Castilla-La Mancha

Consejería de Hacienda y Administraciones Públicas

INSTRUCCIÓN
Seguridad de la Información y Protección de Datos en la prestación de servicios con terceros

CÓDIGO: SPD-GEN-INS-001

Versión: 5.0

Fecha: 10/07/2018

Aprobado
Firmado digitalmente el 17-07-2018 por PILAR CUEVAS HENCHE Cargo: Viceconsejero/a Viceconsejera de Administración Local y Coordinación Administrativa

	Nombre	Fecha
Elaborado por:	Servicio de Seguridad y Protección de Datos (SPD)	12/05/2014
Revisado por:		

HISTÓRICO DEL DOCUMENTO

Versión	Fecha	Descripción	Autor
1.0	12/05/2014	Versión inicial.	SPD
2.0	08/04/2015	Incluir nuevo modelo para la adecuación al ENS	SPD
3.0	15/03/2016	Inclusión de la documentación de seguridad a entregar al prestador de servicios. Actualización en base a la modificación del RD 3/2010	SPD
4.0	15/11/2016	Actualización del apartado del ENS en base a la Guía CCN-STIC-830 y la Instrucción Técnica de Seguridad	SPD
5.0	15/05/2018	Adecuación al Reglamento General de Protección de Datos	SPD

ÍNDICE

1. INTRODUCCIÓN

En las Administraciones Públicas es práctica habitual que existan contratos, convenios, acuerdos, encomiendas de gestión y encomiendas a medios propios personificados para que otros organismos o entidades presten servicios o proporcionen productos que implican el tratamiento de información de la Administración. Este hecho no implica que, por tener parte del tratamiento encargado a un tercero, la Administración deje de ser responsable de dicho tratamiento y, por tanto, del cumplimiento de las normas legales que le son de aplicación.

Por su parte, el artículo 11 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en su en su apartado 1º al regular las "encomiendas de gestión" establece que… "La realización de actividades de carácter material o técnico de la competencia de los órganos administrativos o de las Entidades de Derecho Público podrá ser encomendada a otros órganos o Entidades de Derecho Público de la misma o de distinta Administración, siempre que entre sus competencias estén esas actividades, por razones de eficacia o cuando no se posean los medios técnicos idóneos para su desempeño".

A continuación en el párrafo 2º del apartado 2 indica que "en todo caso, la Entidad u órgano encomendado tendrá la condición de encargado del tratamiento de los datos de carácter personal a los que pudiera tener acceso en ejecución de la encomienda de gestión, siéndole de aplicación lo dispuesto en la normativa de protección de datos de carácter personal"

En la materia que nos ocupa, las normas que la Administración de la Junta de Comunidades de Castilla-La Mancha debe cumplir son las siguientes:

- Siempre que se traten datos personales:
    - **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).
- Siempre que se utilicen medios electrónicos para gestionar las competencias de esta Administración:
    - **Real Decreto 3/2010,** de 8 de enero, por el que se aprueba el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
    - **Real Decreto 951/2015,** de 23 de octubre, de modificación 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.
    - **Resolución de 7 de octubre de 2016,** de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

- **Resolución de 13 de octubre de 2016**, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

Por lo anteriormente expuesto, la Viceconsejería de Administración Local y Coordinación Administrativa, con base en las competencias atribuidas en el Decreto 82/2015, de 14/07/2015, por el que se establece la estructura orgánica y competencias de la Consejería de Hacienda y Administraciones Públicas, modificado por Decreto 220/2015, de 01/12/2015, ha decidido elaborar esta Instrucción como medida de seguridad de tipo organizativo que aumenta el nivel de seguridad de los servicios prestados, con independencia de si un determinado servicio se realiza con recursos propios o externos.

1.1 Objeto

Esta Instrucción tiene por objeto regular, en materia de Seguridad de la Información y de Protección de Datos de Carácter Personal, la relación en las prestaciones de servicios contratadas/convenidas/acordadas por la Administración de la Junta de Comunidades de Castilla-La Mancha con entidades externas u órgano encomendado, en aquellos servicios que incluyan acceso a datos de carácter personal o que de forma indirecta tengan la posibilidad de dicho acceso y en aquellas soluciones tecnológicas o servicios comprendidos dentro del ámbito objetivo de aplicación del Esquema Nacional de Seguridad (sistemas de información sustentados en medios electrónicos dirigidos a gestionar las competencias de la entidad pública correspondiente).

1.2 Ámbito de aplicación

Esta instrucción es de aplicación a la Administración de la Junta de Comunidades de Castilla-La Mancha y las entidades de derecho público vinculadas o dependientes de la misma.

1.3 Definiciones, acrónimos y referencias

1.3.1 Definiciones

Definición	Concepto

1.3.2 Acrónimos

Acrónimo	Concepto
CCN-STIC-830	Guía de seguridad: Ámbito de aplicación del Esquema Nacional de Seguridad del Centro Criptológico Nacional.

Acrónimo	Concepto
ENS	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
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE

1.3.3 Referencias

Los siguientes documentos son aplicables en la medida que se indique en el documento, correspondiéndose sus versiones y fechas con las vigentes en el momento de aplicación del mismo; el resto se han usado simplemente a modo de consulta.

Código	Documento

2. CLÁUSULAS A INCLUIR EN LOS CONTRATOS, CONVENIOS, ACUERDOS Y ENCOMIENDAS

2.1 Cláusulas en convenios, acuerdos y encomiendas

En los convenios/acuerdos/encomiendas que exista tratamiento de datos de carácter personal o, aunque el objeto del encargo no suponga el tratamiento directo a los datos personales pero pueda implicar un acceso ocasional a los mismos, debe existir una cláusula específica que se regirá por lo siguiente:

2.1.1 En materia de Protección de Datos

2.1.1.1 Con acceso a datos de carácter personal

Cuando el servicio objeto del contrato/convenio/acuerdo/encomienda implique el tratamiento de datos de carácter personal, el tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o Español, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categoría de interesados, y las obligaciones y derechos del responsable. El modelo de cláusula para incluir en este supuesto está recogido en el Anexo I.

Es obligación del responsable del tratamiento, elegir únicamente un encargado que ofrezca garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la normativa vigente en materia de protección de datos y garantice la protección de los derechos del interesado. A estos efectos, es conveniente establecer la obligación del encargado del tratamiento de haber designado un Delegado de Protección de Datos, si procede, que reúna los requisitos establecidos en el Reglamento General de Protección Datos y/o de adherirse a códigos de conducta aprobados de conformidad con lo dispuesto en el artículo 40 del Reglamento General de Protección de Datos.

2.1.1.2 Sin acceso a datos de carácter personal

Cuando la prestación del servicio objeto del contrato/convenio/acuerdo/encomienda no implique el acceso directo a datos de carácter personal, se debe limitar el acceso del personal externo a dichos datos mediante una cláusula en el documento que indique la prohibición de acceso a tales datos y así como la obligación de deber de secreto si se accede a ellos. El modelo de cláusula a incluir en este supuesto está recogido en el Anexo II.

2.1.2 En materia de Seguridad de la Información

Cuando el servicio objeto del contrato/convenio/acuerdo/encomienda esté incluido en el ámbito de aplicación 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, el encargado debe cumplir con el Esquema Nacional de Seguridad en los servicios o productos objeto del encargo.

En particular, cuando vaya a prestarse en entornos o sistemas que no sean propiedad de la Junta de Comunidades de Castilla-La Mancha, con carácter previo a la adjudicación del contrato o a la formalización del convenio/acuerdo/encomienda, la entidad u organismo que vaya a actuar como Encargado del tratamiento deberá acreditar la conformidad de sus soluciones o servicios con el Esquema Nacional de Seguridad, en los términos establecidos en la Resolución del 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, y la Guía CCN-STIC-809 "Declaración y Certificación de Conformidad con el ENS y Distintivos de Cumplimiento. El responsable del tratamiento deberá informarle a estos efectos del nivel en que está catalogado el producto o servicio.

El modelo de cláusula a incluir en este supuesto está recogido en el Anexo III.

2.2 Cláusulas a incluir en contratos

Además de las cláusulas anteriores que también se deben especificar en los contratos, con carácter previo a la adjudicación de los contratos, en los Pliegos deberá incluirse una cláusula con la denominación y contenido siguiente:

2.2.1 Cláusula general de Seguridad de la Información y Protección de Datos

Seguridad en la Información y Protección de Datos

1.- la empresa adjudicataria debe cumplir con la normativa europea y estatal vigente en materia de protección de datos.

La empresa adjudicataria y su personal están obligados a guardar secreto profesional respecto a los datos de carácter personal de los que puedan tener conocimiento por razón de la prestación del contrato, obligación que subsistirá aún después de la finalización del mismo.

El adjudicatario deberá formar e informar a su personal de las obligaciones que en materia de protección de datos estén obligados a cumplir en el desarrollo de sus tareas para la prestación del contrato, en especial las derivadas del deber de secreto, respondiendo la empresa adjudicataria personalmente de las infracciones legales en que por incumplimiento de sus empleados se pudiera incurrir.

Las obligaciones del Encargado del tratamiento se especificarán en la formalización del contrato.

[Opcional: para los supuestos en que el servicio vaya a prestarse en entornos o sistemas que no sean propiedad de la Junta de Comunidades de Castilla-La Mancha, además se incluirá el siguiente párrafo:

2.- La empresa adjudicataria deberá cumplir con el Esquema Nacional de Seguridad

La empresa adjudicataria deberá acreditar la conformidad de sus soluciones o servicios con el Esquema Nacional de Seguridad, en los términos establecidos en la Resolución del 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, y la Guía CCN-STIC-809 "Declaración y Certificación de Conformidad con el ENS y Distintivos de Cumplimiento.]

2.2.2 Cláusula para la adquisición de productos relacionados con la Seguridad de la Información

Cláusula a incluir en los contrato de adquisiciones de productos relacionados con la Seguridad de la Información:

Seguridad General de los Productos. Funcionalidades de Seguridad

Los productos que se adquieran a través de estos contratos se ajustarán a la directiva 2001/95/CE relativa a la seguridad general de los productos (R.D. 1801/2003, de 26 de diciembre, sobre seguridad general de los productos B.O.E. de 10 de enero de 2004).

En virtud del artículo 18 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 (en adelante, ENS), en la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad. La certificación indicada anteriormente deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

Para cada producto, el cumplimiento de los requisitos funcionales de seguridad exigidos por el ENS podrá ser acreditado por su inclusión en el "Catálogo de productos STIC (Seguridad de las Tecnologías de la Información y la Comunicación)" del CCN (Centro Criptológico Nacional).

3. DOCUMENTACIÓN DE SEGURIDAD A ENTREGAR AL PRESTADOR DE SERVICIOS

Cuando se contrate/convenie/acuerde/encomiende un servicio que incluya información o servicios, se entregará a los Encargados del tratamiento los documentos que, en materia de Seguridad de la Información, deban conocer para cumplir con su encargo.

Esta entrega de documentación conllevará un acuse de recibo según el modelo del Anexo V.

De forma obligatoria se entregarán los documentos que constituyen la Política de Seguridad de esta Administración:

- Decreto 57/2012, de 23/02/2012, por el que se establece la política de seguridad de la información en la Administración de la Junta de Comunidades de Castilla-La Mancha.
- SPD-SEG-NOR-002 Directrices de Seguridad de la Información.
- SPD-SEG-NOR-012 Requisitos mínimos de Seguridad.
- Orden de 11 de julio de 2012, de la Consejería de Presidencia y Administraciones Públicas y de la Consejería de Fomento, por la que se aprueba la instrucción sobre el uso aceptable de medios tecnológicos en la Administración de la Junta de Comunidades de Castilla-La Mancha.

Del resto de normativas e instrucciones que forman el Marco Normativo de la Seguridad, se entregarán las que apliquen al objeto del contrato/convenio/acuerdo/encomienda. Además se le deberá proporcionar cualquier otro documento que se considere necesario.

4. INFORMACIÓN PARA TRABAJADORES EXTERNOS

Por norma general, las empresas suelen firmar con sus empleados acuerdos de confidencialidad donde establecen los requisitos de confidencialidad en las relaciones empresa/trabajador, y de la misma forma la Administración en sus contratos/convenios/acuerdos/encomiendas recoge cláusulas de este tipo. Sin embargo, no suelen existir documentos que regulen la relación Administración/trabajador externo en materia de Seguridad de la Información y de la Protección de Datos más allá de lo previsto en el propio contrato/convenio/acuerdo/encomienda suscrito.

No obstante, en la Administración existen normas de obligado cumplimiento para su personal que, en ocasiones, vinculan a los trabajadores externos y de los que hay que informarles, normas que garantizan a los ciudadanos que sus datos son tratados con la seguridad adecuada, tanto si los datos son suministrados en papel como si son suministrados mediante servicios electrónicos, con independencia de que los manejen personal interno o externo.

Es por ello, y como medida de seguridad preventiva que minimiza el riesgo en materia de Seguridad de la Información y el riesgo a los derechos y libertades de los ciudadanos, que en el caso de que el servicio objeto del contrato/convenio/acuerdo/encomienda implique la existencia de trabajadores externos que accedan a los Sistemas de Información de la Administración Regional, la entidad externa remitirá a la Administración un documento firmado por cada uno de los trabajadores afectados en el que se les informa de las obligaciones que tienen como usuarios que acceden a nuestros sistemas.

El modelo de documento informativo está recogido en el Anexo IV.

5. ANEXOS

ANEXO I: CASOS EN LOS QUE SE TRATAN DATOS DE CARÁCTER PERSONAL

1. Objeto del encargo del tratamiento

A efectos de lo previsto en el artículo 28.3 del Reglamento (UE) 2016/679 (en adelante RGPD) y el resto de disposiciones vigentes en materia de protección de datos), el responsable del tratamiento es <D.G. / Secretaría General u otro órgano gestor competente> y el encargado del tratamiento es <entidad/ empresa externa/órgano encomendado>.

El tratamiento consistirá en: (descripción detallada del servicio).

Concreción de los tratamientos a realizar:

- *Recogida*
- *Registro*
- *Estructuración*
- *Modificación*
- *Conservación*
- *Extracción*
- *Consulta*
- *Comunicación*
- *Difusión*
- *Interconexión*
- *Cotejo*
- *Limitación*
- *Supresión*
- *Destrucción*
- *Conservación*
- *Comunicación*

Otros:.....

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento, pone a disposición del encargado del tratamiento, la información que se encuentra incluida en la/s siguiente/s actividad/es de tratamiento:

- <denominación del tratamiento> 1, con código RAT…….
- <denominación del tratamiento> 2, con código RAT…….

……..

3. Duración

El presente acuerdo tiene una duración de…..

Una vez finalice el presente contrato, el encargado del tratamiento debe *suprimir/devolver al responsable o /devolver a otro encargado que designe el responsable (indicar la opción que proceda)* los datos personales y suprimir cualquier copia que esté en su poder.

4. Obligaciones del encargado del tratamiento

El encargado del tratamiento y todo su personal se someten a la normativa de protección de datos anteriormente mencionada y de forma específica, las siguientes condiciones:

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

b) Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de carácter nacional, el encargado informará inmediatamente al responsable.

c) Presentar ante el Responsable la adhesión a códigos de conducta aprobados a tenor del artículo 40 del RGPD o a mecanismos de certificación aprobados a tenor del artículo 42 del RGPD.

d) Llevar, por escrito, un registro [1]de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

[1] "Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, salvo que el tratamiento que realice pueda suponer un riesgo para los derechos y las libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1 del RGPD, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 de dicho Reglamento." (Art. 30.5 RGPD).

1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.
2. Las categorías de tratamientos efectuados por cuenta de cada responsable.
3. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.
4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

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

e) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

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

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

f) Subcontratación

(Escoger una de las opciones)

Opción A

No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de....., indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus

datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

Opción B

Se autoriza al encargado a subcontratar con la empresa……. las prestaciones que comporten los tratamientos siguientes:.....

Para subcontratar con otras empresas, el encargado debe comunicarlo por escrito al responsable, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de……

El subcontratista, que también tiene la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

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

h) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, según el modelo facilitado por el responsable del tratamiento, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes.

i) Remitir al responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

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

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

1. Acceso, rectificación, supresión y oposición

2. Limitación del tratamiento

3. Portabilidad de datos

4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

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

l) Derecho de información:

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

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

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 72 horas, y a través de ….[2], las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

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

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

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) El nombre y los datos de contacto del Delegado de Protección de Datos de su empresa o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

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

[2] Indicar el medio por el que se debe comunicar al responsable la violación de seguridad.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

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

o) Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como permitir y colaborar con la realización de las auditorías o las inspecciones realizadas por cuenta del responsable.

p) [solo si la empresa está obligada a ello] Designar un Delegado de Protección de Datos y comunicar su identidad y datos de contacto al responsable.

q) Destino de los datos:

(Escoger una de las tres opciones)

Opción A

Devolver al responsable del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación.

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.

No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Opción B

Devolver al encargado que designe por escrito el responsable del tratamiento, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación.

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.

No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Opción C

Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento.

No obstante, el encargado puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

r) En el caso de que los datos deban incorporarse en dispositivos portátiles, o deban tratarse fuera de los locales del encargado, se necesita autorización expresa del responsable, la cual deberá constar en el documento de seguridad. En cualquier caso, debe garantizarse el correspondiente nivel de seguridad.

s) No prestar el servicio objeto del presente documento mediante tecnología en nube sin la autorización expresa del responsable.

t) Implantar medidas de seguridad:

(Escoger una de las dos opciones)

Opción A

Dado que el tratamiento forma parte de un Sistema de Información incluido en el ámbito de aplicación del Esquema Nacional de Seguridad, las medidas a implantar son las correspondientes a nivel <categoría del sistema>

Opción B

Las medidas de seguridad siguientes, de acuerdo con el análisis de riesgos realizado por……, en fecha…….

…….

En todo caso, se deben implanta mecanismos para:

a. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

d. Seudonimizar y/o cifrar de datos personales, en su caso.

(Opcional) Además este tratamiento está sujeto al código de conducta, sello o certificación……..

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a) Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.
b) Proporcionar al encargado el modelo de información para trabajadores externos
c) Realizar una evaluación del impacto en la protección de datos personales, si procede, de las operaciones de tratamiento a realizar por el encargado.
d) Realizar las consultas previas que corresponda.
e) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.
f) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías a través del delegado de protección de datos del responsable

ANEXO II: PROTECCIÓN DE DATOS SIN ACCESO A DATOS DE CARÁCTER PERSONAL

1. Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este contrato/convenio/acuerdo/encomienda, el personal de la <entidad externa> no puede acceder a los datos de carácter personal que figuran en los archivos, documentos y sistemas informáticos de esta Administración.
2. No obstante lo establecido en el párrafo anterior, cuando el personal de la <entidad externa> acceda a los datos personales de forma casual, estará obligado a guardar secreto incluso después de la finalización de la relación contractual, sin que en ningún caso pueda utilizar los datos ni revelarlos a terceros.
3. La <entidad externa> debe poner en conocimiento de los trabajadores afectados las medidas establecidas en la cláusula anterior y conservar la acreditación del cumplimiento de este deber.
4. La <entidad externa> debe poner en conocimiento de esta Administración, de forma inmediata, cualquier incidencia que se produzca durante la ejecución del contrato/convenio/acuerdo/encomienda que pueda afectar a la integridad o a la confidencialidad de los datos de carácter personal tratados por esta Administración, la cual tendrá que anotarlo en la herramienta que los servicios de informática tienen al efecto.
5. El incumplimiento de lo establecido en los apartados anteriores puede dar lugar a que la <entidad externa> sea considerada responsable del tratamiento, a efectos de aplicar el régimen sancionador y de responsabilidades previsto en la normativa de protección de datos.

ANEXO III: CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

Las terceras partes suministradoras o prestadoras, deberán acreditar la conformidad con el ENS de sus soluciones o servicios, en los términos establecidos en la Resolución del 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, y la Guía CCN-STIC-809 "Declaración y Certificación de Conformidad con el ENS y Distintivos de Cumplimiento.

El Sistema de Información del que forma parte el servicio o producto está catalogado como de nivel <categoría del sistema>

OPCIONAL

Se tendrá especial cuidado con la implantación de las siguientes medidas técnicas y/u organizativas:

……..

Adicionalmente se atenderá a la normativa de la Administración Regional en materia de Seguridad de la Información y la Protección de Datos que se entrega al adjudicatario.

ANEXO IV: INFORMACIÓN PARA TRABAJADORES EXTERNOS

Para el cumplimiento de la normativa en materia de seguridad de la Información y la protección de datos de carácter personal, mediante la firma del presente documento, D./Dª [NOMBRE Y APELLIDOS DE LA PERSONA QUE FIRMA], mayor de edad, con D.N.I. [DNI/NIF DE LA PERSONA QUE FIRMA], como trabajador de <entidad externa> y dentro del [ACUERDO, CONVENIO, CONTRATO o ENCOMIENDA], se compromete y obliga a:

PRIMERO. Atender las instrucciones relativas a la seguridad de la información contenidas en las normas de seguridad de esta Administración, y más en concreto en la Orden de 11/07/2012, de la Consejería de Presidencia y Administraciones Públicas y de la Consejería de Fomento, por la que se aprueba la instrucción sobre el uso aceptable de medios tecnológicos en la Administración de la Junta de Comunidades de Castilla-La Mancha.

SEGUNDO. Guardar secreto sobre las informaciones confidenciales y los datos de carácter personal de los que tenga conocimiento en el ejercicio de las funciones que les sean encomendadas.

TERCERO. Notificar de manera inmediata al responsable de su entidad, cualquier incidente de seguridad sobre los tratamientos realizados o si, en su opinión, una instrucción infringe el Reglamento Europeo u otras disposiciones en materia de protección de datos de la Unión o nacional.

CUARTO. El abajo firmante realizará únicamente las tareas que se le encomienden dentro del mencionado contrato y en la forma indicadas por el responsable del tratamiento, en particular, no debe utilizar la información tratada para otra finalidad.

Con la firma del presente documento el abajo firmante queda informado de que cualquier incumplimiento de estos compromisos y de la legislación vigente, podrá dar origen a las oportunas acciones judiciales para exigir reparación de las posibles responsabilidades en que pudiera incurrir, derivadas del mal uso de los medios tecnológicos que se le faciliten para el desarrollo de las funciones encomendadas.

En a, de de 201

ANEXO V: ACUSE DE RECIBO DE LA DOCUMENTACIÓN

D/Dª							
con DNI:		, empresa					

Mediante la firma del presente documento, declaro que se me ha entregado la siguiente documentación (señalar la que corresponda):

- ☒ Decreto 57/2012, de 23/02/2012, por el que se establece la política de seguridad de la información en la Administración de la Junta de Comunidades de Castilla-La Mancha
- ☒ SPD-SEG-NOR-012 Requisitos mínimos de Seguridad
- ☐ SPD-SEG-NOR-002 Directrices de Seguridad de la Información
- ☒ Orden de 11 de julio de 2012, de la Consejería de Presidencia y Administraciones Públicas y de la Consejería de Fomento, por la que se aprueba la instrucción sobre el uso aceptable de medios tecnológicos en la Administración de la Junta de Comunidades de Castilla-La Mancha
- ☐ SPD-SEG-NOR-003 Clasificación de la Información
- ☐ SPD-SEG-NOR-004 Desarrollo seguro de aplicaciones
- ☐ SPD-SEG-NOR-005 Seguridad de la Red
- ☐ SPD-SEG-NOR-006 Acceso seguro por terceros a la red
- ☐ SPD-SEG-INS-001 Creación y uso de contraseñas de usuario
- ☐ SPD-SEG-INF-006 Requisitos de seguridad en el desarrollo de aplicaciones
- ☐ Otras (indicar)

En		, a		de		de 20	

Firmado:	