Contrato de Prestación de Servicios de Asesoramiento en Ciberseguridad - Básico

Condiciones Generales de Contratación

REUNIDOS

De una parte, el CLIENTE, identificado en las Condiciones Particulares del presente Contrato de Prestación de Servicios LOPDGDD (en adelante Contrato), representada por la persona que en las mismas se indica (en adelante, el CLIENTE) y de otra, CONSTRUYENDO FUTURO INFORMÁTICO SL, con NIF B34222950, domiciliada en Avda. Madrid, 10 · 34004 Palencia · España (en adelante, GRUPO CFI), representada por la persona que se identifica en la Condiciones Particulares del presente Contrato.

MANIFIESTAN

i. Que ambas partes se reconocen capacidad legal suficiente para suscribir el presente Contrato.
ii. Que GRUPO CFI es una empresa de consultoría especializada en el asesoramiento a las empresas en el ámbito de la ciberseguridad, la protección de datos personales y la LSSICE.
iii. Que el CLIENTE es una empresa u organización que está interesada en contratar los servicios de GRUPO CFI.
iv. Que la documentación contractual está constituida por las presentes Condiciones Generales, sus Anexos y las Condiciones Particulares.
v. Que, para efectuar las comunicaciones, así como la entrega de documentación generada con ocasión del presente Contrato, se utilizarán los siguientes medios: a) correo electrónico proporcionado por el CLIENTE para estos fines; b) servicios "online" que GRUPO CFI ponga a disposición del CLIENTE; c) envío al domicilio consignado en las Condiciones Particulares del contrato.
vi. Que ambas partes han acordado celebrar el presente Contrato de asesoramiento y colaboración, con base a las siguientes CONDICIONES GENERALES, ANEXOS y CONDICIONES PARTICULARES.

CONDICIONES GENERALES

01. Términos y definiciones

Estos son algunos de los términos y definiciones contenidos en las presentes Condiciones Generales.

RGPD: 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 y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

LSSICE: Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

LGDCU: Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

DPD o DPO: Delegado de Protección de Datos.

AEPD: Agencia Española de Protección de Datos.

02. Legislación aplicable

La legislación sobre la que se ofrece asesoramiento a través de este Contrato, y en función de los servicios contratados, es, exclusivamente, la siguiente:

- RGPD: 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 y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- SGSI: Norma UNE-EN ISO/IEC 27001:2023.
- ENS: Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

03. Objeto del contrato

El presente Contrato tiene por objeto establecer las condiciones del encargo a GRUPO CFI por el CLIENTE para realizar los servicios objeto de contratación, así como el alcance de dichos servicios, y en su caso, los límites de los mismos.

Las actividades de asesoramiento y apoyo que GRUPO CFI desarrollará para el CLIENTE son las especificadas, expresa y taxativamente, en las Condiciones Particulares del presente Contrato y descritas en su contenido y alcance en los Anexos de estas Condiciones Generales.

04. Duración y vigencia del contrato

Este contrato se formaliza y entra en vigor una vez esté firmado por el CLIENTE y tiene una vigencia máxima de cinco meses.

En todo caso, su vigencia finaliza en el momento en que se presente la justificación de la ayuda vinculada a este contrato y se haya percibido el importe total de los pagos acordados.

05. Obligaciones de GRUPO CFI

Son obligaciones de GRUPO CFI las siguientes:

- Facilitar al CLIENTE los entregables y la documentación correspondiente a los servicios contratados.
- Asesorar al CLIENTE, al personal, a sus representantes y a los órganos de representación especializados a través de la persona que el CLIENTE ha designado como interlocutor, según los servicios contratados.
- Tratar con la debida confidencialidad los datos aportados por el CLIENTE durante la prestación de los servicios.
- Realizar al CLIENTE las actividades contratadas durante el periodo de vigencia del Contrato.
- Presentar la justificación de los trabajos realizados ante Red.es.

06. Obligaciones del CLIENTE

Son obligaciones del CLIENTE las siguientes:

- Permitir el acceso, en su caso, de las personas designadas por GRUPO CFI para prestar todos o parte de los servicios contratados para la correcta ejecución del presente Contrato, así como el uso de medios técnicos necesarios para ello.
- Designar un interlocutor debidamente informado y formado para el intercambio de información entre el CLIENTE y GRUPO CFI respecto a la correcta ejecución del presente Contrato y comunicar a GRUPO CFI cualquier cambio en el mismo. En el caso de que dicha designación no se produzca expresamente, se entenderá que asume estas funciones el firmante del Contrato.
- Poner a disposición de GRUPO CFI todo lo referido a la información y los datos que maneja, los medios y canales utilizados para recabarla y tratarla, proveedores externos, personal, y demás información y documentación necesaria para que GRUPO CFI pueda prestar sus servicios de forma idónea.
- Ofrecer al personal de su organización y, en su caso, a sus proveedores, los documentos pertinentes para su firma y asegurarse de que son firmados por ellos, así como la custodia de los mismos una vez firmados.
- Informar al personal de su organización sobre sus obligaciones y derechos en materia de protección de datos, así como colocar, en su caso, los carteles informativos apropiados.
- Comunicar de forma fehaciente a GRUPO CFI la existencia de personal de nueva incorporación y la solicitud de formación.
- Analizar la documentación que GRUPO CFI le ha facilitado y comunicarle, en su caso, las omisiones, defectos o inexactitudes que puedan existir en la misma, ya que a falta de esta comunicación se entiende que la documentación facilitada ha tenido en cuenta todas las instalaciones, medios e información que maneja el CLIENTE.
- Proporcionar a GRUPO CFI una dirección de correo electrónico a efectos de notificación, comunicación y envío de documentación.
- Asumir directamente y bajo su total responsabilidad la ejecución y puesta en marcha de las tareas y actividades indicadas por GRUPO CFI (en su caso, firma de documentos, colocación de carteles, implantación de medidas, etc.), al ser GRUPO CFI órgano asesor externo al CLIENTE que no puede legalmente ejercer directamente la dirección de las actividades a aplicar por el CLIENTE.

Las actividades encomendadas a GRUPO CFI se efectuarán en función de la información facilitada por el CLIENTE, por lo que, GRUPO CFI no asume responsabilidad alguna de los supuestos de error o ausencia, total o parcial, de dicha información.

El incumplimiento de los anteriores compromisos exonerará a GRUPO CFI de cualquier obligación o responsabilidad derivada de la falta de ejecución total o parcial del concierto o del incumplimiento defectuoso del mismo, derivado de una información parcial, incompleta o inexacta, respondiendo el CLIENTE ante la Administración competente, su personal, socios y colaboradores o terceros.

07. Medios

GRUPO CFI dispondrá de la organización, instalaciones, personal y equipos necesarios para llevar a cabo las actividades contratadas en las Condiciones Particulares, comprometiéndose a dedicar anualmente los recursos humanos y materiales necesarios para la correcta realización de las actividades.

No obstante, GRUPO CFI podrá desarrollar las actividades concertadas con medios propios o subcontratar los servicios que considere precisos para atender las actividades para las que ha sido contratada. A tal efecto, el CLIENTE autoriza a GRUPO CFI a transmitir toda la información necesaria al agente o subcontratista con dicho fin.

Para las actuaciones en remoto, GRUPO CFI será el responsable de gestionar y enviar el enlace al sistema utilizado para realizar la reunión remota (en adelante, “Plataforma Online”). Durante la prestación de los servicios, GRUPO CFI podrá captar, recabar, editar y copiar, en su caso, imágenes, vídeos y sonido con la finalidad exclusiva de prestar los servicios solicitados.

GRUPO CFI no otorga garantía alguna, ni de ningún tipo relacionada directa o indirectamente con el adecuado funcionamiento, disponibilidad y/o seguridad (total ni parcial) de la Plataforma Online. GRUPO CFI tampoco otorga garantía alguna, ni de ningún tipo, relacionada directa o indirectamente con el servicio ininterrumpido ni libre de error (total ni parcial) de la Plataforma Online.

08. Ejecución de los servicios

Los trabajos darán comienzo una vez haya recibido GRUPO CFI las Condiciones Particulares del Contrato firmadas por el CLIENTE y aceptado, por parte del CLIENTE, el Acuerdo de Prestación de Servicio enviado por Red.es que está vinculado a este Contrato.

Una vez recibida la aceptación, GRUPO CFI se pondrá en contacto con la persona indicada en las Condiciones Particulares de este Contrato a través de los medios de contacto que el CLIENTE ha indicado para acordar la/s fecha/s y hora/s en las que se llevará a

cabo la consultoría. Para la consultoría por videoconferencia, se mandará la convocatoria al correo electrónico indicado por la persona de contacto del CLIENTE.

Una vez finalizada la consultoría, GRUPO CFI elaborará la documentación pertinente y se la facilitará al CLIENTE a través de los medios técnicos acordados (en su caso, envío por correo electrónico, puesta a disposición a través de una plataforma para su descarga y/o envío a la dirección postal indicada en las Condiciones Particulares de este Contrato).

En todo momento el CLIENTE dispondrá de los siguientes canales de contacto para solucionar las dudas o consultas que se le planteen en relación a la documentación o los servicios prestados: a) envío de consultas a través la plataforma habilitada para el CLIENTE (canal preferente); b) llamada telefónica al 901 001 802 o 979 699 517.

Deberán mantenerse las siguientes reuniones preceptivas:

- Reunión de inicio (en formato presencial).
- Reunión intermedia (en formato presencial o remoto).
- Reunión final (en formato presencial). Esta reunión final será grabada y puesta a disposición de Red.es y se invitará a un representante de Red.es a la misma, que podrá asistir, o no.

09. Propiedad intelectual de los trabajos

GRUPO CFI ostenta todos los derechos de propiedad intelectual sobre su conocimiento, metodologías, bases de datos de información, referencias, modelos, diseños, herramientas y técnicas que pone a disposición del CLIENTE para la ejecución de los servicios objeto del Contrato y la elaboración de los entregables del mismo.

Dichos derechos de propiedad intelectual no son transferidos al CLIENTE por la ejecución de los servicios y entregables, objeto del Contrato, sino que GRUPO CFI conserva, en todo momento, la titularidad de todos los derechos de propiedad intelectual de todo lo aportado al CLIENTE (incluyendo los entregables), incluso tras la finalización de la prestación de sus servicios.

Con objeto de que el CLIENTE pueda hacer un uso interno de los entregables aportados, se le concede una licencia de uso de dichos entregables al CLIENTE. Esta licencia es concedida, exclusivamente, al CLIENTE contratante y es intransferible.

Aquellos documentos entregados por GRUPO CFI que, tras su firma por terceros, ejerzan un vínculo jurídico entre el CLIENTE y este tercero, son propiedad del CLIENTE con carácter singular, no pudiendo ser usados como modelo para redacción de otros documentos similares, al tratarse de contenido sujeto a la propiedad intelectual definida en este punto.

10. Facturación

La facturación se realizará al finalizar los servicios prestados, por el importe indicado en las Condiciones Particulares del Contrato.

El CLIENTE únicamente deberá abonar el importe relativo al IVA de la factura emitida, que deberá ser abonado en los siguientes cinco días a la emisión mediante transferencia bancaria al nº de cuenta indicado en la factura.

El importe de la factura, excluyendo el IVA, será abonado a GRUPO CFI por Red.es.

11. Justificación de los servicios

Corresponde a GRUPO CFI realizar la justificación ante Red.es de los servicios prestados y al CLIENTE validar, en su caso, los documentos que correspondan.

El CLIENTE debe colaborar con GRUPO CFI en lo que sea necesario para realizar la justificación de los servicios y llevar a buen término el Contrato. Especialmente en las reuniones que Red.es establece como preceptivas y que se indican en el apartado 08.

12. Suspensión o cancelación de los servicios

En caso de que el CLIENTE decida suspender o cancelar los servicios que GRUPO CFI le está prestando, suponiendo la invalidación de la ayuda, deberá abonar a GRUPO CFI el importe de los trabajos ejecutados hasta el momento en que el CLIENTE comunique su suspensión o cancelación a GRUPO CFI por un medio fehaciente.

13. Extinción del Contrato a instancia del CLIENTE

El incumplimiento de cualquiera de las obligaciones asumidas por GRUPO CFI en virtud de este Contrato será causa de resolución del mismo a instancia del CLIENTE contratante. En este caso, será condición imprescindible para que sea efectiva la extinción del Contrato, el envío de un escrito de solicitud de baja firmado por el CLIENTE, en el que indique la causa de resolución y la fecha en la que ha de hacerse efectiva la misma. Una vez tramitada la baja y resuelto el Contrato, GRUPO CFI quedará exonerada de cualquier obligación contractual o responsabilidad en relación a los servicios que venía prestando. En caso de que se hubiesen comenzado los servicios, se atenderá a la cláusula 12 en cuanto al importe de los trabajos realizados que deberá abonar el CLIENTE.

14. Extinción del Contrato a instancia de GRUPO CFI

La falta de pago de la contraprestación económica pactada o de cualquier otra cantidad derivada de la ejecución de este Contrato, el incumplimiento por parte del CLIENTE de su deber de colaboración con GRUPO CFI, así como el incumplimiento de cualesquiera de las obligaciones reseñadas en el punto 06 de este Contrato será causa de resolución del mismo a instancia de GRUPO CFI. En este caso, GRUPO CFI comunicará al CLIENTE contratante su voluntad de resolver el Contrato, quedando exonerada de cualquier obligación contractual o responsabilidad en relación a los servicios que venía prestando desde el momento en que se hubiese producido el hecho motivante de la resolución unilateral y sin que tampoco se pueda responsabilizar a GRUPO CFI desde ese momento de las modificaciones que puedan afectar al contenido de la documentación elaborada para el CLIENTE. En caso de que se hubiesen comenzado los servicios, se atenderá a la cláusula 12 en cuanto al importe de los trabajos realizados que deberá abonar el CLIENTE.

15. Condiciones no recogidas inicialmente

El presente Contrato podrá ser completado, por acuerdo de las partes, mediante otros documentos anexos complementarios que contengan acuerdos sobre otras actividades no recogidas en estas Condiciones Generales y Particulares.

16. Nulidad de Contratos precedentes

Este Contrato anula cualquier otro anterior establecido con GRUPO CFI, salvo que se trate de un anexo complementario en los términos previstos en la cláusula anterior.

17. Uso de la marca

El CLIENTE autoriza a GRUPO CFI para que pueda incluir su nombre comercial y logotipo en los sitios web de GRUPO CFI, así como en soportes publicitarios (como catálogos, folletos, etc.). En caso de que el CLIENTE no desee que GRUPO CFI utilice su nombre comercial y logotipos, tan solo debe comunicarlo a GRUPO CFI.

18. Protección de datos personales

Responsable: Construyendo Futuro Informático, S.L.; Finalidad: Prestar los servicios solicitados, así como el envío de comunicaciones comerciales y boletín informativo; Derechos: Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, indicados en la información adicional, que puede ejercer dirigiéndose a la dirección de correo siguiente: dpd@grupocfi.es; Información adicional: Puede consultar información adicional y detallada sobre nuestras políticas y sus derechos de Protección de Datos en www.grupocfi.es/privacidad (T-03).

GRUPO CFI, para la prestación de los servicios detallados en este contrato, actúa como Encargado del tratamiento del CLIENTE. A tal efecto, y de conformidad con el artículo 28 del 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 y a la libre circulación de estos datos, y el artículo 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ambas partes convienen en suscribir el acuerdo detallado en el Anexo II de este Contrato para regular el acceso a los datos personales en el marco de la prestación de los servicios proporcionados por GRUPO CFI.

19. Responsabilidad

Los servicios de asesoramiento ofrecidos en este Contrato no suponen un traslado de la responsabilidad del CLIENTE hacia GRUPO CFI.

Toda la documentación elaborada, así como el asesoramiento ofrecido, se basa en la información que el CLIENTE suministra a GRUPO CFI y por tanto, el CLIENTE es el único responsable de que dicha información sea veraz y refleje, en todo momento, la realidad de su organización.

El CLIENTE es el único responsable en todo momento del correcto cumplimento de la normativa de protección de datos personales y la LSSICE en su organización, así como de aplicar los protocolos, controles y medidas de seguridad indicadas.

20. Validez de las disposiciones y fuero

Si cualquiera de las disposiciones de las presentes Condiciones Generales se tuviera por no válida, nula o ilegal, la validez, legalidad y cumplimiento de las restantes disposiciones no se verán afectadas ni perjudicadas por ello.

Para cuantas cuestiones se puedan suscitar de la interpretación o aplicación del presente contrato, ambas partes, con renuncia expresa a su propio fuero, se someten a los Juzgados y Tribunales de Palencia.

Y así, en prueba de conformidad del presente Contrato y sus respectivos anexos, las partes intervinientes formalizan y suscriben por duplicado los ejemplares de las Condiciones Particulares de este Contrato.

ANEXOS

Forman parte integrante de este Contrato los siguientes Anexos:

ANEXO I: ALCANCE DE LOS SERVICIOS PRESTADOS

Se prestarán al CLIENTE, exclusivamente, los servicios que están descritos en las Condiciones Particulares del presente Contrato. El alcance de los servicios, y en su caso, las exclusiones, se detallan a continuación.

I. Elaboración del inventario de activos de la organización

Incluye la elaboración del inventario de activos de la organización en base a la información proporcionada por la persona o personas de la organización.

II. Auditoría de los activos identificados y pruebas de penetración pentesting

Incluye la auditoría, en el ámbito de la ciberseguridad de los activos identificados en la organización y la realización de pruebas de penetración tipo "pentesting" así como la elaboración del correspondiente informe de auditoría.

III. Elaboración de un Plan de Protección del Negocio que cubra las necesidades detectadas

Tomado como base la auditoría realizada en el punto anterior, se realización un Plan de Protección del Negocio para corregir las vulnerabilidades detectadas y/o fortalecer la postura de ciberseguridad de la organización. Corresponde a la organización implementar las medidas de seguridad y controles identificados en el Plan de Protección.

IV. Elaboración una Política de Seguridad

Se elaborará una Política de Seguridad para la organización que defina las medidas a implementar sobre medios y sistemas de acceso a la información que incluya:

- Gestión de usuarios. Autenticación, política de contraseñas fuertes.
- Protección de correo electrónico / servidores /end-points.
- Copias de seguridad con mecanismos específicos anti ransomware.
- Actualización y parcheo periódico de software.

V. Elaboración de un Plan de Continuidad de Negocio

Enfocado a la protección de las personas y sistemas de la organización, así como al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a eventos de interrupción o desastre con, al menos, los siguientes puntos clave:

- Gestión ante incidentes de seguridad.
- Gestión de vulnerabilidades.
- Medidas de respuesta y recuperación.

VI. Cumplimiento legal

Elaboración del Registro de Actividades de Tratamiento de la organización, así como el resto de las obligaciones documentales para el cumplimiento de la normativa de protección de datos, análisis de riesgos, ejercicio de derechos, etc. (Excepto EIPD).

VII. Caso de uso sobre un determinado servicio o proceso de la organización

Análisis de vulnerabilidades con resultados de las pruebas realizadas y recomendaciones. Incluye la elaboración de los siguientes documentos:

- Diagrama AS-IS sobre el cual se representen los elementos de los sistemas de información de los que dispone la organización y como se relacionan entre sí.
- Resultados de las pruebas de pentesting: reporte de las pruebas realizadas que incluya un resumen, metodología utilizada, hallazgos e impacto.

VIII. EXCLUSIONES

No se realizará ninguna intervención de tipo técnico en los sistemas, aplicaciones y servicios del CLIENTE para mitigar las vulnerabilidades o debilidades identificadas. Esas labores corresponden al departamento de sistemas del CLIENTE.

ANEXO II: ACCESO A DATOS POR CUENTA DE TERCEROS

El presente ANEXO, que vincula al CLIENTE (en adelante, el responsable del tratamiento) y a GRUPO CFI (en adelante, el encargado del tratamiento) regulará los derechos y obligaciones que deben cumplir ambas Partes siguiendo lo dispuesto en la normativa vigente de protección de datos personales.

Este ANEXO forma parte del Contrato de prestación de servicios subscrito entre el CLIENTE y GRUPO CFI y entrará en vigor una vez que se haya iniciado la prestación del servicio objeto del Contrato.

I. Objeto del encargo

Mediante las presentes cláusulas se habilita al encargado del tratamiento para tratar, por cuenta del responsable del tratamiento, los datos personales necesarios para prestar el/los servicio/s de: Servicios de consultoría, soporte legal, auditoría y, en su caso, Delegación de Protección de Datos para cumplimiento normativo en el ámbito de las normativas de protección de datos personales y los servicios de la sociedad de la información y el comercio electrónico, normas y normativa relacionada con la implantación de sistemas de gestión de seguridad de la información, así como la formación en esos ámbitos, y la puesta a disposición del responsable del acceso a diversas plataformas de gestión de los servicios y documentos, en formato SaaS.

Los tratamientos a llevar a cabo dependen de las modalidad y totalidad de los servicios contratados con el responsable y que forman parte de las Condiciones Generales y Particulares de Contratación.

Concreción de las operaciones a realizar: recogida; registro; estructuración; conservación; consulta; comunicación por transmisión; interconexión; cotejo.

II. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento pone a disposición del encargado del tratamiento la información que se describe a continuación:

a) Datos identificativos de clientes y usuarios.

b) Datos identificativos de proveedores y contactos.

c) Datos identificativos y detalles de empleo del personal, voluntarios y socios.

d) Datos identificativos y académicos de alumnos y personal, en su caso.

La puesta a disposición de la información indicada anteriormente puede realizarse, bien proporcionando al encargado la información indicada, bien habilitándole el acceso a la misma, o debido a que el responsable del tratamiento almacena dicha información en sistemas y/o instalaciones del encargado del tratamiento.

III. Duración

La duración del presente acuerdo está sujeta a la duración del contrato principal de servicios.

IV. Obligaciones del encargado del tratamiento

El encargado del tratamiento, y todo su personal se obliga a:

a) Utilizar los datos personales objeto del tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b) Tratar los datos de acuerdo a las instrucciones del responsable del tratamiento.

Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembro, el encargado informará inmediatamente al responsable.

c) Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de cada responsable, que contenga:

1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.
2. Las categorías de tratamientos efectuados por cuenta de cada responsable.
3. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en su caso, de las transferencias indicadas en el artículo 49, párrafo segundo del RGPD, la documentación de garantías adecuadas, teniendo en cuenta, especialmente, el posible alojamiento de datos en servicios de computación en la nube (servicios *cloud*).
4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:
    i. La seudonimización y el cifrado de datos personales.
    ii. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
    iii. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
    iv. El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d) No comunicar datos a terceras personas (incluidas las transferencias de datos personales a terceros países u organizaciones internacionales), salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. Para obtener la autorización del responsable del tratamiento para transferir datos personales a un tercer país o a una organización internacional, el encargado del tratamiento debe indicar los siguientes conceptos en la solicitud de autorización al responsable del tratamiento:

1. la entidad a la que se van a transferir los datos,

2. la finalidad de dicha transferencia,
3. la identificación de dicho tercer país u organización internacional,
4. la existencia o ausencia de una decisión de adecuación de la Comisión, o,
5. en el caso de las transferencias indicadas en los artículos 46, 47 o el artículo 49, apartado 1, párrafo segundo del RGPD, se debe hacer referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o acceso al texto y medios de formalización de estas garantías.

El encargado del tratamiento no podrá transferir los datos hasta que reciba conformidad expresa por parte del responsable del tratamiento. Si se produce alguna variación posterior de los datos indicados en la solicitud, el encargado debe obtener de nuevo la autorización del responsable del tratamiento cursando una nueva solicitud de autorización.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembro que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que el Derecho lo prohíba por razones importantes de interés público.

El encargado puede comunicar datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

e) Se autoriza al encargado a subcontratar con consultores y auditores externos las prestaciones que comporten los tratamientos siguientes: servicios de consultoría, soporte y auditoría. Para subcontratar con otras empresas, el encargado debe comunicarlo por escrito al responsable, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de 30 días. El subcontratista, que también tiene la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad, etc.) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

f) Mantener el deber de secreto respecto a los datos personales a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g) Garantizar que las personas autorizadas para tratar datos personales se comprometen de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h) Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j) Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición.
2. Limitación del tratamiento.
3. Portabilidad de los datos.
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección indicada por el responsable. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k) Corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos.

l) Notificación de violaciones de la seguridad de los datos:

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso, antes del plazo máximo de 72 horas las violaciones de la seguridad de los datos personales a su cargo de la que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia. Esta comunicación se realizará de la siguiente forma: enviando un correo electrónico a la dirección que indique el responsable.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella, se facilitará, como mínimo, la información siguiente:

1. Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
2. El nombre y datos de contacto del delegado de protección de datos o del otro punto de contacto en el que pueda obtenerse más información.
3. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

4. Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

m) Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n) Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o) Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p) Implantar las medidas de seguridad siguientes: Medidas de seguridad conforme a las declaraciones de aplicabilidad en vigor del Esquema Nacional de Seguridad en Categoría MEDIA y la Norma ISO/IEC 27001 con extensión ISO/IEC 27701.

En todo caso, deberá implantar mecanismos para:

1. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
2. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
3. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
4. Seudonimizar y cifrar los datos personales, en su caso.

En particular, el encargado del tratamiento garantiza que los datos personales que integre en sus sistemas de tratamiento, por cuenta del responsable, sean albergados en servidores propios o subcontratados, los cuáles:

1. Son seguros, conforme a las exigencias detalladas anteriormente.
2. Están localizados en la Unión Europea (salvo que el responsable del tratamiento haya autorizado expresamente la transferencia de los datos a un tercer país o a una organización internacional, según se detalla en el apartado d) del punto IV de este contrato. En todo caso, la localización fuera de la Unión Europea debe respetar y cumplir estrictamente las condiciones previstas a este respecto en el presente contrato y en el RGPD).

q) Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable.

r) Destino de los datos una vez finalice la prestación de los servicios:

Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

V. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a) Entregar, o permitir el acceso, al encargado los datos a los que se refiere la cláusula II de este documento.

b) En su caso, realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.

c) Realizar las consultas previas que corresponda.

d) Velar, de forma previa y durante el tratamiento, por el cumplimiento del RGPD por parte del encargado.

e) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.