POLÍTICA GLOBAL DE SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

COLEGIO SAN AGUSTIN (Madrid)
Calle Padre Damián, 18 - 28036 Madrid (Madrid)

1. INTRODUCCIÓN

El Reglamento General de Protección de Datos (UE) 2016/679 (en adelante RGPD), establece que los datos personales deben ser tratados de tal manera que se garantice una seguridad adecuada de dichos datos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Por ello, la presente Política de Seguridad, redactada en cumplimiento de lo dispuesto en el RGPD, recoge la información requerida por dicho precepto legal, así como las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado para la protección de los datos personales tratados por el centro educativo COLEGIO SAN AGUSTIN (Madrid) (en adelante "el Centro" o el "Responsable del Tratamiento")

Esta Política es el resultado de un análisis de riesgo elaborado por el Responsable del Tratamiento. En función a tal análisis, se considera que las medidas técnicas y organizativas adaptadas en la presente Política de seguridad resultan adecuadas para garantizar la integridad y confidencialidad de los datos personales tratados.

La presente Política deberá mantenerse en todo momento actualizada y será revisada siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información tratada o, en su caso, como consecuencia de los controles periódicos realizados.

Del mismo modo, será objeto de revisión si se producen cambios en la normativa sobre protección de datos de carácter personal, o se modifican los criterios establecidos por las autoridades de control, a través de sus Informes, Recomendaciones o Resoluciones, y, en todo caso, como consecuencia de sentencias de la Audiencia Nacional, Tribunal Supremo o Tribunal Constitucional.

2. CONCEPTOS BÁSICOS

A efectos de la presente Política de Seguridad, de conformidad con lo establecido en el artículo 4 del RGPD, se entenderá por:

Datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Limitación del tratamiento: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

Seudonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin

utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Fichero: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Responsable del tratamiento o responsable: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

Encargado de tratamiento o encargado: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Destinatario: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

Tercero: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Servicio de la Sociedad de la Información: Todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la mediad en que constituyan una actividad económica para el prestador de servicios.

3. ÁMBITO DE APLICACIÓN DE LA POLÍTICA DE SEGURIDAD

La presente Política de Seguridad será puesta en conocimiento de todas las personas que intervengan en las actividades del tratamiento, quienes deberán obligarse al cumplimiento de las medidas técnicas y organizativas dispuestas por el Centro para salvaguardar los datos personales tratados.

Asimismo, la presente Política de Seguridad será de aplicación a los ficheros automatizados o no, sistemas de información, soportes, programas o equipos empleados por el Centro para el tratamiento de los datos personales.

3.1 Responsable del Tratamiento

A continuación, se incluyen los datos identificativos del Responsable del Tratamiento y la dirección exacta donde se encuentran ubicados los ficheros:

COLEGIO SAN AGUSTIN (Madrid)

Calle Padre Damián, 18 - 28036 Madrid (Madrid)

csam@csamadrid.org

CIF: R2800689H

3.2 Responsable Interno de Protección de Datos

El Centro podrá designar un Responsable Interno de Protección de Datos, cuyas funciones se detallan en el apartado 4.2 de la presente Política de Seguridad.

3.3 Delegado de Protección de Datos (DPD)

Delegado de Protección de datos: AD HOC ASESORES LEGALES S.L. - dpo@adhocasesoreslegales.com

3.3.1 Designación del Delegado de Protección de Datos (Articulo 37 RGPD)

El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades.

El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39 del RGPD.

El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

3.3.2 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

La Ley Orgánica de Protección de Datos y garantía de los derechos digitales establece en su artículo 34.1: "Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades: …b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas…".

3.3.3 Posición del Delegado de Protección de Datos (Artículo 38 RGPD)

El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de sus funciones, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El Delegado de Protección de Datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

3.4 Personal del Centro

La presente política deberá ser puesto en conocimiento de todo el personal del Centro, quien deberá obligarse al cumplimiento de las medidas técnica y organizativas dispuesta para salvaguardar los datos personales objeto de tratamiento.

3.5 Encargados de Tratamiento

En virtud de lo establecido en el artículo 28 del RGPD, cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos del interesado.

El Centro llevará un REGISTRO DE ENCARGADOS DEL TRATAMIENTO en donde se identificará a los encargados, el servicio prestado, categoría de interesados a cuyos datos tienen acceso, el tipo de acceso que realizan y la fecha de firma del contrato de encargado de tratamiento de datos.

3.6 Prestadores de servicios sin acceso a datos

También se llevará un REGISTRO DE PRESTADORES DE SERVICIOS SIN ACCESO A DATOS, que trabajan en el Centro y pueden tener acceso a las instalaciones.

3.7 Sistemas de información del Centro

Los sistemas de información del Centro que tratan datos de carácter personal están integrados por los programas, soportes y equipos donde se archivan los datos personales. En cualquier caso, el acceso de las personas a los locales donde están los sistemas de información del Centro está debidamente controlado a través de llave y sólo puede acceder el personal debidamente autorizado.

3.7.1 Programas

Los programas o aplicaciones que el Centro utiliza para tratar los datos de carácter personal se detallan en el REGISTRO DE PROGRAMAS DE TRATAMIENTO DE DATOS.

3.7.2 Soportes

Soporte es todo objeto físico que almacena y/o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos personales.

Los soportes mayormente utilizados son fácilmente transportables, por lo que es evidente la peligrosidad para la seguridad de los datos, y por lo tanto, la importancia de gestionar un control sobre estos medios.

Los soportes que el Centro utiliza para almacenar datos de carácter personal son los relacionados en el REGISTRO DE SOPORTES Y EQUIPOS.

3.7.3 Equipos y estructura de la red

Los equipos que el Centro utiliza para tratar los datos de carácter personal son los relacionados en el REGISTRO DE SOPORTES Y EQUIPOS, en donde también se hace constar el esquema de la red informática del Centro.

3.8 Ficheros no automatizados del Centro

El Centro declara que los ficheros no automatizados con datos personales (en soporte papel), de que dispone, están debidamente almacenados y que controla el acceso del personal interno y de las personas externas, a estos ficheros. En el caso de que los ficheros en soporte papel dejen de ser útiles para las finalidades por las cuales los datos fueron recogidos, el Centro garantiza la completa destrucción física de los mencionados ficheros.

4. FUNCIONES Y OBLIGACIONES DEL PERSONAL

4.1 Responsable del Tratamiento

El Centro, como Responsable del Tratamiento, declara que ha informado debidamente al personal con acceso a los ficheros afectados por esta Política de Seguridad, de las obligaciones que tienen en el ejercicio de sus funciones y de las consecuencias que puede tener para ellos el incumplimiento de estas obligaciones.

Además, como Responsable del Tratamiento, el Centro está obligado a:

- Implantar las medidas establecidas en la presente Política de Seguridad, así como obligar a su cumplimiento.
- Actualizar la Política de Seguridad y el Registro de las Actividades del Tratamiento, siempre que se produzcan cambios relevantes en el sistema de información o en la organización de estos.
- Adecuar los contenidos de la presente Política a la legislación vigente, en todo momento, en materia de protección de datos.
- Con relación con el sistema informático o aplicaciones de acceso a los ficheros, se encargará de que exista una relación actualizada de personas que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso (mediante contraseñas).
- Autorizar, en caso de que sea necesario, el tratamiento de los datos personales en lugar distinto de donde están ubicados los ficheros.
- Deberá verificar que el personal autorizado del Centro, procede a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en ellas o su recuperación posterior.
- Actualizar ordenadores y dispositivos. Deberá mantener actualizados, en la medida de lo posible, los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales.
- Utilizar antivirus. En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales dispondrá de un sistema de antivirus que impida, en la medida de lo posible, el robo y destrucción de la información y datos personales. El sistema de antivirus será actualizado de forma periódica.
- Garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales, a efectos de evitar accesos remotos indebidos a los datos personales.
- Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o medios electrónicos, valorará la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- Habilitar un Registro de Violaciones de la Seguridad de los Datos Personales cuya existencia sea conocida por los empleados del Centro.
- Mantener actualizado un registro de soportes y equipos informáticos que contengan datos de carácter personal.
- Realizar copias de seguridad semanalmente almacenándolas en un lugar con acceso restringido al personal autorizado.
- Revisar periódicamente las medidas adoptadas.

4.2 Responsable Interno de Protección de Datos

El Responsable Interno de Protección de Datos, designado por el Responsable del Tratamiento, tendrá las siguientes funciones:

- Coordinar y controlar la implantación de las medidas de seguridad adoptadas por el Responsable del tratamiento.
- Mantener la presente Política de seguridad actualizada.
- Controlar que el personal cumple sus funciones y obligaciones en materia de protección de datos.
- Comprobar que los usuarios únicamente acceden a los datos que necesitan para ejercer sus funciones.
- Comprobar que el departamento de sistemas implanta las medidas y utiliza los protocolos de seguridad adoptados por el Responsable del Tratamiento.
- Analizar periódicamente la información registrada y elaborar un informe sobre las revisiones y problemas detectados.
- Determinar la pertinencia o no de los sistemas de comunicación propuestos para la transmisión de datos personales.
- Cooperar en la gestión de las violaciones de la seguridad de los datos personales.

- Cooperar en la respuesta ante ejercicio de derechos por los interesados.

4.3 Delegado de Protección de Datos (Artículo 39 RGPD)

El Delegado de Protección de Datos tendrá las siguientes funciones:

- Informar y asesorar al responsable o al encargado de tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en la normativa vigente en materia de protección de datos.
- Ofrecer el asesoramiento que se solicita acerca de la evaluación de impacto relativa a la protección de datos.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la Agencia Española de Protección de datos, o autoridad de control competente, para cuestiones relativas al tratamiento.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines de tratamiento.

4.4 Obligaciones del personal (docente y no docente) del Centro

4.4.1 En el lugar de Trabajo

- No se mostrará, ya sea de forma directa o indirecta, cualquier tipo de dato de carácter personal concerniente a los afectados o interesados que consten en los ficheros del Centro a terceras personas no autorizadas.
- Los puestos de trabajo informáticos estarán bajo la responsabilidad de los usuarios autorizados, garantizándose que la información que se muestra no pueda ser visible por personas no autorizadas. Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.
- Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento bajo llave, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre a su cargo deberá custodiarla e impedir, en todo momento, que pueda ser accedida por persona no autorizada. Política de mesas limpias.
- Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.
- En el caso de las impresoras, deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos del fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
- Deberá procederse a la destrucción de las copias o reproducciones desechadas en las destructoras de papel habilitadas al efecto, de forma que se evite el acceso a la información contenida en ellas o su recuperación posterior.

Del mismo modo se encuentran expresamente prohibidas las siguientes actividades:

- Utilizar plaraformas, programas o aplicaciones que no hayan sido autorizadas por el centro.
- Incluir o crear ficheros paralelos que contengan datos personales tanto en el disco duro del ordenador del usuario, como en pendrives, CD o DVD-ROM o cualquier otro soporte de almacenamiento, salvo autorización expresa del Centro. En todo caso, será necesario encriptar los datos almacenados a efectos de evitar accesos no

autorizados.

- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos del Centro.
- Intentar destruir, alterar, inutilizar o de cualquier otra forma dañar datos, programas o documentos de una forma consciente.
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos.
- Intentar aumentar el nivel de privilegios de un usuario en el sistema.
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.
- Instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- Borrar voluntariamente cualquiera de los programas instalados legalmente.
- Utilizar los recursos telemáticos del Centro, incluido Internet y el correo electrónico, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.

4.4.2 Salvaguarda y protección de la contraseña

Cada usuario será responsable de la confidencialidad de las contraseñas y, en caso de que ésta sea conocida, fortuita o fraudulentamente, por personas no autorizadas, deberá registrarla como una violación a la seguridad de los datos personales y proceder a su cambio.

4.4.3 Violaciones de seguridad de datos

Con el objeto de cumplir la normativa en materia de violaciones de la seguridad de los datos personales, el personal del Centro tiene el deber de comunicar, siguiendo el procedimiento creado a tal efecto (apartado 8), al Responsable de Tratamiento, al Responable Interno de Protección de Datos o al Delegado de Protección de Datos, en su caso, lo antes posible, cualquier violación de la seguridad de los datos personales que se produzca o de la que tengan conocimiento.

4.4.4 Confidencialidad

Salvo en casos de necesidad, debido al estricto cumplimiento de las funciones del cargo o con autorización expresa del Centro, queda prohibido enviar información confidencial del Centro al exterior, mediante soportes materiales, o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso.

Debido a lo anterior, el trabajador se obliga a utilizar toda la información a la que tenga acceso únicamente en la forma que exija el desempeño de sus funciones y a no disponer de ella de ninguna otra forma o con otra finalidad.

Las obligaciones derivadas de la presente Política se mantendrán vigentes de forma indefinida, incluso después de finalizada la relación entre el Centro y el personal.

4.4.5. Normas de uso del material informático y acceso a internet

Todo el personal dado de alta en el sistema deberá atender a las siguientes normas de utilización del material informático:

- Los usuarios serán plenamente responsables del uso adecuado de los terminales, así como sus accesorios desde el momento de su asignación.
- Todo el material informático deberá ser utilizado conforme a las instrucciones dadas por el Responsable de

Tratamiento.

- El material asignado deberá ser utilizado de forma responsable, de tal forma que no afecte o interfiera con el cumplimiento de las obligaciones laborales propias del personal y respete las medidas de seguridad establecidas por el centro en materia de protección de datos de carácter personal.
- Los usuarios podrán acceder únicamente a los recursos que el Centro les haya asignado. En ningún caso intentarán acceder a recursos sin los privilegios necesarios. El Responsable de Tratamiento, en todo momento podrá visualizar el intento de acceso a los mismos.
- Se debe evitar la utilización de dispositivos USB o soportes informáticos, salvo autorización del Responsable de Tratamiento. En caso de que sea estrictamente necesario su utilización para poder dar debido cumplimiento a las funciones propias del personal, el acceso a dicho dispositivo deberá estar protegido con contraseña.
- Se mantendrá bajo estricta confidencialidad las claves de acceso a los recursos, quedando totalmente prohibido pegarlas en las pantallas de los terminales o comunicársela a terceros. En caso de olvido de contraseñas deberán comunicárselo al Responsable de Tratamiento o al Responsable Interno de Protección de Datos.
- El acceso a Internet está sólo autorizado para cuestiones laborales, quedando totalmente prohibida la navegación por ocio, así como la descarga de información, ficheros o programas de Internet.
- La utilización de correo electrónico está sólo autorizada para cuestiones laborales. Como norma general en los correos electrónicos que se envíen a varias personas, de deberán poner las direcciones de correo electrónico en copia oculta (CCO). Así mismo, se deberá prestar especial atención en los destinatarios de los correos enviadas, evitando que la información contenida en los correos sea puesta en conocimiento de personas no autorizadas.
- Facebook, WhatsApp, Twitter así como cualquier otra red social o aplicación de mensajería instantánea está totalmente prohibida, salvo autorización expresa del Responsable de Tratamiento, y siempre por motivos justificados de trabajo. En el caso de tener autorización no podrán descargarse, en ningún caso, ficheros por este medio.

En cualquier caso, el Centro y el personal con acceso a los datos firmarán un documento donde establezcan las condiciones y las finalidades de acceso a los ficheros.

El REGISTRO DEL PERSONAL CON ACCESO A DATOS incluye una relación completa y actualizada del personal del Centro con acceso a los ficheros con datos de carácter personal. Este listado tendrá que incluir, además de los datos identificativos de las personas con acceso a los datos, el nivel de acceso a los ficheros de que cada uno de ellos dispone.

5. MEDIDAS DE SEGURIDAD PARA FICHEROS AUTOMATIZADOS.

En los siguientes apartados se recogen las medidas de índole técnica y organizativas implementadas para el tratamiento de datos personales en ficheros automatizados. Todo ello de conformidad con las exigencias de la normativa vigente en materia de protección de datos.

5.1 Identificación y autenticación

El sistema escogido por el Centro para controlar el acceso a los ficheros con datos personales es a través de usuario y contraseñas robustas. Tanto el usuario como la contraseña son las llaves de acceso a los sistemas y constituyen un componente básico de la seguridad de los datos y deben estar especialmente protegidos:

- Se recomienda disponer de perfiles con derechos a administración para la instalación y configuración del sistema y usuarios sin privilegio o derecho de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos, se dispondrá de un usuario y contraseña especifico.

- Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se dispondrá de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.
- Las contraseñas son estrictamente confidenciales y secretas, y cualquier incidencia que comprometa su confidencialidad debe ser inmediatamente comunicada al Responsable de Tratamiento y subsanada en el menor tiempo posible.
- Cada usuario es responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida, fortuita o fraudulentamente por personas no autorizadas, debe registrarse como una violación de la seguridad de los datos personales y procederse por parte del Usuario a su cambio inmediato.

Se deberán respetar los siguientes parámetros para la gestión de contraseña

- Caducidad: 12 meses.
- Tamaño mínimo: 8 caracteres.
- Características de complejidad avanzada: Combinación alfanumérica.
- Bloqueo de los sistemas tras intentos fallidos de acceso: 3 intentos.

Bloqueo de usuarios y contraseñas: La personas designada por el Responsable de tratamiento deberá establecer un sistema de bloqueo de la contraseña tras un tercer intento fallido de acceso.

5.2 Acceso a los datos a través de redes de telecomunicaciones

Los accesos a datos a través de redes de comunicaciones tendrán que garantizar un nivel de seguridad equivalente al correspondiente a los accesos realizados de forma local.

5.3 Régimen de trabajo fuera de los locales de la ubicación de los ficheros

La ejecución de tratamientos de datos de carácter personal fuera de los locales de la ubicación de los ficheros tendrá que ser autorizado expresamente por el Responsable del Tratamiento y, en cualquier caso, habrá que garantizarse la integridad y confidencialidad de los datos tratados. El REGISTRO DE SOPORTES Y EQUIPOS incluye un modelo de autorización a estos efectos, que podrá firmarse por usuarios determinados o para cierto perfil de usuarios.

5.4 Ficheros temporales

Los ficheros temporales tendrán que cumplir el nivel de seguridad que les corresponda. Cualquier fichero temporal será borrado una vez que haya dejado de ser necesario para las finalidades que motivaron su creación. De forma periódica se procederá a revisar los servidores con la finalidad de asegurar la adecuada destrucción de los ficheros temporales en desuso.

5.5 Copias de seguridad y recuperación de los datos

El Responsable del Tratamiento ha de establecer un sistema de copias de seguridad y recuperación de datos para sus ficheros, que garantizará su reconstrucción en el estado en que se encontraban si se produjera una pérdida o destrucción.

En caso de producirse un fallo del sistema que produzca una pérdida total o parcial de los datos del fichero existirá un procedimiento que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del fichero al estado en que se encontraban en el momento del fallo.

Deberá conservarse una copia de respaldo de los procedimientos de recuperación de los datos en un lugar diferentes

de aquel en que se encuentren los equipos informáticos que los tratan, cumpliendo, en todo caso, las medidas de seguridad exigidas.

En cualquier caso, el Centro revisará, al menos cada 6 meses, el correcto funcionamiento del sistema de copias de seguridad.

5.6. Limitación en el uso de datos reales

Las pruebas anteriores a la puesta en marcha o a la introducción de cambios en los sistemas de información que traten datos de carácter personal, no se realizarán con datos reales, hasta que estos sistemas dispongan de las medidas de seguridad adecuadas. En todo caso y como paso previo a las eventuales pruebas, se realizará una copia de seguridad de la información que pueda verse en riesgo y se dejará constancia documental de la realización y resultado de las citadas pruebas.

5.7 Redes de telecomunicaciones

La transmisión de datos personales a través de redes de telecomunicaciones se realizará cifrando estos datos o mediante cualquier otro sistema que garantice la integridad y la confidencialidad de la información transmitida.

5.8 Gestión de soportes

Soporte es todo objeto físico que almacena y/o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Los soportes mayormente utilizados son fácilmente transportables, por lo que es evidente la peligrosidad para la seguridad de los datos, y por lo tanto, la importancia de gestionar un control sobre estos medios.

5.8.1 Procedimiento de uso de los soportes

En relación con los soportes, deben seguirse las siguientes normas:

- Deben guardarse en un lugar protegido, con acceso restringido a personas no autorizadas. Dicho almacenamiento se realiza bajo el control del Responsable de Tratamiento.
- La salida de estos soportes, fuera de los locales donde están ubicados dichos ficheros protegidos, deberá ser expresamente autorizada por el Responsable de Tratamiento, y el Delegado de Protección de Datos, en su caso, lo hará constar en el registro de salida de soportes establecido al efecto.
- Cuando los soportes con información de carácter personal tengan que salir del lugar de ubicación del fichero para operaciones de mantenimiento o reparación, se establecerán unas medidas de seguridad tendentes a evitar la recuperación de información por terceros no autorizados.
- Los soportes reutilizables deberán ser formateados o sobrescritos con anterioridad a su reutilización libres de información anterior y de forma que los datos que contenían, no se puedan recuperar.

Para la destrucción de los soportes se seguirán las siguientes pautas:

- Destrucción física de los mismos, para ello, se dará de baja previamente en el registro y se darán al Responsable de Tratamiento correspondiente que procederá a su destrucción física.
- En el caso de ficheros no automatizados en soporte papel es necesario el uso generalizado de destructoras de papel.

6. MEDIDAS DE SEGURIDAD PARA FICHEROS NO AUTOMATIZADOS

En relación con las medidas de seguridad aplicables sobre los ficheros no automatizados que contengan datos de carácter personal, el Centro deberá aplicar las siguientes medidas de seguridad:

- Los ficheros que contengan datos de carácter personal en soporte no automatizado, única y exclusivamente, serán tratados por el personal autorizado en función de su puesto de trabajo.
- El acceso a los archivos donde se encuentren ficheros con datos de carácter personal no automatizados deberán restringirse mediante el uso de una llave física.
- En el caso de producirse traslados de cualquier fichero con datos de carácter personal no automatizados, se garantizará la confidencialidad y que dicha información no sea manipulada por terceros durante su transporte.
- Los archivos donde se encuentren los ficheros que contengan datos de carácter personal no automatizados se mantendrán siempre cerrados bajo llave física.
- No se mostrará, ya sea de forma directa o indirecta, cualquier tipo de dato de carácter personal concerniente a los afectados o interesados que consten en los ficheros de los responsables a terceras personas no autorizadas.
- El centro dispondrá de un sistema adecuado de destrucción de soportes físicos de datos de carácter personal. Para ello, existen destructoras de papel que garantizan la destrucción de soportes documentales que contengan datos impidiendo cualquier recuperación posterior de la información almacenada.

7. REGISTRO DE ACCESOS

El Centro establece un sistema de registro de accesos a los ficheros que contengan categorías especiales de datos personales (artículo 9 RGPD), que retendrá, como mínimo, la identificación del usuario y el momento del acceso.

El Responsable del tratamiento es la persona encargada de controlar este sistema de registro de accesos; tendrá la obligación de revisarlo periódicamente.

El sistema de Registro de accesos deberá tener, al menos, las siguientes características:

- Imposibilidad de ser desactivado.
- En caso de que autorice una entrada a los ficheros, será preciso que permita identificar el registro accedido.

8. VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES

Con el objeto de dar cumplimiento a lo establecido en el artículo 33 del RGPD, el Centro dispondrá de un registro y de un procedimiento de notificación, gestión y respuesta ante cualquier violación de la seguridad de los datos personales.

Se entiende por Violación de la Seguridad de los Datos Personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

En caso de violación de la seguridad de los datos personales, el Responsable del Tratamiento la notificará a la Autoridad de control competente sin dilación indebida, y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

9. APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

El centro educativo COLEGIO SAN AGUSTIN (Madrid), aprueba la presente Política de Seguridad y la asume como

propia.

El centro ha adoptado las medidas necesarias para que todos los profesionales de su organización estén familiarizados con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, que establece las obligaciones y procedimientos tendentes a garantizar y proteger los derechos de los titulares de datos personales.

Todos los profesionales del Centro con acceso a datos personales deberán cumplir las prescripciones contenidas en la presente Política, así como las medidas de seguridad en ella contempladas.

Asimismo, el Centro ha establecido las funciones y responsabilidades necesarias para cumplir y hacer cumplir en todo momento el citado Reglamento, haciendo especial énfasis en los procedimientos y medidas de seguridad a adoptar por aquellos profesionales que tienen acceso a datos de carácter personal.

Esta política se mantendrá actualizada y será revisada siempre que se produzcan cambios relevantes en la información u organización de esta. El contenido se adecuará en todo momento a las disposiciones legislativas vigentes en materia de seguridad de los datos de carácter personal, protegiendo el Centro adecuadamente la información conforme a la legislación mencionada.

Firmado por ***5247** ILDEFONSO TRIGUEROS (R: ****0689*) el día 02/02/2023 con un certificado emitido por AC Representación