

GOB 15 – POLÍTICA GENERAL DE PROTECCIÓN DE DATOS PERSONALES

REALIZADO	APROBACIÓN
Pedro de Navasqüés Dacal	Fidel López Soria
Firma:	Firma:
	
Fecha: 19 de diciembre de 2025	Fecha: 19 de diciembre de 2025
Cargo:	Cargo:
Secretario General y Director de Asesoría Jurídica	Consejera Delegado

Revisión Nº	Motivo de la modificación
01	Revisión periódica de la normativa interna para su adaptación a novedades legislativas y recomendaciones de la autoridad de control.

1. OBJETO

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales constituyen en marco normativo básico aplicable en España en materia de protección de datos.

Ambas normas introdujeron importantes novedades para el sector privado en relación con el tratamiento de los datos personales de ciudadanos y empleados, así como respecto al ejercicio de sus derechos.

Una de las principales novedades es el principio de responsabilidad proactiva que conmina, a las empresas que ostenten la condición de encargadas o responsables del tratamiento de datos personales, a adoptar las medidas que procedan (políticas internas de actuación, registros, auditorías, etc.) para el cumplimiento de las obligaciones que establece el vigente marco legislativo, a fin de garantizar un correcto tratamiento de los datos personales y poder demostrar dicho cumplimiento.

A través de la presente política el Grupo Redexis establece el marco de actuación en materia de protección de datos de acuerdo con la mencionada legislación.

2. ALCANCE

La presente Política es de aplicación a todas las empresas y profesionales del Grupo Redexis (en adelante, "Redexis" o "Grupo"). Asimismo, estarán sometidos a las directrices contenidas en la presente Política los terceros que actúen con Redexis con independencia del tipo de relación contractual que les una a ésta.

Las medidas que se adoptan con esta Política se desarrollan de conformidad con (i) la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, "LOPD"); (ii) el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas

en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, “RGPD”); y (iii) los artículos 3¹, 8² y 20³ del Código de Conducta de Redexis.

Para cumplir adecuadamente con el meritado marco normativo, en primer lugar, Redexis ha implantado una estructura de gestión en materia de protección de datos, nombrando un Delegado de Protección de Datos o “*Data Protection Officer*” (“DPO”) que liderará dicha tarea. Dicho DPO ejercerá sus funciones respecto de todas las entidades del Grupo. Además, se ha diseñado una estructura de soporte al DPO constituida, fundamentalmente, por responsables funcionales, encargados de la implementación de determinadas medidas para tratamientos concretos.

En segundo lugar, se han elaborado un Registro de Actividades del Tratamiento o RAT, que recoge los tratamientos efectuados por las distintas empresas que forman parte del Grupo Redexis, estableciéndose un protocolo su mantenimiento y actualización.

En tercer lugar, se ha desarrollado una metodología de gestión de riesgos, que comprende un análisis de riesgos inicial y, en determinados supuestos, la realización de Evaluaciones de Impacto o “*Privacy Impact Assessments*” (“PIA”), en los casos en que ello resulte necesario de conformidad con la normativa aplicable.

En cuarto lugar, se incorpora a la presente Norma el modelo de políticas informativa de privacidad, desarrollado en cumplimiento de los artículos 13 y 14 del RGPD, que deberá adaptarse por parte de las empresas del Grupo Redexis a los distintos tratamientos que efectúan y a los puntos de recogida de datos personales.

En quinto lugar, con la finalidad de dar cumplimiento a los requerimientos establecidos en la normativa en cuanto a la recepción y contestación de peticiones de ejercicio de derechos instados por parte de los interesados, se establece la necesidad de establecer los cauces adecuados para la recepción y contestación de las peticiones recibidas de los interesados en el ejercicio de sus derechos, así como las normas relativas al registro de las peticiones recibidas.

¹ Artículo 3.- Cumplimiento de la legalidad

² Artículo 8.- Derecho a la intimidad de los profesionales

³ Artículo 20.- Confidencialidad de la información

Asimismo, se establece la necesidad de que se determinen los plazos generales de conservación para los datos de carácter personal tratados bajo responsabilidad de Redexis y las normas básicas de conservación y archivo de documentación en soporte papel, así como las cuestiones relativas a su almacenamiento y destrucción.

En séptimo lugar, y en atención a la introducción de la obligación de notificar a la autoridad de control, esto es, a la Agencia Española de Protección de Datos (en adelante, “AEPD”), las brechas de seguridad que afecten a los datos de carácter personal objeto de tratamiento, que incluso, en algunos casos, también se extiende a las personas afectadas, se incorporan las Normas aplicables en materia de gestión de brechas de seguridad.

Por último, con el objeto de garantizar la seguridad del tratamiento de datos por parte de Redexis y el cumplimiento del resto de los principios básicos recogidos en la normativa vigente, se recogen las reglas para verificar el cumplimiento de las obligaciones en materia de protección de datos por todas las unidades y empleados de la Compañía, así como las normas sobre supervisión y realización de auditorías internas y externas al respecto.

3. RESPONSABILIDADES

Todos los empleados y las unidades de Redexis tienen la obligación de conocer la normativa de protección de datos aplicable, de respetarla y de garantizar su cumplimiento en el ámbito de sus funciones.

El Delegado de Protección de Datos promoverá el conocimiento y cumplimiento de la normativa de protección de datos en todos los niveles de la organización y supervisará su efectivo cumplimiento. Asimismo, ejercerá las demás funciones que le atribuye la legislación aplicable.

La Dirección de Recursos establecerá las medidas técnicas adecuadas y proporcionadas para asegurar la integridad y privacidad de los datos de carácter personal.

Asimismo, existirá un responsable funcional por cada actividad de tratamiento desarrollada. Su principal función consistirá en el mantenimiento del Registro de Actividades de Tratamiento relacionadas con las actividades que desempeña, así como en la implementación de medidas relacionadas con la información a los afectados y la recepción de ejercicios de derechos y quejas. Igualmente, los responsables funcionales están obligados a comunicar

cualquier incidencia detectada con relación al tratamiento que gestionan bajo su responsabilidad al DPO.

El cargo de responsable funcional será compatible con el desarrollo de otros cargos o funciones en Redexis.

El Delegado de Protección de Datos se reunirá periódicamente y al menos dos veces al año, con los responsables funcionales y, en su caso, con los técnicos que resulte necesario con el objeto de (i) revisar el cumplimiento de la normativa de protección de datos por las unidades de la empresa, (ii) identificar los nuevos riesgos que puedan ponerse de manifiesto, (iii) resolver aquellas cuestiones que requieran de conocimiento especializado, (iv) analizar las medidas de seguridad que sea razonable y proporcionado incorporar atendiendo a los riesgos y naturaleza de los tratamientos, (v) analizar las necesidades de formación existentes en materia de protección de datos de carácter personal, (vi) analizar cualquier otro aspecto relativo al cumplimiento de la normativa en materia de protección de datos de carácter personal.

El Delegado de Protección de Datos podrá recabar la presencia de cualquier persona de la organización a dichas reuniones de seguimiento, así como convocar, cuando proceda, a asesores técnicos o jurídicos externos. Asimismo, documentará la celebración de las reuniones de seguimiento y las conclusiones adoptadas.

La Dirección de Auditoría interna será responsable de realizar las auditorías internas correspondientes en materia de protección de datos de carácter personal.

4. PRINCIPIOS APLICABLES AL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL

Con el objeto de asegurar el cumplimiento de la normativa en materia de protección de datos de carácter personal, las unidades y empleados de Redexis deberán de respetar los siguientes principios de actuación:

- Cualquier tratamiento de datos debe estar basado en el consentimiento del interesado (prestado libremente tras haber sido informado), en la existencia de un contrato que ampare el tratamiento, en el cumplimiento de una obligación legal, o en un interés legítimo, de conformidad con la legislación aplicable.

- Se informará a todos los afectados del tratamiento que se realiza de sus datos personales, de una forma clara, sencilla y transparente. La información se facilitará a través del medio más adecuados en función del canal de recogida de los datos o de comunicación con el titular de los mismos.
- Los datos personales solamente se utilizarán para los fines concretos, específicos y legítimos de los que se ha informado a los afectados.
- No se solicitará ni se realizará ningún tratamiento de datos que no sean necesario para las finalidades que se pretenden cumplir, o que resulte desproporcionados para llevar a cabo las mismas.
- Se mantendrá un Registro de todas las Actividades del Tratamiento efectuadas por Redexis, que será debidamente actualizado.
- Se llevará a cabo un análisis de los riesgos que presentan los tratamientos efectuados para los derechos y libertades de los titulares de los datos, de acuerdo con una metodología objetiva aprobada y documentada por Redexis. Los tratamientos que presenten un alto riesgos serán sometidos, adicionalmente, a una evaluación de impacto sobre la protección de datos.
- Las medidas de seguridad aplicadas al tratamiento de los datos personales se fijarán en función de los riesgos detectados y se revisarán periódicamente.
- Los datos solo se conservarán durante el plazo determinado en la política de conservación correspondiente y, en ningún caso, durante más tiempo del necesario para cumplir los fines para los que fueron recogidos.
- Se promoverá la sensibilización en materia de protección de datos entre todos los usuarios de Redexis, programándose la realización de cursos o actividades formativas y de concienciación adecuadas a las tareas desempeñadas por cada uno.
- Ningún usuario de Redexis accederá a datos de otros empleados o de terceros, o los solicitará a otra unidad, sin causa justificada (es decir, sin necesitarlos para el desarrollo de sus funciones).
- Se debe mantener en todo momento la confidencialidad adecuada sobre los datos de carácter personal.

- No se facilitarán a terceros los datos de carácter personal, salvo en los supuestos legalmente admitidos y en los casos previstos en las correspondientes Políticas de Privacidad.
- Como norma general, se evitará la recepción de datos de carácter personal en soporte papel.
- Los documentos que se deben generar en papel que afecten a datos de carácter personal deberán ser almacenados en armarios, archivadores o dependencias que dispongan de un sistema de cerrado con llave o mecanismo equivalente (por ejemplo, tarjetas electrónicas, códigos o pins, etc.), de conformidad con los criterios que puedan adoptarse por la Compañía.
- Cualquier duda relativa al cumplimiento de la normativa en materia de protección de datos de carácter personal deberá trasladarse al Delegado de Protección de Datos.

La Compañía podrá aprobar las normas o procedimientos que resulten necesarios para garantizar la aplicación de estos principios.

Del mismo modo, el Delegado de Protección de Datos podrá establecer instrucciones y pautas de actuación internas para clarificar y desarrollar los aspectos que surjan en aplicación de estos principios y de la Política General de Protección de Datos Personales, con pleno respeto a lo dispuesto en ésta y en los anexos que forman parte integrante de la misma.

5. DELEGADO DE PROTECCIÓN DE DATOS O DATA PROTECTION OFFICER (DPO)

De acuerdo con lo dispuesto en la LOPDP y el RGPD, Redexis, como Responsable del tratamiento, tendrá designado un Delegado de Protección de Datos, que ejercerá las funciones previstas en la legislación al respecto.

El Delegado de Protección de Datos realizará la función de intermediación entre el responsable del tratamiento, los titulares de los datos y la autoridad de control.

En el desarrollo de las funciones que la Ley le tiene atribuidas, el DPO deberá actuar con independencia e imparcialidad, velando en todo momento por el correcto cumplimiento de la

normativa de protección de datos. El DPO no podrá ser removido, salvo en los supuestos de dolo o negligencia grave.

El DPO podrá ser único para todas las empresas del Grupo y será nombrado por la Dirección de la Compañía entre personas que tengan conocimientos especializados en el derecho y en la práctica en materia de protección de datos.

El nombramiento del DPO deberá ser comunicado a todos los empleados de Redexis a través de la correspondiente nota informativa, siguiendo el procedimiento habitual de información sobre nombramientos de la Compañía, identificando con claridad su nombre y sus datos de contacto.

Asimismo, el nombre y datos de contacto del DPO deberán ser comunicados a la Agencia Española de Protección de Datos.

Se adjunta como **Anexo I** a la presente Norma, el Estatuto del Delegado de Protección de Datos (DPO), en el que se establecen las normas relativas a su nombramiento y cese, duración, posición dentro del Grupo, principales funciones, facultades y recursos en su actividad, así como sus responsabilidades.

6. RESPONSABLES FUNCIONALES

Se nombrarán responsables funcionales para cada actividad de tratamiento registrada en el RAT de Redexis. Los responsables funcionales asumirán como tarea principal la actualización de los RAT que se encuentren bajo su competencia.

Adicionalmente, los responsables funcionales informarán al DPO de cualquier cambio relevante en los tratamientos del que tengan constancia y le prestarán soporte en la implantación de las medidas legales y organizativas que resulten necesarias.

7. REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

Redexis mantendrá un Registro de Actividades del Tratamiento o RAT que contenga, al menos, la siguiente información: (i) las finalidades del tratamiento; (ii) los sujetos afectados; (iii) las categorías de datos tratados y los plazos de conservación previstos; (iv) las medidas de

seguridad implantadas; (v) los destinatarios de los datos, ya sean cesionarios o encargados del tratamiento; (vi) las transferencias internacionales de datos efectuadas, y (vii) las bases de legitimación del tratamiento.

Los RAT se elaborarán utilizando modelos aprobados por Redexis y se mantendrán actualizados de acuerdo con el protocolo que se adjunta como **Anexo II**.

8. POLÍTICAS DE PRIVACIDAD

Para el cumplimiento de las nuevas obligaciones establecidas en la norma sectorial en materia de protección de datos sobre información a los interesados, transparencia en la información, licitud del tratamiento y condiciones para el consentimiento, Redexis tendrá aprobadas las correspondientes Políticas Informativas de Privacidad o Política de Privacidad.

Cuando los datos personales sean obtenidos del afectado, el responsable del tratamiento podrá dar cumplimiento al deber de información proporcionándole la siguiente información, redactada de forma ordenada, clara y sencilla:

- a) La identidad del responsable del tratamiento y de su representante, en su caso.
- b) La finalidad del tratamiento.
- c) La base de legitimación del tratamiento.
- d) Las categorías de datos tratados.
- e) Los destinatarios de los datos, incluyendo las transferencias internacionales que se efectúen.
- f) Los plazos de conservación previstos.
- g) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del RGPD.
- d) En su caso, que los datos obtenidos van a ser tratados para la elaboración de perfiles, y del derecho que le corresponde de oponerse a la adopción de decisiones individuales automatizadas al respecto.

Las Políticas Informativas de Privacidad tendrán en cuenta las pautas establecidas por la AEPD y, en particular, las que constan en la *“Guía para el cumplimiento del deber de informar”* publicada por la AEPD, que recomienda facilitar la información a los distintos afectados utilizando un sistema de dos capas: la primera capa contendrá un resumen sucinto de la Política Informativa de Privacidad y la segunda capa incluirá el texto completo.

Las Políticas Informativas de Privacidad se elaborarán y utilizarán siguiendo las normas que se establecen en el **Anexo III**.

7. GESTIÓN DE RIESGOS DERIVADOS DE LOS TRATAMIENTO DE DATOS PERSONALES

Antes del inicio de una nueva actividad del tratamiento, Redexis procederá a realizar una evaluación de los riesgos que se derivan de la misma y que pueden afectar a los derechos y libertades de los titulares de los datos. La evaluación de riesgos se llevará a cabo desde el punto de vista legal y organizativo, por un lado, y técnico, por otro. En este último caso, el análisis de riesgos determinará las medidas de seguridad apropiadas al tratamiento efectuado.

La realización del análisis de riesgos técnico y la implantación de las medidas de seguridad apropiadas es responsabilidad del Departamento de Sistemas, de acuerdo con la metodología y modelos aprobados por dicho Departamento. Los informes y planes de acción resultantes se pondrán a disposición del DPO a efectos informativos, dándosele traslado de los principales hallazgos del proceso. Siempre que resulte necesario, se solicitará la opinión del DPO a efectos de determinar el alcance legal de la implantación de las medidas de seguridad propuestas.

La realización del análisis de riesgos legal y técnico corresponderá al DPO, con el soporte de los responsables funcionales del tratamiento. La metodología aplicable a la realización de esta parte del sistema de gestión de riesgos se encuentra recogida en el **Anexo IV**. Dicha metodología también establece los supuestos en los que, debido al alto riesgo de los tratamientos o al cumplimiento de requisitos legales que lo hacen necesario, se procederá a llevar a cabo una Evaluación de Impacto sobre la Protección de Datos o *Privacy Impact Assessment* ("PIA").

Los análisis de riesgos (tanto los técnicos y como los legales y organizativos) y las PIA se revisarán con una periodicidad anual, haciéndose un seguimiento de los planes de acción resultantes.

Los principales riesgos detectados se pondrán en conocimiento de la Dirección de Redexis.

8. NORMAS APLICABLES A LOS CONTRATOS FORMALIZADOS CON TERCEROS

8.1. Contratos con terceros como encargados del tratamiento

Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, Redexis elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento de los datos de carácter personal sea conforme con la legislación aplicable y garantice la protección de los derechos del interesado.

Por tanto, con carácter previo a la contratación de un Encargado del Tratamiento, se deberá verificar la idoneidad de la entidad que se pretende contratar.

Asimismo, se deberá firmar un contrato por escrito que vincule al encargado del tratamiento respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable y del encargado del tratamiento.

El DPO anualmente deberá realizar controles y revisiones periódicas de aquellos encargados del tratamiento que presten servicios de especial relevancia desde el punto de vista de la normativa de protección de datos de carácter personal y comprobará que se cumplen las obligaciones previstas en los contratos suscritos con los encargados de tratamiento.

Se adjunta como **Anexo V** la Política de Gestión de Encargados del Tratamiento.

8.2. Contratos con terceros que no tengan la condición de encargados del tratamiento

En los contratos, acuerdos o convenios que celebre Redexis con terceros y estos no asuman la condición de encargado del tratamiento y, por tanto, no se les cedan datos de carácter personal para que sean tratados por parte de estos, se insertará una cláusula que garantice que las partes asumen las obligaciones que les corresponden de acuerdo con la legislación vigente en materia de protección de datos de carácter personal y que los datos de los firmantes y las personas de contacto serán tratados por las partes en base al interés legítimo de cada entidad, con la exclusiva finalidad de gestionar adecuadamente el contrato y mantener el contacto comercial entre las partes. Asimismo, se hará constar la facultad que

corresponde a los afectados de ejercer los derechos que la legislación reconoce en materia de protección de datos de carácter personal ante el Responsable del Tratamiento.

Se incluye dentro de la Política de Gestión de Encargados del Tratamiento como anexo, modelo de cláusula a introducir en los contratos o acuerdos que se celebren con terceros, en que estos no tengan la condición de encargados del tratamiento.

9. POLÍTICA DE ATENCIÓN AL EJERCICIO DE DERECHOS

Redexis tendrá aprobada una Política de Atención al Ejercicio de Derechos con la finalidad de dar cumplimiento a los requerimientos establecidos en la LOPDP y el RGPD en cuanto a la recepción y contestación de peticiones de ejercicio de derechos instados por parte de los interesados frente a cualquiera de las Sociedades del Grupo.

En particular, se reconoce a los interesados el derecho de acceso a sus datos, el derecho de rectificación, el derecho a instar la supresión de los datos, el derecho al olvido, el derecho a la limitación del tratamiento, el derecho a la portabilidad de los datos, el derecho de oposición y el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado. Estos derechos podrán ser ejercitados de conformidad con lo previsto en la legislación aplicable.

Asimismo, se establecerán los cauces adecuados para la recepción y contestación de las peticiones recibidas de los interesados en el ejercicio de sus derechos, así como las normas relativas al registro de las peticiones recibidas.

Se adjunta como **Anexo VI** la Política de Atención al Ejercicio de Derechos.

10. PLAZOS DE CONSERVACIÓN DE LOS DATOS TRATADOS Y DOCUMENTACIÓN EN SOPORTE PAPEL

Redexis determinará los plazos generales de conservación para los datos de carácter personal tratados bajo responsabilidad de Redexis e informará de ellos a los interesados. Asimismo, se establecerán las normas básicas de conservación y archivo de documentación en soporte papel, así como las cuestiones relativas a su almacenamiento y destrucción.

Se adjunta como **Anexo VII** la Política de Plazos de Conservación de Datos de Carácter Personal y de Documentación en soporte papel.

11. GESTIÓN DE BRECHAS DE SEGURIDAD

La Compañía tendrá establecido un Protocolo de gestión de brechas de seguridad de los datos de carácter personal, que establecerá (i) la forma de detección de las violaciones de seguridad, (ii) los procedimientos de actuación ante violaciones de seguridad, (iii) los procedimientos de notificación a la autoridad de control y a los posibles afectados y (iv) las medidas para mitigar, reparar y supervisar los supuestos de violaciones de seguridad.

Cuando la brecha de seguridad pueda constituir un riesgo para los derechos y las libertades de las personas físicas se realizará una notificación sin dilación a la AEPD sí como a los posibles afectados.

Asimismo, se arbitrarán los mecanismos necesarios para asegurar que los encargados del tratamiento cumplen con la obligación que les corresponde de notificar al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tengan conocimiento.

Se adjunta como **Anexo VIII** el Protocolo de Gestión de Brechas de Seguridad de los Datos de Carácter Personal.

12. FORMACIÓN Y SENSIBILIZACIÓN

El DPO propondrá un plan de formación y sensibilización anual que permita facilitar a los usuarios el conocimiento de los principios básicos en materia de protección de datos, así como el contenido de la presente Política y sus Anexos.

Todos los empleados de Redexis deberán realizar, al menos, un curso básico de protección de datos, con contenidos aprobados por el DPO.

Los responsables funcionales recibirán formación complementaria, acorde a las tareas de soporte al DPO que tienen asignadas.

13. SUPERVISIÓN Y AUDITORÍAS EN MATERIA DE PROTECCIÓN DE DATOS

El DPO supervisará el cumplimiento de la normativa de protección de datos de carácter personal por parte de las unidades y empresas del Grupo, de conformidad con lo dispuesto en la legislación aplicable y en las normas internas aprobadas por la Compañía. El DPO podrá informar de su actuación y de las conclusiones de la misma a las personas o unidades de la empresa que corresponda al objeto de que se adopten las medidas organizativas o disciplinarias que en cada caso procedan.

El DPO revisará anualmente las normas internas en materia de protección de datos de carácter personal, las Políticas de Privacidad aprobadas por parte de la Compañía, las cláusulas a insertar en los contratos celebrados con terceros, la idoneidad de los Registros de Actividades de Tratamiento, así como del resto de políticas y protocolos previstos en la presente Norma, dejando constancia de su revisión. Asimismo, realizará un seguimiento periódico del cumplimiento de la normativa de protección de datos por los empleados y unidades de la Compañía y, en particular, por los responsables funcionales de los tratamientos.

La Dirección de Recursos revisará periódicamente las medidas de seguridad aplicables a los sistemas de información, y podrá encargar las auditorías o análisis de riesgos procedentes al respecto. Con independencia de ello, la Dirección de Auditoría interna realizará auditorías periódicas previstas en el plan de Auditorías de la Compañía, sobre el cumplimiento de la normativa de protección de datos de carácter personal por parte de las unidades y empresas del Grupo. El resultado de las auditorías se documentará en los correspondientes informes, que establecerán, en su caso, las medidas correctoras o el plan de acción que deba realizarse al respecto.

Asimismo, la Compañía, podrá, en cualquier momento, encargar una auditoría externa que verifique el cumplimiento de la normativa de protección de datos de carácter personal por parte de la misma.

14. PUBLICIDAD Y ACCESIBILIDAD A LA INFORMACIÓN SOBRE PROTECCIÓN DE DATOS Y FORMACIÓN

La Compañía remitirá la Política General de Protección de Datos Personales, así como los anexos que forman parte de esta, a todos los empleados, y publicará la misma en la Intranet corporativa.

La Compañía tendrá establecido un apartado específico sobre Protección de Datos en la Intranet corporativa, donde los empleados tendrán acceso a toda la información de interés sobre la materia, incluyendo el acceso a las Políticas de Privacidad y a las normas que regulan el marco de actuación de obligado cumplimiento por parte de los empleados.

Periódicamente se suministrará la formación necesaria a los empleados que corresponda con el objeto de que conozcan sus obligaciones en materia de protección de datos de carácter personal.

Asimismo, la Compañía tendrá establecido un apartado específico sobre Protección de Datos de carácter personal en la web corporativa, con el objeto de facilitar a cualquier tercero el acceso y la transparencia sobre la información de interés relativo al tratamiento de datos de carácter personal realizado por Redexis, incluyendo el acceso a las Políticas de Privacidad y la información respecto al tratamiento que realiza Redexis de los datos personales.

15. MODIFICACIÓN DE LOS ANEXOS

Los anexos que forman parte de esta Política General de Protección de Datos Personales, podrán ser actualizados por el DPO, de oficio o a instancia de cualquiera de los Responsables de los tratamientos, a excepción del Anexo I relativo al Estatuto del DPO. El DPO llevará un registro de las versiones sucesivas de los Anexos, con expresión de su fecha de modificación y entrada en vigor.

Los anexos correspondientes, una vez actualizados, respetarán los criterios de publicidad y accesibilidad establecidos en el apartado anterior.

ANEXO I

ESTATUTO DEL DELEGADO DE PROTECCIÓN DE DATOS (DPO)

1. EL DPO: NOMBRAMIENTO Y DURACIÓN DEL CARGO

El artículo 34.1 i) de la LOPD, en relación con lo dispuesto en el art. 37.1.b) del RGPD, establece la obligación de designar un Delegado de Protección de Datos (DPO) a las empresas que realizan actividades en los ámbitos de la distribución y comercialización de gas o electricidad.

En cumplimiento de lo anteriormente expuesto, Redexis, tendrá designado un DPO, que ejercerá las funciones previstas en la legislación al respecto. El DPO podrá ser único para todas las empresas del Grupo.

La posición de DPO estará desempeñada, preferentemente, por personal contratado de alguna de las compañías del Grupo. No obstante, se podrá designar un DPO externo por motivos organizativos o de eficiencia, por ejemplo, para garantizar la continuidad de las funciones en periodos de baja temporal o en supuestos de reestructuración interna.

Cuando se trate de personal interno, el referido nombramiento se realizará formalmente por la Dirección de la Compañía, y será comunicado por la Dirección de Recursos Humanos. Una vez nombrado y de manera inmediata, se informará del nombre del designado y sus datos de contacto, a estos efectos, a todos los empleados del Grupo a través de la correspondiente nota informativa, siguiendo el procedimiento habitual de información sobre nombramientos de la Compañía.

Igualmente, el nombramiento y cese del DPO será reportado a la Agencia Española de Protección de Datos junto con sus datos de contacto.

El DPO no podrá ser removido ni sancionado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio.

El DPO será designado entre personas que tengan conocimientos especializados en el derecho y en la práctica en materia de protección de datos. Asimismo, se valorará el conocimiento de la regulación sectorial que afecta al Grupo, así como la capacidad de gestión e interlocución con la Dirección y con las entidades y organismos que se relacionan con la Compañía.

La Compañía deberá facilitar la formación necesaria en materia de protección de datos al DPO, de forma que se asegure su continua actualización, con el objeto de que pueda desarrollar sus funciones adecuadamente.

El DPO actúa como asesor y supervisor interno, por lo que, a fin de evitar futuros conflictos de interés, su puesto no será ocupado por personas o empleados que, a la vez, tengan tareas dentro del Grupo que impliquen decisiones esenciales sobre la existencia de tratamientos de datos personales.

2. POSICIÓN Y FUNCIONES

La actuación del DPO deberá estar regida por el principio de control, rendición de cuentas y diligencia debida. El DPO deberá promover el cumplimiento de la normativa de protección de datos personales, con el objeto de proteger la privacidad y seguridad de los datos de carácter persona responsabilidad del Grupo. En consecuencia, la posición del DPO dentro de Redexis implica:

- Su adecuada participación en todas aquellas cuestiones relativas a la protección de datos personales que surjan en el marco de actuación de las empresas que forman el Grupo.
- El efectivo apoyo de la Dirección, empleados, y sociedades del Grupo en sus actuaciones, debiendo facilitarle los recursos que sean necesarios para el correcto desempeño de sus funciones.
- La garantía de su imparcialidad. No recibirá por parte de la Dirección, empleados o sociedades del Grupo ninguna instrucción en lo que respecta al desempeño de sus funciones. No se podrá prever la destitución del cargo o sanción por causas relacionadas con la realización de sus obligaciones.
- La redición de cuentas directamente con la Dirección. La Dirección tomará en consideración las recomendaciones, propuestas y evaluaciones emitidas por el DPO en la toma de decisiones que tengan relación directa con el tratamiento de datos personales.

Asimismo, el DPO ejercerá, además de las responsabilidades señaladas en el cuerpo de la Política General de Protección de Datos Personales y las que legalmente le correspondan, las siguientes funciones:

- Relaciones con las autoridades de supervisión.
- Reporte de riesgos detectados a la Dirección de Redexis.
- Revisión, gestión y mantenimiento de las políticas y procedimientos de protección de datos aprobadas por Redexis.
- Identificación de las bases jurídicas de los tratamientos efectuados.
- Diseño e implantación de medidas para la información a los afectados.
- Gestión de la recogida de consentimientos cuando sea necesario.
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.

- Valoración de las solicitudes complejas de ejercicio de derechos por parte de los interesados.
- Gestión de los contratos firmados con encargados de tratamiento.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- Gestión del Plan de Auditoría de protección de datos.
- Valoración de existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Coordinación en la gestión y comunicación de Brechas de Seguridad.
- Gestión y promoción de la formación interna de empleados.

En el desarrollo de las anteriores funciones, el DPO deberá actuar con imparcialidad, velando en todo momento por el correcto cumplimiento de la normativa de protección de datos que se encuentre vigente en cada momento.

El DPO deberá abstenerse de conocer aquellos asuntos en los que pueda existir alguna incompatibilidad con otras funciones que, en su caso, desarrolle para Redexis, y comunicarlo inmediatamente a la Dirección.

3. RECURSOS Y FACULTADES

La Compañía facilitará al DPO los recursos necesarios para llevar a cabo sus funciones, lo que incluirá:

- El apoyo activo a la función del DPO por la Dirección de la empresa.
- El tiempo suficiente para que el DPO pueda cumplir adecuadamente sus obligaciones.
- El otorgamiento de los recursos materiales que, en su caso, resulte necesario.
- El acceso a las unidades y departamentos de la organización con el objeto de que pueda recibir el apoyo o la colaboración que resulte necesaria para el ejercicio de sus funciones.
- El soporte en determinadas tareas como el mantenimiento de RATs por parte de los responsables funcionales del tratamiento.
- La formación continua en materia de protección de datos.

Para llevar a cabo el desempeño de sus funciones, el DPO podrá recabar la colaboración de todas las unidades y empleados de la Compañía, lo que incluirá la facultad de (i) recopilar

información para identificar las actividades de tratamiento de datos, (ii) analizar y verificar el cumplimiento de las actividades de tratamiento de datos y (iii) informar, aconsejar y emitir recomendaciones al responsable o al encargado del tratamiento.

4. RESPONSABILIDADES

El DPO será responsable de promover el cumplimiento por parte de la Compañía de la legislación aplicable en materia de protección de datos y de ejercer las funciones que la legislación vigente establece para el DPO.

Las unidades, departamentos y empleados de la Compañía serán responsables de seguir las pautas e instrucciones trasladadas por el DPO para el cumplimiento de la normativa de protección de datos de carácter personal y de respetar la normativa interna aprobada al efecto. Asimismo, prestarán la colaboración requerida en cada momento por el DPO para el ejercicio de sus funciones.

ANEXO II

GESTIÓN DE REGISTRO DE ACTIVIDADES DEL TRATAMIENTO (RAT)

1. OBJETIVO Y ÁMBITO DE APLICACIÓN

El artículo 30 del RGPD establece la obligación de los responsables del tratamiento mantener un registro de las actividades de tratamiento que efectúan con un contenido mínimo marcado por dicho precepto. Este registro o RAT tendrá que constar necesariamente por escrito, en formato papel o electrónico, y deberá ser puesto a disposición de la Agencia Española de Protección de Datos u otras autoridades competentes cuando así lo soliciten.

Las entidades que actúan como encargados del tratamiento de terceros están también obligadas a mantener un RAT simplificado reflejando las operaciones que realizan por cuenta de los responsables.

Como complemento de lo señalado en el RGPD, el artículo 31 de la LOPDGDD dispone lo siguiente:

“Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro”.

Teniendo en cuenta lo anterior, para cumplir con la normativa de protección de datos vigentes, Redexis ha elaborado un RAT de tratamientos propios que se encuentra publicado internamente y puede ser consultado por los distintos responsables funcionales y por el DPO. De la misma forma, Redexis ha preparado un RAT de tratamientos efectuados en calidad de encargados del tratamiento.

En este Anexo se establecen los procesos necesarios para revisar periódicamente y mantener actualizados los RAT de Redexis. El alcance de las normas que recoge viene fijado por todos los tratamientos de datos personales desarrollados por Redexis en calidad de Responsable del Tratamiento y de Encargado del Tratamiento.

De esta forma, en los apartados siguientes (i) se asignan responsabilidades en el proceso de actualización y mantenimiento de los RAT; (ii) se explica la información que deberá recoger el RAT, y (iii) se facilitan modelos y registros para dejar constancia de las operaciones efectuadas.

2. NORMA GENERAL PARA LA ACTUALIZACIÓN DEL RAT

El RAT debe reflejar la situación actual de los tratamientos de datos personales llevados a cabo por una entidad. Por tanto, **se tendrá que actualizar cada vez que haya una modificación, adición o supresión de carácter significativo** en las operaciones de tratamiento registradas.

A modo de ejemplo, se citan las siguientes circunstancias que darán lugar a una actualización del RAT:

- Inicio de nueva actividad de tratamiento: Se recogen nuevos datos con finalidades diferentes a las ya registradas.
- Finalización de actividad de tratamiento: Se cesa en uno de los tratamientos registrados por cualquier motivo.
- Adición de nuevos datos o nuevas categorías de afectados: Las circunstancias del tratamiento siguen siendo en esencia las mismas (las finalidades, la aplicación utilizada, etc.), pero se recogen datos adicionales a los registrados o de interesados que no estaban previstos en un principio.
- Modificación sustancial en los proveedores con acceso a datos: Se contrata un proveedor tecnológico nuevo que facilitará un nuevo software de gestión.

La tarea de actualización del RAT requiere un conocimiento suficiente de los tratamientos efectuados. Por ello, el proceso de actualización deberá iniciarse por el responsable funcional asignado que, cuando proceda, recabará la ayuda del Departamento de IT (por ejemplo, a la hora de detallar las aplicaciones o sistemas en los que se realiza el tratamiento).

3. FUNCIONES DE LOS RESPONSABLES FUNCIONALES

Los responsables funcionales que aparecen designados en cada actividad de tratamiento deberán detectar cualquier cambio que afecte al mismo e iniciar el proceso de actualización que corresponda. En este sentido, sus funciones consistirán en:

- Poner en conocimiento del DPO cualquier nuevo tratamiento que se vaya a realizar, en un plazo de una semana (7 días naturales) desde que se tenga conocimiento del proyecto o plan que dará lugar a dicho tratamiento, para que se evalúe su

idoneidad. Se recuerda que la inclusión de nuevas actividades del tratamiento en el RAT debe producirse siempre antes del inicio efectivo de la recogida y/o uso de los datos personales.

- Recabar toda la información que se indica en este procedimiento cuando sea necesario para proceder a la inclusión de un nuevo tratamiento en el RAT.
- Completar la primera versión del registro de las nuevas actividades del tratamiento que vayan a efectuarse, de acuerdo con el modelo que figura en el Apéndice I. Una vez completada, será remitida al DPO.
- Realizar una revisión anual de los RAT de los que son responsables y ya se encuentran registrados para verificar que la información contenida en los mismos es correcta y se encuentra actualizada. Las revisiones anuales deberán efectuarse entre los días 1 y 31 de enero de cada año. Como resultado de esta revisión, se completará el modelo de informe que figura en el Apéndice I, incluso en el caso de que no se haya detectado la necesidad de realizar ningún cambio o modificación.
- Poner en conocimiento del DPO cualquier aspecto que necesite ser modificado o actualizado como resultado de las revisiones anuales. A estos efectos, se utilizará el buzón de correo designado para contactar con el DPO.
- Aclarar con el DPO las dudas que pudieran surgir en relación con las actividades de tratamiento de las que son responsables.

4. FUNCIONES DEL DPO

El DPO es el responsable de custodiar los RAT y de su publicación interna. En este sentido, deberá:

- Recordar anualmente a los responsables funcionales su obligación de iniciar la revisión de los RAT y solicitar el informe escrito resultado de la revisión.
- Resolver las dudas que planteen los responsables funcionales.
- Revisar las propuestas de modificación o actualización de los RAT.
- Llevar a cabo la publicación interna de las nuevas versiones de los RAT.
- Custodiar los informes de revisión anuales.

5. CONTENIDO DEL RAT

La acción de actualización más compleja es aquella que se refiere al registro de nuevas actividades del tratamiento. El siguiente apartado incluye una explicación de la forma en la que deberán ser completados los distintos campos que figuran en el modelo de RAT aprobado por Redexis. Dicho modelo, como se ha indicado, se adjunta a este Anexo como Apéndice I.

El modelo incluye dos versiones de registro:

- Modelo de registro para responsable del tratamiento.
- Modelo de registro para encargado del tratamiento. Este modelo se utilizará cuando el tratamiento se efectúe en calidad de encargado del tratamiento y es una versión simplificada del primero.

Ambos modelos son muy similares. En el segundo, debemos identificar de forma muy clara la identidad y datos de contacto del responsable del tratamiento (así consta en los primeros campos del mismo).

Conviene recordar que los responsables funcionales no pueden realizar ninguna modificación en la estructura de los modelos. Se deben limitar a completar los campos de respuesta con la información que se solicita. Así, por ejemplo, no podrán cambiar los títulos o textos de las preguntas o suprimir filas o columnas.

A continuación, incluimos una explicación del contenido de los principales campos que han de completarse en el RAT, con la finalidad de que sirva de guía a la hora de recopilar la información necesaria e incluirla correctamente en el documento:

- **Finalidades del tratamiento:** Hace referencia a los fines para los que se utilizan los datos o a los objetivos del tratamiento. Existe la posibilidad de incluir una finalidad principal o amplia y subfinalidades. Por ejemplo, la finalidad principal del tratamiento relativo a Recursos Humanos es la gestión de los recursos humanos de la compañía. Como subfinalidades, se podrían señalar: Gestión de nóminas, gestión de altas y bajas y comunicaciones a las TSGG; evaluación de personal y diseño de planes de carrera; formación interna; etc.
- **Categorías de personas afectadas:** Se refiere a los titulares de los datos personales tratados. Por ejemplo, empleados de Redexis, usuarios de la página web, clientes de GLP, etc.

- **Categoría y tipos de datos personales:** En este punto, se incluirá la información que se almacena y usa. Es especialmente importante señalar si el tratamiento incluye datos especialmente protegidos, como datos de salud o datos biométricos. Los datos especialmente protegidos se listarán en un apartado diferenciado del RAT, dado que están sometidos a restricciones y medidas específicas.
- **Plazo de conservación y destrucción de los datos personales:** Los datos solo se pueden tratar durante los plazos en los que son necesarios. No podemos almacenar datos que no vamos a utilizar con una finalidad definida, simplemente por si los queremos consultar en el futuro. El plazo que fijemos de conservación debe tener en cuenta las posibles relaciones contractuales con los titulares de los datos, las obligaciones legales de mantenimiento de los mismos (por ejemplo, el artículo 30 del Código de Comercio, la normativa de prevención de blanqueo de capitales, etc.) y las responsabilidades que se deriven para Redexis del tratamiento. Se seguirán las normas fijadas en el Anexo VII.
- **La base de legitimación del tratamiento:** En este punto, señalaremos una de las siguientes bases legales:
 - Consentimiento (autorización del titular de los datos).
 - Ejecución del contrato.
 - Cumplimiento de una obligación legal (se debe iniciar la referencia de dicha ley).
 - Protección de los intereses vitales del interesado (entendemos que esta base de legitimación no se aplicará, salvo en tratamientos muy concretos como los de los Servicios Médicos).
 - Interés legítimo o interés público.

Se recomienda consultar en todo caso con el DPO antes de fijar la base de legitimación que corresponda.

- **Medidas de seguridad:** Se deben incluir las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el RGPD y la LOPDP, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.
- **Cesiones previstas para cada uno de los tratamientos:** Se deben identificarán las sociedades, proveedores, organismos institucionales, etc. a los que Redexis comunica datos sin que exista una relación de prestación de servicios.

Es conveniente recordar la diferencia entre un destinatario/cesionario de datos y un encargado de tratamiento. El primero no presta un servicio a Redexis, ni está sujeto a sus instrucciones, mientras que el encargado accede a los datos para prestar un servicio a Redexis. El encargado, además de estar sujeto a las instrucciones que dicte Redexis, no puede establecer una relación directa con los interesados y, finalizado el servicio, no puede conservar los datos. Son ejemplos de destinatarios la Agencia Tributaria, y la TGSS en el caso de los datos de trabajadores.

Cuando Redexis es encargada del tratamiento, los proveedores que contrate serán subencargados del tratamiento.

- **Encargados o subencargados del Tratamiento:** Recordamos que estas entidades actúan sin autonomía propia y tienen prohibido destinar los datos a una finalidad distinta de la propia prestación del servicio.
- **Transferencias internacionales:** Se deberán identificar, en su caso, las transferencias de datos fuera del Espacio Económico Europeo, con independencia de si se trata de un encargo de tratamiento o de una comunicación de datos. Asimismo, es necesario indicar las garantías que permiten la realización de esa transferencia, por ejemplo, la aprobación por parte de la AEPD.

6. APÉNDICES

Apéndice I. Modelo de RAT

Apéndice II. Ficha de revisión de RAT

7. APÉNDICE 1



Apéndice I del Anexo
II Modelo de RAT.xlsx

8. APÉNDICE 2



Apéndice II del Anexo
II Plantilla de revision

ANEXO III

GESTIÓN DE POLÍTICAS INFORMATIVAS DE PRIVACIDAD

1. OBJETIVO Y ÁMBITO DE APLICACIÓN

El artículo 13 del RGPD, bajo el epígrafe *“Información que deberá facilitarse cuando los datos personales se obtengan del interesado”*, establece que, siempre que se recojan datos personales directamente del titular, debe facilitarse determinada información que permita al interesado conocer el tratamiento que va a llevarse a cabo.

En particular, el citado precepto determina que se debe facilitar la siguiente información:

- a) La identidad y los datos de contacto del responsable y, en su caso, de su representante;
- b) Los datos de contacto del delegado de protección de datos, en su caso;
- c) Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
- d) Los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
- e) La existencia de transferencias internacionales de datos.
- f) El plazo durante el cual se conservarán los datos personales o
- g) Los derechos que asisten al titular de los datos y la forma de ejercerlos, incluyendo el derecho a presentar una reclamación ante la autoridad de control.
- h) La posibilidad de retirar el consentimiento prestado.
- i) La existencia de decisiones automatizadas que afecten a los titulares de los datos.

El RGPD también determina, en su artículo 12.1, que la información indicada se transmitirá al interesado *“en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo”*.

Para ayudar a los responsables del tratamiento a cumplir con la obligación de información mencionadas, la AEPD publicó el 22 de mayo de 2018 una *“Guía sobre el deber de informar”*¹, donde recoge distintas recomendaciones para organizar, estructurar y redactar políticas y cláusulas informativas de protección de datos que recojan la información obligatoria de forma clara y transparente.

En la citada Guía, la AEPD recomienda la utilización de un sistema de doble capa, de forma que el afectado reciba un resumen al mismo nivel en el que se recogen los datos (por ejemplo, al pie del formulario en soporte papel o electrónico), y pueda consultar una segunda capa informativa, completa y más extensa, en una página web o anexo adicional.

¹ Disponible en: <https://www.aepd.es/sites/default/files/2019-11/guia-modelo-clausula-informativa.pdf>

En la misma línea, el artículo 11 de la LOPDP, establece la posibilidad de facilitar al afectado una “información básica” en el momento de la recogida de datos, la cual deberá ampliarse en un momento posterior, facilitando una dirección electrónica u otro medio equivalente:

“1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

- a) La identidad del responsable del tratamiento y de su representante, en su caso.*
- b) La finalidad del tratamiento.*
- c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679”.*

Este sistema no es obligatorio cuando toda la información requerida por el artículo 13 del RGPD puede facilitarse en una única capa fácilmente accesible por el usuario y de lectura sencilla.

Teniendo en cuenta lo expuesto, Redexis ha elaborado el presente Anexo para establecer instrucciones que permitan el cumplimiento de las obligaciones en materia de información en los distintos procesos de recogida de datos que se desarrollan por parte de las empresas que componen su Grupo.

Este Anexo se aplica a los procesos de generación, actualización e implementación de los textos legales informativos que debe utilizar Redexis con la finalidad de dar cumplimiento al RGPD en los supuestos en los que la Compañía actúa como responsable del tratamiento.

Los objetivos de este Anexo son (i) establecer normas que permitan la elaboración de textos informativos uniformes y (ii) garantizar la correcta implementación de los textos legales elaborados en los distintos puntos de recogida de datos personales que gestiona Redexis.

2. UBICACIÓN DE LAS POLÍTICAS INFORMATIVAS DE PRIVACIDAD

Como se ha indicado, Redexis debe garantizar que todos los puntos de recogida de datos personales cuenten con un texto informativo (denominado Política Informativa de Privacidad o Política de Privacidad) que cumpla con los requisitos exigidos por el RGPD.

Se han identificado como habituales los siguientes puntos de recogida de datos personales, sin perjuicio de que existan otros medios de obtención de datos personales directamente del afectado:

- Formularios en papel.
- Contratos.
- [Otros documentos completados por los interesados]
- Formularios electrónicos (en páginas webs o en el proceso de registro en aplicaciones).
- Cámaras de videovigilancia.
- Servicios de atención telefónica.
- Atención al cliente de forma presencial de forma verbal presencial.
- Toma de fotografías y vídeos en eventos y actos.

En función de lo anterior, se establecen las siguientes normas generales:

1º. Todos los formularios, impresos o solicitudes que se ponga a disposición de los afectados, y a través de los cuales éstos faciliten datos personales, deberán contener una descripción del tratamiento que se efectuará de dichos datos de acuerdo con lo establecido en esta política. Esta obligación se aplica tanto a los formularios que figuren en soporte papel como aquellos que se presenten en formato electrónico (por ejemplo, los que sirven para efectuar un registro on-line).

2º. Cuando se recojan datos verbalmente (por ejemplo, en un mostrador de atención al público), la información figurará en carteles dispuestos de forma que resulten legibles y visibles para el afectado.

3º. Si en algún momento se recogen datos telefónicamente, resultará obligatorio incluir una locución inicial con el texto informativo de protección de datos, que podrá remitir a una segunda capa informativa en una página web.

4º. En los contratos, [listado de documentos/formularios más habituales], la información requerida por el artículo 13 del RGPD se facilitará en una de las cláusulas y, si resulta necesario, se añadirá una segunda capa en forma de anexo.

5º. En los buzones de correo electrónico destinados a la recepción de consultas, quejas o sugerencias que puedan contener datos personales, se utilizará un pie de firma que incluya la información de primera capa con remisión a una página web con la política completa.

6º. Si se toman fotografías de eventos, se seguirá lo dispuesto en la Política de Eventos publicada en la intranet de la Compañía.

7º. En el caso de las cámaras de videovigilancia, se deberán colocar los carteles oficiales que marcan el área como sometida a videovigilancia e igualmente, se dispondrá de una segunda capa con información adicional.

Siempre que sea posible, la información se presentará, siguiendo un sistema de doble capa.

3. GENERACIÓN DE POLÍTICAS INFORMATIVAS DE PRIVACIDAD

El DPO ha aprobado las Políticas Informativas de Privacidad básicas que se encuentran disponibles en la intranet y en <https://www.redexis.es/proteccion-de-datos>.

No obstante, existen distintos supuestos que darán lugar a la generación y/o actualización de las Políticas de Privacidad como, por ejemplo:

- **Inicio de una nueva actividad de tratamiento.** Se trata de casos en los que se recogen nuevos datos con finalidades diferentes a las ya registradas en el Registro de Actividades de Tratamiento (RAT) de.
- **Actualización del tratamiento.** Las Políticas de Privacidad deben reflejar la situación actual respecto al tratamiento de datos personales llevados a cabo en cada caso. Por lo tanto, se deberán actualizar cada vez que se produzcan cambios significativos respecto a la información que se debe facilitar a los interesados.

Las tareas de creación y modificación de cláusulas informativas deberán realizarse de forma coordinada entre los responsables funcionales y el DPO, según la siguiente distribución de tareas y responsabilidades:

1º. El responsable funcional del tratamiento es quien conoce en primer lugar la información relativa a: (i) cualquier nuevo tratamiento que se vaya a realizar para que se evalúe su idoneidad, y (ii) cualquier aspecto que necesite ser modificado o actualizado como en los RAT. Por ello, será el encargado de realizar una primera versión de la Política de Privacidad.

2º. Corresponde al DPO revisar y aprobar el texto presentado por el responsable funcional y proceder a su aprobación.

3º. El responsable funcional realizará un seguimiento de la implantación y uso de la Política de Privacidad aprobada.

La generación de nuevas Políticas de Privacidad se realizará, siempre que sea posible, utilizando el modelo que figura en los Apéndices I y II.

4. CONSENTIMIENTO

El consentimiento es una de las bases de legitimación del tratamiento de datos personales. Como norma general, será la base de legitimación utilizada para el envío de comunicaciones comerciales.

El RGPD define “consentimiento” en su artículo 4.11 como *“toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen”*.

El consentimiento a un determinado tratamiento no se puede imponer en el momento de la recogida de los datos (lo contrario implicaría que no es libre). Por ello, están prohibidas las casillas pre-marcadas o los contratos en los que se obligue al cliente a aceptar recibir publicidad por defecto.

Cuando queramos utilizar los datos personales para finalidades adicionales a la principal del tratamiento, y dichas finalidades adicionales no se deriven de otra base de legitimación (por ejemplo, del cumplimiento de una ley o de la existencia de un contrato), tendremos que recabar el consentimiento del interesado a través de un acto o clara acción afirmativa de su parte.

Una de las formas más habituales de recogida del consentimiento es la utilización de casillas de marcación **no pre-cumplimentadas**, que el afectado puede marcar o no (el consentimiento debe ser libre) en el momento de la obtención de los datos.

Estas casillas de consentimiento deben colocarse en el momento de la recogida de los datos personales, normalmente en los formularios en los que el usuario facilite sus datos. También es posible recabar el consentimiento del usuario posteriormente al momento de recogida inicial de datos, informando respecto a las nuevas finalidades del tratamiento y solicitando una aceptación de las mismas (por ejemplo, cuando solicitamos a un trabajador la cesión de sus derechos de imagen para publicar una fotografía en la web a través de la firma de un documento).

Si el interesado se ve compelido a consentir, o se enfrenta a consecuencias negativas por el hecho de no hacerlo, el consentimiento no resulta válido porque no ha sido prestado libremente. **De esta forma, no se obtiene de forma adecuada el consentimiento cuando al afectado no se le permite continuar si no marca una casilla, o si esta aparece pre-marcada.** El consentimiento exige voluntariedad en la entrega de los datos y en el inicio de la operación de tratamiento.

Como norma general, el envío de boletines, noticias o información comercial de los productos o servicios de Redexis se basará en el consentimiento, y será necesario una clara acción informativa del interesado para llevar a cabo estos tratamientos. También se basará en la cesión de imágenes contenidas en fotografías y vídeos captados en eventos externos o internos (celebraciones corporativas).

Si el usuario revoca su consentimiento, se debe finalizar el tratamiento de los datos. Esto no implica que los datos sean borrados o suprimidos (es posible que deban conservarse para cumplir con obligaciones legales de Redexis, por ejemplo, relativas a plazos de prescripción legal de acciones respecto a ese tratamiento). Sin embargo, no se podrán utilizar para la finalidad específica respecto de la cual se ha revocado el consentimiento.

La revocación del consentimiento no tiene efectos retroactivos, y, por tanto, no afecta a operaciones de tratamientos ya efectuadas ni a los resultados de las mismas.

El DPO ha aprobado determinados textos para la recogida del consentimiento. Dichos textos están asociados a Políticas Informativas de Privacidad. Si un responsable funcional necesita recoger un consentimiento para el que no existe un texto específico aprobado, deberá solicitarlo al DPO. La redacción de los textos de consentimiento, corresponde al DPO.

Por último, debemos resaltar que, aunque los servicios y actividades de Redexis no están dirigidos específicamente a niños, es posible que sea necesario tratar datos de menores de 14 años.

El límite legal para poder consentir un tratamiento de datos por sí mismo, se fija en los 14 años. Las personas de 14 años pueden consentir por sí mismas siempre que se haya facilitado la información necesaria para entender el tratamiento de una forma sencilla y adecuada al nivel de madurez de una persona de la edad del titular de los datos. Por debajo de los 14 años, se deberá contar siempre con la autorización paterna. Cuando sea posible, resulta recomendable solicitar exclusivamente los datos de los padres o acompañantes (tutores) del menor, y no tratar ninguna información del niño.

Si se prevé que algún servicio o actividad de Redexis implique tratamiento de datos personales de menores de 14 años, se deberá contactar con el DPO para que redacte una cláusula informativa acorde a las necesidades del tratamiento concreto, y en su caso, una declaración de consentimiento.

5. APÉNDICES

Apéndice I. Modelo para la redacción de primera capa informativa

Apéndice II. Modelo para la redacción de Política Informativa de Privacidad completa

6. APÉNDICE 1. Modelo para la redacción de primera capa informativa

Responsable del tratamiento	[NOMBRE COMPLETO Y DOMICILIO SOCIAL DEL RESPONSABLE DEL TRATAMIENTO. Ejemplo: Redexis Gas Servicios, S.L.U. Domicilio: calle Mahonia, nº 2, 28043, Madrid]
Finalidades del tratamiento	[USO DE LOS DATOS. DEBE COINCIDIR CON UNA FINALIDAD REGISTRADA EN EL RAT. Ejemplo: Gestionar su solicitud así como la relación contractual relativa a los servicios y productos contratados.]
Sus derechos	Puede revocar su consentimiento, en el caso de que lo haya prestado, y ejercitar sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad dirigiendo un escrito al Delegado de Protección de Datos (dpo@redexis.es)
Consulte más información sobre el tratamiento de sus datos personales en la política de privacidad de [NOMBRE EMPRESA] en [LUGAR DE ACCESO DE LA SEGUNDA CAPA]	

7. APÉNDICE 2. Modelo para la redacción de Política Informativa de Privacidad completa

Política de Privacidad de *[INDICAR SERVICIO O TRATAMIENTO]

[NOMBRE COMPLETO EMPRESA] ("Redexis *") ha redactado la siguiente Política de Privacidad para informarle del tratamiento que realiza de sus datos personales.

Si desea consultar alguna duda o solicitar información adicional, póngase en contacto con nuestro Delegado de Protección de Datos o *Data Protection Officer* en la dirección de correo electrónico dpo@redexis.es

¿Quién es el responsable de los datos que facilita?

El responsable del tratamiento de sus datos personales es [NOMBRE COMPLETO EMPRESA], con domicilio [INDICAR DOMICILIO SOCIAL].

Redexis * es una compañía que ofrece servicios de valor añadido en el sector del suministro energético, como por ejemplo, el *renting* de calderas, y los servicios de mantenimiento y revisión de las mismas.

En el apartado siguiente, se explica qué datos de carácter personal recoge **Redexis *** y para qué finalidades se utilizan.

¿Qué tipo de datos recoge Redexis Servicios?

Redexis * recoge los siguientes datos de carácter personal:

[EJEMPLO:

- Datos identificativos y de contacto (nombre, DNI, teléfono, etc.), información sobre la vivienda que ocupa (dirección, piso, tipo de vivienda, etc.) y datos bancarios. Esta información figura en

el contrato de prestación de los servicios contratados por Ud., puede actualizar en cualquier momento esta información.

- **Datos técnicos de las instalaciones.** Esta información es necesaria para emitir la correspondiente factura y realizar una prestación de los servicios contratados.

LOS DATOS TRATADOS DEBEN COINCIDIR CON LOS INDICADOS EN EL RAT CORRESPONDIENTE].

¿Para qué utilizamos sus datos personales?

Utilizamos los datos con las siguientes finalidades:

[EJEMPLO:

- Facturar el servicio prestado (instalación interior o colocación de aparatos energéticos, servicio de renting de calderas, de venta e instalación de equipos gasodomésticos, de placas fotovoltaicas o de contratación de cualquier otro servicio o equipo relacionado con el consumo energético de su inmueble, mantenimiento y revisión de las mismas o cualesquiera otros servicios de valor añadido que haya contratado con Redexis Servicios).
- Resolver reclamaciones.
- Contestar consultas y peticiones realizadas por Ud.

LAS FINALIDADES DEBEN COINCIDIR CON LAS SEÑALADAS EN EL RAT CORRESPONDIENTE].

¿Cuál es la base que legitima el tratamiento de sus datos?

Tratamos sus datos basándonos en:

[EJEMPLO:

- La existencia de un contrato o pre-contrato.

LAS BASES DE LEGITIMACIÓN DEBEN COINCIDIR CON LAS QUE FIGURAN EN EL RAT CORRESPONDIENTE].

¿Con quién compartimos sus datos?

Los distintos departamentos de **Redexis *** pueden acceder a sus datos de carácter personal para el desarrollo de las funciones enumeradas en esta política. Además, **Redexis *** utiliza distintos prestadores de servicios, entre ellos empresas del grupo Redexis Gas, para la realización de algunas de sus funciones. Estos prestadores de servicios pueden cambiar a lo largo del tiempo. Podrá consultar nuestros principales proveedores en www.redexisgas.es/protecciondedatos

¿Durante cuánto tiempo conservamos sus datos?

Sus datos se conservarán mientras mantengamos una relación contractual con Ud., para poder gestionarla adecuadamente. Una vez finalizada dicha relación, deberemos conservar sus datos para atender nuestras obligaciones legales durante **un plazo de ***.**

Sus derechos

De acuerdo a la normativa vigente de protección de datos, Ud., puede ejercer distintos derechos:

- Solicitar el acceso a sus datos y obtener una copia de los mismos.
- Pedir que se rectifiquen o se supriman en algunos casos.
- Oponerse a la elaboración de perfiles personalizados.
- Solicitar la limitación al tratamiento de sus datos.
- Pedir la portabilidad de aquellos datos que ha facilitado.

En todo momento, si ha consentido el envío de comunicaciones comerciales, tiene derecho a revocar ese consentimiento y a que dejemos de remitirle nuestras ofertas.

Redexis * le reconoce, además, el derecho a presentar una reclamación ante el DPO en caso de que considere que se ha hecho un tratamiento incorrecto de sus datos de carácter personal. Su reclamación se investigará de forma confidencial y recibirá una respuesta de nuestro DPO. También tendrá derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, especialmente cuando no haya recibido satisfacción en el ejercicio de los derechos señalados en este apartado.

Para ejercitar sus derechos, puede ponerse en contacto con nosotros a través de estos medios:

- Dirigiéndonos una carta por correo postal a la dirección: Calle Mahonia n.º 2, 28043 Madrid.
- Por correo electrónico: dpo@redexisgas.es.
- A través del teléfono de atención a clientes 900 811 339.
- A través del área de usuarios registrados de nuestra web.

ANEXO IV

METODOLOGÍA DE GESTIÓN DE RIESGOS

1. INTRODUCCIÓN

El RGPD obliga a los responsables del tratamiento a implantar las medidas necesarias para la adecuada protección de los datos personales que tratan con un enfoque basado en el riesgo. De esta forma, se deberá realizar una valoración del riesgo que implica cada tratamiento y fijar los controles que se deben aplicar en cada caso.

En esta línea, el artículo 24 del RGPD establece lo siguiente en su apartado primero:

“Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario”.

Adicionalmente, el artículo 32.1 del RGPD determina:

“Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- a) la seudonimización y el cifrado de datos personales;*
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento”.*

La AEPD, en su Guía sobre “Gestión del riesgo y evaluación de impacto en tratamientos de datos personales”¹, aclara lo siguiente:

“El RGPD demanda la identificación, evaluación y mitigación, realizadas de una forma objetiva, del riesgo para los derechos y libertades de las personas en los tratamientos

¹ Disponible en: <https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf>

de datos personales. La mitigación ha de realizarse mediante la adopción de medidas técnicas y organizativas que garanticen y, además, permitan demostrar la protección de dichos derechos. Estas deberán determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento. Además, dichas medidas se revisarán y actualizarán cuando sea necesario. En definitiva, el RGPD exige un proceso de gestión del riesgo para los derechos y libertades de los interesados.

En cumplimiento del principio de responsabilidad proactiva o “accountability”, la gestión del riesgo ha de estar documentada. Sin embargo, es importante saber diferenciar los informes que documentan las acciones de gestión del riesgo con la gestión del riesgo en sí misma. La gestión del riesgo no es un documento sino un proceso que se traduce en hechos y que se acredita documentalmente”.

A continuación, se describe y documenta el sistema de gestión de riesgos establecido en Redexis, teniendo en cuenta que:

- 1º. Se detalla la metodología utilizada para la realización de análisis de riesgos legales y evaluaciones de impacto sobre la protección de datos desde un punto jurídico y organizativo.
- 2º. Si bien se incluyen distintas referencias a la gestión de riesgos técnico, la determinación de la metodología empleada para evaluar los riesgos que afectan a la disponibilidad, integridad y confidencialidad de los datos personales, el detalle de los controles o medidas de seguridad que se deberán implementar y la ejecución del proceso correspondiente son responsabilidad del Departamento de Sistemas.
- 3º. Corresponde al Departamento de Sistema la documentación de la metodología correspondiente al análisis de riesgos técnico para la determinación de medidas de seguridad a implantar, así como la realización del mismo y el seguimiento de los planes de acción resultantes.
- 4º. Desde el Departamento de Sistemas se dará traslado al DPO de los resultados de dicho análisis de riesgos técnico a efectos informativos. El DPO asesorará al Departamento de Sistemas en la resolución de las dudas legales que puedan plantearse.

2. ANÁLISIS DE RIESGOS INICIAL DEL TRATAMIENTO

La metodología descrita en este Anexo parte de un análisis inicial de cada actividad de tratamiento registrada en el que se determinan los factores de riesgo que afectan a dicha actividad sobre un catálogo desarrollado por Redexis. En los casos de que el riesgo

detectado a través de este sistema resulte medio o alto, se procederá a una evaluación sistemática.

En el caso de nuevas operaciones de tratamiento que sean objeto de registro como actividades independientes, se llevará a cabo un análisis de riesgos inicial, de acuerdo con el modelo que figura en el **Apéndice I** del presente procedimiento.

El objetivo de este proceso es evaluar el riesgo inherente (denominado “riesgo acumulado” en este documento) de una nueva actividad de tratamiento en función de factores de riesgo detallados e intrínsecos al tratamiento que va a iniciarse. Este análisis permitirá determinar si es posible iniciar el tratamiento con la aplicación de controles básicos o si, por el contrario, el tratamiento requiere de una evaluación de impacto exhaustiva.

El análisis de riesgos inicial incluye:

- Una descripción del ciclo de vida de los datos.
- La evaluación de si se cumplen los requisitos legales exigidos para la elaboración de una evaluación de impacto sobre la protección de datos.
- El análisis de distintos factores de riesgo, que permitirán calcular el riesgo acumulado del tratamiento.
- La inclusión del tratamiento en alguno de los supuestos legales que hacen necesaria la realización de una evaluación de impacto sobre la privacidad tendrá como resultado que se lleve a cabo el análisis descrito en el apartado siguiente, sin que sea necesaria la evaluación de riesgos inicial.

Los tratamientos cuyo riesgo acumulado sea bajo, podrán iniciarse sin necesidad de efectuar una evaluación de impacto sobre la protección de datos, puesto que la aplicación de controles solo podrá tener como efecto bajar aún más el nivel de riesgo detectado. Los tratamientos de riesgo acumulado medio y alto, requerirán que se efectúe dicha evaluación.

Se han identificado distintos factores de riesgos. Para cada uno de ellos, se han señalado circunstancias que implican riesgo medio y alto. En algunos, aparecen igualmente identificadas situaciones de riesgo básico.

Se entenderá por riesgo acumulado la suma de las puntuaciones obtenidas en relación con los distintos factores de riesgo (1 punto por cada circunstancia marcada). El riesgo acumulado se calculará de acuerdo con la siguiente fórmula:

$$\text{RIESGO ACUMULADO} = (\text{Nº SITUACIONES DE RIESGO ALTO} \times 2) + (\text{Nº SITUACIONES DE RIESGO MEDIO} \times 1) + (\text{Nº SITUACIONES DE RIESGO BAJO} \times 0)$$

Para su valoración se aplicará la siguiente tabla de conversión:

ALTO	MEDIO	BÁSICO
>25	20-25	0-19

Cuando el riesgo acumulado del tratamiento que se va a iniciar sea bajo y asumible por la organización con la aplicación de controles sencillos se podrá continuar con el proceso e iniciar la actividad.

Cuando el riesgo acumulado sea medio o alto, se procederá a efectuar una evaluación de impacto sobre la protección de datos.

3. EVALUACIÓN DE IMPACTO SOBRE LA PROTECCIÓN DE DATOS

La finalidad de una Evaluación de Impacto sobre la Privacidad o sobre la Protección de Datos Personales es identificar, evaluar y gestionar los riesgos antes de iniciar un tratamiento. El análisis permite adoptar aquellas medidas de control o mitigación de los riesgos detectados, de forma que el tratamiento que se efectúe tenga el menor impacto posible para los derechos y libertades fundamentales de las personas físicas.

De acuerdo con lo indicado en el artículo 35.1 del RGPD:

- “1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.*
- 2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.”*

El artículo 35.3 del RGPD establece tres supuestos en los que la realización de una EIPD es obligatoria. Dichos supuestos se refieren a los siguientes tratamientos:

- Tratamientos que implican una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan

efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

- Tratamientos a gran escala de categorías especiales de datos.
- Tratamiento que supongan una observación sistemática a gran escala de una zona de acceso público.

Los anteriores supuestos se han definido de forma amplia, poniendo de manifiesto la voluntad del legislador de proporcionar un listado abierto. De esta forma, la Agencia Española de Protección de Datos ha publicado, como complemento de lo anterior, dos listados adicionales:

- Listado de tratamientos que requieren una Evaluación de Impacto sobre la Privacidad².
- Listados de tratamientos que no requieren una Evaluación de Impacto sobre la Privacidad³.

Por su parte, de forma orientativa, Comité Europeo de Protección de Datos ha publicado una guía de tratamientos que con carácter general requerirán una EIDP⁴.

Como se ha explicado, dentro del análisis de riesgos inicial se verifica la inclusión del tratamiento que pretende iniciarse en alguno de los supuestos establecidos en el RGPD o en los listados aclarativos públicos. Entendemos que esto atribuye un riesgo objetivo y automático al tratamiento de nivel alto, que hace necesaria la realización de una EIPD, sin tener en cuenta otras consideraciones. Por tanto, se procederá directamente a la realización de una EIPD. También se efectuará una EIPD, como se ha explicado, en los casos en los que el riesgo acumulado tras valorar los factores de riesgo identificados sea medio o alto.

Para efectuar una evaluación de impacto sobre la protección de datos, se seguirá el modelo establecido en el **Apéndice II**.

Por lo que se refiere al cálculo del riesgo en este segundo análisis, atenderemos a su “probabilidad” (mayor o menor posibilidad de que algo ocurra) y a su “gravedad” (impacto o consecuencias).

Para la valoración de la PROBABILIDAD, se tendrán en cuenta los siguientes criterios:

² Disponible en: <https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf>

³ Disponible en: <https://www.aepd.es/sites/default/files/2019-12/ListasDPIA-35.5I.pdf>

⁴ Disponible en: [listas-dpia-es-35-4.pdf](https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf) (aepd.es)

- **Madurez de los controles (“MC”):** El hecho de que no existan controles para una amenaza, o que existiendo no estén documentados, o que sean revisados periódicamente, hace que la probabilidad de que ocurra la amenaza sea mayor. En cambio, si están documentados, implementados y auditados, la probabilidad de que ocurra la situación de incumplimiento se reduce. Utilizaremos una escala del 1 al 4, de acuerdo con los siguientes criterios:

1	Los controles están documentados e implementados tal y como están documentados, totalmente monitorizados y además auditados (se efectúa una verificación formal como auditoría, sea externa o interna)
2	Los controles están documentados e implementados tal y como están documentados, y parcialmente monitorizados (verificación sistematizada de su funcionamiento, aunque no sea completa)
3	Los controles están implementados, pero deficientemente documentados (el contenido de los documentos no se corresponde con la implementación real)
4	Un único control modifica el riesgo de más de una amenaza; no existen controles

- **Configuración de los controles (“CC”):** Este criterio se basa en el número de controles dedicados a contener o minimizar una amenaza. De esta forma entendemos que, si se establecen más de un control, la probabilidad de que se materialice un riesgo será menor. Se volverá a utilizar una escala del 1 al 4 con los siguientes criterios:

1	<u>Insignificante</u> : Existen varios controles para la misma amenaza, en forma de líneas de defensa
2	<u>Limitada</u> : Existen varios controles para la misma amenaza
3	<u>Significativa</u> : Existe un solo control por amenaza
4	<u>Máxima</u> : Un único control modifica el riesgo de más de una amenaza o no existen controles

La probabilidad de una amenaza se obtendrá sumando los valores obtenidos como resultado de la estimación de los aspectos citados, de acuerdo con la siguiente tabla de conversión:

Descripción del nivel de probabilidad	Valores conversión
Improbable	<5
Baja	=5
Alta	=6
Muy alta	>6

Por ejemplo, para una amenaza concreta en la que tenemos implantados tres controles (RAT documentado, procedimiento de actualización y revisión periódica de los RATs), que están documentados y son objeto de auditoría periódica el cálculo será el siguiente:

MC = 1

CC = 1

Probabilidad= 1+1=2. Improbable

Para la valoración de la **IMPACTO**, es necesario tener en cuenta que el impacto serán los daños para los derechos y libertades de las personas físicas y no el riesgo que la organización pueda sufrir sanciones, multas, pérdidas financieras o pérdida de su reputación derivadas de la violación de la normativa en materia de protección de datos. La metodología propuesta para calcular el IMPACTO que proponemos tiene en cuenta igualmente dos criterios, que habría que sumar para hallar el valor de conversión:

- **Nivel de identificación de los datos personales ("IDP"):** Este criterio hace referencia a la posibilidad de identificación de los afectados en caso de que se materialice un riesgo. Aplicamos igualmente una escala del 1 al 4.

1	<u>Insignificante</u> : la identificación de una persona con sus datos personales parece ser prácticamente imposible
2	<u>Limitado</u> : la identificación de una persona con sus datos personales parece difícil, pero es posible en ciertos casos
3	<u>Significativo</u> : la identificación de una persona con sus datos personales parece ser relativamente fácil
4	<u>Máximo</u> : la identificación de una persona con sus datos personales parece ser extremadamente fácil

- **Gravedad (perjuicio o daño que pueden causar) ("G"):** Tenemos en cuenta el efecto que tendría la materialización del riesgo en el afectado.

1	<u>Insignificante</u> : las personas no se verán afectadas, o tan solo pueden tener algunos inconvenientes, que podrán superar sin ningún problema
2	<u>Limitado</u> : las personas pueden tener inconvenientes importantes, que podrán superar a pesar de algunas dificultades
3	<u>Significativo</u> : las personas pueden sufrir consecuencias significativas, que deberían poder superar, aunque con serias dificultades
4	<u>Máximo</u> : las personas pueden sufrir consecuencias significativas, o incluso irreversibles, que no pueden superar

El impacto de una amenaza se obtendrá sumando los valores obtenidos como resultado de la estimación de los aspectos citados, de acuerdo con la siguiente tabla de conversión:

Descripción del nivel de impacto	Valores conversión
Muy limitado	<5
Limitado	=5
Significativo	=6
Muy significativo	>6

El proceso de cálculo del riesgo deberá efectuarse teniendo en cuenta la situación inicial del tratamiento y la situación prevista tras la implantación de controles (esto es, el riesgo residual).

Los tratamientos solo podrán iniciarse cuando el riesgo residual tras la ejecución del proceso anterior sea bajo.

Los tratamientos cuyo riesgo residual sea medio, se iniciarán únicamente con una autorización de la Dirección.

Los tratamientos cuyo riesgo residual sea alto no podrán efectuarse en ningún caso. Si se desea llevar a cabo el tratamiento, deberá efectuarse una consulta a la autoridad de control competente (en este caso, a la Agencia Española de Protección de Datos).

4. REVISIÓN DE ANÁLISIS DE RIESGOS Y EVALUACIONES DE IMPACTO

Deberá efectuarse un seguimiento de la implantación de las medidas señaladas en el plan de acción de cada análisis de riesgos o evaluación de impacto cada tres meses hasta el cierre efectivo de las mismas.

Los análisis de riesgos y evaluaciones de impacto efectuadas se revisarán con una periodicidad anual y deberán volver a efectuarse en caso de que cambien significativamente las condiciones del tratamiento.

5. APÉNDICES

Apéndice I. Modelo de análisis de riesgos inicial

Apéndice II. Modelo de evaluación de impacto sobre la protección de datos.

APÉNDICE I

Modelo de Análisis de riesgos



Modelo
_Redexis_Análisis de r

APÉNDICE II

Modelo de evaluación de impacto sobre la protección de datos



Modelo_Redexis_Evaluaciones de impacto.x

ANEXO V

POLÍTICA DE GESTIÓN DE ENCARGADOS DEL TRATAMIENTO

1. INTRODUCCIÓN

Los Responsables del Tratamiento tienen la obligación de seleccionar de forma diligente aquellos proveedores de servicios que tendrán acceso a sus datos de carácter personal. Para cumplir de forma adecuada con la obligación arriba referida, con carácter previo a la contratación de un Encargado del Tratamiento, el Responsable del Tratamiento deberá verificar la idoneidad de la organización que pretende contratar.

Adicionalmente, el Responsable del Tratamiento deberá firmar un contrato con el Encargado del Tratamiento seleccionado en el que se contemplen los aspectos detallados en la normativa y durante la vigencia del contrato, el responsable del tratamiento deberá llevar a cabo auditorías (al menos, de los principales proveedores) con la finalidad de verificar el correcto tratamiento de los datos personales objeto del servicio.

2. OBJETIVO Y ÁMBITO DE APLICACIÓN

La presente Política resulta de aplicación a todos los trabajadores y colaboradores de Redexis que desarrollen funciones relacionadas con la selección o contratación con proveedores de servicios con acceso a datos personales responsabilidad de Redexis.

El objetivo de esta es desarrollar un protocolo interno de actuación que permita la gestión de los Encargados del Tratamiento y el cumplimiento de las obligaciones previstas en el artículo 28 del RGPD a las que se ha hecho referencia en el apartado anterior.

Para ello, se establecen instrucciones que deberán seguir los distintos responsables de la contratación de los proveedores y el control del servicio prestado diferenciando cuatro momentos del ciclo de vida del servicio:

- I. Con carácter previo a la contratación.
- II. En el momento de la formalización del contrato.
- III. Durante la prestación del servicio.
- IV. A la finalización del contrato.

La contratación de Encargados del Tratamiento domiciliados fuera del EEE, o que realicen una parte sustancial del tratamiento fuera del mismo, requiere la aplicación de garantías específicas. Si en cualquier fase del ciclo de vida del servicio se detecta que una prestación de servicios implica tratamiento de datos fuera del EEE, dicha circunstancia deberá ser puesta en conocimiento del DPO de Redexis.

3. VERIFICACIONES PREVIAS A LA CONTRATACIÓN DE UN PROVEEDOR

Con la finalidad de valorar la idoneidad del proveedor para ser Encargado del Tratamiento se solicitará al mismo que aporte el formulario que se incorpora como **Apéndice I** debidamente cumplimentado.

En caso de que, tras la valoración de lo expuesto en este apartado, se considere que el Encargado del Tratamiento cumpla de forma satisfactoria con la normativa de protección de datos, se procederá a la firma de un contrato que contenga las garantías establecidas en el RGDP.

4. CONTRATO DE ENCARGADO DEL TRATAMIENTO

Los proveedores seleccionados de acuerdo con el procedimiento descrito firmarán un contrato en el que se regule de forma detallada el tratamiento de Datos que realizarán por cuenta de Redexis. En este sentido, se podrá optar por la firma de un contrato específico sobre protección de datos o por la inclusión de una cláusula en los acuerdos firmados con los proveedores.

No podrá iniciarse ninguna actividad de tratamiento de datos por parte de terceros sin que se haya firmado el correspondiente acuerdo que deberá ser revisado con carácter previo a su firma por la asesoría jurídica de Redexis Gas. En el **Apéndice II**, se incluye el modelo a utilizar en estos casos.

Cualquier subcontratación de servicios por parte del Encargado del Tratamiento seleccionado que implique acceso a datos de carácter personal debe ser autorizada por Redexis por alguno de los siguientes medios:

- En el contrato/cláusula firmada con el Encargado del Tratamiento.
- Mediante comunicación escrita, en cualquier momento posterior a la firma del contrato.

El Encargado del Tratamiento deberá estar en disposición de aportar un listado de subcontratistas en caso de ser requerido para ello por Redexis, y de los correspondientes contratos firmados con ellos en materia de protección de datos.

Los contratos firmados se almacenarán por los responsables del servicio, siguiendo las normas generales para conservación y custodia de otro tipo de acuerdos. Adicionalmente, se remitirá una copia escaneada al DPO quien tendrá una relación actualizada de los

contratos encargados del mantenimiento existentes y de sus características esenciales a efectos de protección de datos de carácter personal.

5. SEGUIMIENTO DEL CONTRATO

A instancias del DPO, se realizarán controles y revisiones periódicas de aquellos Encargados del Tratamiento que presten servicios de especial relevancia desde el punto de vista de la normativa de protección de datos de carácter personal, que podrán consistir en:

- La solicitud de renovación de certificados de auditores/consultores externos.
- La autorización de auditoría presencial por auditores seleccionados por Redexis.
- La exhibición de determinados documentos: por ejemplo, listado de subcontratistas autorizados, registro de actividades de tratamiento efectuadas en nombre de Redexis.

Cualquier revisión o control deberá quedar documentada.

6. FINALIZACIÓN DEL SERVICIO.

A la finalización del servicio el Responsable del Contrato se encargará, según proceda y se haya acordado con el Encargado del Tratamiento, de:

- Solicitar la devolución de los datos a través de un mecanismo seguro.
- Solicitar un certificado emitido por el Encargado del Tratamiento en el que se declare que no se conservan Datos de Redexis, y que cualquier soporte o documento que los contuviera ha sido destruido de forma segura.
- Solicitar un certificado emitido por el Encargado del Tratamiento en el que garantice que los Datos se conservarán bloqueados durante el tiempo necesario para atender las responsabilidades derivadas del servicio, procediéndose tras dicho plazo a su destrucción.

Todos los certificados emitidos como cierre del servicio serán remitidos al DPO para su archivo.

7. PRESTACIONES DE SERVICIOS ENTRE EMPRESAS DEL GRUPO

Cuando el proveedor del servicio con acceso a los Datos sea una empresa del Grupo Redexis, se presumirá que cumple los requisitos de idoneidad necesarios, y se procederá, sin necesidad de control o verificación previa, a la firma del modelo de contrato que figura en el **Anexo II**.

8. CONTRATOS CON TERCEROS QUE NO TENGAN LA CONDICIÓN DE ENCARGADOS DEL TRATAMIENTO

Para aquellos supuestos en los que proceda a la formalización de contratos, acuerdos o convenios con terceros y estos no asuman la condición de encargado del tratamiento y, por tanto, no se les cedan datos de carácter personal para que sean tratados por parte de estos, se insertará una cláusula que garantice que las partes asumen las obligaciones que les corresponden de acuerdo con la legislación vigente en materia de protección de datos de carácter personal y que los datos de los firmantes y las personas de contacto serán tratados por las partes en base al interés legítimo de cada entidad, con la exclusiva finalidad de gestionar adecuadamente el contrato y mantener el contacto comercial entre las partes. Asimismo, se hará constar la facultad que corresponde a los afectados de ejercer los derechos que la legislación reconoce en materia de protección de datos de carácter personal ante el Responsable del Tratamiento.

Se adjunta como **Apéndice III**, a la presente política modelo de cláusula a introducir en los contratos o acuerdos que se celebren con terceros, en que estos no tengan la condición de encargados del tratamiento.

APÉNDICE I
Formulario previo.

ANEXO 1: Información de gobierno corporativo a suministrar por los proveedores del Grupo REDEXIS

1. **Nombre del Proveedor:** _____
Dirección: _____
Teléfono: _____ **E-mail:** _____
2. **¿El Proveedor ha nombrado un Delegado de Protección de Datos o Data Protection Officer (DPO)?**
 Sí _____ No _____
 Si la respuesta es que sí, por favor aporte más información:

3. **¿El Proveedor cuenta con un departamento / área de seguridad de la información o un Chief Security Officer?:**

4. **¿El Proveedor realiza auditorías periódicas para verificar el nivel de seguridad aplicable a los tratamientos que efectúa por terceros?**
 Sí _____ No _____
 Si la respuesta es que sí, por favor, aporte certificado emitido por el auditor o copia del informe correspondiente.

5. **¿El Proveedor cuenta con alguna certificación de seguridad?**
 Sí _____ No _____
 Si la respuesta es que sí, por favor, detalle:

6. **¿El Proveedor o alguna de sus filiales ha sido sancionado o inspeccionado en alguna ocasión por la Agencia Española de Protección de Datos o por alguna autoridad europea de protección de datos?**
 Sí _____ No _____
 Si la respuesta es que sí, por favor, detalle:

7. **¿El Proveedor está adherido a algún código de conducta que marque pautas relativas a protección de datos?**

8. **¿El Proveedor dispone de una política o protocolo interno para la gestión de brechas de seguridad?**

9. **¿El Proveedor mantiene actualizado un registro de actividades de tratamiento (incluyendo las realizadas por cuenta de terceros)?**

10. **¿El Proveedor dispone de una política o protocolo interno relativo a la gestión de derechos de los afectados?**

11. **¿El Proveedor cumple adecuadamente con las obligaciones establecidas en la normativa de protección de datos? ¿Podría aportar certificado de consultores/asesores/auditores externos que así lo acrediten?**

Con la firma del presente documento certifico que la anterior información es veraz y precisa.

Nombre:
Firma:

Cargo:
Fecha:

APÉNDICE II

Modelo de cláusula de Encargado del Tratamiento.

CLÁUSULA [*]. - PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Las Partes asumen las obligaciones que les corresponden de acuerdo con la legislación vigente en materia de protección de datos de carácter personal. El objeto del presente contrato implica el acceso de [*] (en adelante, el "**Encargado del tratamiento**" o el "**Encargado**") a los datos (en adelante, los "**Datos**") de [*] (en adelante, el "**Responsable del tratamiento**" o el "**Responsable**").

2. El tratamiento se efectuará en los locales del Encargado y consistirá en:

*[*Descripción de la finalidad, de las tareas autorizadas a realizar, de los datos de carácter personal objeto del tratamiento y de los afectados]**

3. En cumplimiento de Reglamento de datos personales (en adelante, "RGPD"), el Encargado se compromete a:

- a. Utilizar los Datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este contrato. En ningún caso podrá utilizar los Datos para fines propios.
- b. Tratar los Datos de acuerdo con las instrucciones del Responsable del tratamiento.
- c. Llevar, por escrito, un registro de las actividades de tratamiento efectuadas por cuenta del Responsable, que se encontrará a disposición del Responsable y AEPD.
- d. No comunicar los Datos a terceras personas, salvo que cuente con la autorización expresa del Responsable del tratamiento.

Queda prohibida cualquier transferencia de Datos fuera del Espacio Económico Europeo, que no sea autorizada por escrito por el Responsable.

- e. Mantener el deber de secreto respecto a los Datos a los que haya tenido acceso en virtud del presente contrato, incluso después de que finalice su objeto.
- f. Garantizar la confidencialidad de los datos y la adopción de las medidas de seguridad correspondientes.
- g. Asistir al Responsable en la respuesta al ejercicio de los derechos del afectado, cuando resulte preciso.
- h. Dar apoyo al Responsable en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

- i. Llevar a cabo un análisis de riesgos e implementar medidas de seguridad adecuadas en base al mismo, en caso de realizar tratamientos de Datos fuera de las instalaciones del Responsable.
 - j. Comunicar al Responsable inmediatamente las violaciones de la seguridad de los Datos de las que tenga conocimiento, informándole al menos de la naturaleza de la violación, las medidas adoptadas, las posibles consecuencias de la violación y la identificación de las que pueda obtenerse más información.
 - k. Una vez finalice el presente contrato, suprimir o devolver al Responsable, o a quien éste designe los Datos y destruir cualquier copia que esté en su poder.
 - l. Poner a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el Responsable u otro auditor autorizado por él.
4. El Encargado sólo podrá subcontratar con otras empresas previa autorización expresa del Responsable, en este caso el subcontratista deberá de cumplir las obligaciones establecidas en esta cláusula debiendo el Encargado inicial requerirle para ello, quien a sí mismo responderá ante el Responsable por las actuaciones llevada a cabo por el subcontratista.
5. El Encargado mantendrá indemne al Responsable de cualquier responsabilidad que se derive directa o indirectamente del incumplimiento por parte del Encargado de las obligaciones fijadas en esta cláusula o la normativa aplicable.
6. Los datos de los firmantes serán tratados por el Responsable y el Encargado, en base al interés legítimo de cada entidad, con la exclusiva finalidad de gestionar adecuadamente el contrato y mantener el contacto comercial entre las partes. Los afectados pueden ejercer sus derechos dirigiéndose al Responsable o al Encargado, según corresponda, en las direcciones de contacto que figuran en el encabezamiento de este contrato.

APÉNDICE III**Modelo de cláusula general de protección de datos sin encargado de tratamiento****CLÁUSULA [*]. - PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

Las Partes asumen las obligaciones que les corresponden de acuerdo con la legislación vigente en materia de protección de datos de carácter personal. Los datos de los firmantes y las personas de contacto serán tratados por ambas partes en base al interés legítimo de cada entidad, con la exclusiva finalidad de gestionar adecuadamente el contrato y mantener el contacto comercial entre las partes. Los afectados pueden ejercer sus derechos dirigiéndose al Responsable del Tratamiento en las direcciones de contacto que figuran en este contrato.

ANEXO VI

POLÍTICA DE ATENCIÓN AL EJERCICIO DE DERECHOS

1. OBJETO Y ÁMBITO DE APLICACIÓN

El RGPD en sus artículos 15 a 22 así como la LOPD en su artículo 12 regulan los derechos de los interesados en materia de protección de datos que pueden ser ejercidos directamente ante el Responsable del Tratamiento.

Concretamente la normativa de protección de datos reconoce los siguientes derechos a los titulares de datos de carácter personal que pueden ejercitar frente a la Compañía:

- Derecho de acceso (artículo 15 RGPD y artículo 13 LOPD).
- Derecho de rectificación (artículo 16 y 19 RGPD y artículo 14 LOPD).
- Derecho de supresión / “derecho al olvido” (artículo 17 y 19 RGPD y artículo 15 LOPD).
- Derecho a la limitación del tratamiento (artículos 18 y 19 RGPD y artículo 16 LOPD).
- Derecho a la portabilidad de los datos (artículo 20 RGPD y artículo 17 LOPD).
- Derecho de oposición (artículo 21 RGPD y artículo 18 LOPD).
- Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado (artículo 22 RGPD y artículo 18 LOPD).

2. RECEPCIÓN Y CONTESTACIÓN DE PETICIONES

Cualquier empleado de Redexis que tenga conocimiento o haya recibido por cualquier medio una solicitud de ejercicio de los derechos que reconoce la normativa de protección de datos deberá comunicarlo inmediatamente mediante correo electrónico al Delegado de Protección de Datos en el siguiente buzón: dpo@redexis.es indicando la fecha de su recepción.

Recibida la comunicación de ejercicio de derechos, el DPO procederá a su registro que tendrá carácter electrónico y será analizada de acuerdo a lo establecido a continuación:

1. Se valorará si es necesario solicitar información adicional al ejerciente del derecho, a efectos de verificar su identidad. Como norma general, no se solicitará dicha información:
 - a. A los clientes que utilicen un medio de contacto con Redexis que implique que se ha verificado su identidad previamente por parte de la Compañía (por ejemplo, el área de acceso restringido a clientes, en la que se opera con usuario y contraseña).
 - b. A las personas que pretendan dejar de recibir comunicaciones comerciales u oponerse al tratamiento de sus datos con finalidades relacionadas con la elaboración de perfiles.

2. Se contactará con las áreas implicadas en la atención al ejercicio de derechos (por ejemplo, los responsables de aplicaciones en las que se almacenen datos personales de ejerciente).
3. Se analizará si la atención del ejercicio del derecho requerirá más de un mes.

Una vez analizada se procederá a dar respuesta a la solicitud por el mismo cauce por el que se recibió dicha petición, en el plazo de un mes desde la recepción de la misma, contado de fecha a fecha. Deberá responderse en todo caso al afectado, aunque se deniegue el ejercicio del derecho. En este caso, se informará de las razones por las que se ha denegado y de la posibilidad de acudir a la Agencia Española de Protección de Datos (artículo 12.4 RGPD).

Excepcionalmente, el anterior plazo podrá extenderse en dos meses adicionales, debiendo comunicar dicha circunstancia dentro del primer mes de la ampliación, cuando (i) la atención del ejercicio del derecho resulte especialmente compleja por razones técnicas o (ii) la Compañía haya recibido un número de peticiones un número elevado de peticiones de forma que resulte imposible dar cumplimiento con la respuesta en el plazo de un mes.

ANEXO VII

POLÍTICA DE PLAZOS DE CONSERVACIÓN Y DOCUMENTACIÓN EN SOPORTE PAPEL

1. OBJETIVO Y ÁMBITO DE APLICACIÓN

El objetivo de la presente Política es determinar plazos generales de retención de los datos de carácter personal tratados bajo responsabilidad de Redexis, en cumplimiento de lo dispuesto en el RGPD, que obliga a los Responsables del Tratamiento a fijar plazos de conservación para los datos personales que recogen y almacenan, en función de las finalidades para las que dichos datos fueron recabados inicialmente.

A estos efectos se acompaña a la presente política el **Apéndice I** que incorpora la **Tabla de Plazos Máximos de Conservación por Actividad de Tratamiento**.

Dichos plazos se facilitan de forma orientativa y podrán ser modificados en supuestos justificados, siempre previo análisis y aprobación del DPO de Redexis.

Adicionalmente, esta Política incluye las normas básicas de **conservación y archivo de documentación en soporte papel**. Se regula de esta forma el almacenamiento de la documentación en papel hasta que deba procederse a su destrucción de acuerdo a los plazos fijados en la presente política.

Esta Política resulta de aplicación a todos los trabajadores y colaboradores de Redexis.

2. PLAZOS GENERALES DE CONSERVACIÓN DE DATOS

Sin perjuicio de los plazos recogidos en el Anexo I que se refiere en el apartado anterior y que servirán de marco, cada responsable funcional deberá determinar los plazos de conservación aplicables a los datos personales que genere en su actividad diaria de acuerdo con un criterio de utilidad y operatividad para el desarrollo de la misma. Para ello deberán tener en cuenta al menos, los siguientes factores:

- Existencia de una relación contractual vigente con el usuario, cliente o proveedor.
- Posibilidad de ejercer acciones legales o reclamaciones relacionadas con el tratamiento.
- Utilidad de los datos para Redexis.
- Cumplimiento de obligaciones legales de aplicación a los sectores donde actúa Redexis.

Los responsables funcionales deberán incluir los plazos de conservación en cada RAT y comunicarlo al DPO.

En caso de que detecten que en su área se tratan **datos personales que no puedan ser incluidos en ninguna de las previstas en las actividades de tratamiento recogidas en el Apéndice I**, podrá ponerse en contacto con el DPO para solicitar información adicional.

Transcurridos los plazos de conservación previstos por cada área o departamento, **los datos se bloquearán durante un plazo de tres años** antes de su eliminación definitiva de forma segura.

3. NORMAS ESPECÍFICAS PARA EL ALMACENAMIENTO DE DATOS EN SOPORTE PAPEL

Los departamentos o áreas que generen documentos en papel en el desarrollo de sus actividades diarias deberán almacenarlos en **armarios, archivadores o dependencias que dispongan de un sistema de cerrado con llave o mecanismo equivalente (por ejemplo, tarjetas electrónicas, códigos o pins, etc.)**.

El archivo podrá realizarse:

- En armarios, archivadores, cajoneras, etc. individuales, de forma que cada usuario será el responsable único de la documentación que almacena en los mismos.
- En dependencias comunes. En el caso de que exista una dependencia destinada a servir de archivo común para distintos usuarios, se designará un responsable del archivo, encargado de custodiar la llave el acceso al mismo. Si fuera necesario, se instalarán armarios cerrados con llave dentro de la dependencia común para garantizar que sólo las personas autorizadas pueden consultar la información contenida en los mismos.

Los responsables funcionales de las diferentes actividades de tratamiento fijarán en coordinación con los departamentos o áreas a los que afecte, los **criterios de archivo** de aplicación, en función de sus necesidades, que permitan mantener la información en soporte papel organizada y ordenada de forma lógica, y que faciliten la búsqueda de documentos.

Se recomendará que los criterios de archivo se recojan por escrito.

Los datos conservados en soporte papel también están sometidos a la norma general que obliga a no conservarlos durante más tiempo del necesario. Por tanto, los plazos generales señalados en el Anexo I también resultan de aplicación a los documentos en soporte papel.

4. DESTRUCCIÓN DE DOCUMENTACIÓN EN SOPORTE PAPEL

Cada responsable funcional será el encargado de tratar adecuadamente los documentos en soporte papel una vez **ya no sean necesarios** para el desarrollo de sus funciones.

Los documentos en soporte papel deben depositarse en el buzón de papel confidencial habilitado al efecto o destruirse de forma segura mediante la destructora de papel.

APÉNDICE I

TABLA PLAZOS MÁXIMOS DE CONSERVACIÓN POR ACTIVIDAD DE TRATAMIENTO

A continuación, se incluye la tabla que establece los plazos máximos de conservación establecidos por cada actividad de tratamiento de las sociedades del Grupo Redexis:

Actividad de Tratamiento	Categoría de datos personales	Plazos de conservación
RRHH/Personal Externo	- Datos identificativos y de contacto. - Datos académicos y profesionales. - Datos económicos, financieros y de seguros. - Detalles del empleo. - Circunstancias sociales. - Datos relativos a la utilización de vehículos de empresa y parking para trabajadores. - Datos necesarios para la gestión de viajes y pagos de dietas.	6 años
Selección de Personal	- Datos identificativos y de contacto. - Datos académicos y profesionales. - Circunstancias sociales.	3 años
Prevención Riesgos Laborales	- Datos identificativos y de contacto. - Datos académicos y profesionales. - Detalles del empleo. - Circunstancias sociales. - Datos relativos a la salud.	6 años
Cientes GLP	- Datos identificativos y de contacto. - Datos económicos, financieros y de seguros. - Características personales. - Número CUPS o contador. - Datos de bienes y servicios recibidos. - Datos biométricos con el fin de identificar de manera única a una persona natural.	20 años
Cientes SS	- Datos identificativos y de contacto. - Datos económicos, financieros y de seguros. - Transacciones de bienes y servicios: Bienes y servicios recibidos por afectado. - Número CUPS o contador.	20 años
Asesoría Jurídica	- Datos identificativos y de contacto. - Datos incluidos en expedientes administrativos y judiciales. - Datos que revelan la afiliación sindical.	20 años

Actividad de Tratamiento	Categoría de datos personales	Plazos de conservación
Usuarios de la Red	- Datos identificativos y de contacto. - Datos económicos, financieros y de seguros. - Características personales. - Datos biométricos con el fin de identificar de manera única a una persona natural.	20 años
Inspecciones Obligatorias	- Datos identificativos y de contacto. - Datos de identificación del punto de suministro - Datos bancarios de inspectores - CIF - NIF del instalador - Resultado de la inspección - Factura escaneada	20 años
Atención Incidencias y Centro de Control	- Datos identificativos y de contacto. - Datos sobre incidencias detectadas durante la inspección. - Datos de identificación del punto de suministro.	20 años
Gestión de Reclamaciones	- Datos identificativos y de contacto. - Queja, consulta o reclamación presentada. - Datos de identificación del punto de suministro (dirección postal o nº cups).	20 años
Videovigilancia y Control Acceso	- Datos identificativos y de contacto.	1 mes
Facturación y Contabilidad Proveedores	- Datos identificativos y de contacto. - Datos de facturación.	6 años
Balances y Repartos	- Datos identificativos y de contacto.	20 años
Lecturas	- Datos identificativos y de contacto. - Datos económicos, financieros y de seguros. - Circunstancias sociales: características del alojamiento - nº CUPS	20 años
Sistemas	- Datos identificativos y de contacto. - nº CUPS	20 años
Facturación/Cobros/Contabilidad Clientes	- Datos identificativos y de contacto. - Datos académicos y profesionales. - Datos económicos, financieros y de seguros. - Circunstancias sociales. - Características personales. - nº CUPS.	20 años
Operaciones Domiciliarias y Mantenimiento Movilidad	- Datos identificativos y de contacto. - Características personales. - nº CUPS. - Muestras biométricas.	20 años
Control Horario	- Datos identificativos y de contacto. - Detalles del empleo.	4 años

ANEXO VIII

PROTOCOLO GESTIÓN DE BRECHAS DE SEGURIDAD

1. DETECCIÓN E IDENTIFICACIÓN DE BRECHAS DE SEGURIDAD. COMUNICACIÓN DE BRECHAS DE SEGURIDAD

Se considera “brecha de seguridad de los datos personales” toda **violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados, o la comunicación o acceso no autorizados a dichos datos.**

Cualquier usuario que tenga conocimiento efectivo de una brecha de seguridad, o que sospeche que ha podido producirse, deberá comunicarlo inmediatamente mediante al correo habilitado al efecto: dpo@redexis.es

La notificación contendrá como mínimo la siguiente información la fecha de detección del incidente y la descripción del incidente. Podrá añadirse cualquier otra circunstancia que se considere relevante.

El **Apéndice I** contiene un modelo de comunicación interna de brecha. No obstante, no es necesario disponer de toda la información que se señala en el mismo para llevar a cabo la primera comunicación. Es fundamental que la comunicación de la brecha se realice con celeridad para contener posibles efectos negativos.

2. REGISTRO, ANÁLISIS, E INVESTIGACIÓN DE LAS BRECHAS DE SEGURIDAD

Recibido el aviso de una posible Brecha de Seguridad, ésta será registrada por el DPO en el registro de brechas de seguridad (**Apéndice II**), que tendrá carácter electrónico.

En este registro, el DPO documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en la normativa aplicable. El Registro deberá mantenerse actualizado y contendrá, al menos, la siguiente información: (i) fecha de notificación o detección de la brecha de seguridad, (ii) descripción de la brecha de seguridad, (iii) personas de contacto, (iv) categoría de personas afectadas y número de registros afectados, (v) tipo de datos personales comprometidos, (vi) riesgos detectados, (vii) investigaciones realizadas y medidas adoptadas, (viii) conclusión sobre el origen de la brecha de seguridad y las actuaciones posteriores a realizar al respecto, incluyendo, en su caso, las comunicaciones realizadas a la autoridad de control o a los posibles afectados.

Asimismo, comunicada la existencia de una posible brecha de seguridad, el DPO procederá a analizarla en colaboración con el Departamento de Sistemas, los responsables funcionales de los tratamientos afectados y las unidades internas que se considere conveniente.

Si la gravedad de la situación lo requiere, se formará un Comité de Investigación, que se reunirá de urgencia si es necesario, y que estará formado por el personal técnico y operativo que designe el DPO. También podrá formar parte del Comité cualquier técnico y asesor externo que resulte conveniente a juicio del DPO.

Todo el personal de la compañía deberá colaborar con el DPO en lo que se le solicite con prioridad sobre la realización de cualquier otra tarea.

El DPO documentará el resultado de las tareas de análisis e investigación de la brecha, procediendo a una valoración de su severidad, según lo que se indica en el apartado siguiente.

Igualmente, el DPO trasladará sus conclusiones a las unidades que corresponda al objeto de que adopten las medidas necesarias para mitigar o eliminar los riesgos asociados a la brecha de seguridad. El DPO también informará a la Dirección de la Compañía y a las unidades que corresponda sobre las investigaciones realizadas y las conclusiones a que hubiera llegado al respecto.

3. EVALUACIÓN DE LA SEVERIDAD DE LA BRECHA DE SEGURIDAD

La AEPD en su [“Guía para la notificación de brechas de datos personales”](#), de junio de 2021, proporciona criterios generales para la valoración de las Brechas de Seguridad. Sin embargo, este documento no establece una metodología concreta para realizar el análisis que deba ser implementada por los responsables de tratamiento.

Por ese motivo, Redexis ha elaborado una herramienta propia que permite realizar el análisis de la severidad de la brecha de forma objetiva.

3. 1. Modelo y Criterios de Evaluación de la Severidad de la Brecha de Seguridad

El **Apéndice III** “Informe de Brecha de Seguridad y Evaluación de Severidad” de este procedimiento contiene, en su hoja “2. Evaluación de Severidad”, el modelo de valoración de la gravedad de la Brecha de Seguridad. El objetivo de este modelo es proveer al DPO de un instrumento que le permita realizar una valoración objetiva de las circunstancias en las que se ha producido la Brecha de Seguridad, así como sus posibles consecuencias para los Interesados.

En atención al riesgo para los derechos e intereses de los Afectados que implica cada una de las circunstancias recogidas en **Anexo III – Hoja “2. Evaluación de Severidad”**, se les ha asignado un valor numérico más o menos elevado. La suma de los valores asignados a las circunstancias concurrentes a la Brecha de Seguridad analizada dará como resultado la severidad de la Brecha de Seguridad. Este resultado se clasificará según el siguiente criterio:

Valor de Severidad	
Menos de 10	Baja
Más de 10 pero menos de 20	Media
Más de 20	Alta

Las circunstancias recogidas en el modelo de “Evaluación de Severidad” se han agrupado en torno a los siguientes parámetros:

1º PARÁMETRO – TIPO DE BRECHA DE SEGURIDAD

Se clasificará la Brecha de Seguridad dentro de una de las siguientes categorías:

Confidencialidad	Revelación no autorizada o accidental de los Datos Personales, o su acceso.
Disponibilidad	Pérdida de acceso accidental o no autorizada a los Datos Personales, o su destrucción.
Integridad	Una alteración no autorizada o accidental de los Datos Personales.

Se otorga un mayor valor de severidad a las Brechas de Seguridad de confidencialidad, seguridad de las brechas de disponibilidad y por último las de integridad.

2º PARÁMETRO – NATURALEZA Y VOLUMEN:

- **Naturaleza de los Datos personales afectados**

Se identificarán las categorías de Datos Personales por la Brecha de Seguridad.

A cada categoría identificada se le asignará un valor, siendo este más elevado cuando se trata de categorías de datos especialmente protegidos.

- **Volumen aproximado de Interesados afectados**
- **Número de registros afectado**

Se debe indicar, de manera aproximada, el número de registros afectados por cada interesado. Se entiende por registro los campos o ítems de información referidos a cada individuo, no el número de individuos afectados.

3º PARÁMETRO – FACILIDAD DE IDENTIFICACIÓN DE LOS INTERESADOS

En función de los datos que hayan sido comprometidos por la Brecha de Seguridad, la identificación de los Afectados puede ser más o menos compleja. Cuanto más fácil sea la identificación de los Interesados existe una mayor probabilidad de la brecha de seguridad de lugar a actividades delictivas (por ejemplo, fraudes o suplantaciones de identidad) o a daños reputacionales o psicológicos para los Interesados.

4º PARÁMETRO – CARACTERÍSTICAS DE LOS INTERESADOS

Se identificarán todas las categorías de Interesados cuyos datos se han podido ver comprometidos por la brecha de seguridad (Clientes, empleados, pacientes, etc.).

El modelo de valoración del impacto de la Brecha de Seguridad (**Anexo III - Hoja “2. Evaluación de Severidad”**) asocia un nivel de riesgo concreto a distintas categorías de afectados (clientes, empleados, menore de edad, etc.) .

En atención a la vulnerabilidad de los Interesados se ha atribuido un valor de impacto superior a algunas categorías.

5º PARÁMETRO – GRAVEDAD DE LAS CONSECUENCIAS

El análisis de este parámetro permitirá, según las variables reflejadas en el modelo de evaluación de severidad de la Brecha de Seguridad, determinar la probabilidad de que los Afectados sufran consecuencias negativas derivadas de la misma. Para realizar la valoración de este parámetro se analiza:

- **¿Quiénes han tenido o podrían tener acceso a los datos?** Se diferencia entre aquellas Brechas de Seguridad propiciadas por la acción de terceros y aquellas producidas debido a errores o circunstancias fortuitas.
- **¿Cuáles son las posibles consecuencias de la Brecha de Seguridad?** El riesgo de que los Interesados sufran consecuencias negativas debido a la Brecha de Seguridad debe modularse en función del tipo de datos afectados y la identidad de los terceros que han tenido acceso a los datos.

3.2. Análisis de Conclusiones

Una vez realizada la evaluación de la severidad de la Brecha de Seguridad, el DPO deberá valorar si es necesario notificar la misma a la AEPD y a los Interesados.

- **Notificación a la AEPD:** Si el resultado de la evaluación de la Brecha de Seguridad da un resultado de severidad alta, se deberá informar a la AEPD.

En aquellos casos en los que el resultado es medio, el DPO sopesará si las circunstancias identificadas son lo suficientemente graves como para que sea necesaria la notificación

a la AEPD. Por ejemplo, en todas aquellas Brechas de Seguridad en las que se vean afectados datos bancarios de los Interesados o Datos Personales que puedan dar lugar a una suplantación de identidad, se recomienda notificar a la AEPD.

- **Notificación a los Interesados:** El DPO deberá valorar la necesidad de informar a los Interesados en todos aquellos casos en los que el resultado de la evaluación de la Brecha de Seguridad sea de severidad media o alta.

No obstante lo anterior, el criterio establecido en la evaluación de severidad es meramente orientativo. Por lo tanto, el DPO siempre deberá justificar la toma de decisiones en una valoración completa de las circunstancias en las que se ha producido la Brecha de Seguridad.

El DPO comunicará los resultados de su análisis a la Dirección que será quien determine si se procede o no a realizar la notificación o notificaciones propuestas.

4. ACCIONES CORRECTORAS Y SEGUIMIENTO

Las Brechas de Seguridad que tengan su origen en la inaplicación o defectuosa implantación de controles técnicos, o en ataques externos que vulneren los sistemas de Redexis, requerirán la realización de una auditoría de seguridad efectuada por una consultora independiente.

El DPO revisará anualmente las Brechas de Seguridad notificadas y hará un seguimiento de las acciones correctoras implantadas.

5. APÉNDICES

- **Anexo I:** Ficha de comunicación de Brecha de Seguridad
- **Anexo II:** Registro de Incidentes y Brechas de Seguridad
- **Anexo III:** Informe de Brecha de Seguridad

ANEXO I: Ficha de comunicación de Brecha de Seguridad



Apendice I Ficha de comunicación de Brecha de Seguridad

ANEXO II: Registro Incidentes y Brechas de Seguridad



Apendice II Registro Incidentes y Brechas de Seguridad

ANEXO III: Informe de Brecha de Seguridad



Apendice III Informe de Brecha de Seguridad



ANEXO IX

POLÍTICA DE GESTIÓN DE CAMPAÑAS DE MARKETING

1. OBJETO Y ÁMBITO DE APLICACIÓN

El objeto de este Anexo es definir unas normas generales que sirvan de marco básico para la actividad de diseño y gestión de campañas de marketing.

El envío de comunicaciones por correo electrónico o postal, ya sean internas (a personal de Redexis) o externas (a terceros ajenos a la organización), o la realización de llamadas telefónicas publicitarias, supone un tratamiento de datos personales. Como regla general, para estas operaciones se tratarán datos de identificación y de contacto (nombre y apellidos, correo electrónico, teléfono o domicilio).

No obstante, resulta importante resaltar que, dependiendo del medio por el que se efectúe la comunicación, pueden resultar de aplicación normas distintas al Reglamento General de Protección de Datos con preferencia sobre este:

- El envío de comunicaciones comerciales por medios electrónicos (correo electrónico, SMS, mensajes directos en redes sociales y mensajes “push”, entre otros) está regulado en el artículo 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (“LSSI”).
- La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (“LGT”) establece normas específicas aplicables a las llamadas a teléfonos promocionales fijos y móviles. Cuando se llama por teléfono a una persona que tiene la condición de consumidor (por ejemplo, un abonado al servicio de agua) se debe respetar lo dispuesto en Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (“LGDCU”).

Teniendo en cuenta la complejidad del marco normativo que regula estas actividades, se deberá consultar al DPO en el momento en el que se inicie la planificación de una campaña promocional, antes de tomar ninguna decisión relevante sobre la misma (por ejemplo, aprobación de presupuestos o contratación de proveedores).

2. CONCEPTO DE COMUNICACIÓN COMERCIAL. COMUNICACIONES EXCLUIDAS

Este Anexo se refiere a actividades promocionales, que no debemos confundir con los contactos meramente operativos o de servicio.

Llamamos comunicaciones operativas o de servicio a aquellas que son estrictamente necesarias para la prestación de un servicio contratado (o derivan de una relación

contractual que mantenemos con el receptor) y a aquellas que vienen impuestas por la legislación vigente. Ejemplos de las comunicaciones operativas son el envío de la nómina a un trabajador, la remisión de una factura a un proveedor o la reclamación de una deuda.

Como normal general, por tanto, las comunicaciones operativas derivan de un contrato o de una obligación legal.

El concepto de **comunicación comercial es muy amplio**¹. Comprende cualquier actividad promocional de la imagen y/o de los servicios de una entidad, ya sea directa o indirecta, incluso cuando se trate de asociaciones o fundaciones que no tiene ánimo lucro.

Así, enviar un correo electrónico informando de las acciones llevadas a cabo por una ONG tiene carácter comercial si no se remite a asociados o colaboradores de la misma que deban conocer dichas funciones por razón de su actividad. Son ejemplos de comunicaciones comerciales las comunicaciones relativas a descuentos en restaurantes y gimnasios para los empleados de Redexis, los boletines o *newsletters* en los que se informa sobre la actividad de Redexis, o las comunicaciones con ofertas de productos y servicios nuevos.

3. NORMAS GENERALES APLICABLES A ACCIONES PROMOCIONALES

Se establecen las siguientes normas generales, que se aplicarán independientemente del medio a través del cual se efectúe la promoción (teléfono, envío postal, correo electrónico, SMS u otros medios electrónicos):

1º. Podremos utilizar para la realización de acciones comerciales aquellos datos relativos a personas físicas que hayan sido obtenidos directamente por Redexis del afectado, utilizando las Políticas Informativas de Privacidad y los textos de recogida de consentimiento aprobados por Redexis.

También será posible emplear datos facilitados por terceros que nos garanticen que se han recogido cumpliendo con las obligaciones establecidas en la LSSI, el RGPD y el resto de normas aplicables, y se cumplan con el resto de condiciones establecidas en este Anexo.

2º. Los datos de personas físicas que hayan sido recogidos por Redexis cumpliendo lo indicado en el punto anterior solamente serán utilizados con fines promocionales cuando (i) los datos se encuentren actualizados y (ii) conste una prueba o evidencia del consentimiento del titular de los datos autorizando la recepción de publicidad.

¹ El Anexo a la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico define como comunicación comercial *"toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional"*.

Se **considerarán desactualizados** los datos que tengan una antigüedad mayor a 7 años (contando dicho plazo desde el momento de su recogida) y que no hayan sido utilizados en contactos regulares con el afectado. Es decir, se trata de datos que no consta que el afectado haya utilizado para ponerse en contacto con Redexis ni Redexis ha remitido comunicaciones al afectado empleándolos. Esta medida se ha adoptado en previsión de que circunstancias como fallecimiento del afectado; cambios de domicilio; cambio de teléfono, etc.

La prueba o evidencia del consentimiento podrá ser la correspondiente marcación en el CRM de Redexis.

3º. Entre los datos que se utilizarán para efectuar acciones promocionales figuran los siguientes:

- Datos obtenidos de Internet o Redes Sociales, aunque sean accesibles sin ninguna restricción. El hecho de que los datos estén disponibles en Internet no significa que podamos utilizarlos libremente para finalidades distintas a aquellas que motivaron su publicación.
- Datos obtenidos por Redexis directamente del afectado sin que este haya autorizado la posibilidad de seguir utilizando sus datos (por ejemplo, datos de asistentes a eventos que no han prestado su consentimiento a que mantengamos sus datos y les realicemos nuevas comunicaciones, o datos de usuarios de un servicio que no han aceptado recibir comunicaciones promocionales).
- Datos de personas que nos hayan solicitado expresamente que no volvamos a contactarlos.
- Datos respecto a los cuales no tenemos claro el origen.

4º. Cualquier compra de bases de datos a terceros deberá ser autorizada por el DPO.

5º. Las acciones de publicidad cruzada con otras entidades también deberán ser previamente aprobadas por el DPO.

6º. Los proveedores de servicios involucrados en la realización de campañas promocionales deberán firmar un contrato de encargo del tratamiento, de acuerdo con lo establecido en el Anexo V.

7º. Los datos referidos exclusivamente a empresas, que no incluyan información de personas de contacto, podrán ser utilizados libremente, a excepción de los correos electrónicos.

No obstante, está prohibido el envío de publicidad que no haya sido previamente autorizada por correo electrónico incluso en el caso de direcciones de correo genéricas.

4. NORMAS ESPECÍFICAS APLICABLES A LOS ENVÍOS POR E-MAIL Y OTROS MEDIOS ELECTRÓNICOS

La publicidad por medios electrónicos (e-mail, SMS, *WhatsApp*, servicios de mensajería de Redes Sociales, etc.) se percibe como especialmente molesta por parte de los receptores. Por tal motivo, Redexis ha establecido normas adicionales específicas.

1º. Aunque se cuente con el consentimiento del titular de los datos, no se le remitirán más de 10 comunicaciones comerciales en el plazo de un mes.

2º. Salvo autorización del DPO, las comunicaciones operativas o de servicio no incluirán textos adicionales de contenido publicitario.

3º. Como norma general, las encuestas se consideran comunicaciones comerciales a efecto de aplicación de la LSSI. Los envíos de encuestas a usuarios internos y externos deben ser aprobados por el DPO.

4º. Todas las comunicaciones comerciales deben incluir un método sencillo y gratuito para darse de baja de las mismas. Por ello, se deberá incluir uno de estos textos:

- OPCION 1: *“Si no desea recibir nuevas comunicaciones comerciales, envíe una solicitud indicando “BAJA” en el asunto del correo al buzón: [Indicar correo electrónico para tramitar bajas]”.*
- OPCION 2: *“Para no recibir nuevas comunicaciones, utilice este enlace: [enlace a sistema automático de baja]”.*

5º. Se revisará periódicamente la efectividad de los mecanismos puestos a disposición de los afectados para darse de baja de comunicaciones comerciales no deseadas.