Versión: Final
Fecha de aprobación: Sept 2026
Fecha de revisión: Nov 2027

The British School of Gran Canaria
Protocolo sobre las Expectativas Digitales del Personal

Índice

1. Fundamentos
2. Ámbito de aplicación
3. Principios
4. Conducta digital profesional
5. Salvaguarda y seguridad online
6. Comunicación con los alumnos
7. Dispositivos Personales
8. Dispositivos del Colegio
9. Filtrado y Supervisión
10. Prácticas Digitales en el Aula
11. Dispositivos del Colegio para los Alumnos
12. Dispositivos Personales de los Alumnos de KS5 (Bachillerato)
13. Contraseñas y Seguridad de las Cuentas
14. Protección de Datos y Confidencialidad
15. Correo Electrónico y Comunicación Digital
16. Redes Sociales
17. Inteligencia Artificial
18. Enseñanza y Reuniones Online
19. Ciberseguridad
20. Uso de Soportes Extraíbles
21. Imágenes y Grabaciones Artificiales o Alteradas
22. Accesibilidad e Inclusión
23. Notificación de Incidencias
24. Supervisión y Garantía
25. Formación del Personal
26. Incumplimientos del Protocolo
27. Declaración del personal

1. Fundamentos

The British School of Gran Canaria reconoce que la tecnología digital es una parte esencial de la educación moderna y ofrece importantes oportunidades para mejorar la enseñanza, el aprendizaje, la comunicación y el desarrollo de los alumnos.

Sin embargo, la tecnología también plantea riesgos para los alumnos, el personal y el colegio. Entre ellos se incluyen los contenidos inapropiados en Internet, el ciberacoso, las comunicaciones inapropiadas, las filtraciones de datos, el uso indebido de la inteligencia artificial, el uso excesivo de pantallas, los ciberataques y los intentos de eludir los sistemas de protección y seguridad del colegio.

El objetivo de este protocolo es establecer unas expectativas claras para todo el personal, de modo que la tecnología digital se utilice:

- de forma segura;
- de forma profesional;
- de forma responsable;
- de forma ética;
- de forma adecuada;
- en apoyo de una enseñanza y un aprendizaje de alta calidad; y
- de manera que se proteja a los alumnos y al personal.

El colegio espera que todo el personal comprenda que la protección en línea forma parte de la protección general y que la responsabilidad de proteger a los alumnos de los daños en línea recae en todos.

Este protocolo debe leerse junto con los protocolos y procedimientos del *BSGC* en materia de salvaguarda, protección de datos, empleo y otros aspectos relevantes.

2. Ámbito de Aplicación

Este protocolo se aplica a todos los empleados y adultos que trabajen en nombre del *BSGC*, incluidos:

- el personal docente;
- el personal administrativo y de apoyo;
- el personal interino y temporal;
- los voluntarios;
- los miembros del Consejo Rector cuando actúen en nombre del colegio;
- los trabajadores por cuenta ajena y otros adultos a los que se les haya concedido acceso a los sistemas del colegio.

Estas expectativas se aplican siempre que el personal:

- utilice dispositivos del centro;
- acceda a los sistemas del centro;
- utilice la red del centro;
- se comunique con los alumnos o las familias por vía electrónica;
- imparte clases o supervise a los alumnos en línea; o
- utilice dispositivos personales en el marco de su función profesional.

Cuando un trabajador por cuenta ajena o un tercero tenga acceso a los sistemas del *BSGC*, el centro podrá exigir el cumplimiento de requisitos equivalentes en materia de seguridad digital y protección de menores a través de los acuerdos contractuales pertinentes.

3. Principios

El enfoque del *BSGC* respecto a la tecnología digital se basa en los siguientes principios:
Salvaguarda: la tecnología digital debe respaldar, y nunca socavar, la seguridad y el bienestar de los alumnos.
Profesionalidad: se espera que el personal mantenga en el ámbito digital unos estándares profesionales equivalentes a los que se esperan en el ámbito presencial.
Proporcionalidad: los controles y la supervisión digitales serán adecuados a los fines legítimos de protección, seguridad, educativos y operativos para los que se implementen.
Privacidad: el centro reconoce el derecho a la privacidad de los miembros del personal y no intentará supervisar ni acceder a información personal de forma innecesaria.
Responsabilidad: el personal sigue siendo personalmente responsable de su conducta digital profesional y de comunicar cualquier preocupación.
Seguridad: el personal debe proteger la información, los sistemas, los dispositivos y las cuentas del centro frente al acceso no autorizado.
Mejora continua: los riesgos digitales evolucionan rápidamente y el centro revisará periódicamente sus controles, procedimientos y formación.

4. Conducta Digital Profesional

Se espera que el personal mantenga en Internet los mismos altos estándares de conducta profesional que mantendría en persona.
El personal debe:

- utilizar un lenguaje adecuado y profesional;
- mantener los límites profesionales adecuados;
- tener en cuenta cómo pueden percibir su actividad en Internet los alumnos, los padres, los compañeros y la comunidad en general;
- proteger la reputación del *BSGC*;
- evitar cualquier actividad online que pueda socavar razonablemente la confianza en su función profesional;
- cumplir el Código de Conducta del Personal al utilizar la tecnología digital.

El personal debe partir de la base de que la comunicación digital puede ser conservada, reenviada, copiada o hecha pública, incluso cuando considere que es privada.

Nada de lo dispuesto en este protocolo tiene por objeto regular innecesariamente las actividades privadas lícitas. No obstante, el personal debe reconocer que la actividad pública online puede tener consecuencias profesionales cuando afecte a los límites profesionales, la protección de menores, la confidencialidad o la reputación del colegio. El personal también debe ser consciente de que existen leyes claras y estrictas que regulan y orientan la práctica y el comportamiento en este ámbito, y que la comunidad escolar está sujeta a estas normas.

5. Salvaguarda y Seguridad Online

La protección de los menores es responsabilidad de todos.

El personal debe permanecer alerta ante cualquier problema relacionado con la protección de los menores en Internet, entre los que se incluyen:

- el ciberacoso;
- el abuso o la explotación sexual online;
- la comunicación sexualizada inapropiada;
- el material nocivo o extremista;
- los contenidos relacionados con las autolesiones o el suicidio;
- la radicalización online;
- la captación de menores con fines sexuales;

- el uso inadecuado de las redes sociales;
- el intercambio de imágenes;
- el acoso online;
- las amenazas o la intimidación;
- los contenidos nocivos generados o manipulados por inteligencia artificial.

Cualquier preocupación relacionada con la seguridad online de un alumno debe comunicarse inmediatamente a través de los procedimientos de salvaguarda del colegio.

El personal no debe investigar por su cuenta las preocupaciones relacionadas con la salvaguarda ni intentar determinar si una preocupación es real antes de comunicarla.

El personal nunca debe prometer a un alumno que la información que este comparta con ellos se mantendrá confidencial.

Deben respetarse las medidas de protección del centro, incluidos los protocolos de protección pertinentes del *BSGC* y las responsabilidades del responsable designado de salvaguarda y del coordinador de bienestar y protección.

El *BSGC* impartirá la formación adecuada para que el personal comprenda sus responsabilidades en materia de seguridad digital y de prevención, identificación y denuncia de daños online. Esto se ajusta al marco legal español, que exige a los centros educativos disponer de medidas de protección adecuadas y de formación en seguridad digital.

6. Comunicación con los Alumnos

El personal debe mantener unos límites profesionales adecuados al comunicarse con los alumnos.
Para la comunicación profesional deben utilizarse las plataformas y los sistemas de comunicación aprobados por el centro.

El personal no debe:

- comunicarse con los alumnos a través de cuentas personales en redes sociales;
- utilizar aplicaciones de mensajería personal para la comunicación habitual con los alumnos;
- intercambiar números de teléfono personales con los alumnos, salvo que se autorice expresamente;
- comunicarse con los alumnos a través de servicios privados o de mensajes que se borran automáticamente;
- comunicarse con los alumnos utilizando cuentas de correo electrónico personales;
- crear grupos privados online con los alumnos, salvo que se autorice expresamente con fines educativos.

Cuando sea necesaria la comunicación electrónica con los alumnos, el personal deberá utilizar las plataformas aprobadas por el centro y, cuando proceda, asegurarse de que la comunicación sea visible o accesible para otros miembros del personal.

7. Dispositivos Personales

No se deben utilizar teléfonos móviles personales, ordenadores portátiles, tabletas ni otros dispositivos personales de forma que se ponga en peligro la seguridad de los alumnos, la confidencialidad, la protección de datos o la conducta profesional.

El personal no debe utilizar dispositivos personales para:

- fotografiar o grabar a los alumnos;

- almacenar información sobre los alumnos;
- descargar o conservar documentos escolares confidenciales;
- comunicarse en privado con los alumnos;
- acceder a información sobre la protección de los alumnos o almacenarla;
- grabar reuniones o conversaciones sin la autorización correspondiente.

Cuando sea necesario tomar fotografías o grabar vídeos de los alumnos con fines escolares legítimos, se deberá utilizar el equipo y los procedimientos aprobados por el centro.

No se deben utilizar dispositivos personales durante las clases o las tareas de supervisión, salvo que exista una razón profesional clara o una situación de emergencia.

Privacidad de los dispositivos personales
El centro no supervisa de forma rutinaria los contenidos privados de los dispositivos propiedad del personal.

Cuando se utilice un dispositivo personal para acceder a los sistemas del *BSGC*, el personal seguirá siendo responsable de cumplir con los requisitos de seguridad y protección de datos del centro.

El centro podrá aplicar los controles técnicos de seguridad adecuados al acceso a los sistemas del *BSGC* cuando sea necesario para proteger a los alumnos, los datos personales o la información del centro.

8. Dispositivos del Colegio

Los dispositivos del centro se facilitan principalmente con fines profesionales.
El personal debe:

- mantener los dispositivos seguros;
- utilizar contraseñas seguras;
- bloquear los dispositivos cuando estén desatendidos;
- notificar inmediatamente cualquier pérdida o robo;
- instalar únicamente software autorizado;
- no desactivar el software de seguridad o protección;
- no modificar la configuración del cortafuegos, los filtros o la gestión de dispositivos;
- aplicar las actualizaciones de seguridad cuando sea necesario;
- evitar dejar los dispositivos desatendidos en zonas públicas;
- devolver el equipo cuando se le solicite.

El personal no debe intentar eludir los controles de seguridad del centro.
Esto incluye los intentos de utilizar:

- VPN;
- servicios proxy;
- navegadores no autorizados;
- servicios DNS alternativos;
- aplicaciones no autorizadas;
- dispositivos de almacenamiento externos;
- puntos de acceso personales o redes alternativas;

cuando el objetivo sea eludir los controles de seguridad, filtrado o protección del centro.

9. Filtrado y Supervisión

El *BSGC* utiliza sistemas de filtrado y supervisión para proteger a los alumnos, garantizar su seguridad y proteger los sistemas del centro.

El personal debe tener en cuenta que las actividades realizadas mediante los servicios digitales, los dispositivos y las redes proporcionados por el centro pueden ser objeto de supervisión.

La supervisión puede incluir, cuando sea técnicamente necesario y proporcionado:

- la actividad en Internet;
- el acceso a sitios web;
- los incidentes de seguridad;
- el cumplimiento de las normas por parte de los dispositivos;
- el uso de aplicaciones;
- la actividad en la red;
- los intentos de acceder a contenidos bloqueados;
- los incidentes de ciberseguridad.

La supervisión se lleva a cabo con fines legítimos, entre los que se incluyen:

- la protección de los alumnos;
- la ciberseguridad;
- la protección de los sistemas del centro educativo;
- el cumplimiento de las responsabilidades profesionales;
- la gestión operativa; y
- el mantenimiento de un entorno educativo seguro.

Privacidad y proporcionalidad
La supervisión se llevará a cabo de conformidad con la legislación aplicable en materia de protección de datos y con la política de privacidad del centro.

El centro se comprometerá a:

- recoger únicamente la información necesaria para la finalidad indicada;
- restringir el acceso a la información de supervisión al personal autorizado;
- conservar la información solo durante el tiempo necesario;
- proteger la información de supervisión frente al acceso no autorizado;
- utilizar la información de supervisión de forma proporcionada;
- distinguir entre el control rutinario y la investigación específica.

El centro educativo no utilizará el control como medio de vigilancia sin restricciones del personal.

En el caso de los empleados, el acceso al contenido de los dispositivos digitales facilitados por el empleador está sujeto al marco jurídico español aplicable, incluido el derecho a la privacidad del empleado y el requisito de que el acceso se realice con fines legítimos de control laboral o de integridad del dispositivo.

Se informará al personal de los criterios que rigen el uso de los dispositivos y sistemas digitales proporcionados por el centro educativo.

El personal no debe intentar desactivar, eludir ni interferir en los sistemas de filtrado o supervisión. El personal deberá comunicar inmediatamente al responsable de TI cualquier deficiencia aparente en los sistemas de filtrado o supervisión.

10. Prácticas Digitales en el Aula

La tecnología debe potenciar el aprendizaje, en lugar de convertirse en una distracción.

Los profesores deben:

- utilizar la tecnología de forma adecuada;
- asegurarse de que los alumnos comprendan el objetivo de aprendizaje;
- supervisar a los alumnos cuando utilicen dispositivos;
- vigilar activamente la actividad de los alumnos;
- utilizar los sistemas de vigilancia disponibles en el aula cuando sea pertinente;
- asegurarse de que los alumnos utilicen recursos autorizados;
- reaccionar de inmediato ante cualquier uso inadecuado;
- asegurarse de que los dispositivos se apaguen o se guarden cuando no sean necesarios.

Los sistemas de vigilancia digital constituyen una medida de seguridad adicional y no sustituyen a la supervisión activa en el aula. Los profesores siguen siendo responsables de mantener una supervisión adecuada de los alumnos.

11. Dispositivos del Colegio para los Alumnos

Dado que el *BSGC* no permite utilizar dispositivos propios a los alumnos de *Year 7* a *Year 11*, el personal tiene la responsabilidad específica de dar ejemplo y fomentar el uso responsable de los dispositivos gestionados por el centro.

El personal debe:

- asegurarse de que los dispositivos se utilicen únicamente cuando sea necesario;
- recordar a los alumnos que los dispositivos y las redes del centro están sujetos a filtrado y supervisión;
- denunciar los intentos de eludir la seguridad;
- denunciar los contenidos inapropiados o los comportamientos inadecuados en Internet;
- seguir los procedimientos de conducta del centro en caso de uso indebido de la tecnología;
- colaborar con el personal de TI y de protección de menores cuando surjan problemas.

No se debe permitir a los alumnos utilizar la tecnología de forma que socave los sistemas de filtrado, supervisión o protección del centro.

12. Dispositivos Personales de los Alumnos de KS5 (Bachillerato)

Los alumnos de *Year 12* y *Year 13* pueden utilizar dispositivos personales en el centro, siempre que se respete la Política y el Protocolo sobre dispositivos personales de KS5.

El personal debe comprender y aplicar de forma coherente las expectativas recogidas en dicho protocolo.

En concreto, el personal debe:

- asegurarse de que los dispositivos personales se utilicen con fines educativos adecuados;
- intervenir ante cualquier uso inadecuado;
- informar de cualquier intento de eludir los filtros del centro o los controles de red;
- informar del uso de redes no autorizadas, puntos de acceso personales u otros métodos destinados a eludir los controles del centro;
- seguir el proceso de escalado acordado.

Cuando surja un problema relacionado con la protección de menores, la ciberseguridad o una conducta grave, el personal deberá seguir el procedimiento pertinente del *BSGC* y remitir el asunto al miembro del personal correspondiente.

13. Contraseñas y Seguridad de las Cuentas

El personal debe:

- mantener la confidencialidad de las contraseñas;
- no compartir nunca las contraseñas con los alumnos ni con otros miembros del personal;
- utilizar contraseñas seguras;

- utilizar la autenticación multifactorial cuando esté disponible;
- bloquear los dispositivos cuando los dejen desatendidos;
- notificar inmediatamente cualquier sospecha de que una cuenta haya sido comprometida;
- no utilizar nunca la cuenta de otra persona.

Las contraseñas no deben anotarse en lugares a los que otras personas puedan acceder fácilmente.
El personal debe permanecer alerta ante los intentos de phishing e ingeniería social.

14. Protección de Datos y Confidencialidad

El personal tiene la responsabilidad profesional y legal de proteger la información personal y confidencial.
Esto incluye información relacionada con:

- los alumnos;
- las familias;
- el personal;
- la protección de menores;
- las necesidades médicas;
- los expedientes académicos;
- las evaluaciones;
- los asuntos de personal.

El personal debe:

- acceder únicamente a la información necesaria para el desempeño de sus funciones;
- utilizar sistemas autorizados para almacenar información;
- verificar los destinatarios antes de enviar información sensible;
- evitar enviar información confidencial a través del correo electrónico personal;
- evitar almacenar información del colegio en dispositivos personales;
- utilizar métodos seguros al transferir información sensible;
- notificar inmediatamente cualquier sospecha de violación de datos.

El colegio aplicará los principios de minimización de datos, limitación de la finalidad, confidencialidad, seguridad y conservación adecuada a la información digital.

El uso de plataformas y aplicaciones digitales debe ser autorizado de conformidad con las disposiciones de protección de datos del *BSGC*. Se debe prestar especial atención cuando las plataformas traten datos de menores o transfieran datos a terceros. La AEPD (Agencia Española de Protección de Datos) ha destacado específicamente estos riesgos en sus directrices actuales para los centros educativos.

Los requisitos de protección de datos nunca deben interpretarse como un impedimento para compartir la información necesaria en materia de protección con la persona adecuada.

15. Correo Electrónico y Comunicación Digital

Los correos electrónicos del personal deben ser:

- profesionales;
- precisos;
- proporcionados;
- respetuosos;
- apropiados para su posible divulgación futura.

El personal debe prestar especial atención al comunicarse sobre:

- el comportamiento de los alumnos;
- la protección de menores;
- las quejas;
- las cuestiones disciplinarias;
- las circunstancias familiares confidenciales.

La información sensible solo debe compartirse con aquellas personas que tengan una necesidad legítima de recibirla.

16. Redes Sociales

El personal debe actuar con criterio profesional al utilizar las redes sociales.
El personal no debe:

- publicar información confidencial del centro;
- identificar a los alumnos sin la autorización correspondiente;
- publicar fotografías de los alumnos desde cuentas personales;
- participar en debates inapropiados en Internet sobre los alumnos o sus familias;
- publicar material que pueda socavar razonablemente su papel profesional o la reputación del centro.

El personal debe valorar cuidadosamente si su actividad en las redes sociales podría generar un conflicto entre sus responsabilidades personales y profesionales.

El centro no pretende regular innecesariamente las actividades privadas lícitas. No obstante, el personal debe ser consciente de que la actividad pública en Internet puede tener consecuencias profesionales.

17. Inteligencia Artificial

El *BSGC* reconoce que la IA generativa es una tecnología educativa importante y en rápido desarrollo. Se espera que el personal utilice la IA de forma responsable, ética y profesional.

La IA puede utilizarse para apoyar actividades adecuadas, tales como:

- la planificación de clases;
- la generación de ideas;
- la creación de recursos;
- la diferenciación;
- las tareas administrativas;
- la redacción de comunicaciones no confidenciales;
- el desarrollo profesional.

El personal no debe introducir información confidencial o que permita identificar personalmente a alumnos, padres o miembros del personal en herramientas públicas de IA, a menos que la plataforma haya sido aprobada específicamente por el centro educativo para ese fin.
El material generado por la IA debe revisarse para comprobar:

- su exactitud;
- su imparcialidad;
- su idoneidad;
- cuestiones relacionadas con los derechos de autor;
- errores fácticos;
- su adecuación para los alumnos.

El personal sigue siendo responsable profesionalmente del material producido con la ayuda de la IA.

La IA no debe sustituir al criterio profesional.

18. Enseñanza y Reuniones Online

Cuando el personal imparta clases o se reúna con los alumnos de forma telemática, deberá utilizar plataformas aprobadas por el centro y seguir los procedimientos de protección de menores.
El personal deberá:

- utilizar cuentas profesionales;
- utilizar fondos y ubicaciones adecuados;
- asegurarse de que no se pueda oír ni ver a otras personas de forma involuntaria;
- mantener una vestimenta adecuada y una conducta profesional;
- evitar la comunicación privada individual, salvo que sea necesaria y esté autorizada;
- seguir los procedimientos del centro para la grabación de sesiones en línea.

Cualquier grabación debe tener una finalidad educativa o de protección legítima y gestionarse de acuerdo con la política del centro y los requisitos de protección de datos.

19. Ciberseguridad

Todo el personal forma parte del sistema de protección de ciberseguridad del *BSGC*.
El personal debe:

- completar la formación obligatoria en ciberseguridad;
- mantenerse alerta ante el phishing;
- no abrir archivos adjuntos ni enlaces sospechosos;
- verificar las solicitudes inusuales de información o pagos;
- notificar inmediatamente cualquier sospecha de incidente cibernético;
- proteger los dispositivos del colegio contra el acceso no autorizado.

Entre los ejemplos de incidentes que deben notificarse se incluyen:

- sospechas de phishing;
- dispositivos perdidos o robados;
- divulgación accidental de información;
- contraseñas comprometidas;
- malware;
- correos electrónicos sospechosos;
- acceso no autorizado;
- intentos de eludir los sistemas de seguridad.

El personal debe comunicar cualquier inquietud al responsable de TI y, cuando proceda, al DSL o al director de operaciones.

20. Uso de Soportes Extraíbles

Las memorias USB y otros soportes de almacenamiento extraíbles solo deben utilizarse cuando estén autorizados.

El personal no debe utilizar dispositivos USB desconocidos o personales para transferir información del centro.

La información confidencial no debe transferirse a soportes extraíbles a menos que esté específicamente autorizada y debidamente protegida.

21. Imágenes y Grabaciones Artificiales o Alteradas

El personal debe actuar con especial precaución en lo que respecta a fotografías, vídeos, «deepfakes» y contenidos generados o manipulados mediante inteligencia artificial en los que participen alumnos.

El personal debe informar de cualquier situación preocupante en la que los alumnos parezcan estar:

- creando imágenes inapropiadas;
- manipulando imágenes de otros alumnos;
- compartiendo imágenes sexualizadas;
- utilizando la inteligencia artificial para suplantar la identidad de otras personas;
- creando material amenazante o humillante.

Dichas actividades pueden constituir un problema de protección o de conducta y deben tratarse mediante los procedimientos escolares adecuados.

22. Accesibilidad e Inclusión

La tecnología digital debe facilitar un acceso equitativo al aprendizaje.
El personal debe tener en cuenta las necesidades de los alumnos que requieran:

- tecnología de apoyo;
- funciones de accesibilidad;
- formatos alternativos;
- apoyo digital adicional.

El centro espera que el personal utilice adecuadamente las herramientas de accesibilidad disponibles y que solicite ayuda cuando no se satisfagan las necesidades de acceso digital de un alumno.

23. Notificación de Incidencias

El personal debe informar de lo siguiente:

Incidencia	**Informar a**
Salvaguarda	Protección de menores DSL o adjunto al DSL
Incidencias técnicas/ciberseguridad	Responsable de TI
Protección de datos	Responsable designado de protección de datos
Conductas indebidas	Dirección / Coordinadores (Head of Key Stage)
Incidencias graves o reiteradas	Director / Director de Operaciones / DSL, según corresponda

El personal no debe retrasar la notificación por no estar seguro de si un incidente es lo suficientemente grave.
En caso de duda, hay que informar de ello.

Cuando una preocupación pueda suponer un riesgo inmediato para un menor, el personal deberá seguir sin demora los procedimientos de salvaguarda del centro.

24. Supervisión y Garantía

El centro supervisará el cumplimiento de esta política mediante medidas adecuadas y proporcionadas, entre las que se incluyen:

- informes de seguridad informática;
- informes de filtrado y supervisión;
- informes de gestión de dispositivos;
- registros de protección de menores;

- registros de conducta;
- registros de formación del personal;
- notificación de incidentes;
- revisión periódica de la política;
- auditorías de los sistemas digitales;
- comentarios del personal y del alumnado.

El director de operaciones y el responsable de TI se encargarán de supervisar los controles técnicos.

El responsable de seguridad digital (DSL) se encargará de supervisar las cuestiones relacionadas con la protección *online* dentro de sus respectivas responsabilidades.

El responsable de protección de datos asesorará sobre las implicaciones en materia de protección de datos y el cumplimiento de la normativa.

El director asume la responsabilidad general de garantizar que el centro cuente con las medidas adecuadas.

El Consejo Rector del centro recibirá las garantías oportunas en materia de protección digital, ciberseguridad y riesgos digitales significativos.

25. Formación del Personal

Todo el personal recibirá la formación adecuada sobre:

- protección online;
- uso adecuado de las tecnologías digitales;
- ciberseguridad;
- phishing e ingeniería social;
- protección de datos;
- inteligencia artificial;
- comunicación digital profesional;
- uso de los sistemas de supervisión del centro.

La formación se impartirá:

- durante la incorporación;
- anualmente;
- tras cambios significativos en los sistemas o en las políticas;
- cuando surjan riesgos que requieran formación adicional.

El centro conservará los registros de formación.

26. Incumplimientos del Protocolo

El incumplimiento de estas expectativas puede dar lugar a:

- formación adicional;
- la retirada o restricción del acceso a los sistemas;
- medidas por parte de la dirección;
- medidas disciplinarias;
- la remisión del caso a los procedimientos de protección;
- la remisión del caso a autoridades externas cuando proceda.

La respuesta será proporcionada a las circunstancias y coherente con las políticas pertinentes del centro, los acuerdos contractuales y los procedimientos laborales aplicables.

Cualquier medida disciplinaria que afecte a un empleado se llevará a cabo de conformidad con el marco laboral aplicable y los derechos del empleado.

El intento deliberado de eludir los controles de protección, filtrado o ciberseguridad se considerará un asunto grave.

Ninguna disposición de este protocolo exime ni altera ninguna obligación legal de notificación ni las responsabilidades de protección del centro educativo. Cualquier infracción de la ley deberá ser notificada a las autoridades competentes.

27. Declaración del personal

Todo el personal debe confirmar que:

1. Ha leído y comprendido este protocolo.
2. Entiende que la protección digital forma parte de sus responsabilidades en materia de protección.
3. Utilizará la tecnología del centro de forma responsable y profesional.
4. Mantendrá unos límites profesionales adecuados en Internet.
5. Protegerá la información confidencial.
6. No intentará eludir los controles de filtrado, supervisión o ciberseguridad del centro.
7. Informará sin demora de cualquier preocupación relacionada con la protección de menores, la protección de datos y la ciberseguridad.
8. Entiende que el uso de los sistemas y dispositivos proporcionados por el centro puede ser supervisado con fines legítimos de protección de menores, seguridad y funcionamiento.
9. Entiende que la supervisión se llevará a cabo de conformidad con los requisitos aplicables en materia de protección de datos y con la política de privacidad del centro.
10. Entiende que los dispositivos personales siguen estando sujetos a las expectativas profesionales y de protección del centro cuando se utilizan en el marco de su función profesional.

Nombre: _____

Firma: _____

Fecha: _____