
    - Al enviar correos electrónicos a múltiples destinatarios ajenos a la organización, se utilizará obligatoriamente la opción de **Copia Oculta (CCO)** para evitar la difusión pública de direcciones de correo.

6.3. Obligaciones Específicas del PAS y Personal de Servicios Complementarios

El Personal de Administración y Servicios (PAS) y el personal técnico o de limpieza y mantenimiento mantendrán idénticas garantías en su ámbito de actuación:

- **Atención al público y mostrador de Secretaría:**
    - Durante las gestiones administrativas presenciales o telefónicas, se velará por no exponer datos de terceros a la vista u oído de otras personas presentes.
    - Las pantallas de los ordenadores de administración se orientarán de manera que no sean visibles desde la zona de atención al público.
- **Documentación en soporte papel:**
    - Las solicitudes de matrícula, certificados de empadronamiento, datos bancarios o justificantes de becas se guardarán inmediatamente tras su recepción en cajones o archivadores provistos de llave.
    - El personal no dejará documentación con datos personales desatendida en mostradores, impresoras compartidas o fotocopiadoras.

6.4. Consecuencias e Implicaciones del Incumplimiento

El quebrantamiento del deber de secreto o la revelación indebida de datos personales constituye una infracción muy grave que puede derivar en las siguientes responsabilidades:

1. **Responsabilidad disciplinaria:** Aplicación del régimen disciplinario previsto en el *Estatuto Básico del Empleado Público (EBEP)*, la legislación de Función Pública de la Junta de Andalucía y el *Decreto 327/2010* (Reglamento Orgánico de IES), pudiendo conllevar aperturas de expediente disciplinario, sanciones o suspensión de empleo y sueldo.
2. **Responsabilidad administrativa:** Sanciones o requerimientos formalizados por el *Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA)* o la *Agencia Española de Protección de Datos (AEPD)*.
3. **Responsabilidad civil y penal:** En los casos más graves de revelación ilícita de secretos o vulneración de la intimidad de menores, la conducta podrá derivar en acciones ante los Tribunales de Justicia de conformidad con el Código Penal.

COMPROMISO INSTITUCIONAL DE CONFIDENCIALIDAD

Todo profesional que se incorpore a este centro educativo tomará conocimiento formal del presente Protocolo y asumirá de manera explícita el deber de secreto y reserva profesional sobre todos los datos de carácter personal gestionados.

7. Cesiones y comunicaciones de datos a terceros y encargados del tratamiento

Por regla general, los datos personales del alumnado, de sus familias y del personal del centro no se comunicarán a terceros ajenos a la administración educativa, salvo en los supuestos en los que exista una obligación legal, una misión de interés público o se cuente con el consentimiento previo, expreso e informado de las personas interesadas.

7.1. Comunicaciones y Cesiones de Datos Legítimas (Sin necesidad de consentimiento)

De acuerdo con el marco normativo vigente, las siguientes cesiones de datos están legitimadas por ley (artículos 6.1.c y 6.1.e del RGPD, en relación con la Ley Orgánica de Educación) y no requieren la autorización de las familias o del personal:

1. **Consejería de Desarrollo Educativo y Formación Profesional de la Junta de Andalucía:**

   Transferencia continua y automatizada de datos académicos, de asistencia, matriculación y expedientes a través del sistema corporativo **Séneca**, así como las comunicaciones requeridas por la **Inspección Educativa**.

2. **Ministerio de Educación, Formación Profesional y Deportes:**

   Comunicación de datos con fines estadísticos, de gestión de becas, títulos oficiales y Registro Estatal de Centros Docentes.

3. **Órganos Judiciales, Fiscalía de Menores y Fuerzas y Cuerpos de Seguridad:**

   Cesión de información requerida en el marco de investigaciones judiciales, procesos de protección de menores o requerimientos formales de la Policía Nacional o Guardia Civil.

4. **Servicios Sanitarios y Servicios de Urgencia:**

   Comunicación de datos identificativos y de salud (alergias, patologías, partes de lesiones) en caso de emergencia médica, accidente escolar o situaciones que pongan en riesgo la vida o la salud del alumnado.

5. **Entidades Aseguradoras y Gestión del Seguro Escolar:**

   Comunicación de los datos estrictamente necesarios para la tramitación de coberturas por accidentes sufridos en el ámbito escolar o en actividades complementarias/extraescolares.

6. **Administración Local / Servicios Sociales:**

   Comunicación de datos en el marco de comisiones de absentismo escolar o planes comunitarios de prevención del abandono escolar y protección del menor.

7.2. Cesiones que Requieren Consentimiento Expreso

Cualquier otra comunicación de datos no amparada por la normativa educativa exigirá la previa recogida de autorización explícita:

- **Asociación de Padres y Madres del Alumnado (AMPA):**

  El centro no facilitará listados de familias o alumnado a la AMPA. La gestión de socios y datos de la AMPA corresponde exclusivamente a dicha entidad privada independiente.

- **Entidades privadas, medios de comunicación o empresas para proyectos no oficiales:**

  Cualquier cesión de datos a empresas o entidades externas (por ejemplo, para concursos, intercambios no gestionados por la Consejería o reportajes periodísticos) requerirá la firma previa de un consentimiento informado por parte de los progenitores o del alumnado mayor de 14 años.

7.3. Regulación de los Encargados del Tratamiento (Proveedores Externos)

Tienen la condición de **Encargados del Tratamiento** (artículo 28 del RGPD) aquellas empresas o entidades que prestan un servicio al centro y que, para su desarrollo, necesitan acceder a datos de carácter personal de la comunidad educativa.

- **Servicios habituales en el IES:**
  - Empresas de transporte escolar contratadas para salidas y excursiones.
  - Empresas concesionarias de cafetería.
  - Fotógrafos o empresas encargadas de la elaboración de orlas o reportajes de graduación.
  - Empresas de mantenimiento informático o de software específico.
  - Entidades organizadoras de actividades extraescolares o talleres.
- **Garantías y Contrato de Encargo del Tratamiento:**

Ninguna empresa o profesional externo podrá comenzar a prestar servicios ni acceder a datos del centro sin haber suscrito previamente un **Contrato de Encargo del Tratamiento** (o haberse adherido al correspondiente Pliego de Cláusulas Administrativas de la Junta de Andalucía). Dicho documento garantizará que el prestador:

1. Tratará los datos **únicamente según las instrucciones documentadas** del centro o de la administración.
2. Aplicará las **medidas de seguridad técnicas y organizativas** adecuadas a la sensibilidad de los datos.
3. Garantizará que su personal esté sujeto a **compromiso formal de confidencialidad**.
4. **Destruirá o devolverá** al centro todos los datos personales una vez finalizada la prestación del servicio.
5. Se compromete a **no subcontratar** el servicio a terceros sin autorización previa y escrita.

7.4. Transferencias Internacionales de Datos (TID)

Con carácter general, se prohíbe al personal del centro el uso de aplicaciones, herramientas web o servicios de almacenamiento en la nube (*cloud computing*) cuyos servidores estén ubicados fuera del **Espacio Económico Europeo (EEE)**, a menos que cuenten con una decisión de adecuación de la Comisión Europea o garantías de seguridad equivalentes.

- **Herramientas autorizadas:**

El centro utilizará las herramientas colaborativas e infraestructuras digitales puestas a disposición por la Consejería de Desarrollo Educativo y Formación Profesional (suite corporativa bajo el dominio @g.educaand.es o la identidad digital corporativa), las cuales cuentan con los correspondientes acuerdos de nivel de servicio y anexos de protección de datos adaptados al RGPD y al Esquema Nacional de Seguridad.

8. Derechos de las personas interesadas y procedimiento para su ejercicio

La normativa de protección de datos reconoce a toda la ciudadanía el control sobre su información personal. La comunidad educativa de este instituto (alumnado, familias, tutores legales y trabajadores) puede ejercitar estos derechos de forma gratuita, sencilla y transparente ante el centro o ante la administración educativa.

8.1. Catálogo de Derechos

De conformidad con los artículos 15 a 22 del RGPD y los artículos 12 a 18 de la LOPDGDD, las personas interesadas pueden ejercitar los siguientes derechos:

- **Derecho de Acceso:** Saber si el centro está tratando sus datos personales y, de ser así, obtener información sobre las finalidades, categorías de datos, destinatarios y plazos de conservación, así como recibir una copia de los mismos.
- **Derecho de Rectificación:** Solicitar la corrección de aquellos datos personales que sean inexactos, desactualizados o incompletos (por ejemplo, errores en la filiación, DNI, dirección o teléfonos de contacto).
- **Derecho de Supresión ("Derecho al Olvido"):** Solicitar la eliminación de los datos personales cuando ya no sean necesarios para los fines que motivaron su recogida o cuando se retire el consentimiento otorgado.
    - *Límite legal en el ámbito educativo:* Este derecho **no podrá aplicarse** sobre expedientes académicos, actas de evaluación, registros de matrícula o documentos oficiales mientras persista la obligación legal de conservación establecida por la legislación educativa y el sistema de archivos públicos de Andalucía.
- **Derecho a la Limitación del Tratamiento:** Solicitar que se suspenda o limite temporalmente el tratamiento de los datos mientras se verifica su exactitud o la licitud del tratamiento.
- **Derecho a la Oposición:** Oponerse a que sus datos personales sean objeto de un tratamiento basado en el interés público o legítimo, alegando motivos fundados y legítimos relativos a su situación personal concreta.
- **Derecho de Portabilidad:** Recibir los datos personales en un formato estructurado, de uso común y lectura mecánica, para su transmisión a otro responsable (de aplicación marginal en nuestro ámbito docente público).

8.2. Capacidad Legal y Legitimación para el Ejercicio de Derechos

- **Alumnado menor de 14 años:** El ejercicio de los derechos de protección de datos corresponde **exclusivamente a los padres, madres o representantes legales**, debiendo acreditar debidamente la patria potestad o tutela.
- **Alumnado mayor de 14 años:** Tienen capacidad legal para ejercitar por sí mismos sus derechos en materia de protección de datos personales.
    - *Matiz sobre el derecho a la información académica:* El ejercicio del derecho de supresión u oposición por un alumno mayor de 14 años no impedirá en ningún caso que sus progenitores o representantes legales sigan accediendo a sus calificaciones, partes de faltas o evolución escolar, conforme al derecho reconocido a las familias en la legislación educativa mientras el alumno sea menor de edad y dependa económicamente de ellas.
- **Profesorado y Personal de Administración y Servicios (PAS):** Ejercitarán sus derechos de forma directa e individual.

8.3. Procedimiento y Tramitación de las Solicitudes

Para garantizar la correcta tramitación y el cumplimiento estricto de los plazos legales, se establece el siguiente procedimiento:



1. **Vías de presentación:**
   - **Presencial:** En la Secretaría del instituto, mediante el formulario oficial de solicitud disponible en el centro, acompañando copia del DNI/NIE o documento equivalente para verificar la identidad de la persona solicitante o su representante.
   - **Telemática:** A través de la Presentación Electrónica General de la Junta de Andalucía o mediante comunicación dirigida por correo electrónico al Delegado de Protección de Datos de la Consejería: dpd.ced@juntadeandalucia.es.
2. **Plazos de respuesta y resolución:**
   - La solicitud será atendida y contestada en el plazo máximo de **un mes** a contar desde la recepción de la misma.
   - Excepcionalmente, este plazo podrá prorrogarse **hasta dos meses más** cuando sea necesario, atendiendo a la complejidad o al número de solicitudes. En este supuesto, se informará motivadamente a la persona interesada de la prórroga dentro del primer mes.
3. **Garantía de tutela administrativa:**
   - Si la persona interesada considera que su solicitud no ha sido atendida adecuadamente o se han vulnerado sus derechos, podrá presentar una reclamación de tutela de derechos ante el **Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA)** o ante la Agencia Española de Protección de Datos (AEPD).

8.4. Garantía de Derechos Digitales en el Entorno Escolar

En aplicación del artículo 83 de la LOPDGDD, este Instituto de Educación Secundaria asume el compromiso de garantizar los derechos digitales de la comunidad educativa:

- **Educación y competencia digital segura:** El centro incorporará en su Proyecto Educativo (PE) y en el Plan Digital de Centro contenidos pedagógicos orientados a la formación del alumnado en el uso seguro, crítico y responsable de las tecnologías, con especial atención a la protección de la privacidad, la reputación digital y los derechos propios y ajenos.
- **Prevención de riesgos en la red:** Se implementarán acciones específicas para prevenir y detectar conductas de acoso escolar en entornos digitales (*cyberbullying*), *grooming*, *sexting* o la difusión no consentida de imágenes íntimas o vejatorias entre menores.
- **Derecho a la desconexión digital:** Se respetará el derecho a la desconexión digital del profesorado y del alumnado fuera del horario lectivo y laboral, evitando el envío de comunicaciones o exigencias de respuesta fuera de las jornadas establecidas, salvo situaciones de fuerza mayor o urgencia justificada.

9. Gestión de la imagen del alumnado, web institucional y redes sociales del IES

El tratamiento de la imagen y la voz del alumnado mediante fotografías, grabaciones de vídeo o transmisiones en directo en el entorno escolar exige una protección rigurosa. La imagen constituye un dato de carácter personal de acuerdo con el RGPD y un derecho fundamental protegido por la *Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*.

9.1. Régimen de Autorizaciones y Recogida del Consentimiento

1. **Gestión a través de la matrícula:**

   Al inicio de cada curso académico, durante el proceso de matriculación (vía **iPasen / Séneca** o impreso oficial), el centro recabará de forma clara e independiente la autorización para el uso pedagógico y difusión institucional de la imagen y voz del alumnado.

2. **Criterio por edad:**
   - **Menores de 14 años:** El documento de autorización o denegación será firmado obligatoriamente por los padres, madres o tutores legales.
   - **Mayores de 14 años:** La autorización será otorgada o denegada directamente por el propio alumno o alumna, sin perjuicio de mantener informadas a las familias.

3. **Carácter voluntario y revocable:**

   La concesión de la autorización es completamente voluntaria y su negativa no afectará en absoluto a la escolarización ni a la participación del estudiante en las actividades lectivas o complementarias. Asimismo, el consentimiento podrá ser revocado en cualquier momento mediante comunicación escrita a la Secretaría del centro.

9.2. Pautas de Publicación en Canales Oficiales del Centro

El instituto únicamente difundirá imágenes a través de sus **canales institucionales oficiales** (página web del centro, plataformas corporativas y perfiles oficiales del IES en redes sociales autorizados por el Consejo Escolar):

- **Finalidad exclusivamente educativa:** Las publicaciones se limitarán a documentar actividades complementarias, excursiones, proyectos de innovación (Erasmus+, Escuela Espacio de Paz, Ferias de la Ciencia), eventos deportivos o actos académicos (graduaciones).
- **Minimización y contexto positivo:** Se priorizarán planos generales o de grupo donde el alumnado no sea el elemento central exclusivo, evitando primeros planos o retratos individuales salvo consentimiento específico para premios o reconocimientos expresos.
- **Prohibición de identificación cruzada:** Salvo autorización explícita o reconocimientos académicos oficiales, no se asociará la fotografía del alumno/a con su nombre completo, curso u otros datos identificativos directos en redes sociales abiertas.
- **Prohibición de uso con fines comerciales:** Queda totalmente desautorizada la cesión o utilización de las imágenes para fines publicitarios, promocionales o comerciales ajenos a la función docente.

9.3. Captura de Imágenes por Parte de las Familias en Eventos Escolares

En actos de la comunidad educativa donde se permita la entrada de familias (graduaciones, festivales, competiciones deportivas o jornadas de puertas abiertas):

- **Uso exclusivo personal y doméstico:** La toma de fotografías o vídeos por parte de las familias se considera amparada por la «excepción doméstica» (artículo 2.2.a RGPD), siempre que su destino sea el uso estrictamente familiar o privado.
- **Prohibición de difusión pública sin permiso:** La difusión de dichas imágenes en redes sociales abiertas, plataformas de vídeo o grupos públicos de mensajería (donde aparezcan otros menores cuyos progenitores no hayan dado su consentimiento) no está cubierta por la excepción doméstica y constituye una responsabilidad exclusiva de la persona que las publique.
- **Aviso en eventos:** El centro recordará verbalmente o mediante cartelera esta prohibición antes del inicio de los actos comunitarios.

9.4. Uso de Dispositivos por el Alumnado y Grabaciones no Autorizadas

De acuerdo con el Reglamento de Organización y Funcionamiento (ROF) del centro y la normativa autonómica:

- **Los dispositivos móviles del alumnado** quedan prohibidos salvo situaciones relacionadas con la salud del interesado o concesión particular emitida por dirección.
- **Grabaciones en el aula o recinto escolar:** Si el alumnado puede tener el móvil en el centro, queda expresamente prohibido que realice fotografías, grabaciones de audio o vídeo al profesorado, al personal no docente o a sus propios compañeros/as dentro del recinto escolar sin la autorización previa y explícita del docente responsable de la actividad.
- **Infracción disciplinaria:** La difusión no autorizada de imágenes tomadas en el centro, especialmente si atentan contra la dignidad, el honor o la intimidad de miembros de la comunidad educativa o implican situaciones de acoso (*cyberbullying*), será sancionada conforme a las normas de convivencia del centro (Decreto 327/2010), sin perjuicio de las responsabilidades civiles, administrativas o penales que de ello se deriven.

9.5. Resumen del Protocolo de Imagen

Supuesto	¿Requiere autorización?	Firma de la Autorización	Canal Autorizado
Fotos en Web / Redes del IES	**Sí**	Progenitores (<14 años) / Alumno (≥14 años)	Canales oficiales IES
Plataformas docentes (Moodle/Séneca)	**No** (Base legal: función educativa)	N/A	Entornos corporativos Junta
Fotos de familias en Graduaciones	**No** (Uso privado doméstico)	N/A	Ámbito estrictamente familiar
Publicación de fotos en redes de familias	**Sí** (de los demás menores)	Progenitores de los otros menores	Responsabilidad de quien publica
Grabaciones del alumnado en clase	**Sí** (Autorización del docente)	Profesorado afectado / Dirección	Tareas pedagógicas indicadas

10. Protocolo de actuación y notificación ante brechas de seguridad

Una **brecha de seguridad de datos** es cualquier incidente que origine la destrucción, pérdida, alteración, comunicación o acceso no autorizado a los datos personales gestionados por el instituto, ya sea de forma accidental o ilícita.

Dada la especial sensibilidad de la información del alumnado y del personal del centro, este IES establece un procedimiento de respuesta rápida e inmediata para minimizar los posibles impactos sobre los derechos y libertades de las personas afectadas.

10.1. Ejemplos de Brechas de Seguridad en el Entorno Escolar

Entre las situaciones más habituales que constituyen una brecha de seguridad en el centro se encuentran:

- **Pérdida o robo de dispositivos:** Extravío de un ordenador portátil corporativo, tablet o memoria USB no cifrada que contenga listados de alumnado, calificaciones, informes NEAE o datos de salud.
- **Envíos de correo electrónico erróneos:** Envío masivo de correos a las familias con las direcciones visibles en el campo "Para" o "CC" en lugar de "CCO" (copia oculta), o envío de calificaciones o informes a un destinatario equivocado.
- **Acceso o uso no autorizado:** Intrusión o uso de credenciales de **Séneca**, **iPasen** o correo corporativo por parte de personas no autorizadas o por suplantación de identidad (*phishing*).
- **Ataques informáticos / Malware:** Infección por virus o *ransomware* que bloquee o cifre los servidores o equipos de Secretaría y Dirección impidiendo el acceso a los datos.
- **Documentación física desatendida:** Pérdida, robo o destrucción no controlada de expedientes académicos en papel, boletines de matrícula o exámenes durante su traslado fuera del recinto escolar.

10.2. Procedimiento de Actuación y Flujo de Comunicación

Ante la sospecha o confirmación de una brecha de seguridad, se activará de forma inmediata el siguiente flujo de actuación:

[PASO 1: Detección del Incidente]
↓
[PASO 2: Comunicación Interna Inmediata a la Dirección del IES]
↓
[PASO 3: Medidas Inmediatas de Contención y Mitigación]
↓
[PASO 4: Notificación al DPD de la Consejería (Máximo 24-48h)]
↓
[PASO 5: Notificación a la AEPD / CTPDA por el DPD (Máximo 72h)]
↓
[PASO 6: Comunicación a las Personas Afectadas (Si existe alto riesgo)]

Paso 1 y 2: Detección y Notificación Interna

- CUALQUIER miembro de la comunidad educativa (profesorado, PAS, personal de limpieza, etc.) que detecte una incidencia de seguridad debe comunicarlo de **forma inmediata** a la **Dirección o Jefatura de Estudios** del instituto.
- No se intentará ocultar o resolver la incidencia de forma aislada sin informar previamente a la Dirección.

Paso 3: Contención Inicial y Mitigación

El equipo directivo, en coordinación con los servicios técnicos o el Administrador de Red del centro (en nuestro centro esta figura la asume la coordinadora TDE), aplicará de inmediato las primeras medidas de contención:

- Cambiar las contraseñas de las cuentas comprometidas.
- Desconectar de la red los equipos informáticos afectados (en caso de *malware*).

- Solicitar el borrado remoto de dispositivos portátiles vinculados a cuentas corporativas si han sido robados.
- Intentar la recuperación del mensaje o solicitar la eliminación del correo al destinatario en envíos erróneos.

Paso 4: Notificación al Delegado de Protección de Datos (DPD)

- La Dirección del centro comunicará formalmente el incidente al **Delegado de Protección de Datos de la Consejería de Desarrollo Educativo y Formación Profesional** a través del correo institucional dpd.ced@juntadeandalucia.es.
- La comunicación se realizará a la mayor brevedad posible (idealmente en las primeras 24 horas tras la detección) aportando los siguientes datos:
    1. Naturaleza del incidente y fecha/hora de ocurrencia.
    2. Categorías y número aproximado de personas afectadas (alumnado, familias, personal).
    3. Categoría de datos personales comprometidos (académicos, de contacto, salud, etc.).
    4. Medidas inmediatas adoptadas para contener los daños.

Paso 5: Notificación a la Autoridad de Control

- El DPD de la Consejería evaluará el alcance y, si el incidente entraña un riesgo para los derechos y libertades de las personas, notificará la brecha de seguridad a la **Agencia Española de Protección de Datos (AEPD)** y/o al **Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA)** en un plazo máximo de **72 horas** desde que se tuvo constancia del mismo, conforme al artículo 33 del RGPD.

Paso 6: Comunicación a las Personas Afectadas

- Si la brecha entraña un **alto riesgo** para los derechos de los afectados (por ejemplo, filtración masiva de datos de salud, informes de menores o claves bancarias), el centro, bajo las directrices del DPD, comunicará de forma clara, concisa y comprensible lo sucedido a los progenitores, tutores legales o afectados, indicando las medidas recomendadas para protegerse.

10.3. Registro de Incidencias de Seguridad

El centro mantendrá un **Registro de Incidencias y Brechas de Seguridad** interno, bajo la custodia de la Dirección, en el que se documentarán detalladamente:

- La descripción del incidente y sus causas.
- Las circunstancias en que se produjo y la fecha de detección.
- Sus efectos e impactos reales o potenciales.
- Las medidas correctoras adoptadas para evitar que la situación vuelva a repetirse.

10.4. Plan de Remediación y Revisión Continua

Tras la resolución de una brecha de seguridad, el Equipo Directivo analizará las causas que la originaron y adoptará las acciones preventivas necesarias, tales como:

1. Revisar y reforzar las medidas de seguridad técnicas o físicas del centro.
2. Impartir pautas recordatorias o formación específica al Claustro y al PAS sobre los errores detectados.
3. Actualizar el presente Protocolo si se identifican lagunas operativas durante la gestión de la crisis.

c