



Contrato de Prestación de Servicios SGSI

Condiciones Generales de Contratación

REUNIDOS

De una parte, el CLIENTE, identificado en las Condiciones Particulares del presente Contrato de Prestación de Servicios SGSI (en adelante, el 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).

LOPDPGDD o LOPDGD: 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.

DPD o DPO: Delegado de Protección de Datos.

AEPD: Agencia Española de Protección de Datos.

SGSI: Sistema de Gestión de la Seguridad de la Información (puede ser bajo la ISO 27001, Esquema Nacional de Seguridad u otro).

Plan de Actuaciones: Documento que recoge el alcance del proyecto a realizar y la planificación de las actuaciones que se llevarán a cabo.

02. Normas sobre las que se ofrece el asesoramiento

La norma/s sobre la/s que se ofrece asesoramiento se indican en las Condiciones Particulares del presente Contrato.

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 se hayan abonado, en fecha, el importe de los pagos acordados.

Se acuerda que la duración del presente contrato quedará estipulada en la planificación de fechas de actuación (Plan de Actuaciones). Este Plan debe ser aprobado por GRUPO CFI y por el CLIENTE. Este contrato no excederá en su duración, más allá del 30% del tiempo total del Plan de Actuaciones.



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 la actividad o actividades contratadas durante el periodo de vigencia del Contrato o de cualquiera de sus prórrogas.

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 a los trabajadores sobre sus obligaciones y derechos en materia de seguridad de la información, 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 entregada es correcta y 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, publicación de políticas, aplicación de procedimientos, gestión de registros, colocación de carteles, implantación de medidas y controles, etc.), en virtud de ser ésta un 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 contrato o del incumplimiento defectuoso del mismo, derivado de una información parcial, incompleta o inexacta, respondiendo el CLIENTE ante la Administración competente, sus trabajadores, 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.

Si la prestación se realizase 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 o 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 o parcial) de la Plataforma Online.

08. Ejecución de los servicios y facturación

Los trabajos darán comienzo una vez haya recibido GRUPO CFI las Condiciones Particulares del Contrato firmadas por el CLIENTE.

Una vez recibido dicho documento, 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 una planificación de fechas en las que se llevarán a cabo las actividades necesarias para el desarrollo del proyecto, así como la elección de formato, presencial o remoto en cada caso. Si la actividad es por videoconferencia, se mandará la convocatoria al correo electrónico indicado por la persona de contacto del CLIENTE.

Esta planificación puede sufrir variaciones a lo largo del proyecto debido a las posibles eventualidades surgidas durante su desarrollo. Estas variaciones serán acordadas por ambas partes dejando constancia de los motivos y los nuevos plazos.



GRUPO CFI elaborará la documentación pertinente, en función de los servicios contratados 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 de la plataforma habilitada para el CLIENTE (canal preferente); b) envío de consultas al correo electrónico de soporte soportegsi@grupocfi.es; c) llamada telefónica al 901 001 802.

La emisión de las facturas y el cobro de las mismas se realizará según lo indicado en las Condiciones Particulares del presente Contrato.

Si el CLIENTE requiere de la presencia de algún Consultor de GRUPO CFI, ya sea física o telemática, para alguna cuestión (como por ejemplo, para que asista a reuniones con la organización o con terceras entidades, o para la revisión detallada de alguna de las medidas), fuera de las acciones estipuladas en el Plan de Actuaciones, el tiempo empleado en dichas actividades será facturado al CLIENTE según las tarifas establecidas.

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. Condiciones económicas y estructura de la entidad

Las condiciones económicas del Contrato, forma de pago y periodo de liquidación por la prestación de los servicios quedan establecidas en las Condiciones Particulares del Contrato.

La cantidad económica que allí se estipula se basa en la información declarada por el CLIENTE (total empleados, sedes y otros elementos variables) y las circunstancias conocidas en la fecha de formalización del Contrato y en sus renovaciones posteriores (en su caso).

No obstante, las Condiciones Particulares, así como todas las estipulaciones en estas Condiciones Generales mantendrán su validez mientras que el CLIENTE no varíe su estructura (número total de empleados, sedes, tipo de información que maneja, y otros elementos variables).

Las variaciones que se produzcan en su estructura deben ser comunicadas por el CLIENTE inmediatamente a GRUPO CFI, y en todo caso, en el plazo máximo de un mes, con objeto de llevar a cabo una modificación de las condiciones contratadas por las partes, en aras de posibilitar la eficaz prestación de las actividades objeto del Contrato.

Si al realizar la prestación del servicio se detecta que la estructura declarada por el CLIENTE difiere de la realidad, el contrato se actualizará, en base a la estructura real de la entidad en ese momento o, en su caso, se rescindirá si GRUPO CFI observa que la diferencia entre la realidad y lo declarado es tal que esto invalida la propuesta económica realizada.

Asimismo, el importe de la cuota a abonar por los servicios continuados renovables anualmente podrá ser actualizado en los periodos de duración de este contrato según las variaciones que se produzcan en el IPC (Índice de Precios al Consumo), además de los cambios que de un periodo a otro se produzcan en la estructura de la entidad o servicios a prestar.

11. Política de devoluciones

Cuando la forma de pago elegida sea domiciliación bancaria, la devolución de cada factura pasada al cobro conllevará unos gastos de un 2% del importe de la factura girada, con un mínimo de 8,50€ en concepto de gastos de gestión.

12. Suspensión de los servicios

El retraso en el pago del precio acordado, sea total o parcial, o de cualquiera de los plazos previstos para ello, implicará la suspensión automática de la vigencia del Contrato y de todos los servicios desde la fecha en que se produjo el impago, sin que la regularización de la situación implique recuperar dichos servicios de forma retroactiva, y sin necesidad de comunicación en tal sentido por parte de GRUPO CFI, que podrá suspender inmediatamente la ejecución de las actividades, accesos a documentación y funciones objeto del Contrato en el estado en que se encuentren, exonerándose a GRUPO CFI de cualquier obligación o responsabilidad derivada de la falta de ejecución total o parcial de los servicios, respondiendo por este hecho el CLIENTE ante la Administración competente, sus trabajadores, socios y colaboradores o terceros.

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 existiesen servicios



pendientes de pago por parte del CLIENTE, deberán ser abonados a GRUPO CFI. Así mismo, se acuerda que, independientemente de los importes de los servicios antes señalados, en ningún caso procederá la devolución del importe ya facturado por GRUPO CFI.

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 existiesen servicios pendientes de pago por parte del CLIENTE, deberán ser abonados a GRUPO CFI. Así mismo, se acuerda que, independientemente de los importes de los servicios antes señalados, en ningún caso procederá la devolución del importe ya facturado por GRUPO CFI.

15. Condiciones no recogidas inicialmente o actualización de condiciones

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.

En caso de que exista una actualización de las presentes Condiciones Generales, se notificará al CLIENTE en la cuenta de correo electrónico de contacto facilitada, y en todo caso quedarán publicadas en la página web de GRUPO CFI. En dicha notificación se indicará al CLIENTE dónde puede consultar las nuevas condiciones y la fecha de su entrada en vigor. Si el CLIENTE no manifiesta su disconformidad con los cambios antes del comienzo de su entrada en vigor, se entenderá que acepta las nuevas condiciones.

En caso de que el CLIENTE no esté de acuerdo con las nuevas condiciones, puede rescindir este contrato según lo estipulado en el punto 13.

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 de la situación del SGSI 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. Consultoría personalizada

Incluye la realización de la/s toma/s de datos necesaria/s para prestar el servicio y elaborar documentación requerida para la implantación de la Norma o Normas indicadas en las Condiciones Particulares del Contrato.

Comprende la toma de datos por los medios pactados (principalmente en remoto, salvo las visitas presenciales que sean necesarias para realizar, en su caso, la auditoría del sistema), revisión de documentación, evaluación de riesgos, determinación de flujos de datos y procesos, determinación de controles a aplicar y aquellos análisis necesarios para realizar la implantación de las Normas. No está incluida la implantación de la normativa de protección de datos personales, servicio que, en su caso, sería objeto de la firma de un acuerdo específico.

A tal efecto, el CLIENTE debe facilitar a GRUPO CFI toda la información que le solicite para poder llevar a cabo el servicio.

GRUPO CFI elaborará un Plan de Actuaciones, que debe ser aprobado por el CLIENTE, para la correcta ejecución del proyecto. Si fuera necesario modificar el Plan de Actuaciones, se informará al CLIENTE de las nuevas fechas de ejecución, debidamente motivadas. Asimismo, estas modificaciones también deberán ser aprobadas por el CLIENTE.

II. Evaluación de riesgos

Consiste en la realización del análisis de riesgos exigido, en función de los distintos activos que tenga la organización, y la identificación de los controles que el CLIENTE debe aplicar para mitigarlos.

Es responsabilidad exclusiva del CLIENTE la aplicación de los controles y las medidas de seguridad, técnicas y organizativas indicadas por GRUPO CFI para una eficaz mitigación de los riesgos identificados.

III. Elaboración de la documentación del SGSI

Se realizará la elaboración de la documentación necesaria para cumplir con los requisitos de la Norma o Normas a implantar indicadas en las Condiciones Particulares del Contrato.

En concreto, se elaborará y entregará la siguiente documentación:

- Análisis del Contexto de la organización (solo para ISO 27001).
- Categorización de los sistemas (solo para Esquema Nacional de Seguridad).
- Identificación y documentación de procesos y activos.
- Análisis de riesgos.
- Declaración de Aplicabilidad.
- Plan de tratamiento de riesgos.
- Políticas de seguridad.
- Procedimientos de seguridad.

Dentro de la documentación que GRUPO CFI elaborará no están incluidas las instrucciones técnicas que pudiesen ser necesarias, pues son documentos muy específicos de las tecnologías empleadas y que, necesariamente, debe elaborar el CLIENTE.

Queda bajo responsabilidad exclusiva del CLIENTE, la firma de los contratos y compromisos proporcionados, publicación de políticas, aplicación de los procedimientos, los controles y las medidas de seguridad, y los protocolos correspondientes, así como la comunicación de los cambios que se produzcan en la organización del CLIENTE a GRUPO CFI para que pueda elaborar o modificar la documentación que sea necesaria para el correcto cumplimiento de la Norma correspondiente.

La documentación se facilitará a través del envío de unas credenciales de acceso a una plataforma online para la puesta a disposición, de forma segura, de toda esta documentación al CLIENTE o se enviará por otro medio acordado. El receptor de estas credenciales de acceso es responsable de su uso y custodia.

IV. Asesoramiento en la implantación de controles

Se ofrecerá asesoramiento telefónico o por correo electrónico al CLIENTE en la implantación de los controles y medidas de seguridad identificadas en la evaluación de riesgos.

Este servicio se limita a asesoramiento. GRUPO CFI no realizará la implantación efectiva de ninguno de los controles y medidas de seguridad técnicas que el CLIENTE deba implantar. A tal efecto, GRUPO CFI no instalará ni configurará aplicaciones, servicios, permisos u otras intervenciones técnicas similares. Intervenciones que debe realizar, en exclusiva, el CLIENTE.

V. Acompañamiento y asistencia en la auditoría interna del SGSI

Consiste en el acompañamiento, asesoramiento y asistencia al personal auditor designado por el CLIENTE para la realización de la auditoría interna, previa a la certificación. El acompañamiento se realizará de forma remota o presencial a criterio de GRUPO CFI.

VI. Acompañamiento y asistencia en la auditoría de certificación SGSI

Consiste en el acompañamiento al personal del CLIENTE en la auditoría de certificación de tercera parte para la obtención del certificado correspondiente. El acompañamiento se realizará de forma remota y/o presencial, según criterio de la entidad certificadora.

VII. Formación al personal

Consiste en proporcionar el acceso a los cursos indicados en las Condiciones Particulares del Contrato al número de personas indicadas en dichas Condiciones.



La formación se impartirá en modalidad online, pudiendo acceder el personal en cualquier momento a través de Internet, mediante identificador y contraseña, en la plataforma de formación gestionada por GRUPO CFI.

VIII. Plataforma online de gestión del SGSI

Consiste en proporcionar el acceso en modo SaaS a una plataforma para gestionar el SGSI durante el primer año, a contar desde la fecha de firma del contrato. La renovación de la licencia de acceso a la plataforma de gestión SGSI, a partir del segundo año y siguientes a la firma del contrato, será facturada en periodos anuales según tarifa, indicada en las Condiciones Particulares, con las variaciones estipuladas en el punto 10 de las presentes Condiciones Generales.

La adquisición del derecho de uso únicamente otorga el uso de la plataforma al CLIENTE por un periodo de tiempo limitado, siendo siempre el software propiedad de GRUPO CFI y estando en todo momento en los servidores de GRUPO CFI.

Es requisito imprescindible para el uso de la plataforma que el CLIENTE disponga de conexión a Internet y navegador.

IX. Seguro de Responsabilidad Civil (1.000.000 €)

Este Contrato está cubierto por un seguro de Responsabilidad Civil de hasta 1.000.000 €. Dicho seguro cubre los daños y perjuicios que se puedan ocasionar a un CLIENTE, causados por un posible error o negligencia por parte de GRUPO CFI, en la ejecución de los trabajos objeto del presente Contrato.



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 suscrito 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 de carácter personal necesarios para prestar los servicios de consultoría y auditoría.

El tratamiento consistirá en: servicios de consultoría y auditoría en el ámbito de la gestión de la seguridad de la información y la ciberseguridad, en general.

Los servicios concretos se recogen en el Contrato principal suscrito con el responsable del tratamiento.

Concreción de las operaciones a realizar: registro, conservación; consulta, modificación.

La prestación de los servicios puede ser en los locales del responsable del tratamiento, en los locales del encargado del tratamiento o de forma remota. Igualmente, el encargado del tratamiento puede incorporar datos del responsable del tratamiento en sus sistemas.

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 de personal y/o socios.
- d) Datos alojados en los sistemas del responsable del tratamiento.

Los datos concretos afectados dependerán de los servicios contratados por el responsable del tratamiento.

La puesta a disposición de la información indicada anteriormente puede realizarse, bien proporcionando al encargado la información indicada, bien permitiéndole 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 es: Indefinida.

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:
 - 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.
 - Las categorías de tratamientos efectuados por cuenta de cada responsable.
 - 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.
 - 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.



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.

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.

- e) Se autoriza al encargado a subcontratar cualesquiera de los servicios ofrecidos al CLIENTE con las empresas que sean más idóneas para su prestación (la relación de empresas a las que, en su caso, se podrían subcontratar servicios se puede solicitar en cualquier momento a dpd@grupocfi.es). 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 14 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 facilitada por el responsable del tratamiento (en caso de que no haya facilitado ninguna dirección en particular, se asumirá que es la que aparece en las Condiciones Particulares del Contrato). 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 del tratamiento 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 36 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 facilitada por el responsable (en caso de que no haya facilitado ninguna dirección en particular, se asumirá que es la que aparece en las Condiciones Particulares del Contrato).

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 del tratamiento 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 de acuerdo con la evaluación de riesgos realizada por el encargado del tratamiento:

1. Entorno seguro: los locales donde se tratan los datos deben contar con medios mínimos de seguridad como extintores, alarmas, etc.
2. Funciones y obligaciones del personal: las funciones y obligaciones de cada uno de los usuarios o perfiles de usuario con acceso a datos y a los sistemas estarán claramente definidas y documentadas.
3. Control de acceso: el personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. Se deberán establecer mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Identificación y autenticación: se establecerá un sistema que permita la identificación inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información, y la debida autenticación para verificar la identidad del usuario.
5. Almacenamiento seguro de soportes y documentos: los dispositivos de almacenamiento de los soportes y documentos que contengan datos personales, deberán disponer de mecanismos que obstaculicen su apertura, mediante llaves u otros medios similares.
6. Software anti-malware: en los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema anti-malware que evite, en la medida de lo posible, el robo y la destrucción de la información y los datos.
7. Copias de respaldo: se realizarán copias de respaldo periódicamente, en función del volumen y de la frecuencia de actualización de los datos.
8. Destrucción y reutilización de equipos y soportes: los desechos informáticos, de cualquier tipo, que puedan contener datos personales, deberán ser eliminados o destruidos de forma segura para garantizar que no se va a poder acceder a ellos.
9. Traslado seguro de soportes y documentos: cuando los soportes y/o documentos salgan fuera de los locales de tratamiento, se adoptarán las medidas necesarias para impedir la sustracción, pérdida o acceso indebido a la información durante el transporte.
10. Acceso a través de redes de comunicaciones: los accesos a los datos de personales realizados a través de redes de comunicaciones, sean o no públicas, deberán realizarse de forma segura.

En todo caso, deberá implantar mecanismos para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
 - Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
 - Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
 - Seudonimizar y cifrar los datos personales, en su caso.
- q) El encargado del tratamiento dispondrá de un delegado de protección de datos designado, con el que se podrá contactar a través de estos medios:
 - En la dirección <https://grupocfi.es/dpd>
 - En el correo electrónico dpd@grupocfi.es
 - En el teléfono 901 001 802

- 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 del tratamiento debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento. No obstante, el encargado del tratamiento 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 auditoría.