

The British School of Gran Canaria



Protección de Datos

Índice

1. Objetivo
2. Responsabilidades
3. Procedimiento A – Introducción de una nueva actividad de tratamiento de datos
4. Procedimiento B – Evaluación de impacto relativa a la protección de datos (EIPD)
5. Procedimiento C – Proveedor Externo
6. Procedimiento D – Intercambio de Datos
7. Procedimiento E – Solicitudes de Acceso de los Interesados y otros Derechos
8. Procedimiento F – Vulneración de la Seguridad de los Datos Personales
9. Registro de Vulneración de Datos
10. Procedimiento G – Conservación y Eliminación de Datos
11. Procedimiento H – Fotografías y Vídeos
12. Procedimiento I – Videovigilancia, Filtrado y Supervisión
13. Procedimiento J – Transferencias Internacionales
14. Procedimiento K – Protección de Datos desde el Diseño
15. Procedimiento L – Formación del Personal
16. Procedimiento M – Revisiones de Acceso
17. Procedimiento N – Permisos de Acceso
18. Procedimiento O – Dispositivos Personales
19. Procedimiento P – Auditoría Anual de Protección de Datos
20. Archivos y Registros de Protección de Datos
21. Matriz de Intervención
22. Evidencia y Garantía

1. Objetivo

Los presentes procedimientos proporcionan el marco operativo para la aplicación de la Política de Protección de Datos del *BSGC*. Establecen los procesos que deben seguirse cuando el centro:

1. recopila y utiliza datos personales;
2. introduce un nuevo sistema, tecnología o actividad de tratamiento;
3. contrata o cambia de proveedor externo;
4. comparte información personal;
5. recibe una solicitud de una persona para ejercer sus derechos;
6. sufra una violación de la seguridad de los datos personales;
7. conserve o elimine información;
8. transfiera información a nivel internacional;
9. utilice fotografías, cámaras de CCTV, sistemas de control u otros medios de vigilancia;
10. introduzca inteligencia artificial u otras tecnologías emergentes.

Los procedimientos están diseñados para garantizar que la protección de datos se incorpore a la toma de decisiones diaria del colegio, en lugar de tratarse únicamente como un mero ejercicio de cumplimiento normativo.

2. Responsabilidades

Cargo	Responsabilidad principal
Consejo Rector	Supervisión y garantía
Director	Ejecución general
Director Operativo	Supervisión y coordinación operativas
DPO	Asesoramiento independiente y supervisión del cumplimiento; orientación sobre evaluaciones de impacto relativas a la protección de datos (EIPD), derechos de los interesados y violaciones de la seguridad de los datos personales; punto de contacto con la AEPD. No asume la responsabilidad corporativa del <i>BSGC</i> .
Responsable TI	Seguridad técnica, controles de acceso e incidentes cibernéticos
DSL	Implicaciones en materia de protección de menores derivadas del tratamiento y el intercambio de información
Dirección /Coordinadores de departamento	Garantizar el cumplimiento normativo en sus departamentos
Todo el personal	Tratamiento seguro y adecuado de la información personal

El delegado de protección de datos (DPO) debe participar de forma adecuada y oportuna en todas las cuestiones relacionadas con la protección de datos, y debe gozar de la independencia, los recursos y la ausencia de conflictos de intereses que exige el RGPD. Las instituciones educativas que imparten enseñanza regulada por la legislación en materia de educación tienen la obligación legal de nombrar a un DPO. El DPO asesora y supervisa el cumplimiento normativo, y actúa como punto de contacto para los interesados y la AEPD; la toma de decisiones en materia de cumplimiento y la responsabilidad jurídica recaen exclusivamente en el *BSGC*, en su calidad de responsable del tratamiento.

3. Procedimiento A: Introducción de una nueva actividad de tratamiento de datos

Antes de que el BSGC introduzca un nuevo sistema, proceso o servicio que implique datos personales, el miembro del personal responsable deberá cumplimentar un formulario de evaluación de protección de datos. Esto se aplica, por ejemplo, a:

- nuevo software;
- plataformas educativas;
- aplicaciones;
- sistemas de inteligencia artificial;
- sistemas de vigilancia;
- videovigilancia;
- tecnología biométrica;
- formularios en línea;
- encuestas;
- nuevos sistemas de comunicación;
- servicios de terceros;
- nuevos métodos de recopilación de información sobre los alumnos.

El proponente debe determinar:

¿Qué?

¿Qué información se recopilará?

¿Por qué?

¿Cuál es la finalidad concreta?

¿Quién?

¿De quién se tratará la información?

¿Dónde?

¿Dónde se almacenará la información?

¿Quién la recibe?

¿Se compartirá la información con terceros?

¿Durante cuánto tiempo?

¿Durante cuánto tiempo se conservará?

¿A nivel internacional?

¿Saldrá la información del EEE?

¿Riesgo?

¿Podría el tratamiento suponer un riesgo significativo para las personas?

La evaluación preliminar debe documentar asimismo la base jurídica en función del artículo 6 del RGPD; la condición aplicable en virtud de los artículos 9 o 10, cuando proceda; la fuente de los datos; las obligaciones de transparencia; el impacto sobre los menores; la existencia de elaboración de perfiles o de toma de decisiones automatizada; la clasificación de terceros como responsables o encargados del tratamiento; las transferencias internacionales de datos; y los criterios de conservación de los datos. El tratamiento no debe iniciarse hasta que se hayan completado todas las revisiones y aprobaciones obligatorias.

Aprobación

La evaluación debe ser revisada por la combinación adecuada de:

- delegado de protección de datos (DPO);
- responsable de TI;
- delegado de seguridad de datos (DSL);
- director de operaciones;
- miembro pertinente del equipo directivo (SLT).

Cuando sea probable que el tratamiento suponga un riesgo elevado para los derechos y libertades de las personas, el *BSGC* deberá realizar una EIPD antes de iniciar el tratamiento y solicitar el asesoramiento del responsable de protección de datos (DPO). La EIPD se revisará siempre que se produzca un cambio en el riesgo que plantean las operaciones de tratamiento y se mantendrá como un documento vivo a lo largo de todo su ciclo de vida.

4. Procedimiento B – Evaluación de impacto relativa a la protección de datos (EIPD)

La obligación de llevar a cabo una EIPD recae sobre el *BSGC*, en su calidad de responsable del tratamiento. La preparación práctica puede contar con el apoyo de personal interno o externo, incluidos consultores, sin que ello suponga una transferencia de la responsabilidad. Se consultará al delegado de protección de datos sobre la necesidad, la metodología, las medidas y el resultado de la EIPD, y este supervisará su aplicación. Se debe prestar especial atención a la realización de una EIPD cuando el *BSGC* se proponga:

- seguimiento sistemático;
- tratamiento a gran escala de datos sensibles;
- elaboración de perfiles;
- uso significativo de la inteligencia artificial;
- nuevas tecnologías de vigilancia;
- tratamiento extensivo de datos de menores;
- nuevas tecnologías que plantean riesgos significativos para la privacidad.

Proceso EIPD

1. Describe el tratamiento

- ¿Qué información?
- ¿Quién?
- ¿Por qué?
- ¿Cómo?
- ¿Dónde?

2. Determinar la necesidad y la proporcionalidad

- ¿Es necesario el tratamiento?
- ¿Existe alguna alternativa menos intrusiva?
- ¿Es proporcionada la cantidad de datos?

3. Identificar riesgos

Considerar los riesgos para:

- la privacidad;
- la confidencialidad;
- la seguridad;
- la dignidad;
- la reputación;
- la igualdad;
- los derechos de los menores;
- los intereses económicos;
- la autonomía.

4. Identificar medidas de control

Ejemplos:

- restricciones de acceso;

- cifrado;
- seudonimización;
- minimización;
- límites de conservación;
- formación del personal;
- información para padres y alumnos;
- medidas de control técnicas.

5. Determinar el riesgo residual

El responsable de protección de datos (DPO) asesora sobre el riesgo residual y sobre la idoneidad de las medidas propuestas. La decisión de aceptar el riesgo y seguir adelante o no recae en BSGC, que debe documentar sus motivos y proporcionar una justificación formal para cualquier decisión que se aparte del asesoramiento del DPO.

6. Aprobar o rechazar

No se iniciará ninguna actividad de tratamiento de alto riesgo hasta que se hayan completado la evaluación y las autorizaciones necesarias. Si la EIPD indica que persistiría un alto riesgo en ausencia de medidas de mitigación suficientes, el BSGC consultará a la AEPD antes de iniciar el tratamiento, de conformidad con el artículo 36 del RGPD.

5. Procedimiento C – Proveedor Externo

Antes de que el BSGC designe a un proveedor encargado del tratamiento de datos personales, el centro debe llevar a cabo una evaluación de protección de datos y una verificación de diligencia debida del proveedor.

Esto se aplica especialmente a:

- plataformas de aprendizaje;
- sistemas de protección;
- sistemas de recursos humanos;
- nóminas;
- transporte;
- restauración;
- servicios médicos;
- almacenamiento en la nube;
- proveedores de inteligencia artificial;
- aplicaciones educativas.

El centro educativo debe establecer:

- qué datos se tratan;
- por qué se tratan;
- dónde se tratan;
- las medidas de seguridad;
- el plazo de conservación;
- las medidas de supresión;
- los subencargados del tratamiento;
- las transferencias internacionales;
- si los datos se utilizan con fines publicitarios o de elaboración de perfiles;
- si el proveedor utiliza la información para entrenar modelos de inteligencia artificial.

Cuando un proveedor tenga la intención de utilizar los datos del *BSGC* para sus propios fines, con fines publicitarios, de elaboración de perfiles o para el entrenamiento de modelos de inteligencia artificial, su función jurídica y su base legal deberán evaluarse y documentarse por separado. Dicho uso no estará autorizado de forma predeterminada.

Cuando un proveedor actúe como encargado del tratamiento, deberá ofrecer garantías suficientes, y la relación deberá formalizarse, antes de cualquier acceso a los datos, mediante un contrato u otro acto jurídico vinculante, de conformidad con el artículo 28 del RGPD. El contrato deberá abarcar, entre otros requisitos, las instrucciones documentadas, la confidencialidad, las medidas de seguridad, la asistencia en materia de derechos de los interesados y notificaciones de violaciones, la autorización y supervisión de los subencargados del tratamiento, las transferencias internacionales de datos, la devolución o supresión de datos, y los derechos de auditoría e información del *BSGC*.

Autorización de proveedores

Ningún departamento podrá adquirir ni poner en marcha, por iniciativa propia, ningún servicio digital que trate datos personales relativos a alumnos o personal.

Adquisición → Revisión de TI y seguridad → Revisión de la protección de datos (con el asesoramiento del delegado de protección de datos) → Revisión del contrato → Aprobación por parte de la autoridad designada.

6. Procedimiento D – Intercambio de datos

Antes de compartir datos personales fuera del *BSGC*, el personal debe preguntarse:

1. ¿Es necesario compartir los datos?
2. ¿Quién los recibe?
3. ¿Cuál es la base legal?
4. ¿Cuál es la información mínima necesaria?
5. ¿Está autorizado el destinatario?
6. ¿Existe un acuerdo adecuado?
7. ¿Se encuentra el destinatario fuera del EEE?
8. ¿Incluye la información datos sensibles o de protección?
9. ¿Se ha informado debidamente a la persona afectada?
10. ¿Se ha registrado el intercambio cuando procede?

El personal nunca debe enviar una base de datos o un archivo completo simplemente porque resulte más cómodo, si solo se requiere una pequeña cantidad de información.

7. Procedimiento E –Solicitudes de acceso de los interesados y otros derechos

Las solicitudes relativas a los datos personales de una persona deben remitirse inmediatamente al canal interno designado y al delegado de protección de datos (DPO) para que este preste asesoramiento. El *BSGC*, en su calidad de responsable del tratamiento, se encarga de dar respuesta a dichas solicitudes y de cumplir los plazos legales. Esto incluye solicitudes del tipo: “Quiero ver toda la información que tienen de mi hijo”.

El personal no debe:

- decidir por su cuenta que la solicitud no es válida;
- eliminar información;
- modificar registros;
- realizar búsquedas selectivas;
- divulgar información directamente sin recibir instrucciones.

Procedimiento de gestión de derechos: el *BSGC* (con el asesoramiento del delegado de protección de datos)

1. Recibir y registrar la solicitud.
2. Verificar la identidad cuando proceda.
3. Determinar el alcance.
4. Identificar los sistemas y registros pertinentes.
5. Coordinar las búsquedas.
6. Identificar la información de terceros.
7. Aplicar las exenciones o restricciones pertinentes.
8. Revisar la información.
9. Preparar la respuesta.
10. Responder sin demora injustificada y, en cualquier caso, en el plazo de un mes desde la recepción de la solicitud. Dicho plazo podrá prorrogarse por dos meses más cuando sea necesario, teniendo en cuenta la complejidad y el número de solicitudes, informando al interesado de dicha prórroga en el plazo de un mes desde la recepción, junto con los motivos del retraso.
11. Finalizar el registro.

El centro educativo deberá llevar un registro de los derechos de los interesados. Las respuestas y comunicaciones relacionadas con el ejercicio de dichos derechos se facilitarán de forma gratuita, salvo en las circunstancias excepcionales de solicitudes manifiestamente infundadas o excesivas previstas en el RGPD. Cualquier verificación de identidad deberá ser proporcionada a la información solicitada y a los riesgos que ello conlleva.

8. Procedimiento F – Vulneración de la Seguridad de los Datos Personales

Se entiende por vulneración de la seguridad de los datos personales cualquier incidente de seguridad que dé lugar a la destrucción, pérdida, alteración, divulgación no autorizada o acceso no autorizado a datos personales, ya sea de forma accidental o ilícita. Puede incluir, entre otros incidentes:

- destrucción;
- pérdida;
- alteración;
- divulgación;
- acceso a información personal.

La pérdida de dispositivos, el envío de correos electrónicos a destinatarios equivocados, el acceso no autorizado a bases de datos, la eliminación accidental y los ataques de phishing pueden constituir violaciones de datos personales. Norma para el personal: en caso de duda, notifíquelo inmediatamente.

En caso de duda, comunícalo.

El personal debe comunicar inmediatamente cualquier sospecha de infracción al punto de notificación interno designado.

Ejemplos:

- correo electrónico enviado al padre o madre equivocado;
- información de un alumno adjunta a un correo electrónico equivocado;
- pérdida de un ordenador portátil;
- robo de un teléfono que contiene información del centro;
- envío incorrecto de un documento sobre protección de menores;
- acceso no autorizado a la base de datos de alumnos;

- ataque de phishing;
- ransomware (secuestro de datos);
- subida de información confidencial a una herramienta de IA no autorizada.

8.1 Respuesta inmediata

La persona que reciba la denuncia debe:

1. Contener la situación - impedir, en la medida de lo posible, que se siga divulgando la información o se acceda a ella.
2. Conserva las pruebas: no borres los correos electrónicos, archivos o registros relevantes.
3. Notificar - Informar:
 - DPO/DPD (Responsable de Protección de Datos /Delegado de Protección de Datos);
 - Responsable de TI, cuando se trate de cuestiones técnicas;
 - DSL, cuando se trate de la protección de menores;
 - Director de Operaciones/Equipo Directivo (SLT), cuando sea relevante.
4. Evaluar - Determinar:
 - qué ha ocurrido;
 - qué datos se han visto afectados;
 - cuántas personas;
 - quiénes se han visto afectadas;
 - si se han visto implicados menores o personas vulnerables;
 - la probabilidad de que se produzca un perjuicio;
 - la gravedad del posible perjuicio.
5. Decidir: BSGC, en su calidad de responsable del tratamiento, decide y documenta si debe notificar a la autoridad de control y/o comunicar la violación de datos a las personas afectadas, teniendo en cuenta la evaluación de riesgos y el asesoramiento del delegado de protección de datos.

La vulneración de datos deberá notificarse a la autoridad de control sin demora injustificada y, cuando sea posible, a más tardar 72 horas después de que el BSGC haya tenido conocimiento de la misma, salvo que sea improbable que dicha vulneración de datos suponga un riesgo para los derechos y libertades de las personas físicas. Cuando sea probable que la vulneración de datos suponga un riesgo elevado, el BSGC deberá comunicar también la vulneración a los interesados afectados sin demora injustificada, salvo que se aplique una exención legal. Cuando la notificación a la autoridad no se realice en un plazo de 72 horas, deberá ir acompañada de los motivos del retraso.

9. Registro de Vulneraciones de Datos

El BSGC asumirá la responsabilidad última de investigar y documentar todas las vulneraciones de datos personales. Los consultores en protección de datos podrán prestar apoyo durante la investigación, y el delegado de protección de datos (DPO) asesorará y supervisará el proceso desde su función independiente. El registro central deberá recoger:

- fecha y hora;
- persona que lo notifica;
- descripción;
- sistemas afectados;
- datos afectados;

- personas afectadas;
- causa;
- medidas de contención;
- evaluación de riesgos;
- impacto real o previsto sobre las personas afectadas;
- decisión relativa a la notificación;
- medidas adoptadas;
- lecciones aprendidas;
- medidas preventivas.

Es importante destacar que deben registrarse todas las vulneraciones, incluidas aquellas que, tras una evaluación, se considere que no requieren notificación. La AEPD considera que el mantenimiento de un registro de las vulneraciones y de las decisiones adoptadas forma parte del requisito de rendición de cuentas.

10. Procedimiento G –Conservación y Eliminación de Datos

Cada categoría principal de datos personales debe estar sujeta a un plazo de conservación específico o a criterios de cálculo objetivos, basados en las obligaciones legales, las necesidades educativas u operativas documentadas y el principio de limitación del almacenamiento.

Algunos ejemplos son:

- expedientes de los alumnos;
- expedientes de protección de menores;
- asistencia;
- información sobre evaluaciones;
- expedientes de selección de personal;
- expedientes de personal;
- expedientes financieros;
- imágenes de videovigilancia;
- correo electrónico;
- registros de control de acceso.

El centro educativo deberá mantener un calendario de conservación de datos aprobado y actualizado que identifique el tipo de registro, el responsable interno del mismo, el hecho desencadenante o el plazo para calcular el período de conservación, la justificación subyacente o los criterios de conservación, y el método de eliminación. Las expresiones genéricas, como “período definido”, deben sustituirse en el calendario operativo por plazos específicos o criterios cuantificables.

Registro	Titular	Plazo de conservación	Método de eliminación
Expedientes académicos de los alumnos	Académico	El colegio deberá mantener un calendario de conservación de datos aprobado y actualizado en el que se identifique el tipo de registro, el responsable interno del mismo, el hecho desencadenante o el plazo para calcular el período de conservación, la justificación subyacente o los criterios de conservación, y el método de eliminación. Las expresiones genéricas, como “período	Eliminación o archivo seguro

Registro	Titular	Plazo de conservación	Método de eliminación
		definido”, deben sustituirse en el calendario operativo por plazos específicos o criterios cuantificables.	
Protección de menores	DSL	De conformidad con la legislación aplicable en materia de protección y seguridad infantil y con el anexo aprobado	Eliminación segura
Personal	Recursos Humanos	De conformidad con la legislación aplicable en materia de protección y seguridad infantil y con el anexo aprobado	Borrado seguro
CCTV (Circuito Cerrado de Televisión)	TI/Operaciones	Un mes como máximo desde su recogida, salvo que se conserven como prueba de incidentes de conformidad con el artículo 22.3 de la LOPDGDD.	Borrado automático
Selección de Personal	Recursos Humanos	De conformidad con la legislación laboral aplicable y el calendario de conservación de datos aprobado	Borrado seguro

Eliminación

Papel → trituración confidencial.

Datos digitales → eliminación segura.

Dispositivos → borrado seguro antes de su eliminación o reasignación.

11. Procedimiento H – Fotografías y vídeos

Antes de tomar o publicar fotografías o vídeos en los que se pueda identificar a personas, el personal deberá determinar:

- la finalidad;
- el público destinatario;
- el lugar de publicación;
- la base jurídica aplicable;
- si se requiere un consentimiento específico;
- las restricciones pertinentes;
- las condiciones de conservación.

Se debe prestar especial atención a:

- páginas web;
- redes sociales;
- materiales promocionales;
- logros de los alumnos;
- excursiones;
- actuaciones;
- eventos deportivos.

Las fotografías y los vídeos en los que aparezcan personas identificables constituyen datos personales. El personal no debe:

- utilizar cuentas personales en redes sociales para publicaciones del centro;

- subir fotografías de alumnos a plataformas no autorizadas;
- publicar información sobre los alumnos sin la autorización correspondiente;
- dar por sentado que un permiso general de los padres cubre todos los usos posibles.

Cuando el consentimiento constituya la base legal para un uso opcional de las imágenes, se deberán registrar formalmente su alcance, los canales de publicación y la fecha; su retirada deberá ser sencilla y se deberán respetar estrictamente las restricciones comunicadas. La denegación o la retirada del consentimiento no perjudicará la prestación de la enseñanza cuando el uso de la imagen no sea necesario para dicha prestación.

12. Procedimiento I – Videovigilancia, Filtrado y Supervisión

Antes de implantar tecnología de supervisión, el *BSGC* deberá establecer:

- la finalidad;
- la necesidad;
- la proporcionalidad;
- la base jurídica;
- los derechos de acceso;
- el plazo de conservación;
- la información sobre privacidad;
- la seguridad;
- las disposiciones de revisión.

Cuando la supervisión plantee riesgos significativos para la privacidad, se deberá considerar la realización de una EIPD.

Solo el personal autorizado con una necesidad legítima debe tener acceso a la información de vigilancia.

En el caso de la videovigilancia de seguridad, las grabaciones se borrarán en un plazo máximo de un mes desde su captura, salvo que sea necesario conservarlas para acreditar incidentes de conformidad con la LOPDGDD. Se colocarán carteles visibles y se facilitará el acceso a la información de primer nivel prescrita en el artículo 13 del RGPD. No se instalarán cámaras en aseos, vestuarios ni zonas de descanso del personal; la vigilancia en las aulas solo se contemplará en circunstancias excepcionales y estrictamente proporcionadas. Cuando se vea afectado el personal, se respetará la obligación de notificación previa prevista en el artículo 89 de la LOPDGDD. La grabación de audio seguirá siendo estrictamente excepcional y requerirá una justificación específica y proporcionada.

13. Procedimiento J –Transferencias Internacionales

Antes de contratar a cualquier proveedor que pueda transferir datos personales fuera del EEE o permitir el acceso remoto desde un tercer país, cuando ello constituya una transferencia internacional, el *BSGC* deberá identificar el destino;

1. identificará al proveedor y a los subencargados del tratamiento;
2. establecerá el mecanismo de transferencia;
3. evaluará las garantías aplicables;
4. considerará medidas complementarias cuando sea necesario;
5. documentará la decisión;
6. solicitará el asesoramiento del delegado de protección de datos (DPO) o del responsable de protección de datos (DPD), cuando proceda.

El mecanismo deberá basarse, según proceda, en una decisión de adecuación con arreglo al artículo 45 del RGPD, en las garantías adecuadas previstas en el artículo 46 —incluidas las cláusulas contractuales tipo y, cuando sea necesario, una evaluación de impacto de la transferencia y medidas complementarias— o, con carácter excepcional, en una excepción prevista en el artículo 49. La decisión y su revisión periódica deberán quedar plenamente documentadas. Esto reviste especial importancia para:

- las plataformas en la nube;
- los servicios de inteligencia artificial;
- los proveedores de tecnología con sede en EE. UU.;
- las plataformas de aprendizaje en línea;
- los servicios de comunicaciones.

14. Procedimiento K – Protección de Datos desde el Diseño

La protección de datos debe tenerse en cuenta antes, y no después, de la implantación de un nuevo sistema o proceso. En todo nuevo proyecto de envergadura se debe plantear la siguiente pregunta: «¿Podemos alcanzar el mismo objetivo educativo u operativo recopilando o divulgando menos datos personales?». El responsable del proyecto debe tener en cuenta:

- la minimización;
- el acceso;
- la conservación;
- la seguridad;
- la transparencia;
- los derechos de los alumnos;
- la protección;
- el acceso de terceros.

15. Procedimiento L – Formación del Personal

Personal nuevo: la formación en protección de datos debe formar parte del programa de incorporación.

Personal actual: la formación de actualización anual debe abarcar:

- los principios del RGPD;
- la confidencialidad;
- el phishing;
- las violaciones de datos;
- el correo electrónico seguro;
- la información de los alumnos;
- la protección de datos;
- las fotografías;
- la inteligencia artificial;
- los dispositivos personales;
- el intercambio de datos.

Formación específica: se debe impartir formación adicional cuando:

- un departamento maneje información especialmente sensible;
- se introduzca un nuevo sistema;
- un incidente ponga de manifiesto una deficiencia en la formación;
- confidencialidad;

16. Procedimiento M – Revisiones de Acceso

Nuevos empleados: la formación en protección de datos formará parte integrante del proceso de incorporación.

Personal actual: formación de actualización anual que aborde lo siguiente:

- ¿Sigue necesitando esta persona acceso?
- ¿Es adecuado el nivel de acceso?
- ¿Ha cambiado de puesto el empleado?
- ¿El empleado ha dejado la empresa?
- ¿Se están utilizando cuentas compartidas?
- ¿Están justificados los privilegios de administrador?

Empleados que abandonan la empresa: el acceso debe retirarse sin demora cuando finalice la relación laboral o el acceso autorizado.

Cambios de puesto: el acceso debe ajustarse cuando el personal cambie de puesto.

17. Procedimiento N – Permisos de Acceso

El responsable de TI, en colaboración con los propietarios de los sistemas correspondientes, revisará los permisos de acceso al menos una vez al año y siempre que se produzcan incorporaciones, bajas o cambios de funciones. Las cuentas con privilegios o administrativas se revisarán con una frecuencia proporcional al riesgo. La revisión deberá abarcar:

- la descarga de listas de alumnos;
- fotografías;
- expedientes de protección de menores;
- información de RR. HH.;
- información sobre exámenes;
- correspondencia confidencial.

18. Procedimiento O – Dispositivos Personales

Cuando se permita al personal utilizar dispositivos personales con fines escolares, el dispositivo deberá cumplir los requisitos de seguridad digital pertinentes de BSGC, incluyendo un bloqueo de pantalla robusto, cifrado cuando proceda, parches de seguridad actualizados y controles de acceso adecuados. El personal no deberá almacenar información escolar sensible de forma local a menos que se autorice expresamente, y deberá informar de inmediato de la pérdida, el robo o la sospecha de compromiso de cualquier dispositivo. Siempre que sea técnicamente viable, la BSGC aplicará medidas para la gestión, la contenerización o separación, o el borrado remoto de los datos corporativos.

Se debe prestar especial atención a:

- la descarga de listas de alumnos;
- las fotografías;
- los registros de protección de menores;
- la información de RR. HH. o de personal;
- los materiales de examen;
- la correspondencia confidencial

19. Procedimiento P - Auditoría Anual de Protección de Datos

El responsable de protección de datos (RPD) coordinará la revisión operativa anual y participará de forma independiente para asesorar sobre el alcance de la misma y supervisar el cumplimiento, con la facultad de presentar recomendaciones directamente al equipo directivo superior (SLT) y al Consejo Rector. La revisión abarcará:

Consejo Rector

- ¿Está actualizado el protocolo?
- ¿Son adecuadas las medidas relativas al RPD?
- ¿Se mantienen adecuadamente los registros y los archivos?

Sistemas

- ¿Están todos los sistemas debidamente inventariados?
- ¿Son adecuados los controles de acceso?
- ¿Se revisan los proveedores externos?

Datos

- ¿Se respeta el principio de minimización de datos?
- ¿Se respetan los plazos de conservación?
- ¿Se eliminan de forma segura los registros obsoletos?

Personal

- ¿Ha completado el personal la formación obligatoria?
- ¿Se comprenden claramente las funciones y responsabilidades?

Incidentes

- ¿Cuántas violaciones de datos personales se produjeron?
- ¿Cuáles fueron las causas fundamentales?
- ¿Qué medidas correctivas y reparadoras se aplicaron?

Derechos

- ¿Cuántas solicitudes de los interesados se recibieron?
- ¿Se cumplieron los plazos legales de respuesta?
- ¿Existen tendencias o problemas recurrentes?

AEPD

- ¿Se han requerido o llevado a cabo nuevas AEPD?
- ¿Se han revisado y actualizado las AEPD existentes?

Proveedores

- ¿Están todos los contratos y los acuerdos de tratamiento de datos (DPA) actualmente en vigor?
- ¿Cumplen los encargados del tratamiento sus obligaciones?
- ¿Se han verificado las transferencias internacionales de datos?

20. Archivos y Registros de Protección de Datos

El BSGC mantendrá seis registros centrales:

1. **Registro de actividades de tratamiento (RoPA)**
Qué datos personales trata el colegio y por qué motivos.
2. **Registro de violaciones de datos personales**
Qué falló y cómo se resolvió.
3. **Registro de derechos de los interesados**
Solicitudes recibidas y respuestas formales facilitadas.
4. **Registro de evaluaciones de impacto relativas a la protección de datos (DPIA)**
Evaluaciones de riesgo realizadas para operaciones de tratamiento de datos significativas.
5. **Registro de encargados del tratamiento externos**

Quién trata los datos de BSGC y en virtud de qué acuerdos contractuales.

6. Calendario y registro de conservación de datos

Qué información se conserva y durante cuánto tiempo.

21. Matriz de Intervención

Incidencia	Primer Punto de Contacto	Responsable
Consulta rutinaria sobre protección de datos	Delegado de Protección de Datos	Director de Operaciones
Fuga de datos personales	DPO + TI	Equipo Directivo (SLT)
Incidente relacionado con la protección de datos de salvaguarda	DSL	DPO + Director del centro
Ciberataque	Responsable de TI	DPO + SLT
Data Subject Access Request (DSAR)	DPO	Director de Operaciones
Nueva tecnología educativa (EdTech)	TI + DPO	SLT
Nueva herramienta de IA	Responsable de IA + DPO	SLT
Nuevo proveedor	Operaciones / Adquisiciones	DPO
Transferencia internacional de datos	DPO	SLT
Tratamiento de datos de alto riesgo	DPO	SLT / Consulta a las autoridades reguladoras cuando sea necesario

22. Evidencia y Garantía

Informe de garantía de protección de datos

El responsable de protección de datos (DPO) deberá presentar al equipo directivo (SLT) y al Consejo Rector un informe de garantía independiente y conciso que incluya:

- índices de cumplimiento de la formación;
- volumen y desglose de las violaciones de datos personales;
- incidentes significativos;
- solicitudes relacionadas con los derechos de los interesados (DSAR y otras);
- evaluaciones de impacto relativas a la protección de datos (DPIA) finalizadas;
- sistemas recién aprobados;
- revisiones de proveedores externos;
- transferencias internacionales de datos;
- cumplimiento de los plazos de conservación;
- revisiones del control de acceso;
- medidas pendientes;
- riesgos identificados;
- prioridades estratégicas recomendadas para el año siguiente.