
POLÍTICA SOBRE EL TRATAMIENTO Y SEGURIDAD DE LA INFORMACIÓN CONFIDENCIAL

4 de noviembre de 2020

1. Introducción y finalidad

El grupo de sociedades cuya entidad dominante, en el sentido establecido por la ley, es “Cofares Sociedad Cooperativa Farmacéutica Española” (el “**Grupo Cofares**” o el “**Grupo**” y “**Cofares**” o la “**Cooperativa**”, respectivamente) es un referente en el sector sanitario y una de las principales empresas de distribución de medicamentos en España.

El Consejo Rector de la Cooperativa, consciente del papel fundamental que la información del Grupo Cofares y sus activos juegan en la consecución de sus objetivos empresariales, y teniendo en cuenta los avances tecnológicos y el alto grado de interconexión, ha aprobado la presente *Política sobre el tratamiento y seguridad de la información confidencial* (la “**Política**”), con objeto de que la información del Grupo Cofares goce de las máximas garantías de seguridad y privacidad.

En este sentido, esta Política establece una serie de normas con la finalidad de: (i) reducir el riesgo de accesos no autorizados, fuga, alteración o destrucción de la Información Confidencial (según este término se define más adelante); (ii) prevenir la revelación de secretarios; (iii) facilitar la localización de la información; y (iv) minimizar el riesgo de incumplimiento legal.

2. Definiciones

Salvo que se encuentren definidos en el articulado de esta Política, los términos que aparecen en mayúsculas tendrán el significado que se les atribuye en el **Anexo 1**.

3. Ámbito de aplicación

Esta Política resulta aplicable a: (i) los socios de Cofares; (ii) todos los administradores de las sociedades y entidades que integran el Grupo Cofares, incluyendo a las personas físicas que designen los administradores personas jurídicas para representarlos en el ejercicio de su cargo; (iii) los patronos, directivos y empleados de la Fundación Cofares y quienes representen a cualquier sociedad o entidad del Grupo Cofares en asociaciones empresariales y otras entidades u organismos, tanto nacionales como internacionales; (iv) cualesquiera miembros de otros órganos sociales y comités; y a (v) los Profesionales (las “**Personas Obligadas**”).

Las Personas Obligadas que, en el desempeño de sus funciones, gestionen o dirijan equipos de personas deberán velar por que los empleados directamente a su cargo conozcan y cumplan esta Política.

4. Interpretación

Corresponde al Comité resolver cualesquiera consultas o dudas relacionadas con el contenido, interpretación, aplicación o cumplimiento de esta *Política*. Asimismo, el Comité podrá establecer y modificar criterios, definiciones y procedimientos en relación con esta *Política* cuando ello fuese necesario para su correcta interpretación e implementación.

5. La Información Confidencial

5.1. Definición de Información Confidencial

Tendrá la consideración de “**Información Confidencial**” toda documentación e información (de tipo económico, financiero, técnico, comercial, estratégico o de otro tipo) que se refiera directa o indirectamente al Grupo y que hubiese sido obtenida, de cualquier forma (oral, escrita o en cualquier soporte) y en cualquier momento, incluso de manera fortuita, por cualquier Persona Obligada como consecuencia o no del ejercicio de su cargo.

En particular, la Información Confidencial comprende, pero no se limita a, toda documentación e información: (i) marcada como tal; (ii) identificada por el Grupo, sus Órganos de Dirección o las Personas Obligadas, bien de forma escrita o bien de forma verbal, como Información Confidencial; (iii) que no sea conocida en el mercado o la industria; o (iv) que por su naturaleza o por las circunstancias en que se produzca la revelación, deba de buena fe estimarse como tal.

No tendrá la consideración de Información Confidencial la que sea pública o llegue a ser pública, salvo que adquiera este carácter a causa de un incumplimiento de las obligaciones contractuales, estatutarias, profesionales o de cualquier otro tipo, imputable a una Persona Obligada.

En caso de duda sobre si una información tiene carácter de Información Confidencial, se deberá consultar al superior jerárquico, a la persona responsable de clasificar la información interna del Grupo Cofares y velar por su seguridad y su custodia o al Comité.

5.2. Un tipo de Información Confidencial: la Información Reservada

La “**Información Reservada**” es la Información Confidencial altamente sensible o especialmente valiosa, cuya divulgación (tanto interna como externa), relevación o destrucción no autorizada podría causar: (i) un perjuicio grave para el Grupo Cofares, pérdidas financieras, pérdida significativa de la confianza de sus clientes, pérdida de cuota de mercado y daños reputacionales; o (ii) un incumplimiento legal o regulatorio con sanción.

Se entenderá, sin carácter limitativo, que una información es altamente sensible o especialmente valiosa cuando se refiera a modificaciones estructurales o corporativas del Grupo o a operaciones o hechos que puedan tener un impacto en sus cuentas consolidadas de, al menos, un importe equivalente al 1 % de la cifra de negocios a nivel consolidado (a la fecha de aprobación de esta Política, el 1 % de la cifra de negocios asciende a, aproximadamente, 35 millones de euros).

5.3. Principios básicos en relación con la protección de la Información Confidencial

La protección de la seguridad e integridad de la Información Confidencial se llevará a cabo de acuerdo con los siguientes principios básicos de actuación:

- (a) Cumplir la legislación vigente que resulte aplicable en materia de seguridad, privacidad y protección de datos de carácter personal.
- (b) Aplicar el *Código de Conducta* y las demás políticas y normas internas del Grupo Cofares.
- (c) Establecer niveles adecuados de acceso a los sistemas del Grupo Cofares, de tal manera que los Usuarios únicamente puedan acceder a la información y a los recursos que sean estrictamente necesarios para el desempeño de sus funciones.
- (d) Posibilitar y desplegar la trazabilidad al acceso de la información, de forma tal que en caso de un mal uso o filtración existan medidas adoptadas para conocer el origen.
- (e) Incorporar la gestión del riesgo en la toma de decisiones relativas a la protección de la seguridad y la integridad de la Información Confidencial y establecer medidas de mitigación del riesgo.
- (f) Mantener un nivel de protección de la Información Confidencial que sea adecuado para garantizar la continuidad del negocio.
- (g) Proporcionar formación adecuada sobre esta Política y asegurar su divulgación entre las personas a las que resulta aplicable.
- (h) Introducir, implementar y revisar los protocolos y su divulgación para lograr una correcta aplicación de esta Política, así como de las normas y demás instrucciones que la desarrollen.

6. Obligaciones relativas a la Información Confidencial

6.1. Obligaciones generales

Las personas referidas en el apartado 3 que dispongan de Información Confidencial deberán:

- (a) Guardar secreto de la Información Confidencial y salvaguardar su confidencialidad, sin perjuicio de su deber de comunicación y colaboración con las autoridades judiciales y administrativas en los términos previstos en la legislación aplicable.
- (b) No revelar Información Confidencial, incluso a otras personas a las que resulte aplicable la presente Política cuando no sea imprescindible para el desarrollo de la actividad corporativa o profesional, o usarla para fines propios o de cualquier tercero, sin perjuicio de las obligaciones de transparencia que imponga la legislación aplicable.
- (c) Adoptar las medidas adecuadas para evitar que la Información Confidencial pueda ser objeto de utilización abusiva, ilícita o desleal.
- (d) Comunicar al Responsable de la Oficina de Cumplimiento, de forma inmediata, cualquier uso abusivo, ilícito o desleal, pérdida, extravío, hurto o robo de Información Confidencial del que tengan conocimiento. Asimismo, en caso de que dicha Información Confidencial

contenga datos personales, también se informará al Delegado de Protección de Datos (DPO).

A efectos aclaratorios, en caso de pérdida, extravío, hurto o robo de cualquier dispositivo proporcionado por el Grupo Cofares no hará falta informar al Responsable de la Oficina de Cumplimiento de esta circunstancia y se seguirá lo dispuesto en el artículo 3.3 del *Protocolo para la utilización e intervención de dispositivos informáticos*, que exige que se ponga en conocimiento del Área de Sistemas (cuyos datos de contacto son omadrid@cofares.es o 625 36 26 34).

Estas obligaciones de confidencialidad tienen carácter indefinido y, por tanto, el deber de reserva perdura incluso después de haberse resuelto el vínculo con el Grupo Cofares. La quiebra de ese deber permitirá al Grupo Cofares adoptar las medidas judiciales o de otro tipo a las que tenga derecho y a reclamar las indemnizaciones y daños y perjuicios que correspondan.

6.2. Obligaciones relativas a la protección de la Información Confidencial

A continuación, se establecen las directrices para la protección de la Información Confidencial desde su creación u obtención hasta que deje de tener esta condición, en función del tipo de soporte. Deberá tenerse en cuenta que si la información contiene datos de carácter personal se deberán cumplir cualquiera otros requerimientos previstos en el Reglamento General de Protección de Datos.

6.2.1. Documentos electrónicos

Los requisitos de seguridad aplicables a los documentos *office* (Word, PowerPoint, Excel, etc.), PDFs, ficheros multimedia y otros documentos electrónicos que contengan Información Confidencial, son los siguientes:

- (a) Se prohíbe el envío de Información Confidencial del Grupo Cofares a cuentas de correo electrónico personales o mediante aplicaciones de mensajería multimedia no corporativas.
- (b) Las personas a las que resulta aplicable esta Política utilizarán los espacios de archivo corporativos de los ordenadores, tanto portátiles como no, (frente al archivo de documentación en el disco duro local de dichos ordenadores) para el almacenamiento de Información Confidencial.

En caso de que temporalmente sea necesario archivar la Información Confidencial en el disco duro local de los ordenadores, tan pronto como sea posible: (i) se deberá guardar dicha información en un espacio de archivo corporativo; y (ii) borrarla del espacio personal.

- (c) En ningún caso se podrá archivar Información Reservada en los discos duros de los ordenadores personales.
- (d) Las personas a las que resulte aplicable esta Política tendrán la máxima precaución para evitar que personas que no tengan acceso a la Información Confidencial que manejan puedan ver los documentos confidenciales mientras estén trabajando con ellos desde el ordenador, el teléfono móvil o cualquier otro dispositivo.

- (e) En ningún caso se emplearán lápices de memoria o memorias USB para almacenar o transmitir Información Confidencial, salvo con la expresa autorización escrita del Director del Área.
- (f) Los dispositivos de almacenamiento no deberán dejarse abandonados, a la vista, sobre mesas, salas de reuniones o cualquier otro lugar interno o externo. En caso de ausencias prolongadas de la Persona Obligada, se deberán guardar en armarios con llave.
- (g) Los documentos confidenciales deberán imprimirse en impresoras del Grupo, mediante el mecanismo de identificación personal para imprimir puesto a disposición de las Personas Obligadas, y se deberán recoger y custodiar inmediatamente después de su impresión.
- (h) En caso de que cualquier Persona Obligada reciba, por error, Información Confidencial que no iba dirigida a él, se lo notificará al remitente y procederá a su borrado.
- (i) La Información Confidencial será accesible solamente para un grupo limitado de Personas Obligadas, controlado y validado por el Propietario la Información. El Propietario de la Información deberá ser notificado inmediatamente en caso de pérdida o robo de la Información Confidencial.

6.2.2. Documentos en papel

A continuación, se indican los requisitos de seguridad aplicables a la Información Confidencial contenida en documentos en papel:

- (a) La documentación en papel no deberá dejarse abandonada, a la vista, sobre mesas, salas de reuniones o cualquier otro lugar interno o externo. Esta documentación deberá guardarse en zonas de acceso restringido (tales como despachos y archivos) y depositarse en archivadores (que, como regla general, deberán permanecer cerrados). En caso de ausencias prolongadas de la Persona Obligada se deberá guardar en armarios cerrados con llave.
- (b) En caso de utilizar una pizarra o similar en salas de reuniones, la información deberá ser borrada antes de abandonar la sala.
- (c) Se recomienda realizar copias únicamente en caso de resultar necesario. Asimismo, solo se podrán utilizar impresoras que pertenezcan al Grupo Cofares para imprimir o escanear. Cuando por motivos de urgencia o necesidad se deban imprimir documentos confidenciales en impresoras no corporativas, se deberá solicitar autorización previa al Director del Área de Sistemas.
- (d) Los documentos deberán enviarse en cajas o sobres cerrados de un solo uso (con la posibilidad de detectar si han sido abiertos), a la atención de personas concretas (evitando utilizar destinatarios genéricos) y con una marca indicando la naturaleza de la información que contiene (por ejemplo, "INFORMACIÓN CONFIDENCIAL"). La recogida y entrega de los documentos confidenciales deberá realizarse en mano, evitando depositarla en bandejas o en la mesa del destinatario sin estar este presente.

En los envíos al exterior, sea a otros edificios del Grupo Cofares o no, el transporte de los documentos confidenciales deberá realizarse con medidas que garanticen su transporte seguro. Si el envío se realiza fuera del Grupo se deberá llevar a cabo a través de mensajero, con albarán de entrega.

Se recomienda remitir un correo electrónico al receptor para advertirle, con carácter previo, del envío de documentación confidencial por correo postal y solicitarle que confirme su recepción. En caso de pérdida, hurto o robo, el receptor deberá comunicárselo inmediatamente al remitente y al Propietario de la Información.

- (e) Se deberá evitar el uso del fax como medio de transmisión de Información Confidencial. En caso de ser imprescindible su uso, deberá avisarse al destinatario en el momento del envío para asegurarse de que recoge el documento en el mismo momento de su impresión en destino.
- (f) En caso de que alguien reciba documentación del Grupo Cofares por error, se lo notificará al remitente y le devolverá la documentación en papel con las medidas de protección que se recogen en la presente Política.
- (g) En los viajes, se tendrá la máxima precaución en lugares y transportes públicos para evitar el olvido, extravío o robo de los documentos confidenciales e impedir que otras personas puedan ver su contenido de forma accidental o intencionada.

En particular, las Personas Obligadas deberán mantener los documentos confidenciales bajo su control en todo momento, evitando depositarlos en equipajes que vayan a facturarse, dejarlos en el interior de un vehículo o en una habitación de hotel al ausentarse de ella. Si fuera imprescindible dejar los documentos confidenciales en un hotel, se deberá hacer uso de la caja fuerte.

6.3. Obligaciones relativas al etiquetado de la Información Confidencial¹

El Propietario de la Información deberá clasificar y etiquetar los documentos (electrónicos o en papel) que contentan Información Confidencial en el momento de su creación (indicando si se trata de Información Confidencial o de Información Reservada) de tal manera que cualquier persona que acceda a ellos pueda conocer el nivel de protección requerido.

El Propietario de la Información deberá analizar el tipo de información para garantizar que el nivel de protección no sea demasiado alto (con objeto de evitar controles excesivos que perjudiquen la eficiencia operativa) ni demasiado bajo (lo que podría comprometer la confidencialidad de la información).

Asimismo, se aplicarán las siguientes reglas:

- (a) Ninguna persona distinta del Propietario de la Información podrá modificar o eliminar el etiquetado sin la autorización previa y por escrito del Propietario de la Información.

¹ Las obligaciones previstas en este apartado 6.3 entrará en vigor el 1 de enero de 2022.

- (b) El Propietario de la Información será responsable de actualizar, en caso de que fuese necesario, la clasificación y el etiquetado del documento.
- (c) En función del tipo y soporte de la información, la clasificación, la identificación del Propietario de la Información y la fecha de creación, deberán ser incluidos en:
 - Documentos: en el encabezamiento o pie del documento, en todas las páginas.
 - Correos electrónicos: en el asunto del correo.
 - Conversaciones: el receptor de la información deberá ser informado, de forma previa, si la información que va a recibir es confidencial o reservada y si requiere alguna cautela específica.

Adicionalmente, la Información Confidencial o Reservada que incluya datos de carácter personal: (i) será etiquetada como “Contiene Datos Personales” o “Datos Personales Sensibles”; y (ii) deberá cumplir las disposiciones vigentes sobre protección de datos personales que resulten de aplicación.

6.4. Determinación del período de retención

A continuación, se establecen las reglas para, en función del tipo de soporte, fijar el período de tiempo en el que será necesario guardar los documentos que contengan Información Confidencial:

- (a) Para los documentos *office* (Word, PowerPoint, Excel, etc.), PDFs, ficheros multimedia, otros documentos electrónicos y documentación en papel, cada área de negocio o función corporativa establecerá su propio esquema de retención de la información conforme a los siguientes requisitos:
 - Criterios de negocio: el período durante el cual se considera que la información tiene relevancia para el negocio o la función corporativa de que se trate.
 - Criterios legales: período de tiempo adicional en el que es necesario guardar la información para cumplir determinados requisitos legales o para atender posibles inspecciones, reclamaciones o demandas judiciales. Para la determinación de estos criterios, se contará con la colaboración de la Asesoría Jurídica de Cofares.

La fecha de creación de cada documento deberá incluirse en su encabezamiento o en el pie de página, de tal manera que, una vez fijado el período de retención de cada documento, sea posible determinar la fecha de borrado o eliminación.

- (b) En el caso de los correos electrónicos corporativos, el período de retención será de 5 años, salvo en caso de inspecciones, requerimientos o demandas judiciales, en cuyo caso deberán almacenarse en espacios de almacenamiento o redes corporativos, que podrán tener un plazo de retención más alto.

6.5. Transmisión de Información Confidencial a terceros

La transmisión de Información Confidencial a los Receptores Externos deberá restringirse a aquellos supuestos en los que resulte imprescindible y se ajustará a lo dispuesto en este apartado:

- (a) Con anterioridad a la transmisión de cualquier Información Confidencial, los Receptores Externos deberán ser informados y conocedores de las medidas de clasificación, retención, protección y destrucción recogidas en esta Política.
- (b) De forma previa a la firma de cualquier contrato con un Receptor Externo, se deberá realizar un análisis del tipo de información que se va a compartir y generar durante la relación contractual y los riesgos asociados.
- (c) Los Receptores Externos deberán suscribir un compromiso de confidencialidad con la entidad del Grupo de que se trate, salvo cuando el Receptor Externo esté sometido a un régimen legal o contractual que recoja el deber de confidencialidad. Se incorpora como **Anexo 2** el modelo de acuerdo de confidencialidad con las cláusulas que, al menos, deberán tener los contratos que se suscriban con los Receptores Externos de conformidad con lo previsto en este apartado.

En todo caso, los Receptores Externos serán informados y deberán manifestar, al menos, que conocen el carácter confidencial de la información transmitida, así como que disponen de los medios necesarios para garantizar dicho carácter. Cuando se les transmita Información Reservada, se les informará, adicionalmente, de su inclusión en el Registro de Iniciados (salvo que el Receptor Externo lleve su propio Registro de Iniciados y así se lo indique, por escrito, a la sociedad del Grupo que corresponda).

Se exigirá, asimismo, la firma de dicho compromiso de confidencialidad a aquellos Receptores Externos con los que se contacte en una fase preliminar y a los que se presenten las líneas generales de una operación para solicitar ofertas de financiación o asesoramiento, aunque finalmente no participen en la misma.

- (d) El Director del Área podrá condicionar su transmisión electrónica a los Receptores Externos a la encriptación de los documentos confidenciales a través de cualquier procedimiento informático que restrinja el acceso a la Información Confidencial a los Receptores Externos.
- (e) Antes de enviar cualquier documento (electrónico o en papel) con Información Confidencial o Reservada, se deberá verificar que el documento está debidamente etiquetado de acuerdo con lo dispuesto en el apartado 6.3.
- (f) Cuando se considere conveniente o necesario, se realizarán auditorías de terceros con objeto de verificar que estos cuentan con controles que protejan adecuadamente la información que el Grupo Cofares comparte con ellos.
- (g) Una vez finalice el contrato que vincula al Receptor Externo con alguna entidad o sociedad del Grupo Cofares, el tercero deberá eliminar (remitiendo el correspondiente certificado) o devolver toda la información que el Grupo Cofares le hubiera proporcionado.

- (h) En el caso de que el tercero trate datos de carácter personal como encargado de tratamiento, deberá cumplir lo dispuesto en el Reglamento General de Protección de Datos.

6.6. Eliminación de la Información Confidencial

Finalizado el período de retención, la Información Confidencial deberá borrarse o destruirse de forma segura, en función del tipo de soporte.

- (a) En el caso de los documentos de *office* (Word, PowerPoint, Excel, etc.), PDFs, ficheros multimedia y otros documentos electrónicos: (i) la información almacenada en directorios o recursos corporativos, se borrará una vez finalizado el período de retención; (ii) los correos electrónicos se borrarán automáticamente una vez superados los 5 años; y (iii) si se retira un dispositivo corporativo (disco, portátil, teléfono móvil, tablet, etc.) con información del Grupo Cofares o si se va a cambiar su Usuario, el Área de Sistemas del Grupo Cofares deberá eliminarla, utilizando una herramienta de borrado seguro.
- (b) En cuanto a la información en papel: (i) finalizado el período de retención, los documentos que ya no sean necesarios deberán ser eliminados de forma responsable mediante el uso de destructoras de papel o contenedores destinados a la destrucción de papel; (ii) sin perjuicio de lo dispuesto en el párrafo siguiente, la destrucción de documentación e Información Confidencial será llevada a cabo por personal autorizado, utilizando mecanismos que imposibiliten su reconstrucción; y (iii) cuando se utilice un servicio de destrucción externo, en el contrato que se suscriba con el proveedor de este servicio deberán incluirse cláusulas que garanticen la confidencialidad de la documentación a la que tenga acceso y el Propietario de la Información requerirá la expedición de un certificado acreditativo de la destrucción segura de los documentos confidenciales por parte del agente externo.

A los efectos de lo dispuesto en este apartado, deberá tener en cuenta que no solo han de destruirse versiones definitivas de los documentos confidenciales, sino también todos los borradores, copias, extractos y demás documentos de trabajo que contengan Información Confidencial.

6.7. Protección de conversaciones

Las conversaciones que las que se trate Información Confidencial se llevarán a cabo con las cautelas que sean necesarias para garantizar el adecuado aislamiento acústico y visual y evitar irrupciones imprevistas de personas que no tengan acceso a dicha información. No deberán enviarse nunca mensajes de voz que traten sobre Información Confidencial.

7. Protocolo de actuación en caso de filtración o uso ilícito de Información Confidencial

En el supuesto de que cualquier Persona Obligada detecte una posible filtración o un uso ilícito de Información Confidencial, se procederá conforme a lo dispuesto seguidamente:

- (a) El denunciante trasladará, lo antes posible, la filtración o uso ilícito de Información Confidencial del que haya tenido conocimiento al Comité por cualquiera de los canales previstos en el artículo 2.4.3. del *Código de conducta* de Cofares.
- (b) El Comité analizará y comprobará la veracidad de la información proporcionada por el denunciante, a cuyos efectos podrá solicitar a cualquier dirección o área del Grupo aquellos datos e informaciones adicionales que estime necesarios.
- (c) Si la filtración o uso ilícito de la Información Confidencial es atribuible a un miembro del Consejo Rector de Cofares o a su Director General, el Comité lo pondrá en conocimiento del Consejo Rector, quien, a propuesta del Comité, valorará la conveniencia de abrir un expediente disciplinario.

Asimismo, si dicha filtración o uso ilícito es atribuible a un administrador, consejero o cargo equivalente de cualquier entidad o sociedad del Grupo distinta de Cofares, el Comité lo pondrá en conocimiento del órgano de administración que corresponda para que aplique las medidas disciplinarias previstas en su normativa interna y en el *Programa de cumplimiento* del Grupo.

- (d) En el supuesto de que el Comité considere que la filtración o uso ilícito de la Información Confidencial es atribuible a algún Profesional del Grupo, el Comité lo pondrá en conocimiento de la Dirección de Recursos Humanos de Cofares (o del área o dirección que asuma funciones equivalentes en la sociedad del grupo de que se trate), que aplicará las medidas disciplinarias conforme al régimen de faltas y sanciones previsto en el Convenio Colectivo aplicable a la entidad del Grupo a la que pertenezca dicho empleado o en la legislación laboral que resulte de aplicación. Asimismo, evaluará la procedencia de emprender, en su caso, las acciones legales que correspondan contra el Profesional responsable de la filtración o uso ilícito de la Información Confidencial, conforme a la legislación vigente en cada momento.
- (e) Finalmente, en el supuesto de que la filtración o uso ilícito de la Información Confidencial sea atribuible a un Receptor Externo o a cualquier otra persona o entidad ajena al Grupo, el Comité lo pondrá en conocimiento de la Asesoría Jurídica de Cofares con el objeto de determinar la adopción de las medidas que se estimen convenientes respecto de la persona o entidad responsable de la filtración o uso ilícito de la Información Confidencial.
- (f) Sin perjuicio de lo anterior, si, como consecuencia de una filtración o uso ilícito de Información Confidencial, se generasen noticias o rumores relativos a una Información Confidencial que no haya sido previamente publicada, resultarán de aplicación, asimismo, las disposiciones contenidas en la *Política de comunicación y gestión de rumores* (o cualquier otra norma que la sustituya en cada momento). Asimismo, en caso de que dicha Información

Confidencial contenga datos personales, también se informará de la filtración al Delegado de Protección de Datos (DPO).

8. Medidas adicionales aplicables a la protección de la Información Reservada

8.1. Clasificación de la Información Confidencial como Información Reservada

- (a) Cuando el Propietario de la Información, clasifique cierta información como Información Reservada, deberá comunicárselo al Comité a la mayor brevedad posible, mediante la remisión de un correo electrónico al responsable de la Asesoría Jurídica de Cofares que sea en cada momento miembro del Comité.
- (b) La Información Reservada dejará de tener esta consideración cuando: (a) deje de ser Información Confidencial; o (b) así lo decida el Comité, a propuesta del Propietario de la Información. En caso de que el Comité rechace la propuesta del Propietario de la Información, deberá fundar debidamente su decisión y explicarle los motivos de la discrepancia.
- (c) Cuando la Información Reservada pierda esta consideración el Propietario de la Información deberá comunicárselo al Comité y remitir una comunicación por escrito a todos los Iniciados para informarles de que: (i) han dejado de ostentar dicha condición; (ii) las medidas establecidas en el apartado 8.3 han dejado de ser aplicables respecto de la información desclasificada; y (iii) en caso de que dicha información siga teniendo carácter confidencial, el Propietario de la Información deberá advertirlo en la referida comunicación.
- (d) Corresponde al Propietario de la Información autorizar o denegar el acceso a la Información Reservada, que solo se concederá a las personas cuyo acceso resulte imprescindible por motivo de su trabajo.

8.2. El Registro de Iniciados

- (a) El Propietario de la Información clasificada como Reservada deberá crear y mantener actualizado un Registro de Iniciados, para cuya confección deberá usar la plantilla que se incluye en el **Anexo 3**. Asimismo, deberá remitir una copia de dicho listado y de sus sucesivas actualizaciones al Comité.
- (b) El Propietario de la Información deberá actualizarlo inmediatamente cuando sea necesario añadir una nueva persona al registro o cuando un Iniciado que conste en el Registro de Iniciados deje de tener acceso a Información Reservada.
- (c) El Comité conservará los datos inscritos en un Registro de Iniciados al menos durante cinco años a contar desde la fecha de creación del registro o, de ser posterior, desde su última actualización.
- (d) El Propietario de la Información remitirá una comunicación dirigida a las personas inscritas en el Registro de Iniciados informándoles de su sujeción a esta Política y de su obligación

de informarle de la identidad de cualquier otra persona a quien se proporcione la Información Reservada, con el fin de incluirla en el Registro de Iniciados.

- (e) En caso de que el Propietario de la Información sea cesado o sustituido en el ejercicio de sus funciones, la persona que pase a ocupar su cargo como responsable de la operación o proceso interno de que se trate asumirá la función de responsable del Registro de Iniciados de dicha operación o proceso interno.

8.3. Medidas reforzadas de salvaguarda de la Información Reservada

Con carácter adicional a las medidas previstas en los apartados anteriores de esta Política, se aplicarán las siguientes medidas reforzadas para salvaguardar la confidencialidad de la Información Reservada:

- (a) Nombre en clave: el Propietario de la Información asignará un nombre en clave a la operación, a fin de que se utilice en todas las comunicaciones relacionadas con ella.
- (b) Copia de Información Reservada: se prohíbe la realización de copias de documentos que contengan Información Reservada, salvo que el Propietario de la Información lo autorice, previa y expresamente, para la entrega de dichas copias a un Iniciado. Únicamente los Iniciados podrán realizar copias de documentos que contengan Información Reservada. Las copias de dichos documentos estarán sujetas a los mismos requerimientos de protección y control que los originales.

La distribución o transmisión, interna o externa, de Información Reservada se llevará a cabo previa autorización expresa y por escrito del Director del Área o del Propietario de la Información.

8.4. Información Reservada puesta a disposición de las Personas Afectadas

- (a) En todo caso, tendrá la consideración de Información Reservada la documentación, datos e información que se trate o que se genere en reuniones de los Órganos de Dirección o por los miembros de los Órganos de Dirección, el Director General de Cofares o el Asesor Jurídico de su Consejo Rector en el ejercicio de sus funciones.
- (b) Se entenderá que los miembros de los Órganos de Dirección, así como el Director General de Cofares y el Asesor Jurídico de su Consejo Rector (las "**Personas Afectadas**") tienen acceso permanente a Información Reservada, por lo que tendrán la condición de Iniciados de manera permanente.
- (c) En consecuencia, no será necesario que se abra un Registro de Iniciados cada vez que se trate o genere Información Reservada en cualquiera de dichos Órganos de Dirección o se ponga Información Reservada a disposición de las Personas Afectadas.
- (d) Además de las personas indicadas en este apartado 8.4(b), también tendrán la consideración de Personas Afectadas aquellas otras que designe el Comité en cada momento, en atención a su acceso habitual y recurrente a información que pueda considerarse Información Reservada a los efectos de los establecido en estas Política.

- (e) Debido a su condición permanente de Iniciados, todas las Personas Afectadas deberán conocer y respetar las normas de salvaguarda previstas en el apartado 8.3 respecto de la documentación, datos e información que se trate o genere en reuniones de los Órganos de Dirección o se ponga a disposición de las Personas Afectadas.
- (f) Sin perjuicio de lo dispuesto en los párrafos anteriores de este artículo 8.4, cuando una Persona Afectada participe en una operación o proceso que exija la apertura de un Registro de Iniciados, el Propietario de la Información que sea responsable de dicho registro deberá incluir en él a la referida Persona Afectada.

9. Responsabilidades

Sin perjuicio de otras responsabilidades que puedan ser atribuidas en otras secciones de esta Política, en este apartado se asignan responsabilidades y funciones para preservar la seguridad, integridad y disponibilidad de la información.

- (a) Propietarios de la Información: (i) clasificar la información según lo dispuesto en esta Política y el esquema de retención aprobado por el director del negocio o función corporativa de que se trate; (ii) definir el período de retención; (iii) identificar las restricciones de acceso a la información y otro tipo de medidas de seguridad con respecto al almacenamiento, procesado, distribución y destrucción de la información; y (iv) borrar o destruir la información según los procedimientos establecidos.
- (b) Profesionales: (i) conocer el nivel de clasificación de la información que manejan y aplicar las medidas de protección adecuadas; (ii) asegurarse de que los terceros que accedan a la información cumplen las medidas técnicas y organizativas establecidas en su contrato; (iii) notificar cualquier indicio de fuga al Comité de Cumplimiento Normativo; (iv) en caso de finalización de la relación laboral, devolver cualquier información al Grupo Cofares, incluyendo documentos y dispositivos de almacenamiento, subsistiendo, en todo caso, el deber de confidencialidad del Profesional.
- (c) Asesoría Jurídica: asistir a los Propietarios de la Información en la determinación de los períodos de retención derivados de requisitos legales, regulatorios o asociados a la necesidad de atender cualquier reclamación o procedimiento judicial.
- (d) Directores del Área: (i) definir el esquema de retención de la información generada en su negocio o función corporativa, con el apoyo de la Asesoría Jurídica; y (ii) verificar que sus empleados cumplen las responsabilidades asignadas en esta Política.
- (e) Recursos Humanos: (i) asegurar que los empleados conocen esta Política; y (ii) definir e implantar medidas disciplinarias en caso de incumplimiento de esta norma por los empleados del Grupo Cofares.
- (f) Comité de Ciberseguridad y Privacidad: (i) la gestión, supervisión y actualización de esta Política; (ii) la monitorización y medida del grado de cumplimiento de esta Política; y (iii) proporcionar aclaraciones, asesoramiento y recomendaciones a los Usuarios sobre el contenido de la Política.

10. Aprobación y revisión

Sin perjuicio de las funciones atribuidas al Comité de Ciberseguridad y Privacidad en el artículo 9 (f), el Comité de Cumplimiento Normativo y el Comité de Ciberseguridad y Privacidad revisarán periódicamente el contenido de esta Política y propondrán al Consejo Rector de la Cooperativa las modificaciones y actualizaciones que contribuyan a su desarrollo y mejora continua.

Esta *Política sobre el tratamiento y la seguridad de la información confidencial* fue aprobada por el Consejo Rector de Cofares el 4 de noviembre de 2020 y deroga las *Normas internas para el tratamiento de la información confidencial del Grupo Cofares* y la *Política de seguridad de la información*.

* * *

ANEXO 1 DEFINICIONES

A efectos de esta Política se entenderá por:

- Comité: Comité de Cumplimiento Normativo.
- Director del Área: se refiere al director del área de cualquier sociedad del Grupo en la que se genere Información Confidencial. En relación con la Información Reservada, el Director del Área es el responsable de la coordinación de los trabajos u operación a la que se refiera dicha información, así como de la custodia de dicha información.
- Grupo: cualquiera de las entidades integradas en el grupo cuya entidad dominante, en el sentido establecido por la ley, sea Cofares.
- Iniciados: las personas, incluidos los Receptores Externos, que de forma temporal o transitoria tienen acceso a Información Reservada con motivo de su participación o involucración en una operación o en un proceso interno que conlleve el acceso a dicha información, durante el tiempo en el que figuren incorporados a un Registro de Iniciados en virtud de lo dispuesto en el apartado (d) de esta Política, y hasta que la Información Reservada que dio lugar a la creación del citado registro deje de tener dicha consideración y, en todo caso, cuando así se lo notifique el Director del Área responsable de la operación o del proceso interno de que se trate (por ejemplo, con motivo de la suspensión o el abandono de la operación que dio lugar a la Información Reservada).

Esta definición se entenderá sin perjuicio de lo dispuesto en el artículo 8.4 de la Política, relativo a las Personas Afectadas (según como este término se define en dicho artículo).

- Órganos de Dirección: el Consejo Rector, la Comisión Permanente, el Comité, las Comisiones de Información Territorial, la Comisión de Información Interterritorial, la Comisión Económica, el Comité Ejecutivo, el Comité de Dirección, el Comité de Riesgos, la Intervención, el COMEX, el Comité de Ciberseguridad y Privacidad, la Comisión Ejecutiva Delegada, la Comisión de Nombramientos y Retribuciones y la Comisión de Auditoría de “Cofares Corporación, S.L.” (Sociedad Unipersonal), así como los órganos de administración y cualesquiera otros comités o comisiones de cualquier otra sociedad del Grupo.
- Profesionales: se consideran profesionales del Grupo Cofares, a los efectos de esta Política, a los directivos y empleados (incluyendo becarios y personal en prácticas) de todas las sociedades y entidades que integran el Grupo Cofares (incluyendo la Fundación Cofares).
- Propietario de la Información: el Director del Área o, en el caso de una operación concreta, la persona que inicie los contactos para que esta se lleve a cabo. El Propietario de la Información será la persona responsable de: (i) establecer (y, cuando corresponda y esté justificado, modificar) el nivel de sensibilidad de la información y

de clasificarla de acuerdo con su sensibilidad y el valor que tiene para el Grupo Cofares; (ii) fijar los requisitos de seguridad; y (iii) determinar el período de retención de la información.

- Registro de Iniciados: registro regulado en el apartado (d) de esta Política.
- Receptores Externos: se refiere a aquellas personas distintas de las referidas en el apartado 3. de esta Política que necesiten conocer la Información Confidencial para, entre otras cuestiones, poder prestar sus servicios profesionales (por ejemplo, asesorar o analizar alguna operación) o realizar transacciones con el Grupo (tales como, financiar alguna operación), las cuales no estarán obligadas al cumplimiento de esta Política con excepción de lo dispuesto en el apartado 6.5.
- Usuario: cualquier empleado, proveedor, consultor o tercero con acceso a Información Confidencial.

ANEXO 2

ACUERDO DE CONFIDENCIALIDAD

[D. / Dña.] [●]

[Razón social del Receptor Externo]

[Dirección del Receptor Externo]

10.1.1. Acuerdo de Confidencialidad

1. Con la firma del presente acuerdo (el “**Acuerdo**”), [razón social del Receptor Externo] (en adelante, el “**Receptor Externo**”) reconoce y declara que toda la información y documentación facilitada por [razón social de la sociedad del grupo Cofares que transmite la Información Confidencial] (la “**Sociedad**”) o cualquiera de las entidades integradas en el grupo cuya entidad dominante, en el sentido establecido por la ley, sea “Cofares, Sociedad Cooperativa Farmacéutica Española” (el “**Grupo**”), en virtud de [los servicios de [naturaleza del servicio contratado] contratados o que se contraten]², tiene carácter confidencial.

A estos efectos, tendrá la consideración de “**Información Confidencial**” toda documentación e información proporcionada por la Sociedad o el Grupo al Receptor Externo, sus empleados o colaboradores, con independencia de cuál sea su naturaleza (comercial, económica, financiera, científica, jurídica, técnica o de cualquier otra índole), el medio o soporte a través del cual se proporciona y el momento en el que se facilita, resultando el presente Acuerdo extensible a cualesquiera informaciones y documentos a los que el Receptor Externo haya podido tener acceso en el pasado con motivo de [su trabajo para/colaboración con]³ la Sociedad o cualquier otra sociedad del Grupo. Estas obligaciones de confidencialidad se extienden también al resultado de su trabajo.

Los datos de carácter personal, según estos constan descritos en el punto (viii) del presente Acuerdo, tendrán, en todo caso, la consideración de confidenciales.

2. El Receptor Externo se compromete a cumplir, y hacer cumplir por sus empleados o colaboradores, lo siguiente:

- (i) No utilizar la información o documentación suministrada para un fin distinto del encomendado.

² **Nota:** en caso de que el Receptor Externo no fuese un proveedor de servicios, habría que adaptar el texto entre corchetes para explicar el motivo en virtud del cual el Receptor Externo tiene acceso a la Información Confidencial.

³ **Nota:** adaptar de conformidad con la relación (e.g., proveedor, colaborar, etc.) que, en su caso, hubiese vinculado al Receptor y a la Sociedad o el Grupo en el pasado.

- (ii) Seguir en todo momento las instrucciones e indicaciones que, en su caso, le puedan ser impartidas razonablemente por la Sociedad.
- (iii) No divulgar, difundir, entregar, revelar o publicar cualquier información, dato o documento del que tengan conocimiento con ocasión de su [trabajo para/colaboración con]⁴ la Sociedad, ya se encuentren estos referidos a personas físicas, personas jurídicas o Administraciones Públicas.

En el caso de ser requeridos por autoridad judicial o administrativa para revelar, total o parcialmente, Información Confidencial a la que hayan tenido acceso por razón de su [trabajo para/colaboración con]⁵ para la Sociedad, deberán, con carácter previo a cualquier otra actuación, comunicar el requerimiento recibido a [●] y adoptar cuantas medidas resulten necesarias o simplemente convenientes para preservar su confidencialidad. En particular, el Receptor Externo se compromete a adoptar las medidas que razonablemente les pueda indicar [●] y buscar los medios adecuados para que la autoridad requirente preserve la confidencialidad de la información entregada.

- (iv) Limitar al mínimo imprescindible el número de personas con acceso a la Información Confidencial. En particular, el Receptor Externo se compromete a no comunicar Información Confidencial a ninguna persona física o jurídica salvo que: (a) esa persona sea un empleado o un colaborador suyo que merezca su plena y total confianza, fundada en una experiencia histórica plenamente satisfactoria; y, además, (b) esa comunicación sea necesaria para la realización del trabajo encomendado.
- (v) Establecer y definir las medidas necesarias para que sus empleados o colaboradores respeten las obligaciones contraídas por medio del presente Acuerdo. En particular, el Receptor Externo se asegurará de que sus empleados o colaboradores con acceso a la Información Confidencial asuman por escrito compromisos de confidencialidad en términos acordes con el presente Acuerdo.
- (vi) No conservar copia, total o parcial, de la Información Confidencial, cualquiera que sea su soporte, una vez hayan finalizado [las tareas encomendadas/el proyecto/la colaboración]⁶. Este compromiso de no conservación se extiende a los trabajos que puedan realizar, los cuales solo podrán conservar durante el tiempo estrictamente

⁴ **Nota:** adaptar de conformidad con la relación (e.g., proveedor, colaborar, etc.) que, en su caso, hubiese vinculado al Receptor y a la Sociedad o el Grupo en el pasado.

⁵ **Nota:** adaptar de conformidad con la relación (e.g., proveedor, colaborar, etc.) que vincule al Receptor Externo y a la Sociedad.

⁶ **Nota:** adaptar de conformidad con la relación (e.g., proveedor, colaborar, etc.) que vincule al Receptor Externo y a la Sociedad.

necesario para cumplir con sus obligaciones legales y contractuales, asegurándose de que su archivo sea secreto y confidencial.

- (vii) Comunicar a [●] cualquier incumplimiento del presente Acuerdo por el Receptor Externo, sus empleados o colaboradores. Esta comunicación no servirá para exonerar de responsabilidad al Receptor Externo, sus empleados o colaboradores, si bien la ausencia de comunicación dará lugar a cuantas responsabilidades se deriven de dicha omisión en particular.
- (viii) En el supuesto de que la información o documentación suministrada incluya datos de carácter personal relativos a los clientes, empleados, personas de contacto, proveedores, etc., de [●], cuando sean personas físicas identificadas o identificables, además de lo indicado en los apartados anteriores, el Receptor Externo se compromete a cumplir con las obligaciones previstas en el Apéndice de este Acuerdo.

3. El Receptor Externo será responsable de cualquier incumplimiento de las obligaciones de confidencialidad que se derivan del presente Acuerdo, aun cuando tal incumplimiento sea imputable a un tercero con el que trabaje o colabore.

Estas obligaciones perdurarán incluso después de haber expirado el Acuerdo y su incumplimiento podrá ser castigado con, entre otros, las penas previstas en los artículos 197, 199, 200, 278 y 279 del Código Penal.

4. Las comunicaciones con [●] a las que se refieren los apartados (iii),(vii) y (viii) de la sección 2. del presente Acuerdo deberán realizarse por correo electrónico. Este correo electrónico deberá enviarse a: **(a)** la persona de [●] que les encomendó los trabajos que hayan dado lugar a la comunicación; y, además, **(b)** a la siguiente dirección de correo electrónico: [●].

5. El presente Acuerdo se regirá por las leyes españolas. Las partes, con renuncia expresa a cualquier otro fuero, se someten a la jurisdicción y competencia de los Juzgados y Tribunales de la ciudad de [Madrid](España) para cualesquiera desavenencias que pudieran derivarse de este Acuerdo.

Les rogamos nos confirmen su aceptación del presente Acuerdo, firmando y devolviéndonos la copia que les adjuntamos. En [●], a [●].

[Razón social de la Sociedad]

P.p.

10.2.D. [●]

Acceptado y conforme:

[Razón social del Receptor Externo]

P.p.

10.3.D. [●]

10.3.1. Apéndice - encargo del tratamiento

1. **Objeto y duración**

El acceso y tratamiento de los datos personales responsabilidad de la Sociedad necesarios para [prestar el servicio/llevar a cabo la colaboración]⁷ objeto del Acuerdo (los “**Datos Personales**”) se realizará conforme a lo previsto en el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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* (el “**RGPD**”).

Los Datos Personales y las categorías de interesados a las que tendrá acceso el Receptor Externo (a los efectos de este Anexo, el “**Encargado**”) incluirán cualesquiera categorías de datos e interesados a los que tenga acceso el Encargado con objeto de [la prestación de sus servicios/la colaboración]⁸. El presente encargo del tratamiento tendrá la misma duración que el Acuerdo.

2. **Obligaciones del Encargado**

El Encargado se obliga, como encargado del tratamiento, a:

- A. No utilizar ni aplicar los Datos Personales con una finalidad distinta a la prestación de [los servicios/los trabajos/la colaboración]⁹ objeto del Acuerdo. En ningún caso podrá utilizar los datos para fines propios.
- B. Tratar los Datos Personales conforme a las instrucciones de la Sociedad documentadas en el presente Acuerdo (o aquellas que el Encargado reciba por escrito en cada momento).

El Encargado informará inmediatamente a la Sociedad cuando, en su opinión, una instrucción sea contraria a la normativa de protección de datos aplicable en cada momento.

⁷ **Nota:** adaptar de conformidad con la relación (e.g., proveedor, colaborar, etc.) que vincule al Receptor Externo y a la Sociedad.

⁸ **Nota:** adaptar de conformidad con la relación (e.g., proveedor, colaborar, etc.) que vincule al Receptor Externo y a la Sociedad.

⁹ **Nota:** adaptar de conformidad con la relación (e.g., proveedor, colaborar, etc.) que vincule al Receptor Externo y a la Sociedad.

C. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de la Sociedad que contenga el contenido previsto en el artículo 30.2 del RGPD.

D. No comunicar ni ceder los Datos Personales a terceros, ni siquiera para su conservación, salvo que cuente con la autorización expresa de la Sociedad o en los supuestos legalmente admisibles.

Salvo autorización expresa de la Sociedad, no tratará los Datos de Personales fuera del Espacio Económico Europeo. Si el Encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del aplicable en cada momento, informará a la Sociedad de esa exigencia legal de manera previa, salvo que tal la normativa lo prohíba por razones importantes de interés público.

E. Mantener la más absoluta confidencialidad sobre los Datos Personales a los que tenga acceso para la prestación de los servicios así como sobre los que resulten de su tratamiento, cualquiera que sea el soporte en el que se contengan. Esta obligación se extiende a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta del Encargado.

F. Comunicar y garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a cumplir con las obligaciones relativas al deber de secreto, el cumplimiento de medidas de seguridad y la recepción de instrucciones de la Sociedad. El Encargado pondrá a disposición de la Sociedad copia del documento donde consten dichas comunicaciones.

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

H. Asistir a la Sociedad, siempre que sea posible, para que éste pueda cumplir y dar respuesta a las solicitudes de los afectados sobre sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles) (conjuntamente, los “**Derechos ARCO**”).

En particular, dará inmediatamente — y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud— traslado escrito a la Sociedad, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud de cualquier solicitud que hubiera recibido de los afectados sobre sus Derechos ARCO.

I. Comunicar a la Sociedad, de forma inmediata y a más tardar en el plazo de 48 horas, cualquier fallo en su sistema de tratamiento y gestión de la información, que haya tenido o pueda tener,

que ponga en peligro la seguridad de los Datos Personales, así como cualquier posible vulneración de la confidencialidad como consecuencia de la puesta en conocimiento de

terceros de los datos e informaciones obtenidos durante la prestación de los servicios objeto del Acuerdo, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

- J. Colaborar con la Sociedad en el cumplimiento de su obligaciones propias en materia de medidas de seguridad, comunicación y/o notificación de brechas de seguridad (logradas e intentadas) a las autoridades competentes o los interesados, y colaborar en la realización de evaluaciones de impacto relativas a la protección de datos y de consultas previas a las autoridades competentes a este respecto; teniendo en cuenta la naturaleza del tratamiento y la información de la que disponga.

Asimismo, pondrá a disposición de la Sociedad toda la información necesaria para demostrar el cumplimiento de las obligaciones previstas en este Acuerdo y demás documentos contractuales, y colaborará en la realización de auditoras e inspecciones llevadas a cabo, en su caso, por la Sociedad.

- K. Implantar las medidas técnicas y organizativas de seguridad necesarias o convenientes para asegurar la confidencialidad, secreto e integridad de los datos personales a los que tenga acceso de acuerdo con los criterios de seguridad y el contenido previsto la normativa aplicable de protección de datos y el artículo 32 del RGPD. En particular, sin carácter limitativo y salvo instrucción en contra por parte de la Sociedad, se obliga a aplicar las medidas de seguridad de nivel básico de conformidad con lo previsto en el Título VIII del reglamento de desarrollo de la Ley Orgánica de Protección de Datos.
- L. Una vez finalizada la prestación de los servicios objeto del Acuerdo, se compromete a devolver o destruir, a elección de la Sociedad, (i) los Datos Personales a los que haya tenido acceso; (ii) los Datos Personales generados por el Encargado por causa de la prestación de los servicios; y (iii) los soportes y documentos en que cualquiera de estos Datos Personales consten, sin conservar copia alguna; salvo que se permita por ley la conservación de los mismos.

Las obligaciones contempladas en esta cláusula constituyen el contrato de encargo de tratamiento entre la Sociedad y el Encargado y no son retribuíbles de forma distinta que lo previsto en este Acuerdo y demás documentos contractuales.

3. Sub-encargo del tratamiento

El Encargado no recurrirá a otro encargado para la prestación de todo o parte de los servicios sin la autorización previa por escrito (específica o general) de la Sociedad en la que se identificará de forma clara e inequívoca el servicio que haya sido sub-encargado y la identidad del sub-encargado. En este último caso, el Encargado firmará un acuerdo por escrito con el sub-encargado del tratamiento con términos no menos restrictivos que los previstos en el presente Acuerdo, siéndole de aplicación las mismas obligaciones *-mutatis mutandi-* que al

Encargado, quien garantizará que el sub-encargado cumplirá con las instrucciones facilitadas por la Sociedad e informará a la Sociedad de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así a la Sociedad la oportunidad de oponerse a dichos cambios.

ANEXO 3
MODELO DE REGISTRO DE INICIADOS

Fecha y hora (de creación del registro de iniciados, es decir, el momento en que se haya tenido conocimiento de la información reservada de que se trate): [aaaa-mm-dd; hh: mm]

Fecha y hora (última actualización): [aaa-mm-dd, hh:mm]

Nombre(s) de la persona con acceso a información reservada	Apellido(s) de la persona con acceso a información reservada	Número de identificación nacional (en su caso)	Número de teléfono profesional (línea directa fija y móvil)	Dirección profesional completa (calle; número; ciudad; código postal; país)	Razón social de la sociedad del Grupo	Función y motivo por el que se tiene acceso a Información Reservada	Obtención	Cese del acceso (fecha y hora en que la persona cesó de tener acceso a la información reservada)
[Texto]	[Texto]	[Número y/o texto]	[Texto]	[Texto]	[Texto]	[Texto especificativo del papel y la función desempeñadas y el motivo por el que se figura en la lista]	[aaaa-mm-dd, hh:mm]	[aaaa-mm-dd, hh:mm]