

The British School of Gran Canaria



Protocolo Protección de Datos

Contenidos

1. Objetivo y Justificación
 2. Marco Jurídico y Normativo
 3. Ámbito de Aplicación
 4. ¿Qué son los datos personales?
 5. Categorías especiales e información sensible
 6. Principios de protección de datos
 7. Tratamiento lícito
 8. Avisos sobre transparencia y privacidad
 9. Datos de niños y jóvenes
 10. Seguridad de los datos
 11. Responsabilidades del personal
 12. Intercambio de datos
 13. Proveedores externos y tecnología educativa
 14. Evaluaciones de Impacto en la Protección de Datos
 15. Registro de actividades de tratamiento
 16. Conservación y eliminación
 17. Derechos personales en materia de protección de datos
 18. Solicitudes de acceso de los interesados y otras solicitudes relacionadas con los derechos de información
 19. Vulneraciones de la seguridad de los datos personales
 20. Fotografías, vídeos y grabaciones de audio
 21. CCTV, Filtrado y Supervisión
 22. Inteligencia Artificial
 23. Transferencias internacionales
 24. Protección de datos y protección de menores
 25. Formación y Sensibilización
 26. Funciones y Responsabilidades
 27. Incumplimiento
 28. Seguimiento y revisión
- Anexo 1 – Principios de protección de datos del *BSGC*: Guía rápida para el personal

1. Objetivo y Justificación

The British School of Gran Canaria reconoce que la gestión responsable y la protección de los datos personales son fundamentales para la seguridad, la privacidad, la dignidad y la confianza de nuestros alumnos, familias, personal y comunidad en general.

El *BSGC* recopila y trata datos personales con una amplia variedad de fines educativos, de protección, administrativos, laborales y operativos. El colegio se compromete a garantizar que los datos personales se recopilen, utilicen, almacenen y compartan de forma lícita, leal, transparente y segura.

El presente Protocolo establece los principios y responsabilidades que rigen el tratamiento de datos personales en el *BSGC* y respalda el cumplimiento por parte del colegio de la legislación aplicable en materia de protección de datos.

A efectos del RGPD, el *BSGC* actuará como responsable del tratamiento en relación con aquellas actividades en las que el colegio determine los fines y los medios del tratamiento. Los terceros que traten datos personales de conformidad con las instrucciones documentadas del *BSGC* actuarán como encargados del tratamiento, salvo que la naturaleza del servicio requiera que se documente una clasificación jurídica diferente.

2. Marco Jurídico y Normativo

El *BSGC* cumplirá con la legislación aplicable en materia de protección de datos y privacidad, incluyendo, según proceda:

- el Reglamento General de Protección de Datos de la UE (Reglamento (UE) 2016/679 – RGPD);
- la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD);
- el Reglamento (UE) 2024/1689 sobre inteligencia artificial (Ley de IA de la UE), cuando sea aplicable a los sistemas de IA utilizados por el colegio y de conformidad con su calendario de aplicación;
- la legislación española aplicable en materia de educación, empleo, protección de menores, confidencialidad y registros;
- los requisitos aplicables en materia de transferencias internacionales de datos personales;
- El RGPD del Reino Unido y la Ley de Protección de Datos del Reino Unido de 2018, cuando sean aplicables a determinadas actividades de tratamiento, personas, servicios, transferencias o acuerdos contractuales;
- Las directrices y decisiones emitidas por las autoridades de control pertinentes, incluida la Agencia Española de Protección de Datos (AEPD) y, cuando proceda, la Oficina del Comisionado de Información del Reino Unido (ICO).

El centro revisará periódicamente sus medidas de protección de datos a medida que evolucionen la legislación y las directrices normativas.

3. Ámbito de aplicación

Este protocolo se aplica a:

- todos los alumnos;
- padres, tutores y familias;
- miembros del consejo rector;
- personal docente y de apoyo;
- personal temporal y de agencias;
- voluntarios;
- contratistas y consultores;

- proveedores externos que traten información en nombre del BSGC;
- cualquier otra persona que tenga acceso a los datos personales del BSGC.

Se aplica a los datos personales tratados:

- por vía electrónica o digital;
- en expedientes en papel;
- a través de los sistemas de información del centro educativo;
- a través de tecnologías educativas y plataformas en línea;
- a través del correo electrónico y los sistemas de comunicación;
- a través de fotografías, vídeos y audio;
- a través de sistemas de videovigilancia, control de acceso y seguridad;
- a través de la inteligencia artificial y otras tecnologías emergentes;
- en dispositivos personales propiedad del centro educativo o autorizados por este;
- por parte de organizaciones externas en nombre del centro educativo.

El Protocolo se aplica tanto si la información se trata en las instalaciones del centro, a distancia, durante excursiones o viajes escolares, como en el marco de otras actividades escolares.

4. ¿Qué son los datos personales?

Los datos personales son información relativa a una persona física viva, identificada o identificable.

Esto puede incluir, por ejemplo:

- nombre y datos de contacto;
- fecha de nacimiento;
- dirección;
- registros de asistencia;
- información académica y de evaluación;
- registros de comportamiento;
- fotografías y vídeos;
- información de identificación y autenticación;
- comunicaciones;
- información sobre protección;
- información médica;
- información sobre necesidades educativas especiales;
- información financiera;
- registros de empleo y contratación;
- identificadores en línea e información técnica;
- información generada a través de los sistemas escolares, el filtrado y la supervisión.

Los datos personales pueden existir tanto en formato electrónico como físico.

5. Categorías especiales e información sensible

Algunos datos personales requieren una protección adicional debido a su carácter especialmente sensible. Entre ellos se incluye la información relacionada con ámbitos como:

- la salud;
- el origen racial o étnico;
- las creencias religiosas o filosóficas;
- la información biométrica utilizada para la identificación;
- la orientación sexual;
- determinada información relacionada con la protección de menores;
- otras categorías identificadas por la legislación aplicable.

El BSGC solo tratará dicha información cuando exista una base jurídica adecuada y se cumplan las condiciones legales adicionales pertinentes. El personal debe actuar con especial cuidado al acceder, comentar, almacenar o compartir información sensible.

6. Principios de protección de datos

El BSGC aplicará los principios de protección de datos establecidos por la legislación vigente. Los datos personales deben ser:

Lícitos, leales y transparentes: la información debe tratarse de forma lícita y las personas deben comprender cómo y por qué se utiliza su información.

Limitados a fines específicos: la información debe recopilarse para fines específicos, explícitos y legítimos, y no debe utilizarse posteriormente de forma incompatible con dichos fines.

Adecuados y limitados: solo debe recopilarse y utilizarse la información necesaria para el fin previsto.

Exactos: deben adoptarse medidas razonables para garantizar que la información sea exacta y se mantenga actualizada cuando sea necesario.

Almacenados de forma adecuada: la información no debe conservarse durante más tiempo del necesario.

Seguridad: deben adoptarse medidas técnicas y organizativas adecuadas para proteger la información contra el acceso no autorizado, la pérdida, la alteración, la divulgación o la destrucción.

Responsabilidad: el BSGC debe poder demostrar que cumple con estos principios.

Protección de datos desde el diseño y por defecto: la privacidad se integrará desde el inicio de los proyectos y, por defecto, solo se tratarán los datos estrictamente necesarios para cada finalidad prevista, con períodos de acceso y conservación restringidos en consecuencia.

7. Tratamiento lícito

El BSGC solo tratará datos personales cuando exista una base jurídica adecuada. Dependiendo de las circunstancias, esto puede incluir:

- una obligación legal;
- el cumplimiento de un contrato con el interesado o la aplicación de medidas precontractuales a petición de este;
- el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos, cuando exista una base jurídica aplicable;
- la protección de los intereses vitales del interesado o de otra persona física;
- los intereses legítimos, cuando proceda;
- el consentimiento, cuando proceda.

El consentimiento no se utilizará automáticamente por el mero hecho de que resulte conveniente. Cuando se recurra al consentimiento, este deberá obtenerse de forma adecuada, ser informado y poder ser retirado, con sujeción a los requisitos legales aplicables.

En el caso de las categorías especiales de datos, BSGC deberá identificar, además de una base jurídica con arreglo al artículo 6 del RGPD, una condición aplicable con arreglo al artículo 9, apartado 2. Los datos relativos a condenas penales y delitos solo se tratarán de conformidad con lo dispuesto en el artículo 10 del RGPD y la legislación española aplicable.

El personal no debe dar por sentado que puede utilizar la información personal simplemente porque el centro ya la tenga en su poder.

8. Avisos sobre transparencia y privacidad

BSGC facilitará a las personas la información adecuada en materia de privacidad, explicando:

- la identidad y los datos de contacto de BSGC como responsable del tratamiento;
- los datos de contacto del delegado de protección de datos (DPO);
- las finalidades del tratamiento y, en su caso, las categorías de datos personales de que se trate;
- la base jurídica del tratamiento y, cuando se invoque el interés legítimo, los intereses legítimos perseguidos;
- los destinatarios o las categorías de destinatarios de los datos personales;
- cualquier transferencia internacional prevista y el mecanismo de transferencia o las garantías aplicables;
- el plazo de conservación o, cuando ello no sea posible, los criterios utilizados para determinar dicho plazo;
- los derechos aplicables, incluido el derecho a retirar el consentimiento cuando el tratamiento se base en el consentimiento, y el derecho a presentar una reclamación ante la AEPD (Autoridad Española de Protección de Datos);
- cuando los datos personales no se obtengan directamente del interesado, las categorías de datos personales y la fuente de la que proceden; y, en su caso, la existencia de decisiones automatizadas o elaboración de perfiles, junto con la información significativa exigida por el RGPD;
- si el suministro de datos personales es un requisito legal o contractual, o un requisito necesario para celebrar un contrato, y las posibles consecuencias de no facilitar dichos datos.

La información sobre la privacidad se facilitará de forma accesible y adecuada a la edad de los alumnos, especialmente en el caso de estos.

Los avisos de privacidad se revisarán periódicamente y siempre que se produzcan cambios significativos en las actividades de tratamiento de datos del centro educativo.

9. Datos de niños y jóvenes

El BSGC reconoce que los alumnos requieren una atención y protección especiales a la hora de tratar sus datos personales. El colegio:

- tener en cuenta la edad y el nivel de comprensión de los alumnos a la hora de explicar el uso de los datos;
- proporcionar información adecuada y accesible sobre la protección de datos;
- garantizar que los datos de los menores se traten de forma leal y proporcionada;
- aplicar medidas de seguridad adecuadas a la tecnología educativa;
- evaluar cuidadosamente los riesgos asociados a la elaboración de perfiles, la vigilancia y el tratamiento automatizado;
- prestar especial atención a la hora de introducir nuevas tecnologías que impliquen el tratamiento de datos de menores.

El centro tendrá en cuenta las directrices normativas pertinentes relativas a los datos personales de los menores y a la tecnología educativa.

En España, cuando el tratamiento se basa en el consentimiento de un menor, los alumnos mayores de 14 años pueden dar su consentimiento por sí mismos, salvo que la ley exija la asistencia de quienes ejercen la patria potestad o la tutela para el acto concreto de que se trate. En el caso de los menores de 14 años, el tratamiento basado en el consentimiento solo será lícito si dicho consentimiento lo otorga

el titular de la patria potestad o la tutela. Esta norma no implica que todo tratamiento de datos personales de los alumnos deba basarse en el consentimiento.

10. Seguridad de los datos

El BSGC aplicará las medidas técnicas y organizativas adecuadas para proteger los datos personales.

Entre ellas pueden figurar:

- controles de acceso;
- contraseñas y autenticación;
- permisos basados en roles;
- cifrado, cuando proceda;
- redes seguras;
- dispositivos gestionados;
- filtrado y supervisión;
- copias de seguridad seguras;
- protección contra malware y de los terminales;
- seguridad física;
- eliminación segura;
- formación del personal;
- gestión de incidentes.

El acceso a la información personal se basará en una necesidad legítima y en la autorización correspondiente.

El personal no debe acceder a la información simplemente porque técnicamente tenga la capacidad de hacerlo.

11. Responsabilidades del personal

Toda persona que maneje datos personales en nombre de BSGC tiene la responsabilidad de protegerlos.

El personal debe:

- utilizar la información personal únicamente con fines escolares legítimos;
- acceder únicamente a la información que necesite para el desempeño de sus funciones;
- mantener la información segura;
- evitar copias o descargas innecesarias;
- utilizar los sistemas aprobados por el centro;
- cumplir los requisitos de conservación y eliminación de datos;
- verificar los destinatarios antes de enviar información;
- actuar con la debida diligencia al tratar asuntos confidenciales;
- notificar sin demora las posibles infracciones;
- realizar la formación obligatoria en materia de protección de datos.

El personal no debe:

- compartir contraseñas;
- dejar información confidencial sin vigilancia;
- enviar información personal a destinatarios no autorizados;
- utilizar cuentas de correo electrónico personales para información confidencial del colegio;
- almacenar información del colegio en dispositivos o servicios no autorizados;
- subir información confidencial a herramientas de IA no aprobadas;
- revelar información a padres o terceros sin la autorización correspondiente.

12. Intercambio de datos

El BSGC podrá compartir información personal cuando exista una base legal y una justificación adecuada.

La información podrá compartirse, por ejemplo, con:

- autoridades gubernamentales o reguladoras;
- instituciones educativas;
- organismos de evaluación y certificación;
- profesionales sanitarios o de protección infantil;
- proveedores de servicios;
- aseguradoras;
- asesores jurídicos o profesionales;
- otras organizaciones cuando así lo exija o lo permita la ley.

El BSGC aplicará los principios de necesidad, proporcionalidad y minimización de datos a la hora de compartir información. Cuando proceda, se establecerán acuerdos formales de intercambio o tratamiento de datos.

13. Proveedores externos y tecnología educativa

Antes de incorporar un servicio que trate datos personales en nombre del BSGC, el centro tendrá en cuenta:

- la finalidad y la necesidad del tratamiento;
- los datos en cuestión;
- las medidas de seguridad del proveedor;
- las condiciones contractuales;
- las disposiciones relativas al tratamiento de datos;
- las transferencias internacionales;
- la conservación de datos;
- los subencargados del tratamiento;
- las medidas de supresión;
- el uso que el proveedor hace de los datos con fines de análisis, elaboración de perfiles o entrenamiento de IA;
- los riesgos para los alumnos y el personal.

Cuando proceda, se llevará a cabo una evaluación de impacto en la protección de datos (EIPD) antes de que comience el tratamiento. Las directrices escolares vigentes señalan que las EIPD revisten especial importancia cuando es probable que el tratamiento suponga un alto riesgo para los derechos y libertades de las personas, y recomiendan realizar una nueva evaluación cuando se produzcan cambios significativos.

Los proveedores externos deben firmar un acuerdo de tratamiento de datos, siempre que sea posible.

Cuando un proveedor actúe como encargado del tratamiento, la relación deberá formalizarse mediante un contrato u otro acto jurídico vinculante, de conformidad con el artículo 28 del RGPD, que incluya las disposiciones mínimas obligatorias, antes de que el proveedor tenga acceso a cualquier dato personal.

Antes de la contratación, BSGC llevará a cabo y documentará la diligencia debida necesaria para verificar que el proveedor ofrece garantías suficientes de conformidad con el artículo 28, apartado 1, del RGPD y el considerando 81, incluidas las medidas de seguridad, los subencargados del tratamiento, la ubicación de los datos, las transferencias internacionales, la conservación, la devolución o supresión de los datos y las capacidades de auditoría.

El proveedor no utilizará los datos del *BSGC* para sus propios fines, con fines publicitarios, para la elaboración de perfiles ni para el entrenamiento de modelos de inteligencia artificial, a menos que dicho fin, la función jurídica del proveedor y la base jurídica correspondiente hayan sido evaluados exhaustivamente y autorizados expresamente por el *BSGC*.

14. Evaluaciones de Impacto en la Protección de Datos

La obligación de llevar a cabo una EIPD recae en el *BSGC*, en su calidad de responsable del tratamiento. La elaboración práctica puede requerir apoyo interno o externo, incluidos consultores contratados, pero el *BSGC* seguirá siendo responsable de garantizar su correcta realización, de aplicar las medidas resultantes y de documentar la decisión. Se consultará al delegado de protección de datos (DPO), quien supervisará la aplicación de la EIPD. Se llevará a cabo una EIPD antes del tratamiento cuando este pueda suponer un riesgo elevado para los derechos y libertades de las personas físicas, en particular al introducir:

- nuevas tecnologías;
- sistemas de vigilancia de gran envergadura;
- sistemas de inteligencia artificial;
- tratamiento a gran escala;
- sistemas que impliquen información sensible;
- nuevas formas de elaboración de perfiles o de toma de decisiones automatizada;
- cambios significativos en el tratamiento existente.

Una EIPD debe identificar:

- la finalidad del tratamiento;
- la información objeto del mismo;
- los interesados afectados;
- la base jurídica;
- los riesgos potenciales;
- las medidas para mitigar dichos riesgos;
- los riesgos residuales;

La decisión documentada del *BSGC* sobre si se debe proceder, especificando las condiciones aplicables y las medidas de mitigación.

Si la evaluación de impacto relativa a la protección de datos (DPIA) concluye que persiste un riesgo elevado que no puede mitigarse de forma razonable, el *BSGC* consultará a la AEPD antes de iniciar el tratamiento, de conformidad con el artículo 36 del RGPD.

15. Registro de actividades de tratamiento

El *BSGC* mantendrá un registro actualizado de las actividades de tratamiento, de conformidad con el artículo 30 del RGPD. El registro identificará, según proceda, las categorías de datos personales;

- las categorías de interesados;
- las finalidades del tratamiento;
- las bases legales;
- los destinatarios;
- las transferencias internacionales;
- los plazos de conservación;
- las medidas de seguridad;
- los sistemas y terceros pertinentes.

El “Registro de actividades de tratamiento” es un importante mecanismo de rendición de cuentas y se menciona expresamente en las directrices vigentes sobre protección de datos en el ámbito escolar.

16. Conservación y eliminación

El *BSGC* conservará los datos personales únicamente durante el tiempo que sea necesario o según lo exijan la ley, la normativa, los requisitos contractuales o los fines legítimos del centro.

El centro mantendrá un control adecuado de conservación y eliminación de datos.

Cuando la información ya no sea necesaria, se procederá de forma segura a:

- su eliminación;
- su destrucción;
- su eliminación por otros medios.

Se prestará especial atención a la eliminación de documentos en papel, ordenadores, dispositivos de almacenamiento y demás equipos que contengan datos personales.

17. Derechos personales en materia de protección de datos

Sin perjuicio de los requisitos legales aplicables, las personas pueden tener derechos como, entre otros:

- el derecho a ser informado;
- el derecho de acceso;
- el derecho de rectificación;
- el derecho de supresión;
- el derecho a la limitación del tratamiento;
- el derecho a la portabilidad de los datos;
- el derecho de oposición;
- los derechos relativos a la toma de decisiones automatizada y a la elaboración de perfiles.

La disponibilidad de un derecho concreto depende de las circunstancias y de la base jurídica del tratamiento. El *BSGC* facilitará el ejercicio de estos derechos de forma gratuita, salvo en las circunstancias excepcionales previstas en el RGPD, y responderá sin demora injustificada y, en cualquier caso, en el plazo de un mes desde la recepción de la solicitud. Cuando proceda, este plazo podrá prorrogarse por dos meses más si fuera necesario, teniendo en cuenta la complejidad y el número de solicitudes, informando al interesado dentro del primer mes. Los interesados podrán presentar una reclamación ante la AEPD.

18. Solicitudes de acceso de los interesados y otras solicitudes relacionadas con los derechos de información

Las solicitudes relativas a datos personales deben remitirse sin demora al canal interno designado y al delegado de protección de datos (DPO) para que este preste asesoramiento. La responsabilidad de responder y cumplir con los plazos legales recae en el *BSGC*, en su calidad de responsable del tratamiento. El personal no debe responder, rechazar, modificar ni eliminar ninguna información por iniciativa propia cuando se enfrente a una solicitud. Esto incluye solicitudes que puedan parecer informales, como: «¿Puedo ver toda la información que tiene el colegio sobre mi hijo?». Dichas solicitudes pueden constituir un ejercicio de los derechos de información y, por lo tanto, deben remitirse adecuadamente.

19. Vulneraciones de la seguridad de los datos personales

Una vulneración de la seguridad de los datos personales puede incluir:

- la pérdida o el robo de un dispositivo;
- el envío de información a una persona equivocada;
- el acceso no autorizado;
- la divulgación accidental;
- la piratería informática;
- el phishing;
- el malware o el ransomware;
- el intercambio inadecuado de información;
- la pérdida de registros en papel;
- la eliminación accidental de información que no se pueda recuperar.

Cualquier sospecha de vulneración de datos personales debe notificarse inmediatamente mediante el Procedimiento de vulneración de datos del BSGC. El personal no debe retrasar la notificación por la incertidumbre sobre si un incidente constituye una vulneración. El delegado de protección de datos (DPO) proporcionará asesoramiento sobre la evaluación de riesgos y las obligaciones de notificación; sin embargo, la decisión final y la responsabilidad legal recaen en el BSGC como responsable del tratamiento. Cuando sea probable que la vulneración suponga un riesgo para los derechos y libertades de las personas, deberá notificarse a la autoridad de control sin demora injustificada y, siempre que sea posible, en un plazo de 72 horas desde que el BSGC tenga conocimiento de la misma. Cuando exista un riesgo elevado, también deberá comunicarse a los interesados afectados sin demora injustificada, salvo que se aplique una exención legal.

20. Fotografías, vídeos y grabaciones de audio

Las fotografías y las grabaciones de vídeo y audio que permitan identificar a personas constituyen datos personales. BSGC se asegurará de que la recogida y el uso de imágenes y grabaciones sean legales, proporcionados y transparentes. Se prestará especial atención a:

- las páginas web del colegio;
- las redes sociales;
- los materiales promocionales;
- las actuaciones;
- los eventos deportivos;
- las excursiones escolares;
- cámaras de videovigilancia;
- trabajos de los alumnos;
- grabaciones en las que participen menores.

Las directrices escolares vigentes también consideran que las fotografías y los vídeos de personas identificables son datos personales que requieren una base jurídica adecuada.

21. CCTV, Filtrado y Supervisión

Cuando el BSGC utilice sistemas de CCTV, supervisión de redes, filtrado de contenidos, gestión de dispositivos y otros sistemas de supervisión digital, estos se utilizarán de forma lícita, proporcionada y transparente. El centro educativo deberá:

- identificar la finalidad específica de la supervisión;
- restringir el acceso a los datos y registros de supervisión;

- en el caso de las cámaras de seguridad, eliminar las grabaciones en un plazo máximo de un mes desde su grabación, salvo que deban conservarse como prueba de incidentes de conformidad con la LOPDGDD;
- proporcionar la información adecuada sobre privacidad y, en el caso de las cámaras de seguridad, instalar señalización visible que garantice un fácil acceso a la información exigida en el artículo 13 del RGPD;
- formar al personal autorizado;
- realizar una EIPD cuando sea necesario;
- abstenerse de instalar cámaras en aseos, vestuarios o zonas de descanso del personal; la vigilancia en el interior de las aulas u otras zonas especialmente intrusivas solo se considerará con carácter excepcional, necesario y proporcionado.

La vigilancia no se implantará por el mero hecho de que la tecnología lo permita.

Cuando la vigilancia afecte al personal, también se respetarán estrictamente los derechos de privacidad en el lugar de trabajo y la obligación de notificación previa. La grabación de audio seguirá siendo estrictamente excepcional y solo se llevará a cabo cuando exista una justificación específica, necesaria y proporcionada.

22. Inteligencia Artificial

Las herramientas de IA pueden suponer riesgos significativos para los datos personales y los derechos fundamentales. Por consiguiente, el BSGC velará por el cumplimiento de los requisitos establecidos en su Política de Inteligencia Artificial y en el Procedimiento de uso y aprobación de la IA, llevará a cabo la evaluación previa de protección de datos correspondiente y evaluará las obligaciones derivadas del Reglamento (UE) 2024/1689 (Ley de IA de la UE) de acuerdo con su calendario de aplicación. El personal y los alumnos no deben introducir información personal, confidencial, relativa a la protección de menores u otra información sensible en herramientas de IA no autorizadas.

Cuando se utilice la IA para apoyar actividades educativas o administrativas, BSGC tendrá en cuenta:

- la necesidad;
- la precisión;
- la transparencia;
- la protección de datos;
- la protección de menores;
- el sesgo;
- la supervisión humana;
- la adecuación a la edad;
- la seguridad.

La IA no debe sustituir al criterio profesional adecuado en decisiones importantes relativas a los alumnos o al personal. No se tomará ninguna decisión basada exclusivamente en un tratamiento automatizado que produzca efectos jurídicos o que afecte de manera igualmente significativa a una persona, salvo que se aplique una excepción legal prevista en el artículo 22 del RGPD y se implementen las garantías necesarias, incluida una intervención humana significativa cuando sea apropiado.

23. Transferencias internacionales

El BSGC cumplirá los requisitos establecidos en los artículos 44 a 49 del RGPD cuando se transfieran datos personales fuera del Espacio Económico Europeo (EEE), incluido el acceso remoto desde un tercer país cuando dicho acceso constituya una transferencia. Antes de cualquier transferencia, se identificarán el país de destino, el importador de datos y cualquier subencargado del tratamiento, y se documentará el mecanismo de transferencia aplicable: una decisión de adecuación; las garantías

adecuadas con arreglo al artículo 46 —incluidas, cuando proceda, las cláusulas contractuales tipo (CCT) y una evaluación del impacto de la transferencia (EIT) acompañada de medidas complementarias—; o, con carácter excepcional, una excepción con arreglo al artículo 49. Se prestará especial atención a los servicios en la nube, la tecnología educativa (EdTech) y las plataformas de inteligencia artificial.

Cuando se aplique el RGPD del Reino Unido en virtud de su ámbito de aplicación territorial o de una actividad de tratamiento específica, el *BSGC* evaluará y documentará por separado los requisitos pertinentes del Reino Unido, sin perjuicio de sus obligaciones vigentes en virtud del RGPD de la UE.

24. Protección de datos y protección de menores

La protección de datos y la protección de menores están estrechamente relacionadas. El *BSGC* no utilizará los requisitos de protección de datos como motivo para impedir la adopción de medidas adecuadas de protección de menores cuando sea necesario compartir información para proteger a un menor u otra persona. Al mismo tiempo, la información relativa a la protección de menores debe tratarse con la confidencialidad y la seguridad adecuadas. El personal deberá solicitar asesoramiento al responsable designado de protección de menores (DSL) y al delegado de protección de datos (DPO) cuando exista alguna duda sobre el intercambio de información relativa a la protección de menores.

25. Formación y Sensibilización

BSGC impartirá la formación adecuada en materia de protección de datos al personal y a los voluntarios pertinentes. La formación deberá abarcar:

- principios básicos de protección de datos;
- confidencialidad;
- uso seguro de los sistemas;
- phishing y ciberseguridad;
- violaciones de la seguridad de los datos personales;
- derechos de los interesados;
- protección de la información;
- uso de fotografías y grabaciones;
- la inteligencia artificial y la tecnología educativa;
- la comunicación segura;
- los procedimientos de notificación.

La formación se impartirá durante la incorporación y se actualizará periódicamente, con formación adicional cuando las funciones o los riesgos lo requieran.

26. Funciones y Responsabilidades

Consejo Rector: el Consejo Rector se encarga de supervisar y garantizar que se apliquen las medidas adecuadas de protección de datos.

Director/a del centro: el/la director/a del centro tiene la responsabilidad operativa general de garantizar que el centro aplique esta política y mantenga una cultura eficaz de protección de datos.

Director/a de Operaciones: el director de operaciones colabora en la aplicación de las medidas de protección de datos en todas las funciones operativas del colegio y garantiza el cumplimiento de los procedimientos y controles pertinentes.

Delegado de Protección de Datos (DPO): el DPO se encargará de:

- asesorar al *BSGC* sobre las obligaciones en materia de protección de datos;
- supervisar el cumplimiento normativo;

- asesorar sobre las evaluaciones de impacto relativas a la protección de datos (DPIA);
- prestar apoyo en las auditorías de protección de datos;
- asesorar sobre las violaciones de datos;
- prestar apoyo en las solicitudes de acceso a la información;
- asesorar sobre políticas y procedimientos;
- actuar como punto de contacto adecuado con la autoridad de control cuando sea necesario.

El delegado de protección de datos (DPO) participará, de forma adecuada y oportuna, en todas las cuestiones relacionadas con la protección de datos personales, actuará con independencia y no recibirá instrucción alguna en relación con el ejercicio de sus funciones. El delegado de protección de datos (DPO) dispondrá de los recursos adecuados, tendrá acceso a las operaciones de tratamiento y podrá informar directamente al más alto nivel directivo; ninguna otra función que se le asigne dará lugar a un conflicto de intereses. Sus datos de contacto se publicarán y se comunicarán a la AEPD. El DPO informará y asesorará, supervisará el cumplimiento, prestará asesoramiento en relación con las evaluaciones de impacto relativas a la protección de datos (DPIA) y actuará como punto de contacto para la autoridad de control, sin asumir la responsabilidad corporativa que recae en el *BSGC*.

Consultores en protección de datos: el *BSGC* podrá contratar a una empresa externa para que preste apoyo especializado en materia de auditorías, gestión de violaciones de seguridad, evaluaciones de impacto relativas a la protección de datos (DPIA) y cuestiones relacionadas. Dicho apoyo no eximirá al *BSGC* de su responsabilidad en materia de cumplimiento. En caso de que el proveedor externo preste también servicios de delegado de protección de datos (DPO), se respetarán estrictamente los principios de independencia, ausencia de conflictos de intereses y obligaciones legales establecidos en los artículos 38 y 39 del RGPD. La realización efectiva de las evaluaciones de impacto relativas a la protección de datos (EIPD) o de las investigaciones por parte de los consultores no altera el hecho de que todas las decisiones y la responsabilidad jurídica recaen en el *BSGC*.

Responsable de TI: el responsable de TI se encarga de los controles técnicos adecuados, entre los que se incluyen:

- gestión de accesos;
- ciberseguridad;
- seguridad de los dispositivos;
- copias de seguridad;
- configuración del sistema;
- supervisión técnica;
- respuesta ante incidentes de seguridad.

Responsable designado de protección de menores (DSL): el DSL se encarga de garantizar que las consideraciones relativas a la protección de datos favorezcan, en lugar de obstaculizar, la protección efectiva de los menores.

Todo el personal: todo el personal es responsable de proteger la información personal y de seguir los procedimientos del *BSGC*; todas las personas que trabajan en un centro educativo tienen la responsabilidad de proteger los datos personales, no solo el delegado de protección de datos (DPO).

27. Incumplimiento

El incumplimiento de la presente Política puede dar lugar a:

- formación adicional;
- restricción del acceso a la información o a los sistemas;
- medidas por parte de la dirección;

- medidas disciplinarias, cuando proceda;
- remisión a los procedimientos de protección;
- notificación a las autoridades pertinentes, cuando sea necesario.

La respuesta del centro será proporcional a la naturaleza y gravedad del incidente. El uso indebido deliberado o imprudente de la información personal se tratará con especial severidad.

28. Seguimiento y revisión

El *BSGC* supervisará el cumplimiento mediante medidas adecuadas, entre las que se incluyen:

- la revisión de las solicitudes de acceso de los interesados y de otros derechos;
- la revisión de los proveedores externos;
- los registros de formación del personal;
- la revisión de los permisos de acceso;
- la revisión de las disposiciones de conservación;
- la revisión periódica del Registro de actividades de tratamiento.

El protocolo se revisará al menos una vez al año y con mayor frecuencia cuando se produzcan cambios significativos en la legislación, las directrices reglamentarias, la tecnología o las prácticas escolares.

Anexo 1 –Principios de protección de datos del *BSGC*: Guía rápida para el personal

La siguiente lista de control es una herramienta destinada a hacer que este importante protocolo resulte práctico y accesible para todo el personal.

Antes de utilizar datos personales, pregúntate:

1. ¿Los necesito?

Utiliza únicamente la información que sea necesaria.

2. ¿Puedo utilizarlos?

Asegúrate de que existe una base legal.

3. ¿Lo sabe la persona en cuestión?

Valora si el uso está contemplado en la política de privacidad del centro.

4. ¿Son correctos?

Comprueba la información importante.

5. ¿Quién necesita verlos?

Compártela únicamente con personas autorizadas que la necesiten.

6. ¿Está segura?

Utiliza sistemas homologados y protege los dispositivos, las contraseñas y los documentos.

7. ¿Cuánto tiempo debo conservarla?

No conserves información innecesariamente.

8. ¿Y si algo sale mal?

Notifícalo inmediatamente; no esperes a averiguar si se trata «realmente» de una violación de datos.