GOBIERNO DE ESPAÑA MINISTERIO DE SANIDAD

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN Instituto de Salud Carlos III

05.03.2020

CONVENIO ENTRE EL MINISTERIO DE SANIDAD Y EL INSTITUTO DE SALUD "CARLOS III" PARA LA CUSTODIA Y GESTIÓN DEL REGISTRO ESTATAL DE ENFERMEDADES RARAS.

En Madrid, a

Por una parte, Dña. Pilar Aparicio Azcárraga, en nombre y representación del Ministerio de Sanidad en su calidad de Directora General de Salud Pública, Calidad e Innovación en virtud del Real Decreto 805/2018, de 29 de junio (B.O.E de 30 de junio de 2018) y actuando en el ejercicio de la competencia que le otorga el apartado sexto.2.c) de la Orden SSI/131/2013, de 17 de enero, sobre delegación de competencias del Ministerio de Sanidad.

Y de otra parte, Dña. Raquel Yotti Álvarez, como Directora del Instituto de Salud Carlos III (en adelante, ISCIII), Organismo Público de Investigación adscrito al Ministerio de Ciencia e Innovación, nombrada por Real Decreto 1029/2018, de 3 de agosto (BOE nº 188,de 4 de agosto), actuando en nombre y representación del mencionado Instituto y en ejercicio de las competencias atribuidas por el artículo 11del Real Decreto 375/2001, de 6 de abril, por el que se aprueba su Estatuto.

Interviniendo en función de sus respectivos cargos que han quedado expresados y en el ejercicio de sus mutuas facultades que a cada uno le están conferidas, con plena capacidad para formalizar este Convenio, y por ello.

EXPONEN

Primero.

La Ley 14/1986, de 25 de abril, General de Sanidad, habilita en su artículo 23 a las Administraciones Sanitarias para crear registros y analizar la información necesaria para el conocimiento de las distintas situaciones de las que pueden derivarse acciones de intervención de la autoridad sanitaria.

La Ley 16/2003, de 28 mayo, de cohesión y calidad del Sistema Nacional de Salud, regula en su artículo 53 que el Ministerio de Sanidad y Consumo, actual Ministerio de Sanidad, establecerá un sistema de información sanitaria del Sistema

Nacional de Salud que garantice la disponibilidad de la información y la comunicación reciprocas entre las Administraciones sanitarias.

La Estrategia en Enfermedades Raras del Sistema Nacional de Salud, aprobada por el Consejo Interterritorial del Sistema Nacional de la Salud, reunido el 3 de Junio de 2009 y actualizada el 11 de junio de 2014, pone en evidencia la necesidad de estimar de modo apropiado la incidencia y prevalencia de cada enfermedad, así como de mejorar el conocimiento sobre la historia natural de las enfermedades raras con el fin de adaptar las actuaciones en materia de atención sanitaria y poder realizar un mejor seguimiento de las mismas.

Por todo ello, y con el fin de garantizar la disponibilidad de la información y la comunicación recíprocas entre las administraciones sanitarias, se crea el Registro Estatal de Enfermedades Raras mediante el Real Decreto 1091/2015, de 4 de diciembre, por el que se crea y regula dicho Registro.

Segundo.

El ISCIII, como organismo de información sanitaria y documentación científica tiene como funciones, entre otras," la custodia y gestión de todo tipo de registro de interés sanitario que le sea encomendada por la autoridad y los Organismos científicos y profesionales" (artículo 3.7 del Real Decreto 375/2001, de 6 de abril).

Tercero.

El Real Decreto 1091/2015, de 4 de diciembre, establece que el Registro Estatal de Enfermedades Raras estará adscrito a la Dirección General de Salud Pública, Calidad e Innovación del Ministerio de Sanidad, siendo el órgano responsable del mismo (artículo 4.1), si bien, la gestión del registro se podrá encomendar al Instituido de Salud Carlos III, a través del Instituto de Investigación de Enfermedades Raras (artículo 4.2) (en adelante IIER) para el desarrollo de las funciones recogidas en el artículo 5.1 b),c), d), e) y f.

Cuarto.

Teniendo en cuenta la convergencia de los objetivos y la complementariedad de las acciones programadas tanto por la Dirección General de Salud Pública, Calidad e Innovación como por el ISCIII, de conformidad con el artículo 47 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, las partes acuerdan suscribir el presente Convenio que se regirá por las siguientes:

CLÁUSULAS

Primera. *Objetivo.*

El Ministerio de Sanidad (Dirección General de Salud Pública, Calidad e Innovación), órgano responsable del Registro Estatal de Enfermedades Raras y, por lo tanto responsable del tratamiento, requiere del ISCIII, como encargado del

tratamiento, la realización de las siguientes funciones recogidas en el artículo 5.1. del Real Decreto 1091/2015:

b) Organizar y gestionar el Registro Estatal de Enfermedades Raras.

c) Adoptar medidas que garanticen la confidencialidad, seguridad e integridad de los datos contenidos en el registro.

d) Obtener, depurar, integrar, procesar, analizar, comparar y evaluar la información sobre los casos de enfermedades raras en España, normalizándola de acuerdo con pautas homologadas internacionalmente.

e) Realizar informes y publicaciones periódicas que contendrán únicamente información disociada y, en su caso, agregada.

f) Colaborar y coordinarse en sus actuaciones con otros sistemas de información y registros de enfermedades raras autonómicas y de las ciudades con Estatuto de Autonomía.

Segunda. *Obligaciones de las partes*

1. ***Obligaciones de ambas.***

Las Partes se comprometen a cumplir la normativa aplicable en materia de protección de datos de carácter personal, que incluye:

a) las leyes y reglamentos locales aplicables en materia de protección de datos de carácter personal, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, 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 por el que se deroga la Directiva 95/46/CE ("Reglamento General de Protección de Datos"), la ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y

b) cualquier otra normativa vigente en el futuro que los complemente o sustituya.

2. Obligaciones del Instituto de Salud Carlos III.

El ISCIII, como encargado del tratamiento del Registro Estatal de Enfermedades Raras (ReeR), a través del director del IIER, se compromete a:

a) Desarrollar, mantener, actualizar y gestionar la aplicación informática del ReeR. Esto implica el desarrollo de las siguientes funciones:

1º. Gestión de los ficheros de datos enviados desde las Comunidades Autónomas.

- Asesoramiento y apoyo a las CCAA en las dudas de envío.
- Recepción de ficheros enviados desde las CCAA.
- Valoración de los ficheros desde el punto de vista de integridad y formato.
- Valoración del contenido de los ficheros revisando: el orden y la presencia o ausencia de las variables necesarias, los valores admitidos y no admitidos en

cada una de las variables, y posibles inconsistencias en el contenido de cada caso.
- Valoración de casos duplicados.
- Generación de mensajes de error indicando a la comunidad autónoma que información debe corregir: por fallo en la sintaxis del fichero y/o por fallo de contenido del fichero.
- Evaluación de la calidad de los datos.

2º. Generación del número de registro estatal que es el número asignado por el ReeR a cada individuo una vez que haya sido incorporado a la base de datos central y su envío a la comunidad autónoma correspondiente.

3º. Creación y mantenimiento de las tablas maestras.

4º. Gestión de los usuarios, perfiles, roles y privilegios de acceso.

5º. Explotación de los datos
- Definición del formato de informe
- Procesamiento y análisis estadístico de los datos
- Desarrollo del formato y su estandarización
- Elaboración de informes.

b) Tratar los datos personales siguiendo las instrucciones recogidas en el artículo 5.1. del Real Decreto 1091/2015, Los datos personales tratados son:
   1º. De las personas afectadas: datos identificativos (nombre y apellidos, NIF, número de la seguridad social, identificador de tarjeta sanitaria, número de registro autonómico y nacional, código del Sistema Nacional de Salud), datos socio-demográficos, sexo, edad, lugar de residencia, país de nacimiento, fecha y causa de defunción, datos clínico-epidemiológicos (enfermedad, fecha diagnóstico, base del diagnóstico, fuente de información y fecha de detección).
   2º. De los responsables y personas con acceso al registro: Nombre y apellidos, NIF, correo electrónico y teléfono y vinculación profesional.

c) Controlar que todos los miembros de su personal, autorizados para acceder a los datos personales del registro o para tratar esos datos, se hayan comprometido a respetar la confidencialidad de los datos personales sujetos a tratamiento, y que reciben la formación adecuada en materia de protección de datos de carácter personal.

d) Adoptar las medidas técnicas y organizativas apropiadas previstas en el Anexo II del Real Decreto 3/2010, de 8 de Enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, que permitan al Ministerio de Sanidad respetar plenamente los derechos de los interesados, incluidos los derechos de acceso, rectificación y/o supresión de sus datos personales y el derecho de limitación del tratamiento, en su caso; o

cualquier solicitud de una autoridad de supervisión formulada en virtud de la Normativa de Protección de Datos.

e) Ayudar al Ministerio de Sanidad a garantizar el cumplimiento de las obligaciones establecidas en los artículos 3 2 a 36 del Reglamento General de Protección de Datos, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del ISCIII.

f) Aplicar todas aquellas medidas descritas en los documentos que conforman la Política de protección de datos y la seguridad de la información del ISCIII. Dar apoyo al Ministerio de Sanidad en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

g) Apoyar al Ministerio de Sanidad en la realización de las consultas previas a la autoridad de control, cuando proceda.

h) Con motivo del vencimiento o resolución anticipada del Convenio, conservará los datos personales el tiempo necesario en virtud del derecho de la Unión Europea o de los Estados miembros, y cuando sea necesario para el cumplimiento de una misión realizada en interés público en el ámbito de la salud pública, con fines de investigación científica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamación, de conformidad con el Considerando 65 del Reglamento General de Protección de Datos.

i) Poner a disposición del Ministerio de Sanidad toda la información necesaria para que pueda realizar directamente o a través de un tercero que actúe en su nombre, cualquier comprobación, incluidas las auditorías en las instalaciones del ISCIII, que considere oportuna para verificar el cumplimiento de las obligaciones que se establecen en el presente convenio. La auditoría deberá ser notificada con una antelación mínima de cinco días y se deberá llevar a cabo durante el horario de apertura, sin que la actividad del ISCIII se vea afectada.

j) Adoptar las medidas técnicas y organizativas apropiadas a fin de proteger los datos personales del Ministerio de Sanidad incluidos en el registro frente a toda destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, teniendo en cuenta tanto la naturaleza como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas. Estas medidas deberán incluir, en particular:

1º. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

2º. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

3º. Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

k) No contratar a otro encargado del tratamiento para que lleve a cabo las operaciones de tratamiento de los datos personales del Ministerio de Sanidad sin la autorización previa y por escrito de este último, salvo para la gestión y/o mantenimiento de las aplicaciones informáticas necesarias para llevar a cabo las operaciones de tratamiento descritas.

   Cuando el ISCIII contrate a otro encargado del tratamiento (en adelante, el "subencargado del tratamiento") con arreglo a las condiciones descritas en el párrafo anterior, el subencargado del tratamiento deberá celebrar un contrato que recoja las mismas obligaciones que se establecen en estas cláusulas, en particular, en relación con la adopción de medidas de confidencialidad, de medidas técnicas y organizativas de seguridad apropiadas.

   El ISCIII es responsable de garantizar que el subencargado del tratamiento ofrezca las mismas garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento cumpla los requisitos de la Normativa de Protección de Datos.
   Si el subencargado del tratamiento incumpliese las obligaciones que le incumben en materia de protección de datos, el ISCIII responderá plenamente frente al Ministerio de Sanidad del cumplimiento de las obligaciones de dicho subencargado del tratamiento.

l) Notificar al Ministerio de Sanidad cualquier violación de la seguridad de los datos personales sin dilación indebida y, a más tardar, en un plazo de 72 horas a contar desde que tenga conocimiento de dicha violación, a través de correo electrónico u otros medios escritos trazables.
   Esta notificación deberá ir acompañada de cualquier documentación que permita al Ministerio de Sanidad, si procede, notificar dicha violación de la seguridad de los datos personales a la autoridad de supervisión competente y a los interesados afectados por ella. Como mínimo, esta documentación deberá incluir:

   1º. La descripción de la naturaleza de la violación de la seguridad de los datos personales, que incluirá, cuando sea posible, las categorías y el número aproximado de interesados afectados, así como las categorías y el número aproximado de registros de datos personales afectados.

   2º. La descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

   3º. La descripción de las medidas de corrección y prevención adoptadas.

m) Adoptar todas las medidas de corrección necesarias para subsanar la violación de la seguridad de los datos personales;

n) En el caso de ser necesaria la transferencia de datos personales a un tercer país o una organización internacional, requerirá la autorización del Ministerio de Sanidad, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público.

3. Obligaciones del Ministerio de Sanidad.

El Ministerio de Sanidad se compromete a:

1. Elaborar, en coordinación con los órganos responsables de los sistemas de información y registros de enfermedades raras autonómicos y de las ciudades con Estatuto de Autonomía y, en su caso, con el órgano encargado del tratamiento de los datos, el manual de procedimientos del registro, así como aprobarlo y modificarlo, previo informe favorable del Consejo Interterritorial del Sistema Nacional de Salud. El manual contendrá todos aquellos aspectos necesarios para la puesta en funcionamiento del registro.

2. Aportar apoyo técnico para el desarrollo y mantenimiento del registro.

3. Detentar, junto al ISCIII, el rol de administrador de la aplicación informática del registro.

4. Facilitar al ISCIII los datos personales necesarios para que este pueda cumplir las finalidades del tratamiento.

5. Supervisar el tratamiento, lo que podría incluir realizar auditorías e inspecciones al ISCIII en relación con el registro.

6. Documentar por escrito las instrucciones dirigidas al ISCIII en relación con el tratamiento de los datos de REER.

Tercera*. Obligaciones de naturaleza económica.*

Este Convenio no generará compromiso financiero alguno para ninguna de las partes. Como se ha indicado, el ISCIII realizará los trabajos recogidos en la Cláusula segunda con los medios propios actuales del ISCIII.

Cuarta. *Medios materiales y humanos.*

El ISCIII aportará, para la ejecución y mantenimiento de cada una de las actividades descritas, los recursos humanos y materiales necesarios con los medios propios actuales de que dispone.

Quinta. Comisión de Seguimiento.

Para velar por la adecuada realización del presente convenio se constituirá una Comisión de Seguimiento que tendrá como principal función velar por la organización, gestión y seguimiento de las acciones objeto del presente Convenio, interpretar los términos del mismo que lo requieran y resolver las dudas que puedan surgir en su aplicación e interpretación. La Comisión se constituirá en el plazo de 15 días contados desde la publicación del convenio en el "Boletín Oficial del Estado" y dictará las normas internas de su funcionamiento, debiéndose reunir siempre que lo solicite alguna de las partes.

La Comisión de Seguimiento, tendrá carácter paritario y su composición será:

Por parte del Ministerio de Sanidad:

- La Subdirectora General de Calidad e Innovación o persona en quien ésta delegue.
- La coordinadora técnica de la Estrategia de Salud de Enfermedades Raras del Sistema Nacional de Salud o persona en quien ésta delegue.

Por parte del ISCIII:

- El Subdirector General de Servicios Aplicados, Formación e Investigación del ISCIII o persona en quien éste delegue.
- El Director del Instituto de Investigación de Enfermedades Raras del ISCIII o persona en quien éste delegue.

Se reunirá con carácter ordinario al menos una vez al año y de forma extraordinaria cuando lo solicite justificadamente cualquiera de las partes.

Su funcionamiento se ajustará al régimen de funcionamiento de los órganos colegiados, establecido en la Sección 3ª del capítulo II del título Preliminar de la Ley 40/2016, de 1 de octubre, de Régimen Jurídico del Sector Público.

Cuando concurra cualquiera de las causas de resolución del Convenio existiendo actuaciones en curso de ejecución, la Comisión de Seguimiento podrá acordar la continuación y finalización de las actuaciones en curso que considere oportunas, estableciendo un plazo improrrogable para su finalización, trascurrido el cual deberá realizarse la liquidación de las mismas.

Sexta. *Titularidad de las competencias.*

De acuerdo con el artículo 48.1 de la Ley 40/2015, de 1 de octubre, el presente Convenio no supone cesión de la titularidad de las competencias ni de los elemento sustantivos de su ejercicio, atribuidas a las partes.

Séptima. ***Propiedad de los Trabajos.***

La propiedad intelectual de los resultados de la explotación de los datos pertenece exclusivamente al Ministerio de Sanidad, único titular de los mismos.

En ningún caso el ISCIII podrá hacer difusión de dichos datos sin el permiso explícito del Ministerio de Sanidad.

Octava. ***Garantía de confidencialidad.***

Cada una de las partes se compromete a guardar la máxima confidencialidad durante la vigencia del presente Convenio, y una vez finalizado, respecto a la información y/o documentación sensible, pertenecientes a la otra parte a las que haya podido tener acceso durante su vigencia y a hacer que esta obligación sea respetada por todas las personas que participan en la ejecución del mismo.

Novena. Acceso y cesión de los datos.

El acceso y la cesión de los datos se realizarán de acuerdo con lo establecido en el manual de procedimientos del registro.

Décima. Resolución del convenio.

El Convenio se extinguirá por el cumplimiento de las actuaciones que constituyen su objeto o por incurrir en causa de resolución.

Son causas de resolución:

a. El transcurso del plazo de vigencia del Convenio sin acordarse la prórroga del mismo.

b. El acuerdo unánime de los firmantes.

c. El incumplimiento de las obligaciones y compromisos asumidos por alguno de los firmantes.

d. Por decisión judicial declaratoria de nulidad del Convenio.

e. Por cualquier otra causa prevista en la legislación vigente.

En el caso de incumplimiento recogido en el apartado c), la otra parte podrá notificar a la parte incumplidora -a través de sus representantes en la Comisión de Seguimiento-, un requerimiento para que en el plazo de 30 días naturales cumpla con las obligaciones o compromisos incumplidos. Si transcurrido dicho plazo persistiera el incumplimiento, la parte que lo detectó notificará a la incumplidora la concurrencia de

la causa de resolución y se entenderá resuelto el Convenio con eficacia del mismo día de la recepción de la notificación. Dicha terminación no perjudicará cualquier otro derecho o reclamación que la parte afectada pueda ostentar o tener con respecto de la parte infractora.

De acuerdo con el artículo 52.3 de la Ley 40/2015, de 1 de octubre, en caso de resolución del Convenio, las partes a propuesta de la comisión de seguimiento, vigilancia y control del convenio podrá acordar la continuación y finalización de la actualizaciones en el curso que consideren oportunas, estableciendo un plazo improrrogable para su finalización, transcurrido el cual deberá realizarse la liquidación de las mismas en los términos establecidos en el artículo 52.2 .de la Ley 40/2015, de 1 de octubre.

Undécima. Modificación del convenio.

El presente Convenio podrá ser modificado por acuerdo unánime de las partes, para ello se comunicará a las partes para su estudio y aprobación. De acordarse por unanimidad la modificación, se suscribirá la correspondiente adenda, a fin de incorporar las propuestas de mejora que se hayan considerado pertinentes para el logro de los objetivos previstos, la cual formará parte íntegra del Convenio.

Duodécima. Validez y Eficacia.

De conformidad con el artículo 48.8 de la Ley 40/2015, de Régimen Jurídico del Sector Público, el presente Convenio se perfeccionará con el consentimiento de las partes manifestado mediante su firma, y desplegará los efectos una vez sea inscrito en el Registro Electrónico Estatal de Órganos e Instrumentos de Cooperación del Sector Público Estatal y haya sido publicado en el Boletín Oficial del Estado.

Mantendrá su vigencia por un periodo de cuatro años, pudiendo acordarse unánimemente una prorroga antes de finalizar este plazo, por cuatro años adicionales o su extinción.

Decimotercera. Régimen Jurídico y Resolución de Controversias.

El presente convenio tiene naturaleza administrativa y se regirá por lo establecido en el Título Preliminar, Capítulo VI, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público en el que se regula los acuerdos adoptados por las Administraciones Públicas, lo organismos públicos y entidades de derecho público vinculados o dependiente o las Universidades Púbicas entre sí o con sujetos de derecho privado para un fin común.

Las partes se comprometen a intentar resolver, de buena fe y de manera amistosa, cualquier desacuerdo que pueda surgir en el desarrollo del presente convenio, que deberán solventarse, en primer término, por la Comisión de Seguimiento prevista en la

cláusula quinta de este convenio y sin perjuicio de la aplicación, en su caso y cuando proceda, de la utilización del mecanismo contemplado en la Disposición Adicional Única de Ley 11/20011, de 20 de mayo, de reforma de la ley 60/2003, de 23 de diciembre, de Arbitraje y de regulación del Arbitraje institucional en la Administración General de Estado, para la resolución de las controversias jurídicas relevantes resultará competente el Orden Jurisdiccional Contencioso-Administrativo.

En prueba de conformidad, y para la debida constancia de todo lo acordado, ambas partes firman el presente Convenio por duplicado ejemplar y en todas sus hojas, en el lugar y fecha al principio indicados.

LA DIRECTORA GENERAL DE SALUD PÚBLICA, CALIDAD E INNOVACIÓN	LA DIRECTORA DEL INSTITUTO DE SALUDCARLOS III
Pilar Aparicio Azcárraga	Raquel Yotti Álvarez

ANEXO

MEDIDAS DE SEGURIDAD

El ISCIII como ENCARGADO DEL TRATAMIENTO debe aplicar y mantener medidas técnicas y organizativas apropiadas, controles internos y rutinas de seguridad de la información a fin de proteger los datos personales del RESPONSABLE DEL TRATAMIENTO frente a todo acceso, comunicación, alteración, pérdida o destrucción accidental, ilícito o no autorizado, en los términos siguientes:

1. Organización de la seguridad de la información
   a. El ENCARGADO DEL TRATAMIENTO debe nombrar a uno o varios responsables de seguridad, responsables de coordinar y supervisar las normas y procedimientos de seguridad.
   b. El personal del ENCARGADO DEL TRATAMIENTO que tenga acceso a los Datos del RESPONSABLE DEL TRATAMIENTO debe estar sujeto al cumplimiento de obligaciones de confidencialidad.
   c. El ENCARGADO DEL TRATAMIENTO debe realizar una evaluación de riesgos de las operaciones de tratamiento de datos.

2. Gestión de activos
   a. El ENCARGADO DEL TRATAMIENTO debe llevar un registro de las personas autorizadas para el tratamiento de los datos del RESPONSABLE DEL TRATAMIENTO.
   b. El ENCARGADO DEL TRATAMIENTO debe clasificar los Datos del RESPONSABLE DEL TRATAMIENTO para ayudar a identificarlos y permitir la debida restricción de acceso a los mismos (p. ej., mediante claves de acceso individuales).
   c. El ENCARGADO DEL TRATAMIENTO debe disponer de procedimientos para deshacerse de los materiales impresos que contengan esos datos, salvo que sea necesario para el correcto tratamiento.

3. Seguridad en materia de Recursos Humanos
   a. El ENCARGADO DEL TRATAMIENTO debe informar a su personal sobre los procedimientos de seguridad pertinentes y sus respectivas funciones. El ENCARGADO DEL TRATAMIENTO debe informar también a su personal de las posibles consecuencias de incumplir las normas y procedimientos de seguridad.

4. Seguridad física y medioambiental
   a. El ENCARGADO DEL TRATAMIENTO debe limitar el acceso a las instalaciones en las que se ubiquen los sistemas de información que tratan Datos del RESPONSABLE DEL TRATAMIENTO a personas autorizadas y que acrediten su identidad.
   b. El ENCARGADO DEL TRATAMIENTO restringirá el uso de soportes entrantes y salientes a aquellas personas autorizadas en el documento de seguridad.
   c. El ENCARGADO DEL TRATAMIENTO debe hacer uso de los diversos sistemas

habituales en el sector para protegerse contra la pérdida de datos debida a los fallos de suministro eléctrico o de las comunicaciones.

5. Gestión de las comunicaciones y las operaciones

   a. El ENCARGADO DEL TRATAMIENTO debe disponer de documentos de seguridad que describan sus medidas de seguridad y los procedimientos y responsabilidades pertinentes aplicables a los miembros de su personal con acceso a los Datos del RESPONSABLE DEL TRATAMIENTO.

   b. Con carácter permanente y, como mínimo, una vez a la semana (salvo que los datos del RESPONSABLE DEL TRATAMIENTO no se actualicen durante ese período), el ENCARGADO DEL TRATAMIENTO debe conservar varias copias de los Datos del RESPONSABLE DEL TRATAMIENTO que permitan recuperar tales datos.

   c. El ENCARGADO DEL TRATAMIENTO debe conservar las copias de los Datos del RESPONSABLE DEL TRATAMIENTO y los procedimientos de recuperación de datos en un lugar diferente de aquel donde se ubique el equipo informático principal de tratamiento de los Datos del RESPONSABLE DEL TRATAMIENTO.

   d. El ENCARGADO DEL TRATAMIENTO debe disponer de procedimientos específicos para regular el acceso a las copias de los Datos del RESPONSABLE DEL TRATAMIENTO.

   e. El ENCARGADO DEL TRATAMIENTO debe revisar los procedimientos de recuperación de datos como mínimo cada seis meses.

   f. El ENCARGADO DEL TRATAMIENTO debe registrar los intentos de recuperación de los datos, incluyendo la persona responsable, la descripción de los datos recuperados y los datos que (en su caso) se hayan tenido que introducir manualmente en el proceso de recuperación de datos.

   g. El ENCARGADO DEL TRATAMIENTO debe disponer de mecanismos de control contra códigos maliciosos para evitar que programas maliciosos, incluidos los que tienen su origen en redes públicas, accedan a los Datos del RESPONSABLE DEL TRATAMIENTO sin estar autorizados.

   h. El ENCARGADO DEL TRATAMIENTO debe cifrar los Datos del RESPONSABLE DEL TRATAMIENTO que se transmitan a través de redes públicas.

   i. El ENCARGADO DEL TRATAMIENTO debe restringir el acceso a los Datos del RESPONSABLE DEL TRATAMIENTO contenidos en soportes que salgan de sus instalaciones (p. ej., mediante el cifrado).

   j. El ENCARGADO DEL TRATAMIENTO debe registrar el acceso y uso de los sistemas de información que contengan Datos del RESPONSABLE DEL TRATAMIENTO y hacer constar la identidad de acceso, hora, concesión o denegación de la autorización y actividad de que se trate.

6. Control de acceso

   a. El ENCARGADO DEL TRATAMIENTO debe mantener un registro de los privilegios de seguridad de las personas que tengan acceso a datos del RESPONSABLE DEL TRATAMIENTO.

   b. El ENCARGADO DEL TRATAMIENTO debe mantener y actualizar un registro del personal autorizado para acceder a los sistemas que contengan Datos del RESPONSABLE DEL TRATAMIENTO.

c. El ENCARGADO DEL TRATAMIENTO debe identificar al personal que pueda dar, alterar o suprimir el acceso autorizado a datos y recursos.

d. El ENCARGADO DEL TRATAMIENTO debe garantizar que, cuando más de una persona tenga acceso a sistemas que contengan Datos del RESPONSABLE DEL TRATAMIENTO, cada una de ellas disponga de un identificador/clave de acceso independiente.

e. El personal de soporte técnico del ENCARGADO DEL TRATAMIENTO únicamente debe tener permiso para acceder a los datos del RESPONSABLE DEL TRATAMIENTO cuando sea necesario.

f. El ENCARGADO DEL TRATAMIENTO debe restringir el acceso a los Datos del RESPONSABLE DEL TRATAMIENTO exclusivamente a aquellas personas que lo necesiten para desempeñar sus funciones laborales.

g. El ENCARGADO DEL TRATAMIENTO debe dar instrucciones al personal para que cierre las sesiones de administración cuando abandone las instalaciones o cuando los ordenadores se queden sin vigilancia por cualquier otro motivo.

h. El ENCARGADO DEL TRATAMIENTO debe almacenar las contraseñas de modo que sean ininteligibles, mientras sean válidas.

i. El ENCARGADO DEL TRATAMIENTO debe atenerse a las prácticas habituales del sector para identificar y autentificar a los usuarios que traten de acceder a los sistemas de información.

j. Cuando los mecanismos de autentificación consistan en contraseñas, el ENCARGADO DEL TRATAMIENTO debe exigir que las contraseñas se cambien con regularidad y que tengan, al menos, ocho caracteres.

k. El ENCARGADO DEL TRATAMIENTO debe garantizar que no se asignen a otras personas los nombres de identificación desactivados o caducados.

l. El ENCARGADO DEL TRATAMIENTO debe supervisar los intentos reiterados de acceso al sistema de información utilizando una contraseña incorrecta.

m. El ENCARGADO DEL TRATAMIENTO debe respetar los procedimientos habituales del sector para desactivar las contraseñas que se hayan visto comprometidas o hayan sido reveladas involuntariamente.

n. El ENCARGADO DEL TRATAMIENTO debe aplicar las prácticas de protección de contraseña habituales del sector, incluidas las diseñadas para preservar la confidencialidad y la integridad de las contraseñas cuando se cedan y distribuyan, así como durante su almacenamiento.

o. El ENCARGADO DEL TRATAMIENTO debe disponer de mecanismos de control para evitar que otras personas se arroguen derechos de acceso que no se les hayan reconocido sobre Datos del RESPONSABLE DEL TRATAMIENTO, a cuyo acceso no estén autorizadas.

7. Gestión de software

a. El ENCARGADO DEL TRATAMIENTO debe disponer de mecanismos de control para garantizar el tratamiento adecuado de los Datos del RESPONSABLE DEL TRATAMIENTO en aplicaciones informáticas.

b. El ENCARGADO DEL TRATAMIENTO debe restringir el acceso a códigos fuente exclusivamente a aquellas personas que necesiten dicho acceso para el desarrollo en entornos relacionados con los Datos del RESPONSABLE DEL TRATAMIENTO.

c. El ENCARGADO DEL TRATAMIENTO debe limitarse a utilizar datos anónimos en entornos de desarrollo y ensayo.

8. Gestión de incidentes de seguridad de la información

a. El ENCARGADO DEL TRATAMIENTO debe supervisar los eventos e intrusiones de seguridad atípicos en los sistemas de información donde se almacenen Datos del RESPONSABLE DEL TRATAMIENTO y debe activar un proceso vertical para tratar tales eventos.

b. El ENCARGADO DEL TRATAMIENTO debe mantener un registro de violaciones de la seguridad en el que se incluya una descripción de la violación, su alcance temporal y consecuencias, el nombre del denunciante y de la persona a la que se dirigió la denuncia, y el procedimiento de recuperación de datos.

c. El ENCARGADO DEL TRATAMIENTO debe hacer un seguimiento de las comunicaciones de Datos del RESPONSABLE DEL TRATAMIENTO, con indicación de los datos que se han comunicado, la persona destinataria y la hora.

d. El responsable de seguridad del ENCARGADO DEL TRATAMIENTO debe comprobar los registros como mínimo cada seis meses, al objeto de proponer, en su caso, medidas correctivas.

9. Gestión de amenazas y vulnerabilidad

a. El ENCARGADO DEL TRATAMIENTO debe identificar y subsanar sin dilación cualquier amenaza y vulnerabilidad significativa sobre todos los sistemas de información que traten Datos del RESPONSABLE DEL TRATAMIENTO.

b. El ENCARGADO DEL TRATAMIENTO debe instalar parches de seguridad de manera regular y, como mínimo, una vez al mes, a no ser que se trate de parches críticos, para los que el ENCARGADO DEL TRATAMIENTO debe contar con un proceso de emergencia que prevea su instalación en un plazo más breve.

10. Gestión de la continuidad de la actividad

a. El ENCARGADO DEL TRATAMIENTO debe disponer de planes de emergencia y contingencia para las instalaciones en las que se ubiquen los sistemas de información que traten Datos del RESPONSABLE DEL TRATAMIENTO.

b. El almacenamiento redundante del ENCARGADO DEL TRATAMIENTO y sus procedimientos de recuperación de datos deben estar diseñados para tratar de restaurar los Datos del RESPONSABLE DEL TRATAMIENTO a su estado original anterior a su pérdida o destrucción.