V

POLITICA DE PROTECCIÓN DE DATOS

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. (VIVA)

Esta *Política de protección de datos personales* fue aprobada el 5 de julio de 2018.

POLÍTICA DE PROTECCIÓN DE DATOS

La entidad SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. a través, de su gerencia y órganos de dirección mantiene la responsabilidad de determinar la estrategia y aprobar las *Políticas corporativas* de la organización, así como de disponer los sistemas de control interno. En el ejercicio de estas responsabilidades, y con el objeto de establecer los principios generales que deben regir el tratamiento de los datos personales en la entidad, se aprueba esta *Política de protección de datos personales.*

Esta Política de Protección de Datos es efectiva desde la fecha que aparece en la página anterior, y hasta que sea reemplazada por una nueva Política.

1. Finalidad

La *Política de protección de datos personales* establece los principios y pautas comunes de actuación que deben regir en la corporación en materia de protección de datos personales, garantizando, en todo caso, el cumplimiento de la legislación aplicable. En particular, la *Política de protección de datos personales* tiene la finalidad de garantizar el derecho a la protección de sus datos de todas las personas físicas que se relacionan con la entidad, asegurando el respeto del derecho al honor y a la intimidad en el tratamiento de los diferentes tipos de datos personales, procedentes de diferentes fuentes y con fines diversos en función de la actividad empresarial desarrollada por SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L., como cualquier otro organismo depende, en mayor o menor medida, de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.
El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos que conforman la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

2. Ámbito de aplicación

La *Política de protección de datos personales* será de aplicación a la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L., a todos los sistemas TIC, a sus administradores, directivos y empleados, así como a todas las personas que se relacionen con ellos, sin excepciones.

3. Principios del tratamiento de los datos personales

Los principios por los que se rige la *Política de protección de datos personales* son los siguientes:

a) Principios generales: SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. cumplirá escrupulosamente con la legislación de su jurisdicción en materia de protección de datos, la que resulte aplicable en función del tratamiento de datos personales que se lleve a cabo y la que se determine conforme a normas o acuerdos vinculantes adoptados.
SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. promoverá que los principios recogidos en esta *Política de protección de datos personales* sean tenidos en cuenta (i) en el diseño e implementación de todos los procedimientos que impliquen el tratamiento de datos personales, (ii) en los productos y servicios ofrecidos, (iii) en todos los contratos y obligaciones que formalicen con personas físicas y (iv) en la implantación de cuantos sistemas y plataformas permitan el acceso por parte de empleados o de terceros a datos personales y/o la recogida o tratamiento de dichos datos.

b) Principios relativos al tratamiento de datos personales:

(i) *Principios de legitimidad, licitud y lealtad en el tratamiento de datos personales.*
El tratamiento de datos personales será leal, legítimo y lícito conforme a la legislación aplicable. En este sentido, los datos personales deberán ser recogidos para uno o varios fines específicos y legítimos conforme a la legislación aplicable. En los casos en los que resulte obligatorio conforme a la legislación aplicable, deberá obtenerse el consentimiento de los interesados antes de recabar sus datos. Asimismo, cuando lo exija la ley, los fines del tratamiento de datos personales serán explícitos y determinados en el momento de su recogida. En particular, SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. no recabará ni tratará datos personales relativos al origen étnico o racial, a la ideología política, a las creencias, a las convicciones religiosas o filosóficas, a la vida u orientación sexual, a la afiliación sindical, a la salud, ni datos genéticos o biométricos dirigidos a identificar de

manera unívoca a una persona, salvo que la recogida de los referidos datos sea necesaria, legítima y requerida o permitida por la legislación aplicable, en cuyo caso serán recabados y tratados de acuerdo con lo establecido en aquella.

(ii) Principio de minimización.

Solo serán objeto de tratamiento aquellos datos personales que resulten estrictamente necesarios para la finalidad para los que se recojan o traten y adecuados a tal finalidad.

(iii) Principio de exactitud.

Los datos personales deberán ser exactos y estar actualizados. En caso contrario, deberán suprimirse o rectificarse.

(iv) Principio de limitación del plazo de conservación.

Los datos personales no se conservarán más allá del plazo necesario para conseguir el fin para el cual se tratan, salvo en los supuestos previstos legalmente.

(v) Principios de integridad y confidencialidad.

En el tratamiento de los datos personales se deberá garantizar, mediante medidas técnicas u organizativas, una seguridad adecuada que los proteja del tratamiento no autorizado o ilícito y que evite su pérdida, su destrucción y que sufran daños accidentales. Los datos personales recabados y tratados por SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. deberán ser conservados con la máxima confidencialidad y secreto, no pudiendo ser utilizados para otros fines distintos de los que justificaron y permitieron su recogida y sin que puedan ser comunicados o cedidos a terceros fuera de los casos permitidos por la legislación aplicable.

(vi) Principio de responsabilidad proactiva.

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. será responsables de cumplir con los principios estipulados en esta *Política de protección de datos personales* y los exigidos en la legislación aplicable y deberán ser capaces de demostrarlo, cuando así lo exija la legislación aplicable. SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. deberá realizar un análisis de necesidad de evaluación del riesgo de los tratamientos que realicen, con el fin de determinar las medidas a aplicar para garantizar que los datos personales se tratan conforme a las exigencias legales. En los casos en los que la ley lo exija, se evaluarán de forma previa los riesgos que para la protección de datos personales puedan comportar nuevos productos, servicios o sistemas de información y se adoptarán las medidas necesarias para eliminarlos o mitigarlos. SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. deberá llevar un registro de actividades en el que se describan los tratamientos de datos personales que lleven a cabo en el marco de sus actividades. En el caso de que se produzca un incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizado a dichos datos, deberán seguirse EL PROTOCOLO DE NOTIFICACION DE QUIEBRAS DE SEGURIDAD,

establecido a tal efecto y, en su caso, los que establezca la legislación aplicable. Dichos incidentes deberán documentarse y se adoptarán medidas para solventar y paliar los posibles efectos negativos para los interesados. En los casos previstos en la ley, se designará a delegados de protección de datos con el fin de garantizar el cumplimiento de la normativa.

(vii) Principios de transparencia e información.

El tratamiento de datos personales será transparente en relación con el interesado, facilitándole la información sobre el tratamiento de sus datos de forma comprensible y accesible, cuando así lo exija la ley aplicable. A fin de garantizar un tratamiento leal y transparente, SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. en su calidad de responsable del tratamiento deberá informar a los afectados o interesados cuyos datos se pretende recabar de las circunstancias relativas al tratamiento conforme a la legislación aplicable.

(viii) Adquisición u obtención de datos personales.

Queda prohibida la adquisición u obtención de datos personales de fuentes ilegítimas, de fuentes que no garanticen suficientemente su legítima procedencia o de fuentes cuyos datos hayan sido recabados o cedidos contraviniendo la ley.

(ix) Contratación de encargados del tratamiento.

Con carácter previo a la contratación de cualquier prestador de servicios que acceda a datos personales que sean responsabilidad de SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L., así como durante la vigencia de la relación contractual, estas deberán adoptar las medidas necesarias para garantizar y, cuando sea legalmente exigible, demostrar, que el tratamiento de datos por parte del encargado se lleva a cabo conforme a la normativa aplicable.

(x) Transferencias internacionales de datos.

Todo tratamiento de datos personales sujeto a la normativa de la Unión Europea que implique una transferencia de datos fuera del Espacio Económico Europeo deberá llevarse a cabo con estricto cumplimiento de los requisitos establecidos en la ley aplicable en la jurisdicción de origen.

(xi) Derechos de los interesados.

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. deberá permitir que los interesados puedan ejercitar los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición que sean de aplicación en cada jurisdicción, estableciendo, a tal efecto, los procedimientos internos que resulten necesarios para satisfacer, al menos, los requisitos legales aplicables en cada caso.

4.Gestión de riesgos.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente,
- Cuando cambie la información manejada o los sistemas de información,
- Cuando cambien los servicios prestados,
- Cuando ocurra un incidente grave de seguridad,
- Cuando se reporten o detecten vulnerabilidades graves.

5. Implementación.

Conforme a lo dispuesto en esta *Política de protección de datos personales*, SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. desarrollará y mantendrán actualizada la normativa interna de gestión global de protección de datos y será de obligado cumplimiento para todos los directivos y empleados de la Sociedad.

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. dispondrá de un equipo jurídico externo responsable de reportar a la Dirección de entidad los desarrollos y novedades normativas que se produzcan en este ámbito.

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L., a través de sus técnicos (internos o externos) será la encargada de implementar en los sistemas de información de la organización, los controles y desarrollos informáticos que sean adecuados para garantizar el cumplimiento de la normativa interna de gestión global de la protección de datos y velará por que dichos desarrollos estén actualizados en cada momento.

6. Control y evaluación

La Gerencia de SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. supervisará el cumplimiento de lo dispuesto en esta *Política de protección de datos personales* por parte de la Entidad. Lo anterior se entenderá, en todo caso, sin perjuicio de las responsabilidades que correspondan a otros órganos y direcciones de la corporación. Para verificar el cumplimiento de esta *Política de protección de datos personales* se realizarán auditorías periódicas con auditores internos o externos.

VI

PROCEDIMIENTO DE GESTIÓN DE EJERCICIOS DE DERECHOS DE INTERESADOS EN

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. (VIVA)

Este *Procedimiento de Gestión de Ejercicios de Derechos* fue aprobado el 4 de julio de 2018.

PROCEDIMIENTO DE GESTIÓN DE EJERCICIOS DE DERECHOS EN PROTECCIÓN DE DATOS.

La entidad SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. a través, de su gerencia y órganos de dirección mantiene la responsabilidad de determinar la estrategia y aprobar las *Políticas corporativas* de la organización, así como de disponer los sistemas de control interno. En el ejercicio de estas responsabilidades, se establece el presente protocolo que permitirá que los interesados puedan ejercitar los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición que sean de aplicación.

1. Objetivos

Establecer el procedimiento de ejercicio por parte de los interesados respecto de sus derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición, respecto a los tratamientos de datos realizados en SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

2. Destinatarios

Personas físicas titulares de sus datos de carácter personal, objeto de tratamiento en SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

3. Procedimiento

El artículo 12 del RGPD, bajo el epígrafe, “transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado” recoge un conjunto de previsiones que SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L., como responsable del tratamiento debe tener en cuenta para dar cumplida respuesta a un ejercicio de derechos, en lo que tiene que ver con aquellos reconocidos en el RGPD.

Bajo este marco normativo se concluye que, en primer lugar, SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. debe facilitar al interesado el ejercicio de sus derechos (información relativa a sus actuaciones sobre la base de una solicitud):

- de acceso.
- de rectificación.
- de supresión (derecho al olvido).
- la limitación del tratamiento.
- portabilidad de los datos.
- de oposición.

- a las decisiones individuales automatizadas, incluida la elaboración de perfiles.

En los supuestos de tratamientos que no requieren identificación del interesado SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. deberá dar cumplida respuesta al ejercicio de los derechos salvo que "pueda demostrar que no está en condiciones de identificar al interesado" (artículo 12.2 RGPD).

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L., como responsable del tratamiento debe dar cumplida respuesta al ejercicio del derecho interesado en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes.

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. debe informar al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación.

Por tanto, SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. debe informar al interesado sobre las actuaciones derivadas de su petición en el plazo de UN MES, que podrá extenderse a DOS MESES MAS, cuando la solicitud sea especialmente compleja, debiéndose notificar esta ampliación dentro del primer mes.

Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará de forma electrónica cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

Si SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. no da curso a la solicitud del interesado, le deberá informar sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

Toda la información que se preste por SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. en el marco del ejercicio de los derechos deberá darse a título gratuito. No obstante, cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. podrá:

- cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o
- negarse a actuar respecto de la solicitud.

En cualquier caso, SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. tiene la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

Cuando SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud de ejercicio de derechos, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. debe utilizar todas las medidas razonables para verificar la identidad de los interesados que soliciten acceso, en particular en el contexto de los servicios en línea y los identificadores en línea.

4.-Responsables de la gestión de ejercicios de derechos.

Dentro de la organización, todos los ejercicios de derechos que se formalicen deben ser dirigidos, a fin de darles oportuna respuesta, a las personas siguientes:

NOMBRE Y APELLIDOS	CARGO/DEPARTAMENTO
Elena Martín Mantecón	Gerente.
Carolina Fernández McGucken	Responsable de protección de datos.

Todas las actuaciones, se deberán dejar perfectamente documentadas a fin de gestionar y controlar todos los derechos, atendiendo escrupulosamente a los plazos establecidos en el RGPD.

5.-Modelos de contestación.

A.-MODELO DE CONTESTACIÓN ANTE UN EJERCICIO DE ACCESO

En ....., a ..... de ..... de 20...

Estimado Sr./Sra. .....:

En virtud de lo establecido en el artículo 15 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, le comunicamos que usted tiene derecho a acceder a un conjunto de información sobre el tratamiento de sus datos de carácter personal realizado por esta entidad.
Por todo ello, en relación con la solicitud contenida en su escrito, con registro de entrada de ..... de ..... de 20..., le comunicamos que la siguiente información:

- *El fin del tratamiento es …*
- *Las categorías de datos objeto de tratamiento son datos identificativos (nombre apellidos, DNI, domicilio); …*
- *No se van a realizar comunicaciones de datos a terceros.*
- *El plazo previsto para la conservación de los datos es de 5 años, atendiendo a la normativa actual civil de prescripción de acciones.*
- *Los datos han sido obtenidos directamente del interesado y con su consentimiento.*
- *El responsable no emplea técnicas automatizadas de elaboración de perfiles.*

- *No se producen transferencias internacionales de sus datos.*

Le recordamos, por mandato del artículo 15 del Reglamento, que puede solicitar la rectificación o supresión de sus datos personales o la limitación del tratamiento de datos relativos a su persona, o a oponerse a dicho tratamiento; así como su derecho a presentar una reclamación ante la Agencia Española el Protección de Datos.

Para cualquier otra aclaración, o cuestión, no dude en ponerse en contacto con nosotros.
Reciba un cordial saludo,

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

B.-MODELO DE CONTESTACIÓN ANTE UN EJERCICIO DE SUPRESIÓN

En ..... , a ..... de ..... de 20 .....

Estimado Sr./Sra. ..... :
Atendiendo a su solicitud de cancelación con fecha de entrada de ..... de ..... de 20 ..... y en virtud de lo establecido en el artículo 17 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, le comunicamos que:
Con fecha ..... de ..... de 20 ..... , dentro del plazo legalmente establecido, se ha procedido a suprimir sus datos de carácter personal de los tratamientos efectuados y para los cuales ejerce el derecho.
(en su caso)
2.- No procede la supresión de datos solicitada, toda vez que su solicitud se haya dentro de las excepciones al derecho de supresión (u olvido) del interesado, según el apartado 3º del artículo 17 REPD.

No cabrá el derecho cuando el tratamiento sea necesario: (SEÑALAR LA QUE CORRESPONDA):

- *para ejercer el derecho a la libertad de expresión e información;*
- *para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;*
- *para la formulación, el ejercicio o la defensa de reclamaciones.*

2. Que se ha requerido, conforme al artículo 19 del RGPD, a todos aquellos posibles destinatarios de los datos para que supriman igualmente los datos en sus tratamientos.
3. Que la cancelación no procede ya que, atendiendo a la normativa precitada, sus datos personales deben ser conservados mientras dure la relación contractual o negocial que actualmente mantiene con nuestra empresa.
4.- (EN CASO DE DENEGACIÓN DEL EJERCICIO DEL DERECHO) Le informamos, finalmente, que tiene el derecho de presentar una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es), así como de ejercitar las acciones judiciales que considere.

Sin otro particular, y en la confianza de saberle informado,
Reciba un cordial saludo.
.....

C.-MODELO DE CONTESTACIÓN ANTE UN EJERCICIO DE RECTIFICACIÓN

En ..... , a ..... de ..... de 20 .....

Estimado Sr./Sra. .....

Atendiendo a su solicitud de entrada con fecha ..... de ..... de 20 ..... , y de conformidad con lo previsto en el artículo 16 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, el artículo 16 de la Ley Orgánica 15/1999, y en los artículos 31 y siguientes del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, le informamos de lo siguiente:

1. Ya se ha atendido su petición procediéndose, dentro del plazo legal, a rectificar sus datos de nuestros tratamientos ficheros, tal y como nos indicó.

2. Que se ha requerido a todos aquellos cesionarios que, conforme al elenco normativo de protección de datos, tratan sus datos para prestarle correctamente el servicio que tiene contratado, para que rectifiquen igualmente sus datos en sus ficheros, con el fin de respetar el principio de actualización calidad de los datos.

(En su caso)
(EN CASO DE DENEGACIÓN DEL EJERCICIO DEL DERECHO) Le informamos, finalmente, que tiene el derecho de presentar una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es), así como de ejercitar las acciones judiciales que considere.

Sin otro particular, y en la confianza de saberle informado,

Reciba un cordial saludo.
.....

D.-MODELO DE CONTESTACIÓN ANTE UN EJERCICIO DE OPOSICIÓN

En ..... , a ..... de ..... de 20 .....

Estimado Sr./Sra. ..... :
Atendiendo su solicitud de oposición con fecha de entrada de ..... de ..... de 20 ..... , y en virtud de lo establecido en el artículo 21 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y una vez analizados los motivos expuestos en su escrito, le comunicamos que:

- ☐ *Con fecha de ..... de ..... de 20 ..... , dentro del plazo legalmente establecido, se ha procedido ESTIMAR su solicitud y por tanto, se ha anotado en nuestra base de datos dicha oposición a que el tratamiento realizado sean aquellos realizados por el responsable al que me dirijo y estén basados en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos incluida la elaboración de perfiles.*
- ☐ *aquellos necesarios para la satisfacción de pretendidos intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, incluida la elaboración de perfiles.*
- ☐ *aquellos tratamientos de datos del responsable que tienen una finalidad comercial o de marketing directo.*
- ☐ *aquellos tratamientos de datos con fines de investigación científica o histórica o fines estadísticos.*

(EN CASO DE DENEGACIÓN DEL EJERCICIO DEL DERECHO) Le informamos, finalmente, que tiene el derecho de presentar una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es), así como de ejercitar las acciones judiciales que considere.

Lamentando las molestias que se le hayan podido ocasionar,
Reciba un cordial saludo.
.....

E.-MODELO DE CONTESTACIÓN ANTE EL EJERCICIO DEL DERECHO DE OPOSICION FRENTE A DECISIONES INDIVIDUALES AUTOMATIZADAS

En ..... , a ..... de ..... de 20 .....

Estimado Sr./Sra. ..... :

Atendiendo a su solicitud de oposición con fecha de entrada de ..... de ..... de 20 ....., en virtud de lo establecido en el artículo 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y una vez analizados los motivos expuestos en su escrito, le comunicamos que:

Se acuerda ESTIMAR SU DERECHO, y a tal fin se le indica, conforme exige el meritado precepto:

1.-Descripción de la aplicación empleada en los tratamientos automatizados destinados a analizar……
2.-Criterios de valoración utilizados:
……

Le informamos, por todo ello, que se adoptarán las medidas adecuadas para salvaguardar sus derechos y libertades e intereses legítimos, entre ellos, el derecho a obtener intervención humana, y a expresar su punto de vista y a impugnar la decisión, llegado el caso.

3.-Debido a su revocación del consentimiento, prestado legítimamente en su momento, le informamos que nuestra empresa se abstendrá de realizar más valoraciones sobre usted en el futuro.

(EN CASO DE DENEGACIÓN DEL EJERCICIO DEL DERECHO) Le informamos, finalmente, que tiene el derecho de presentar una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es), así como de ejercitar las acciones judiciales que considere.

Lamentando las molestias que se le hayan podido ocasionar, reciba un cordial saludo.
.....

VII

PROTOCOLO DE GESTION Y NOTIFICACION DE BRECHAS DE SEGURIDAD

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. (VIVA)

PROTOCOLO DE NOTIFICACION DE QUIEBRAS DE SEGURIDAD

I.-Introducción.

El Esquema Nacional de Seguridad (ENS) (Real Decreto 3/2010) define un "incidente de seguridad" como aquel "suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información". En la misma línea, la Directiva NIS define "incidente" como "todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información".

El Reglamento General de Protección de Datos (RGPD) define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Es importante tener en cuenta que, aunque todas las brechas de datos personales son incidentes de seguridad, no todos los incidentes de seguridad son necesariamente brechas de datos personales.

De acuerdo con el RGPD, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales debe efectuar la correspondiente notificación a la autoridad de control competente, sin dilación y a más tardar en las 72 horas siguientes.

Cuando en el momento de la notificación no fuese posible cumplir con la obligación de facilitar toda la información exigida se facilitará de manera gradual, a la mayor brevedad y sin dilación. La única excepción a esta obligación de notificación tendría lugar cuando, conforme al principio de responsabilidad proactiva, el responsable pueda demostrar que la brecha de la seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de las personas físicas.

Por el contrario, cuando la brecha de seguridad entrañe un alto riesgo para los derechos y libertades de los titulares de los datos, además de la comunicación a la autoridad de control, el responsable del tratamiento deberá, adicionalmente, comunicar a los afectados la brecha de seguridad sin dilación indebida y con lenguaje claro y sencillo, de forma concisa y transparente, salvo en algunos supuestos.

II.-Gestión de brechas de seguridad: Preparación

En todas las organizaciones se tienen incidentes de seguridad y por tanto, se debe proceder a gestionar este tipo de incidentes en mayor o menor grado.

Es necesario un proceso previo de Preparación en el que se decidirán las medidas técnicas y organizativas para poder afrontar un incidente. Esto incluye la identificación de los agentes implicados en la gestión de la brecha, el análisis de riesgos y/o evaluación de impacto en caso de que sean necesarias y la definición de los "planes de respuesta a incidentes" o "plan de contingencia".

En la **SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.** se han decidido las siguientes medidas preparatorias, previas a un incidente:

Personal implicado en la gestión de la brecha de seguridad	Puesto o departamento	Función
Elena Martín Mantecón	Gerente	Gestión de la brecha
Carolina Fernández McGucken	Responsable de protección de datos	Asesoramiento jurídico

Se ha realizado un **análisis de riesgos** en la organización, con las conclusiones que se determinan en el informe dedicado al efecto.

III.-Detención de incidentes de seguridad.

Durante esta fase de detección e identificación se deberán concretar las situaciones que se consideran incidentes de seguridad y las herramientas, mecanismos de detección o sistemas de alerta con los que el responsable (bien por su cuenta, bien por cuenta de un encargado) va a contar para detectar un incidente, así como el análisis de la información que proporcionen dichas herramientas o sistemas de alerta.

Durante esta fase de detección e identificación se deberán concretar las situaciones que se consideran incidentes de seguridad y las herramientas, mecanismos de detección o sistemas de alerta con los que el responsable (bien por su cuenta, bien por cuenta de un encargado) va a contar para detectar un incidente, así como el análisis de la información que proporcionen dichas herramientas o sistemas de alerta. Estos mecanismos permitirán a la organización identificar una brecha de seguridad en caso de que se produzca.

El momento en que se detecta e identifica una brecha de seguridad es importante ya que el RGPD establece que el responsable del tratamiento debe notificar a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella. En determinados casos se deberá notificar también a los afectados.

La identificación de un incidente de seguridad puede producirse a través de fuentes internas a la organización o fuentes externas.

IDENTIFICACIÓN DE INCIDENTES DE SEGURIDAD		
FUENTES INTERNAS	**A.- Seguridad física**	**1.** Políticas específicas de mesas limpias, bloqueo de pantallas, accesos con usuario y contraseña, etc. **2.** Controles físicos como detección de intrusos, videovigilancia, control y registro de accesos a determinadas zonas, etc. **3.** Controles y procedimientos frente a daños ambientales o desastres naturales
	B.- Ciberseguridad.	**4.** Notificaciones de usuarios: presencia de archivos con caracteres inusuales, recepción de correos electrónicos con archivos adjuntos sospechosos, comportamiento extraño de dispositivos, imposibilidad de acceder a ciertos servicios, extravío/robo de dispositivos de almacenamiento o equipos con información. **5.** Alertas generadas por software antivirus. **6.** Consumos excesivos y repentinos de memoria o disco en servidores y equipos. **7.** Anomalías de tráfico de red o picos de tráfico en horas inusuales. **8.** Alertas de sistemas de detección/prevención de intrusión (IDS/IPS). **9.** Alertas de sistemas de correlación de eventos. **10.** Análisis de registros de conexiones realizadas a través de proxys corporativos o conexiones bloqueadas en los cortafuegos. **11.** Análisis de registro de servidores y aplicaciones con intentos de acceso no autorizados. **12.** Análisis de registros en herramientas DLP (Data Loss Prevention).
FUENTES EXTERNAS	**13.** Comunicación de un tercero (proveedores de servicios informáticos, proveedores de servicios de internet o fabricantes de soluciones de seguridad), **14.** Comunicación por un cliente o **15.** Comunicación o notificación que realicen a la empresa los distintos organismos públicos como el Instituto Nacional de Cyberseguridad (INCIBE), el Centro Criptológico Nacional (CCN), Fuerzas y Cuerpos de Seguridad del Estado. **16.** Información publicada en medios de comunicación.	

El análisis de las fuentes de información anteriores permite determinar si se está ante un incidente de seguridad o no, así como su naturaleza, clase, tipo, si dicho incidente ha afectado a datos de carácter personal y por tanto constituye una “brecha de los datos de carácter personal” descrita en el RGPD, y el nivel de riesgo al que se enfrenta la organización.

IV.-Análisis/Clasificación de los incidentes de seguridad en la organización.

Los factores que se pueden considerar a la hora de establecer criterios de clasificación son, entre otros: el tipo de amenaza: código dañino, intrusiones, fraude, etc.; el contexto u origen de la amenaza (interna o externa); la categoría de seguridad de los sistemas y datos afectados; perfil de los usuarios afectados; el número y tipología de los sistemas afectados; el impacto del incidente en la organización y en los derechos y libertades de los afectados; los requerimientos legales y regulatorios; o el vector de ataque o método.

TIPOLOGÍAS DE SUPUESTOS QUE PUEDEN DAR LUGAR A UN INCIDENTE DE SEGURIDAD		
1	**0-day (vulnerabilidad no conocida):**	Vulnerabilidad que permite a un atacante el acceso a los datos en la medida en que es una vulnerabilidad desconocida. Esta vulnerabilidad estará disponible hasta que el fabricante o desarrollador la resuelva.
2	**APT (ataque dirigido)**	Se refiere a diferentes tipos de ataques dirigidos normalmente a recabar información fundamental que permita continuar con ataques más sofisticados. En esta categoría se encuadraría por ejemplo una campaña de envío de email con software malintencionado a empleados de una empresa hasta conseguir que alguno de ellos lo instale en su equipo y proporcione una puerta de entrada al sistema.
3	**Denegación de servicio (DoS/DDoS)**	Consiste en inundar de tráfico un sistema hasta que no sea capaz de dar servicio a los usuarios legítimos del mismo.
4	**Acceso a cuentas privilegiadas:**	El atacante consigue acceder al sistema mediante una cuenta de usuario con privilegios avanzados, lo que le confiere libertad de acciones. Previamente deberá haber conseguido el nombre de usuario y contraseña por algún otro método, por ejemplo un ataque dirigido.
5	**Código malicioso:**	piezas de software cuyo objetivo es infiltrase o dañar un ordenador, servidor u otro dispositivo de red con finalidades muy diversas. Una de las posibilidad para que el código dañino alcance a una organización es que un usuario lo instale de forma involuntaria.
6	**Compromiso de la información**	Recoge todos los incidentes relacionados con el acceso y fuga, modificación o borrado de información no pública.
7	**Ingeniería social**	Son técnicas basadas en el engaño, normalmente llevadas a cabo a través de las redes sociales, que se emplean para dirigir la conducta de una persona u obtener información sensible. Por ejemplo, el usuario es inducido a pulsar sobre un enlace haciéndole pensar que es lo correcto.
8	**Robo y/o filtración de datos**	Se incluye en esta categoría la pérdida/robo de dispositivos de almacenamiento con información.
9	**Desfiguración (Defacement):**	Es un tipo de ataque dirigido que consiste en la modificación de la página web corporativa con la intención de colgar mensajes reivindicativos de algún tipo o cualquier otra intención. La operativa normal de la web queda interrumpida, produciéndose además daños reputacionales.
10	**Explotación de vulnerabilidades de aplicaciones**	Cuando un posible atacante logra explotar con éxito una vulnerabilidad existente en un sistema o producto consiguiendo comprometer una aplicación de la organización.

Una brecha de seguridad se puede clasificar en una o varias de las siguientes categorías:

Brecha de confidencialidad	Tiene lugar cuando partes que no están autorizadas, o no tienen un propósito legítimo para acceder a la información, acceden a ella. La severidad de la pérdida de

	confidencialidad varía según el alcance de la divulgación, es decir, el número potencial y el tipo de partes que pueden haber accedido ilegalmente a la información.
Brecha de integridad	Se produce cuando se altera la información original y la sustitución de datos puede ser perjudicial para el individuo. La situación más grave ocurre cuando existen serias posibilidades de que los datos alterados se hayan utilizado de una manera que pueda dañar al individuo.
Brecha de disponibilidad	Su consecuencia es que no se puede acceder a los datos originales cuando es necesario. Puede ser temporal (los datos son recuperables, pero tomará un periodo de tiempo y esto puede ser perjudicial para el individuo), o permanente (los datos no pueden recuperarse).

Valoración del alcance de la brecha de seguridad.

La gestión de una brecha de seguridad requiere determinar la peligrosidad potencial del incidente y la estimación de la magnitud del impacto potencial en los individuos. Para esta evaluación se deberá recurrir al análisis de riesgos o evaluación de impacto realizado antes de la puesta en marcha de las actividades de tratamiento y a la clasificación previa del incidente.

FACTORES PARA VALORAR EL ALCANCE DE LA BRECHA DE SEGURIDAD	
La categoría o nivel de criticidad respecto a la seguridad de los sistemas afectados.	☐ Crítico (afecta a datos valiosos, gran volumen y en poco tiempo) ☐ Muy Alto (Cuando dispone de capacidad para afectar a información valiosa, en cantidad apreciable) ☐ Alto (Cuando dispone de capacidad para afectar a información valiosa) ☐ Medio (Cuando dispone de capacidad para afectar a un volumen apreciable de información) ☐ Bajo (Escasa o nula capacidad para afectar a un volumen apreciable de información).
Naturaleza, sensibilidad y categorías de los datos personales afectados.	☐ Datos de escaso riesgo: datos de contacto, de educación, familiares, profesionales, biográficos ☐ Datos de comportamiento: localización, tráfico, hábitos y preferencias, ☐ Datos financieros: transacciones, posiciones, ingresos, cuentas, facturas, ☐ Datos sensibles: de salud, biométricos, datos relativos a la vida sexual, etc.
Datos legibles/ilegibles.	☐ Datos protegidos mediante algún sistema de seudonimización (por ejemplo, cifrado o hash)
Volumen de datos personales	☐ Expresados en cantidad (registros, ficheros, documentos) y/o en periodos de tiempo (una semana, un año, etc.)
Facilidad de identificación de individuos	☐ Facilidad con la que se puede deducir la identidad de los individuos a partir de los datos involucrados en la brecha

Severidad de las consecuencias para los individuos:	☐ Baja: Las personas no se verán afectadas o pueden encontrar algunos inconvenientes que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.). ☐ Media: Las personas pueden encontrar inconvenientes importantes, que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.). ☐ Alta: Las personas pueden enfrentar consecuencias importantes, que deberían poder superar aunque con serias dificultades (malversación de fondos, listas negras de los bancos, daños a la propiedad, pérdida de empleo, citación judicial, empeoramiento de la salud, etc.). ☐ Muy alta: Las personas pueden enfrentar consecuencias significativas, o incluso irreversibles, que no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.).
Características especiales de los individuos:	☐ Si afectan a individuos con características especiales o con necesidades especiales.
Número de individuos afectados:	☐ Más de 100 individuos. ☐ Entre 100 y 500 individuos. ☐ Entre 1.000 y 5.000 individuos. ☐ Más de 5.000 individuos.
Características especiales del responsable del tratamiento	☐ En base a la actividad de la entidad.
El perfil de los usuarios afectados	☐ su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.
El número y tipología de los sistemas afectados.	
El impacto que la brecha puede tener en la organización.	Desde los puntos de vista de la protección de la información, la prestación de los Servicios, la conformidad legal y/o la imagen pública. Va a estar relacionado con la categoría o criticidad de los servicios afectados y personas afectadas. ☐ Bajo (perjuicio limitado) ☐ Medio (perjuicio grave) ☐ Alto (perjuicio muy grave)
Los requerimientos legales y regulatorios.	☐ Notificación de la brecha a la autoridad de control. ☐ Comunicación a Fuerzas y Cuerpos de Seguridad del Estado. ☐ Otro requerimiento regulatorio.

V.-Gestión de brechas de seguridad: Plan de actuación.

Una vez se ha detectado e identificado una brecha de seguridad es necesario poner en marcha un plan de actuación previamente definido y aprobado para solucionar el incidente.

En caso de que el incidente de seguridad se acabe clasificando como una brecha de seguridad en la que se han comprometido datos personales se deberá iniciar también el proceso de notificación mediante el cual se notificará a la autoridad de control competente y se comunicará con los afectados cuando se cumplan las condiciones que exige el RGPD.
Se pueden poner en marcha una serie de medidas tempranas de contención y se puede valorar una posible notificación temprana a la autoridad de control y/o los afectados. Posteriormente se podrá en marcha el proceso de respuesta y en caso de que sea necesario el proceso de notificación.

1.-Análisis y Clasificación

Dentro de esta fase deben tenerse en cuenta los siguientes aspectos:

- **Recopilación y análisis de la información relativa a la brecha.**
- **Clasificación de la brecha de seguridad.**
- Es especialmente **importante determinar si efectivamente se está ante una brecha de seguridad**, en cuyo caso es imprescindible evaluar el nivel de perjuicio que puede causar el incidente a los derechos y libertades de los afectados, determinando con el mayor grado de precisión posible el nivel de severidad de las consecuencias para los individuos. Es así mismo imprescindible determinar si se trata de una brecha de confidencialidad, integridad o disponibilidad, categoría y número de afectados, categoría y número de registros de datos, etc.
- **Investigación, comunicación y coordinación de los medios internos/externos implicados:** Es importante tener establecido de antemano cómo se va a tratar una incidencia de seguridad, quien se va a encargar de cada tarea y cómo se escalan a los equipos internos o externos adecuados.
- **Puesta en marcha del plan de respuesta:** Especialmente de las primeras medidas de contención, tratando de limitar en lo posible los daños causados por el incidente.
- **Puesta en marcha del proceso de notificación**, empezando por una valoración de notificación temprana a la autoridad de control competente, a afectados y en caso necesario a Fuerzas y Cuerpos de Seguridad del Estado.
- **Estudio y activación de las posibles medidas a adoptar** para contener, mitigar o eliminar los daños que pudieran sufrir los afectados, esto es, un Plan de Contingencia elaborado previamente en la fase de preparación.

FASES DE LA INCIDENCIA	
ESTADO	**DESCRIPCIÓN**
Pendiente	Estado por el que comienzan todos los informes, advirtiendo un problema de seguridad.
Resuelto	Estado que surge cuando el problema ha sido solucionado o corregido. En el campo de Resolución se deben incluir la fecha, su estado y la descripción completa.
Irreproducible	No es posible volver a reproducir el problema.
Retrasado	Se reconoce la existencia de un problema, pero su resolución se pospone, debiendo indicarse el motivo.
Según el procedimiento	No se trata realmente de una incidencia. El comportamiento refleja lo afirmado en el procedimiento.
Sin solución técnica	El problema no puede resolverse por motivos técnicos.
Sin solución	El problema no puede resolverse por motivos derivados de la política de la organización.
Anulado por el responsable	Si el usuario que comunicó la incidencia considera que fue un error, puede solicitar su anulación, decidiendo la persona responsable el paso a este estado.
Necesidad de más información	Es necesario que el informante de la incidencia aporte más información acerca de ésta.

2.-Respuesta a brechas de seguridad

Durante el proceso de respuesta, en una primera fase se intenta contener el incidente, tras lo cual se erradica la situación generada por el incidente y se termina con las acciones de recuperación oportunas. Estas fases no están perfectamente diferenciadas y es habitual que haya cierto solapamiento entre las mismas.

Fases de Respuesta de Incidentes

2.1.-Contención del incidente.

La contención del incidente proporciona tiempo para desarrollar una estrategia de respuesta a medida. Una parte esencial de la contención es la toma de decisiones rápidas como puede ser cerrar un sistema, aislarlo de la red, deshabilitar ciertas funciones, etc.

Las medidas de contención podrán ser inmediatas o de aplicación progresiva en función del desarrollo de la resolución del incidente.

Es conveniente determinar las medidas a implantar estableciendo un orden de prioridad, los responsables asignados, tiempos estimados y los efectos esperados.

Medidas de contención que podrían ser de aplicación en función de cada caso:

- Si es posible, impedir el acceso al origen de la divulgación: dominios, puertos, servidores, la fuente o los destinatarios de la divulgación. Dependiendo del vector de ataque, impedir el acceso al origen: dominios, conexiones, equipos informáticos o conexiones remotas, puertos, parches, actualización del software de detección (antivirus, IDS, etc.) bloqueo de tráfico, deshabilitar dispositivos, servidores, etc.
- Suspender las credenciales lógicas y físicas con acceso a información privilegiada. Cambiar todas las contraseñas de usuarios privilegiados o hacer que los usuarios lo hagan de manera segura.
- Hacer una copia del sistema (clonado), hacer una copia bit a bit del disco duro que contiene el sistema, y luego analizar la copia utilizando herramientas forenses.
- Aislar el sistema utilizado para revelar los datos con el fin de realizar un análisis forense más tarde.
- Si los datos han sido enviados a servidores públicos, solicitar al propietario (o webmaster) que elimine los datos divulgados.
- Si no es posible eliminar los datos divulgados, proporcionar un análisis completo al departamento correspondiente (Legal, Compliance, RRHH, etc.) o a quien ejerza dichas funciones en la empresa.
- Vigilar la difusión de los documentos/datos filtrados en los diferentes sitios web y redes sociales (FB, Twitter, etc.) así como los comentarios y reacciones de los usuarios de Internet.

2.2.-Solución / erradicación

Las tareas de erradicación deben contar con una descripción de las tareas, así como de la responsabilidad (equipo interno o externo e identificación del responsable de equipo) de cada una de ellas.

Algunos ejemplos de **tareas de erradicación** podrían ser las que se enumeran a continuación:

- Definir el proceso de desinfección, basado en firmas, herramientas, nuevas versiones/revisiones de software, etc. y probarlo. Asegurar que el proceso de desinfección funciona adecuadamente sin dañar servicios.
- Comprobar la integridad de todos los datos almacenados en el sistema, mediante un sistema de hashes por ejemplo, que permita garantizar que los ficheros no han sido modificados, especial atención debe ser tenida con relación a los ficheros ejecutables.
- Revisar la correcta planificación y actualización de los motores y firmas de antivirus.
- Análisis con antivirus de todo el sistema, los discos duros y la memoria.
- Restaurar conexiones y privilegios paulatinamente. Especial acceso restringido paulatino de máquinas remotas o no gestionadas.
- Tareas organizativas, en el supuesto de resultar de aplicación atendiendo a la naturaleza de la incidencia.

Con objeto de planificar la respuesta al incidente deberá fijarse un plazo para la implementación de las tareas de erradicación.

Además, se deberán de tomar medidas que eviten o eliminen la posibilidad de que un incidente vuelva a producirse.

El plan de actuación para la gestión de brechas de seguridad requiere de determinadas tareas de seguimiento y cierre. Entre ellas:

- Valoración de contratación de un análisis forense digital experto.
- Valoración de promoción de un procedimiento judicial, en reclamación de daños y perjuicios.

2.3.-Recuperación

Esta fase tiene como objetivo el restablecimiento del servicio en su totalidad, confirmando su funcionamiento normal y evitando en la medida de lo posible que sucedan nuevos incidentes basados en la misma causa.

Esto puede implicar la adopción no solo de medidas activas, sino también implementando controles periódicos y eficaces que permitan el seguimiento pormenorizado de los procesos de mayor riesgo.

2.4.-Recolección y custodia de evidencias

La documentación de todo el proceso de respuesta es muy importante de cara a comunicaciones a partes interesadas de carácter interno o externo, y a la elaboración de un informe de respuesta que tras su análisis permita extraer conclusiones.

La información registrada por los sistemas involucrados puede resultar útil para su aportación en procedimientos judiciales y administrativos.

2.5.-Comunicación/Informe de resolución (Interna/Externa)

Todo el proceso de respuesta al incidente debe quedar debidamente documentado, incluyendo las conclusiones de los técnicos y responsables del equipo para extraer lecciones aprendidas y ser incluidas en un informe de resolución.

Se recomienda disponer de la siguiente información para poder elaborar el citado informe:

- Descripción objetiva del incidente.
- Controles existentes en el momento del incidente.
- Enumeración de medidas efectivas de respuesta.
- Declaración de si a igual casuística el incidente se repetiría.
- Medidas de detección aplicadas para identificar nuevos casos.
- Registro de comunicaciones durante la respuesta.

La comunicación es fundamental durante todo el ciclo de vida del proceso de respuesta, y debe hacerse de una manera continua de modo que la dirección y responsables de seguridad tengan una visibilidad clara tanto del incidente como de las acciones tomadas para afrontarlo. Es especialmente importante cuando el incidente trasciende el perímetro de la organización y toma relevancia pública, ya que muy posiblemente los directivos serán preguntados por las acciones que se están llevando a cabo y posibles consecuencias.

Las tareas de comunicación no buscan la aprobación de la gerencia ni su toma de decisiones, simplemente se trata de un cuaderno de bitácora lo suficientemente actualizado para informar a la dirección y otras partes interesadas, de forma que también puedan cumplir con sus propias obligaciones.

Con un carácter meramente interno, el informe de resolución de la incidencia debe facilitar a todos los equipos involucrados en la respuesta al incidente, el entendimiento sobre el porqué de las acciones tomadas, así como las acciones marcadas para seguimiento en el corto, medio y largo plazo. También serán tenidos en cuenta los cambios necesarios que deberían ser incluidos en el análisis de riesgos de la organización.

En la medida de lo posible este informe debe incluir detalles técnicos sobre las diferentes acciones llevadas a cabo. Este informe se nutrirá en gran medida de la documentación elaborada durante el proceso de respuesta.

El informe de resolución se debe presentar en forma de línea temporal, de modo que facilite el seguimiento de las diferentes acciones, y debería incluir al menos información relativa a los siguientes apartados:

- Alcance e impacto del incidente.
- Controles preventivos existentes.
- Acciones de respuesta tomadas sobre las diferentes alternativas consideradas para la resolución de la brecha.
- Acciones tomadas para la prevención de futuras brechas.
- Impacto en la resolución del incidente de las acciones de respuesta tomadas.
- Acciones definidas para el seguimiento.

3.-Notificación de brechas de seguridad

Según el artículo 33 del RGPD, en caso de brecha de la seguridad que afecte a los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Así mismo, el artículo 34 del RGPD establece que cuando sea probable que la brecha de seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará a los afectados sin dilación indebida.

Se incluye, a continuación, el formulario de notificación de brechas de seguridad a la AEPD.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

1. Datos de la notificación

Tipo de notificación: ○ Inicial, ○ Adicional, ○ Completa
Referencia notificación inicial:_____ Fecha notificación inicial:_____

2. Identificación del Delegado de Protección de Datos o persona de contacto

NIF/NIE: _____ Nombre:_____
Apellidos:_____ Cargo:_____
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

3. Identificación del responsable del tratamiento

Nombre de la Organización: _____
Tipo de Organización: ○ Privada, ○ Pública
CIF:_____ Dirección distinta del DPD o persona de contacto: ☐
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

4. Identifiación del encargado del tratamiento

¿Hay otra organización implicada en la brecha de seguridad? ☐
Nombre de la Organización: _____
Tipo de Organización: ○ Privada, ○ Pública
CIF:_____
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

5. Información temporal de la brecha

Fecha detección de la brecha: _____ ○ Exacta, ○ Estimada.
Medios de detección de la brecha:

_____
_____
_____

Justificación de notificación tardía (notificación pasadas 72h desde la detección):

_____
_____
_____

Fecha inicio de la brecha: _____ ○ Exacta, ○ Estimada.
¿Está resuelta la brecha? ☐ Fecha de resolución: _____ ○ Exacta, ○ Estimada.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

6. Sobre la brecha

Resumen del incidente:

_____

_____

_____

Tipología:

- ☐ Brecha de confidencialidad (acceso no autorizado)
- ☐ Brecha de integridad (modificación no autorizada)
- ☐ Brecha de disponibilidad (desaparición o pérdida)

Medio por el que se ha materializado la brecha:

- ☐ Datos personales residuales en dispositivos obsoletos.
- ☐ Documentación perdida, robada o depositada en localización insegura.
- ☐ Eliminación incorrecta de datos personales en formato papel.
- ☐ Hacking.
- ☐ Malware (e.j. ransomware).
- ☐ Phishing.
- ☐ Correo perdido o abierto.
- ☐ Dispositivo perdido o robado.
- ☐ Publicación no intencionada.
- ☐ Datos personales mostrados al individuo incorrecto.
- ☐ Datos personales enviados por error.
- ☐ Revelación verbal no autorizada de datos personales.
- ☐ Otros: _____

Contexto:

- ○ Interna (acción no intencionada)
- ○ Externa(acción no intencionada)
- ○ Otros:
- ○ Interna (acción intencionada)
- ○ Externa (acción intencionada)

Medidas preventivas aplicadas antes de la brecha:

_____

_____

_____

_____

7. Sobre los datos afectados

Categoría de datos afectados:

- ☐ Datos básicos
- ☐ Credenciales de acceso o identificación
- ☐ Datos de contacto
- ☐ DNI, NIE y/o Pasaporte
- ☐ Datos económicos o financieros
- ☐ Datos de localización
- ☐ Sobre condenas e infracciones penales
- ☐ Otros: _____

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

Categorías especiales de datos:

☐ Sobre el orígen racial ☐ Sobre la opinión política
☐ Sobre la religión o creencia ☐ Sobre la afiliación sindical ☐ Sobre la vida sexual
☐ De salud ☐ Genéticos ☐ Biométricos
☐ Desconocidos ☐ Otros: _____

Número aproximado de registros de datos personales afectados:

8. Sobre los sujetos afectados

Perfil de los sujetos afectados:

☐ Clientes ☐ Usuarios ☐ Empleados ☐ Suscriptores
☐ Estudiantes ☐ Pacientes ☐ Otros: _____

Número aproximado de personas afectadas:

9. Posibles consecuencias

Brecha de confidencialidad:

☐ Divulgación a terceros /difusión en internet ☐ Los datos pueden ser explotados con otros fines
☐ Enriquecimiento de otras bases de datos ☐ Otras: _____

Brecha de integridad:

☐ Datos han sido modificados aunque hayan quedado inservibles o irrecuperables ☐ Datos han sido modificados y utilizados para otros fines
☐ Otras: _____

Brecha de disponibilidad:

☐ Imposibilidad de la prestación de un servicio a los interesados ☐ Deterioro de las condiciones de prestación de un servicio a los interesados
☐ Otras: _____

Naturaleza del impacto potencial sobre los sujetos:

☐ Pérdida de control sobre sus datos personales ☐ Limitación de sus derechos ☐ Discriminación
☐ Usurpación de identidad ☐ Fraude ☐ Pérdidas financieras
☐ Reidentificación no autorizada ☐ Perdida de confidencialidad de datos afectados por secreto profesional
☐ Daños a la reputación ☐ Otras: _____

Severidad de las consecuencias para los individuos: ○ Baja ○ Media ○ Alta ○ Muy alta

Medidas tomadas para solucionar la brecha y minimizar el impacto sobre los afectados:

_____
_____
_____
_____
_____

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

10. Comunicación a los interesados

¿Se ha comunicado la brecha a los interesados?

○Si — Fecha en la que se informó: _____
Número de sujetos informados: _____
Medios o herramientas de comunicación: _____

○No, pero serán informados — Fecha en la que se informará: _____

○No serán informados — Justificación para no informar: _____

○Pendiente de decidir

(Adjuntar contenido de la comunicación a los interesados)

11. Implicaciones trasfronterizas

¿Hay sujetos de otros Estados miembros de la UE afectados por la brecha? ☐

Marque los Estados que puedan estar afectados (A) y aquellos a los que haya notificado(N) la misma brecha de seguridad:

A	N		A	N		A	N	
☐	☐	Alemania	☐	☐	Austria	☐	☐	Bélgica
☐	☐	Bulgaria	☐	☐	Chipre	☐	☐	Croacia
☐	☐	Dinamarca	☐	☐	España	☐	☐	Eslovaquia
☐	☐	Eslovenia	☐	☐	Estonia	☐	☐	Finlandia
☐	☐	Gran Bretaña	☐	☐	Grecia	☐	☐	Hungría
☐	☐	Irlanda	☐	☐	Italia	☐	☐	Letonia
☐	☐	Lituania	☐	☐	Luxemburgo	☐	☐	Malta
☐	☐	Países Bajos	☐	☐	Polonia	☐	☐	Portugal
☐	☐	Rep. Checa	☐	☐	Rumania	☐	☐	Suecia

12. Documentos adjuntos

(Adjuntar documentos)

En_____,a___de_____20__

4.-Registro de incidentes de seguridad en la organización.

REGISTRO DE INCIDENTES DE SEGURIDAD

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

Clasificación del INCIDENTE		☑☒	**Brecha de seguridad** (afecta a datos personales)
		☑☒	**Incidente de seguridad**
Nº de Incidencia: ____/2018		**Fecha de la detección:**	
		Hora de la detección:	
ESTADO DE LA INCIDENCIA		**Pendiente / Resuelto /….**	
1	***Descripción de la violación de seguridad***		
2	***Forma de detección e identificación de la violación de seguridad:***	☐ **Interna:**	
		☐ **Externa:**	
3	***Vector de ataque o método:***	La ruta o medio por el que se ha materializado el incidente es…..	
4	***Supuesto que ha dado lugar al incidente de seguridad (marcar la que corresponda).***	**0-day (vulnerabilidad no conocida):**	
		APT (ataque dirigido):	
		Denegación de servicio (DoS/DDoS):	
		Acceso a cuentas privilegiadas:	
		Código malicioso:	
		Compromiso de la información:	
		Robo y/o filtración de datos:	
		Desfiguración (*Defacement*)	

		Explotación de vulnerabilidades de aplicaciones:	
		Ingeniería social:	
5	***Categoría de brecha de seguridad***	**Brecha de confidencialidad**	
		Brecha de integridad	
		Brecha de disponibilidad	
6	***La categoría o nivel de criticidad respecto a la seguridad de los sistemas afectados.***	☐ Crítico ☐ Muy Alto ☐ Alto ☐ Medio ☐ Bajo	
7	***Naturaleza, sensibilidad y categorías de los datos personales afectados.***	☐ Datos de escaso riesgo ☐ Datos de comportamiento ☐ Datos financieros ☐ Datos sensibles	
8	***Datos legibles/ilegibles.***	☐ Datos seudonimizados ☐ Datos cifrados ☐ Otro	
9	***Volumen de datos personales***	☐ Número aproximado de registros, ficheros y documentos afectados:_____ ☐ Periodos de tiempo:	
10	***Facilidad de identificación de individuos***	☐ Facilidad para deducir la identidad de los individuos ☐ Dificultad media para deducir la identidad de los afectados ☐ Dificultad alta para deducir la identidad de los afectados	
11	***Severidad de las consecuencias para los individuos:***	☐ Baja ☐ Media. ☐ Alta. ☐ Muy alta.	
12	***Características especiales de los individuos:***	☐ SI afectan a individuos con características especiales o con necesidades especiales. ☐ NO afectan a individuos con características especiales o con necesidades especiales.	
13	***Número de individuos afectados:***	☐ Más de 100 individuos. ☐ Entre 100 y 500 individuos. ☐ Entre 1.000 y 5.000 individuos. ☐ Más de 5.000 individuos.	

14	***Características especiales del responsable del tratamiento***		
15	***El perfil de los usuarios afectados***		
16	***El número y tipología de los sistemas afectados.***		
17	***El impacto que la brecha puede tener en la organización.***	☐ Bajo ☐ Medio ☐ Alto	
18	***Los requerimientos legales y regulatorios.***	☐ Notificación de la brecha a la autoridad de control. ☐ Comunicación a Fuerzas y Cuerpos de Seguridad del Estado. ☐ Otro requerimiento regulatorio:_____	
19	***Identificación del delegado de protección de datos o persona de contacto.***		
	Identificación de la persona que detecta la violación de seguridad		
20	***Equipo de incidentes de seguridad en la organización:***	**Gerencia**	
		Personal de Informática	
		Prensa	
		Abogados	
		Técnicos externos	
21	***Posibles consecuencias de la violación de seguridad de datos personales***		
22	***Medidas tempranas de contención del incidente:***	☐ Descripción de las medidas tempranas adoptadas:……..	
		☐ Notificación temprana a la autoridad de control y a los afectados:	
23	***Medidas de erradicación adoptadas***	**Tecnológicas:**	
		Organizativas:	
24	***Medidas de recuperación.***	**Medidas activas implementadas:**	
		Medidas dirigidas a evitar nuevos incidentes por la misma causa:	
25	***Resumen de las evidencias***		

	obtenidas		
26	***Se dispone de informe de resolución de la incidencia.***	**SI**	**Interno** **Externo**
		NO	
27	***(En su caso) Autoridad de Control a la que notificar la violación de seguridad***	*Agencia Española de Protección de Datos*	
28	***Identificación del responsable de notificación a la Autoridad de Control.***		
29	***(En su caso) Fecha y hora de la notificación a la Autoridad de Control***		
30	***(En su caso) Justificación de la NO notificación de la incidencia en el plazo de 72 horas***		

VI

CLÁUSULAS INFORMATIVAS ADAPTADAS AL RGPD PARA LA

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. (VIVA)

REVISION DE CLÁUSULAS INFORMATIVAS

1.-Justificación.

Las nuevas exigencias en cuanto a la transparencia del tratamiento obligan a revisar el contenido de las cláusulas informativas que se empleaban hasta ahora para informar a las personas afectadas. En cuanto a la información recogida antes de la entrada en vigor del RGPD, se recomienda emplear los medios que estén al alcance para poder completar la información ofrecida con el contenido adicional establecido por el Reglamento. Por ejemplo, se pueden publicar las cláusulas informativas adecuadas en la web de la entidad o aprovechar las comunicaciones que mantienen con las personas interesadas para completar la información ofrecida.

Por el **principio de transparencia** (arts. 12.1 REPD y 11 P LOPD) la información a los interesados debe proporcionarse con un **lenguaje claro y sencillo; de forma concisa, transparente, inteligible y de fácil acceso.**

2.-Cláusulas.

2.1.-Política de privacidad. Para incluir en el sitio web: smviva.com, recomendando que la URL sea www.smviva.com/privacidad

POLÍTICA DE PRIVACIDAD

Tal y como establece, 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, le informamos de lo siguiente:

1.-RESPONSABLE DEL TRATAMIENTO

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.
C.I.F nº B47314976.
Dirección: Plaza de la Rinconada, 5- 47001 Valladolid
Telf.: 983 360 230 / Fax: 983 360 273
E-mail: informacion@smviva.com

2.-FINALIDAD DEL TRATAMIENTO

¿Con qué finalidad tratamos tus datos personales?	En VIVA tratamos los datos personales de solicitantes de los distintos servicios que prestamos en el desarrollo de la política de promoción de viviendas protegidas del Ayuntamiento de Valladolid. Concretamente, VIVA tiene como objeto social la gestión directa de la actividad económica de promoción, construcción, rehabilitación de viviendas y edificaciones que comprenderá, entre otras, las siguientes facultades: — El planeamiento, la urbanización, parcelación, adquisición y cesión de terrenos. — La promoción y construcción de viviendas, edificios y locales. — La adjudicación y contratación de toda clase de obras, estudios y proyectos para la construcción o rehabilitación de viviendas, edificios y locales. — El desarrollo de todas las competencias, facultades y actividades que realice, le sean transferidas o encomendadas por el Ayuntamiento de Valladolid sobre promoción de suelo, vivienda y prestación de servicios, actividades económicas o promocionales. Igualmente se tratan los datos personales con la finalidad de informar, por medios electrónicos, al interesado de las actividades indicadas en el párrafo anterior. Puedes *oponerte a la recepción de estas comunicaciones desde aquí.*
¿Por cuánto tiempo se conservarán sus datos?	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se obtuvieron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos.

3.-¿CUÁL ES LA LEGITIMACIÓN PARA EL TRATAMIENTO DE SUS DATOS?

La base legal para el tratamiento de los datos personales es:

- El consentimiento del interesado.
- La necesaria ejecución de una relación jurídica impulsada por el interesado.
- Cumplimiento de una obligación legal aplicable, y el cumplimiento de una misión en interés público.

Para más información consulte EL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

4.-¿A QUIÉN SE COMUNICARÁN SUS DATOS?

En el marco de la solicitud realizada por el interesado, sus datos pueden ser objeto de comunicación a las Notarías encargadas de la realización de los sorteos; al Ayuntamiento de Valladolid, y ser objeto de publicación en el sitio web tanto de VIVA, como de la Corporación indicada, a efectos de publicidad del procedimiento. En este último supuesto se procurará implementar los medios técnicos necesarios que eviten la indexación de la información, por parte de los buscadores de Internet.

5.-¿CUÁLES SON SUS DERECHOS y DÓNDE EJERCITARLOS?

- Cualquier interesado tiene derecho a obtener confirmación sobre si en SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. estamos tratando datos personales que les conciernan, o no. Las personas interesadas tienen derecho a si acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos.
- En determinadas circunstancias, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.
- En determinadas circunstancias y por motivos relacionados con su situación particular, los interesados podrán oponerse al tratamiento de sus datos. SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. dejará de tratar los datos, salvo por motivos legítimos, o el ejercicio o la defensa de posibles reclamaciones.
- Le advertimos de su derecho a retirar, en cualquier momento, el consentimiento prestado para tratar sus datos, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada. Finalmente, le recordamos, por imperativo legal, su derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es), si considerara que el tratamiento de datos no es acorde a la normativa europea.
- Puede ejercer sus derechos, acreditando su identidad (fotocopia del DNI), remitiendo un email a la dirección: privacidad@smviva.es

2.2.- Política de cookies:

DEBE CREARSE UN APARTADO (NORMALMENTE AL LADO DE LA POLITICA DE PRIVACIDAD). Hay que informar y recabar el CONSENTIMIENTO de los usuarios que acceden a la web.

Debe salir una ventana emergente en la que se diga algo así como:

"Esta web utiliza cookies para facilitar la navegación. Puede obtener información sobre todas ellas y como desactivarlas desde aquí.
ACEPTO EL USO DE COOKIES EN ESTE SITIO WEB.

ACLARACIÓN:
Este apartado debe completarse por VIVA, determinando los técnicos que gestionan el sitio web que tipo de cookies están almacenadas. Hemos verificado que existen cookies de marketing. Adjuntamos informe de presencia de cookies en el sitio web de VIVA.

TEXTO PARA EL APARTADO DE COOKIES:

En la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. utilizamos cookies con el objetivo de prestar un mejor servicio y proporcionarle una mejor experiencia en su navegación. Queremos informarle de manera clara y precisa sobre las cookies que utilizamos, detallando a continuación, que es una cookie, para que sirve, que tipos de cookies utilizamos, cuales son su finalidad y como puede configurarlas o deshabilitarlas si así lo desea.

Una cookie es un fichero de texto que se descarga en el dispositivo del usuario en el momento de acceder a determinadas páginas web para almacenar y recuperar información sobre la navegación que se efectúa desde dicho equipo.

+ info sobre lo que es una cookie disponible en Wikipedia.

En VIVA utilizamos las siguientes cookies que se detallan en el cuadro siguiente:

2. ***Cookies* necesarias** para la prestación de servicios que solicita el usuario. Se advierte que si se desactivan estas cookies no se podrá garantizar el correcto uso y recepción de nuestros servicios y contenidos.
3. **Cookies analíticas** para el seguimiento y análisis estadístico del comportamiento del conjunto de los usuarios.

COOKIES ACTIVAS EN www.smviva.com		
COOKIES PROPIAS	**Finalidad**	**Desactivación**
Necesarias para la navegación	La prestación de servicios de la sociedad de la información que han sido solicitados por el propio usuario.	No es posible.
COOKIES DE TERCEROS	**Finalidad**	**Desactivación**
Google Analytics	**Realización de estadísticas de navegación de los usuarios.**	**Desactivar**

El usuario puede elegir, en todo momento qué cookies permite que estén activas en este sitio web mediante:

- Una correcta configuración del concreto **navegador que esté utilizando el usuario**: **Chrome**; **Explorer**; **Firefox**; o Safari
- **Sistemas específicos** (denominados opt-out) indicados anteriormente. Con el fin de desactivar la concreta cookie este tipo de sistemas pueden exigir la instalación en el equipo del usuario de una cookie denominada "de rechazo".
- Herramientas de terceros, que permiten a los usuarios detectar las cookies en cada sitio web que visita y gestionar su desactivación, como, por ejemplo:
  - *http://www.criteo.com/deactivate-criteo-banners/*
  - *http://youronlinechoices.eu/*
  - *http://www.networkadvertising.org/choices/*
  - *http://www.aboutads.info/choices/*

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L no puede hacerse responsable del contenido y actualización de las políticas de privacidad de terceros que han sido enlazadas anteriormente.

+ información en nuestra Política de Privacidad.

2.3.-Aviso Legal para el sitio web: smviva.es

Aviso Legal

1.-Información legal.

En cumplimiento de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, le informamos que el prestador de servicios es la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

- Inscrita en el Registro Mercantil de Valladolid en el tomo 509, folio 135, Hoja VA-4547 y C.I.F nº B47314976.
- Dirección: Plaza de la Rinconada, 5- 47001 Valladolid
- Telf.: 983 360 230 / Fax: 983 360 273
  E-mail: informacion@smviva.com

2.-Aceptación de las condiciones de utilización.

El acceso al presente sitio web exige la aceptación de las normas de utilización que en cada momento se encuentren vigentes en esta dirección electrónica.

3.-Política de privacidad.

Puede *consultar aquí nuestra política de privacidad.*

Por otro lado, en cumplimiento de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, le informamos que en todo momento puede oponerse al tratamiento de sus datos con el fin de remitirle comunicaciones comerciales para estos fines, para lo cual es suficiente con dirigir una comunicación a la dirección **informacion@smviva.co**

4.-Cookies

Una cookie es un pequeño fichero de texto que un sitio web guarda en su ordenador o dispositivo móvil cuando usted visita el sitio. Las cookies se utilizan con mucha frecuencia para que los sitios funcionen, o para que funcionen mejor, así como para facilitar información a los propietarios del sitio.

Puede *consultar aquí nuestra política de cookies.*

5.-Propiedad Intelectual.

La titularidad de los derechos de propiedad intelectual de todos los contenidos, incluidos los recursos gráficos contenidos en el sitio web, la ostenta y mantiene en todo momento la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. y, en su caso, los autores, que han transmitido los derechos de explotación comercial. El usuario reconoce que la reproducción, comercialización, comunicación pública, distribución o transformación no autorizadas de tales obras, salvo para uso personal y privado, constituye una infracción de los derechos de propiedad intelectual sancionable de conformidad con la legislación vigente. Queda terminantemente prohibido al usuario realizar cualquier tipo de distribución comercial a terceros de los datos obtenidos en el presente sitio web sin la previa autorización expresa y por escrito de la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

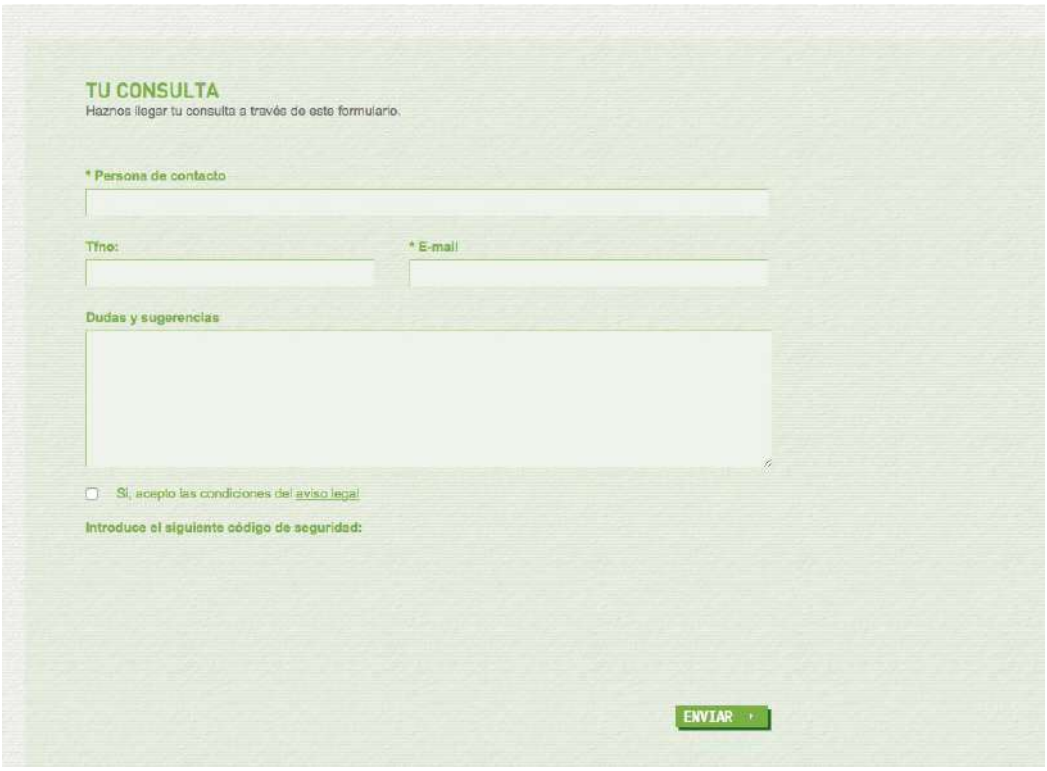
6.-Responsabilidades.

La función de los enlaces que aparecen en el sitio web es la de informar sobre la existencia de diversas fuentes de información de interés ampliando los contenidos de este sitio web. la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. no es responsable del contenido, validez y exactitud de la información contenida en dichos enlaces, ni igualmente, de los posibles daños o perjuicios que pudieran acaecer como consecuencia de la utilización de los contenidos del sitio web, siendo de exclusiva responsabilidad del usuario que accede a los mismos.

7.-Jurisdicción.

Para todas aquellas cuestiones que pudieran suscitarse con motivo de la interpretación, ejecución o eventual incumplimiento de las presentes condiciones de utilización, los intervinientes, con renuncia a su fuero propio, y con independencia del lugar donde se suscite cualquier disputa, se someten expresamente a la competencia y jurisdicción de los juzgados y tribunales de la ciudad de Valladolid Las presentes condiciones se regirán, en todo caso, por la legislación española.

2.4.-Cláusulas a incluir en los FORMULARIOS DE LA WEB smviva.com

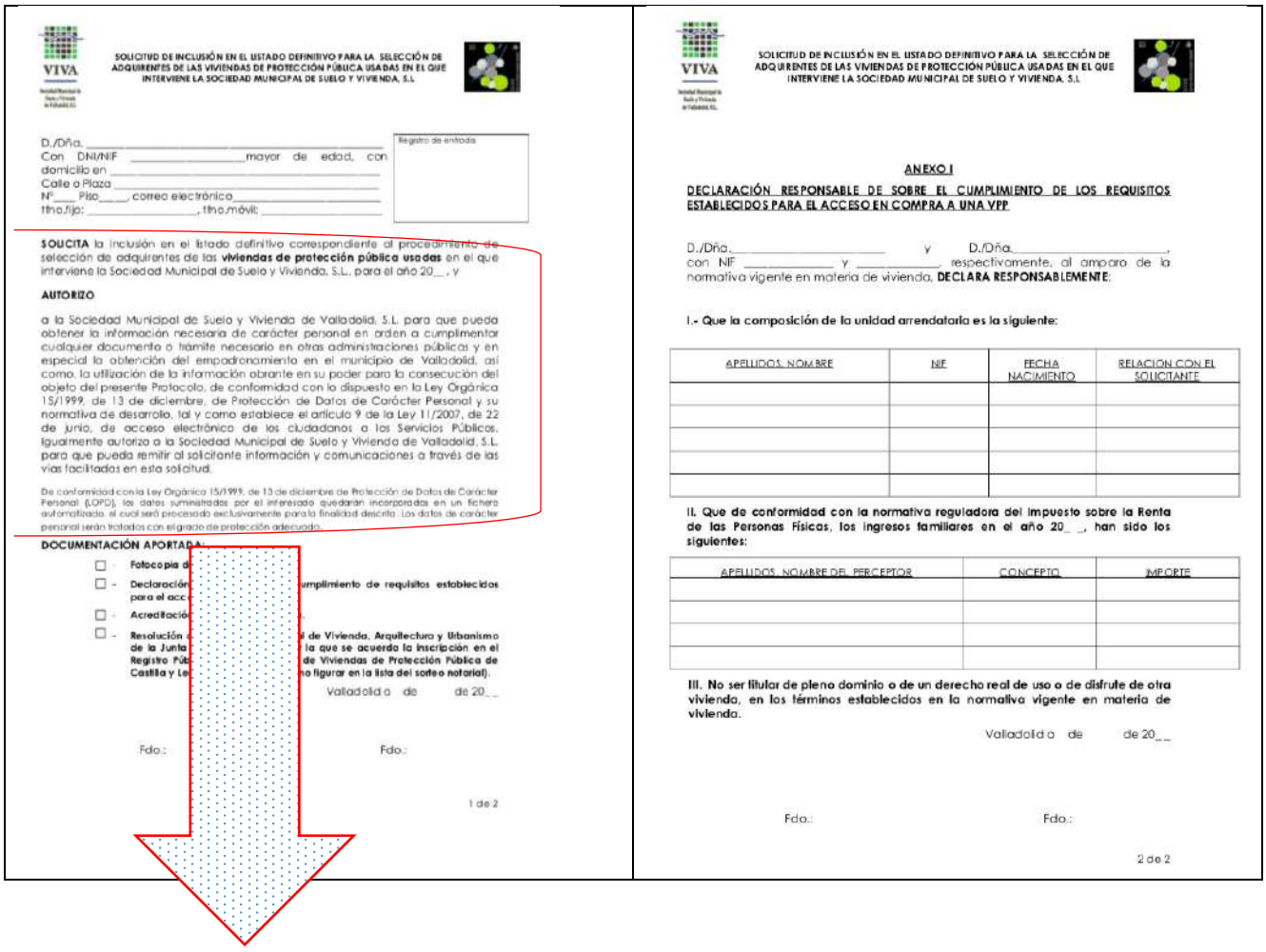


En TODOS LOS FORMULARIOS, EN LOS QUE SE RECOJAN DATOS, debajo, en una "cajita" debe incluirse la leyenda siguiente:

Atendiendo a lo establecido en el Reglamento General de Protección de Datos, el responsable del tratamiento es la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. Utilizaremos tus datos para gestionar la petición, o los servicios que nos solicitas. El tratamiento es necesario para el correcto desenvolvimiento de la relación negocial o prenegocial que pudiera existir, y en su caso, para la remisión de información electrónica de los servicios de VIVA. Tus datos son comunicados a terceros, bien por exigencia legal o por necesidad de la propia prestación del servicio del que nos solicitas información. Tienes derecho a acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional, que puedes consultar en nuestra Política de Privacidad. Igualmente, puedes consultar nuestro Registro de Actividades de Tratamiento.

2.5.-Cláusulas a incluir en la SOLICITUD de inclusión en el listado definitivo correspondiente al procedimiento de selección de adquirentes de las viviendas de protección pública usadas.

Estos son los modelos actuales.



SOLICITUD DE INCLUSIÓN EN EL LISTADO DEFINITIVO PARA LA SELECCIÓN DE ADQUIRENTES DE LAS VIVIENDAS DE PROTECCIÓN PÚBLICA USADAS EN EL QUE INTERVIENE LA SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA, S.L.

D./Dña. _____
Con DNI/NIF _____ mayor de edad, con domicilio en _____
Calle o Plaza _____
Nº____ Piso____, correo electrónico_____
tfno.fijo: _____, tfno.móvil: _____

Registro de entrada

SOLICITA la inclusión en el listado definitivo correspondiente al procedimiento de selección de adquirentes de las **viviendas de protección pública usadas** en el que interviene la Sociedad Municipal de Suelo y Vivienda, S.L., para el año 20__ , y

AUTORIZO

a la Sociedad Municipal de Suelo y Vivienda de Valladolid, S.L. para que pueda obtener la información necesaria de carácter personal en orden a cumplimentar cualquier documento o trámite necesario en otras administraciones públicas y en especial la obtención del empadronamiento en el municipio de Valladolid, así como, la utilización de la información obrante en su poder para la consecución del objeto del presente Protocolo, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, tal y como establece el artículo 9 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Igualmente autorizo a la Sociedad Municipal de Suelo y Vivienda de Valladolid, S.L. para que pueda remitir al solicitante información y comunicaciones a través de las vías facilitadas en esta solicitud.

De conformidad con la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD), los datos suministrados por el interesado quedarán incorporados en un fichero automatizado, el cual será procesado exclusivamente para la finalidad descrita. Los datos de carácter personal serán tratados con el grado de protección adecuado.

DOCUMENTACIÓN APORTADA:

- ☐ - Fotocopia d
- ☐ - Declaración … cumplimiento de requisitos establecidos para el acc…
- ☐ - Acreditació…
- ☐ - Resolución … de la Junta … de Vivienda, Arquitectura y Urbanismo … la que se acuerda la inscripción en el Registro Púb… de Viviendas de Protección Pública de Castilla y Le… no figurar en la lista del sorteo notarial).

Valladolid a de de 20__

Fdo.: Fdo.:

1 de 2

SOLICITUD DE INCLUSIÓN EN EL LISTADO DEFINITIVO PARA LA SELECCIÓN DE ADQUIRENTES DE LAS VIVIENDAS DE PROTECCIÓN PÚBLICA USADAS EN EL QUE INTERVIENE LA SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA, S.L.

ANEXO I

DECLARACIÓN RESPONSABLE DE SOBRE EL CUMPLIMIENTO DE LOS REQUISITOS ESTABLECIDOS PARA EL ACCESO EN COMPRA A UNA VPP

D./Dña._____ y D./Dña._____, con NIF _____ y _____, respectivamente, al amparo de la normativa vigente en materia de vivienda, **DECLARA RESPONSABLEMENTE:**

I.- Que la composición de la unidad arrendataria es la siguiente:

APELLIDOS, NOMBRE	NIF	FECHA NACIMIENTO	RELACIÓN CON EL SOLICITANTE

II. Que de conformidad con la normativa reguladora del Impuesto sobre la Renta de las Personas Físicas, los ingresos familiares en el año 20__ , han sido los siguientes:

APELLIDOS, NOMBRE DEL PERCEPTOR	CONCEPTO	IMPORTE

III. No ser titular de pleno dominio o de un derecho real de uso o de disfrute de otra vivienda, en los términos establecidos en la normativa vigente en materia de vivienda.

Valladolid a de de 20__

Fdo.: Fdo.:

2 de 2

Después de los campos de recogida de datos personales, proponemos el siguientes TEXTO LEGAL.

D./Dña….

(….)

*SOLICITA su inclusión en el listado definitivo correspondiente al procedimiento de selección de adquirentes de las **viviendas de protección pública usadas**, en el que interviene la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. (en adelante, VIVA).*

Para tal finalidad, y conforme establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, le informamos que el responsable del tratamiento es VIVA con dirección: Plaza de la Rinconada, 5- 47001 Valladolid Telf.: 983 360 230 / Fax: 983 360 273. E-mail: informacion@smviva.com. Sus datos serán tratados únicamente para gestionar la presente solicitud y para la remisión de información electrónica de los servicios de VIVA. Sus datos serán comunicados a terceros, bien por exigencia legal o por necesidad de la propia prestación del servicio solicitado. Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional, que puede consultar en nuestra ***Política de Privacidad*** *(www.smviva.com/privacidad). Igualmente, para más información, puede acceder al* ***Registro de Actividades de Tratamiento de VIVA****. (www.smviva.com/registrodeactividades)*

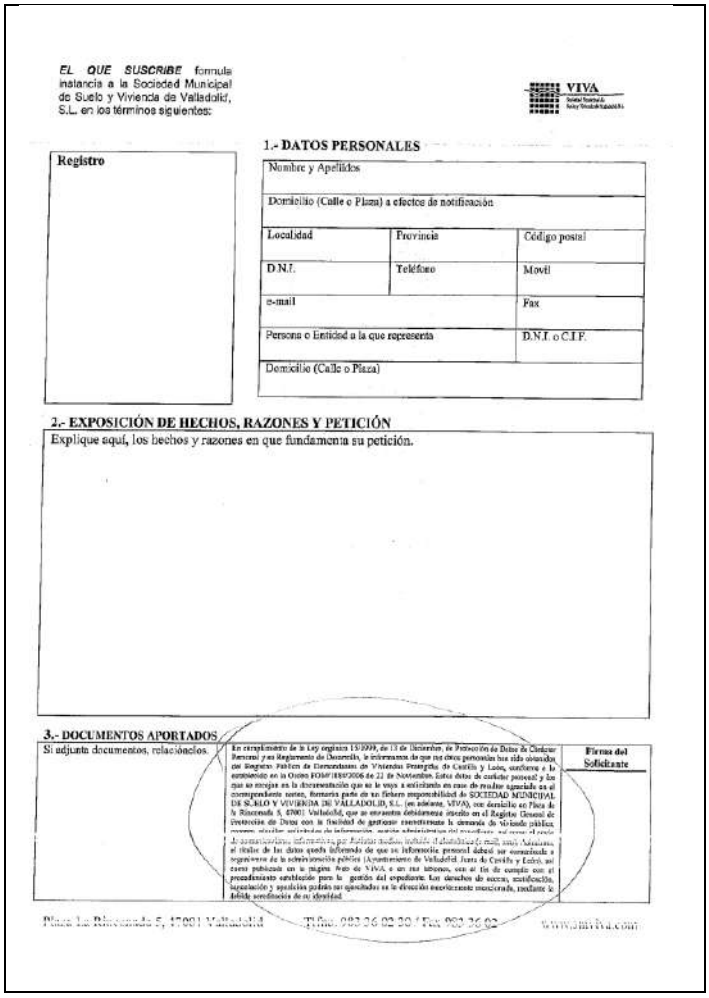
☐ *Autorizo explícitamente a la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. a obtener el volante de empadronamiento directamente del Ayuntamiento de Valladolid.* ***IMPORTANTE: En el supuesto de NO autorizarse la comunicación el interesado debe aportar dicho certificado.***

Documentación aportada:
(esto si se quiere, que se deje igual)

Nombre y apellidos
Fecha
Firma

2.6.-Cláusulas a incluir en el modelo de SOLICITUD general.

Este es el modelo actual.



EL QUE SUSCRIBE formula instancia a la Sociedad Municipal de Suelo y Vivienda de Valladolid, S.L. en los términos siguientes:

VIVA

1.- DATOS PERSONALES

Registro	Nombre y Apellidos	
	Domicilio (Calle o Plaza) a efectos de notificación	
	Localidad / Provincia / Código postal	
	D.N.I. / Teléfono / Móvil	
	e-mail / Fax	
	Persona o Entidad a la que representa / D.N.I. o C.I.F.	
	Domicilio (Calle o Plaza)	

2.- EXPOSICIÓN DE HECHOS, RAZONES Y PETICIÓN

Explique aquí, los hechos y razones en que fundamenta su petición.

3.- DOCUMENTOS APORTADOS

Si adjunta documentos, relaciónelos.

Firma del Solicitante

En cumplimiento de la Ley orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal y su Reglamento de Desarrollo, le informamos de que sus datos personales han sido obtenidos del Registro Público de Demandantes de Vivienda Protegida de Castilla y León, conforme a lo establecido en la Orden FOM/1859/2006 de 22 de Noviembre. Estos datos de carácter personal y los que se recojan en la documentación que se le vaya a solicitando en caso de resultar agraciado en el correspondiente sorteo, formarán parte de un fichero responsabilidad de SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA DE VALLADOLID, S.L. (en adelante, VIVA), con domicilio en Plaza de la Rinconada 5, 47001 Valladolid, que se encuentra debidamente inscrito en el Registro General de Protección de Datos con la finalidad de gestionar exclusivamente la demanda de vivienda pública, [illegible] información, por [illegible] medio, [illegible] Asimismo, el titular de los datos queda informado de que su información personal deberá ser comunicada a organismos de la administración pública (Ayuntamiento de Valladolid, Junta de Castilla y León), así como publicada en la página Web de VIVA, a los mismos, con el fin de cumplir con el procedimiento establecido para la gestión del expediente. Los derechos de acceso, rectificación, cancelación y oposición podrán ser ejercitados en la dirección anteriormente mencionada, mediante la debida acreditación de su identidad.

Plaza de la Rinconada 5, 47001 Valladolid — Tlfno.: 983 36 02 30 / Fax: 983 36 02 — www.smviva.com

Conforme establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, le informamos que el responsable del tratamiento es la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. con dirección: Plaza de la Rinconada, 5- 47001 Valladolid Telf.: 983 360 230 / Fax: 983 360 273. E-mail: informacion@smviva.com. Sus datos serán tratados únicamente para gestionar la presente solicitud y para la remisión de información electrónica de los servicios de VIVA. Sus datos serán comunicados a terceros, bien por exigencia legal o por necesidad de la propia prestación del servicio solicitado. Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional, que puede consultar en nuestra ***Política de Privacidad*** *(www.smviva.com/privacidad). Igualmente, para más información, puede*

*acceder al **Registro de Actividades de Tratamiento de VIVA**. (www.smviva.com/registrodeactividades)*

2.7.-Cartel de videovigilancia adaptado al RGPD

Se adjunta el pdf cumplimentable (para cambios) en el ANEXO.

IX

REGISTRO DE ENCARGADOS DE TRATAMIENTO Y SUS CONTRATOS SOBRE PROTECCIÓN DE DATOS EN

LA SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

1.-Justificación.

El Reglamento General de Protección de Datos, define en su artículo 4 (punto 7) como "**responsable del tratamiento**" o «responsable» a: *"(…) la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".*

Por otro lado, en el apartado 8, señala que el "**encargado del tratamiento**" como: *"(…) la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".* Según el Reglamento General de Protección de Datos, **el responsable debe adoptar medidas apropiadas, incluida la elección de encargados, de tal forma que garantice y esté en condiciones de probar que el tratamiento de datos se está realizando conforme a lo que establece el Reglamento Europeo (art. 28.1 RGPD)**. Esta previsión se extiende igualmente al encargado cuando subcontraten servicios que impliquen acceso a datos, con otros subencargados.

El RGPD prevé que la adhesión a códigos de conducta o la posesión de un certificado de protección de datos pueden servir como mecanismos de prueba. En todo caso, no es un catálogo *numerus clausus,* pudiendo el responsable acreditarlo de cualquier otra forma, que debería ser valorada, llegado el caso, por la autoridad de control.

La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un **contrato o de un acto jurídico similar que los vincule.** El contrato o acto jurídico debe constar **por escrito, inclusive en formato electrónico**.

> Señala el primer apartado del artículo 28.3 del REPD que: "El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, 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 categorías de interesados, y las obligaciones y derechos del responsable (…)"
>
> La posibilidad de regular esta relación a través de un acto jurídico unilateral del responsable es una de las novedades que se presentan en el Reglamento. En cualquier caso, debe tratarse de un acto jurídico que establezca y defina la posición del encargado, siempre que ese acto vincule jurídicamente al encargado del tratamiento. Este sería el caso, por ejemplo, de una resolución administrativa que conste notificada al encargado del tratamiento.
>
> Apartado 9 del artículo 28 REPD: "El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico".

2.-Registro de encargados de tratamientos que prestan servicios con acceso a datos personales.

ENCARGADO	OBJETO DE LA PRESTACION	CONTRATO SUSCRITO RGPD	FECHA	CERTIF./ COD. CONDUCTA
Techco Securit	Mantenimiento del sistema de videovigilancia	☒		☒
Bitlan Asesores informáticos CB	Mantenimiento de los sistemas de información	☒ INSUFICIENTE		☒
Auditor de cuentas (El que se determine en cada momento)	Auditoría de cuentas	☒	Anual	☒
Ayuntamiento de Valladolid	- Publicación de listados de sorteos (Convenio). - Control horario (A través de su *software*). - Consulta al padrón de habitantes previo consentimiento del interesado.	☒ INSUFICIENTE		☒
Europac	Destrucción documental	☒ INSUFICIENTE		☒
Garrigues Abogados	Consultores contables	☒		☒

Allí donde se señala en *"Contrato suscrito RGPD"* con una ☒ se requiere la suscripción de un contrato adaptado en materia de protección de datos. Proponemos el siguiente modelo que debe personalizar la entidad, atendiendo a las prestaciones existentes en cada momento.
Estas condiciones pueden incluirse (en su parte esencial recogida en el Punto 4º del modelo de Contrato) en los correspondientes pliegos de contratación.

3.-Modelo de Contrato para suscribir entre LA SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. y los distintos encargados de tratamientos, adaptado al RGPD.

_____, a ____ de _____ de 2018

REUNIDOS

DE UNA PARTE:

La SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.», con domicilio social en Plaza de la Rinconada, 5 - CP 47001 Valladolid y con CIF: B47314976, inscrita en el Registro Mercantil de Valladolid en el tomo 509, folio 135, Hoja VA-4547, debidamente representada en este acto por D. /Dña._____.

En calidad de RESPONSABLE DEL FICHERO, en adelante, «EL RESPONSABLE»,

DE OTRA PARTE:

«ENTIDAD B», con domicilio social en _____, C/_____ y con CIF: _____, debidamente representada en este acto por D./Dña. _____.

En calidad de ENCARGADO DEL TRATAMIENTO, en adelante, «EL ENCARGADO».

Ambas partes se reconocen mutuamente la capacidad legal suficiente para suscribir este contrato de encargo de tratamiento de datos personales y para quedar obligadas en la representación en que respectivamente actúan, en los términos convenidos en él. A tal fin,

EXPONEN

I. Que «EL RESPONSABLE» es una Sociedad Municipal que tiene como principal función el desarrollo de la política de promoción de viviendas protegidas del Ayuntamiento de Valladolid.

II. Que «EL ENCARGADO» es una empresa dedicada, entre otras actividades propias de su objeto social, a las de ……

III. Que entre ambas partes existe una relación contractual por la cual «EL ENCARGADO» presta servicios relacionados con la …… a favor de «EL RESPONSABLE», que puede implicar un tratamiento del fichero con datos personales titularidad de este último (en adelante, LOS SERVICIOS).

IV. Que, al objeto de dar cumplimiento a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, ambas partes están interesadas en suscribir un contrato de encargo de tratamiento de datos personales, el cual formalizan de común acuerdo, sobre la base de las siguientes

ESTIPULACIONES

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a la entidad....., encargada del tratamiento, para tratar por cuenta de la *SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.* responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio de..... .
El tratamiento consistirá en: (*descripción detallada del servicio*)

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad *SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.* responsable del tratamiento, pone a disposición de la entidad ....., encargada del tratamiento, la información que se describe a continuación:

- ……

- .....

3. Duración

El presente acuerdo tiene una duración de .....

Una vez finalice el presente contrato, el encargado del tratamiento debe suprimir/devolver al responsable/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 obliga a:

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 *Reglamento (UE) 2016/679* o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

c. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

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 *Reglamento (UE) 2016/679*, la documentación de garantías adecuadas.
4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:
   - La seudoanimización y el cifrado de datos personales.
   - La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
   - La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
   - El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d. No comunicar 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 de este 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.

e. 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 ..... (NOTA: Se recomienda establecer un plazo mínimo de antelación para realizar la comunicación)....., 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.

f. El Encargado del Tratamiento deberá observar en todo momento, y en relación con los ficheros de datos de carácter personal a los que tuviera acceso o le pudieren ser entregados por el Responsable, para la realización en cada caso de los trabajos y servicios que pudieren acordarse, el **deber de confidencialidad y secreto profesional** que, de conformidad con lo dispuesto en el artículo 10 de la Ley Orgánica 15/1999, de Protección de Datos, subsistirá aun después de finalizar la relación de los trabajos encargados en relación con cualquier fichero así como, en su caso, tras la finalización por cualquier causa del presente contrato.

g. Garantizar que las personas autorizadas para tratar datos personales **se comprometan, de forma expresa y por escrito, a respetar la confidencialidad** y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

NOTA: Si existe una obligación de confidencialidad de naturaleza estatutaria o legal (por ejemplo, abogados) deberá quedar constancia expresa de la naturaleza y extensión de esta obligación.

h. Mantener a disposición del responsable la **documentación acreditativa del cumplimiento** de la obligación establecida en el apartado anterior.

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

j. Asistir al responsable del tratamiento en la respuesta al **ejercicio de los derechos** de:

- Acceso, rectificación, supresión y oposición
- Limitación del tratamiento
- Portabilidad de datos
- A no ser objeto de decisiones individualizadas automatizadas (incluida
- la elaboración de perfiles)

(Escoger una de las opciones)

Opción A

El encargado del tratamiento debe resolver, por cuenta del responsable, y dentro del plazo establecido, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, en relación con los datos objeto del encargo.
(NOTA: A pesar de que la delegación en el encargado es una decisión que corresponde al responsable, resulta especialmente recomendable en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado).

Opción B

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.

(NOTA: Plazo y medio recomendados a fin de que el responsable pueda resolver la solicitud dentro del plazo establecido).

k. Derecho de información

(Escoger una de las opciones)

Opción A

El encargado del tratamiento, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.

Opción B

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

l. Notificación de violaciones de la seguridad de los datos
El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas y a través de..... , 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:

- 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.
- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- 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.
- 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.

m. Dar apoyo al responsable del tratamiento en la realización de las **evaluaciones de impacto** relativas a la protección de datos, cuando proceda.
n. Dar apoyo al responsable del tratamiento en la **realización de las consultas previas a la autoridad de control**, cuando proceda.
o. Poner 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.
p. En cuanto a las **medidas de seguridad**, en encargado **deberá implantar mecanismos para:**

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
- Seudonimizar y cifrar los datos personales, en su caso.

q. Designar (en caso de ser exigible al encargado, atendiendo al art 37 del RGPD) un **delegado de protección de datos** y comunicar su identidad y datos de contacto al responsable.

r. Destino de los datos:

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 comporta 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.

5.-Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

1. Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.
2. Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.
3. Realizar las consultas previas que corresponda.
4. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del *Reglamento (UE) 2016/679* por parte del encargado.
5. Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

6.-Responsabilidad del encargado del tratamiento.

a) El Encargado del Tratamiento será considerado responsable del tratamiento en el caso de que destine los datos a otra finalidad, los comunique o los utilice incumpliendo el presente contrato. En estos casos, el Encargado del Tratamiento responderá de las infracciones en que hubiera incurrido personalmente.

b) El Encargado del Tratamiento indemnizará al Responsable del Tratamiento por los daños y perjuicios, de cualquier naturaleza, que pudieran resultar del incumplimiento de las obligaciones contraídas en virtud del presente contrato.

c) A título enunciativo, y no limitativo, dicha indemnización incluirá los daños morales e imagen, costes publicitarios o de cualquier otra índole que pudieran resultar para su reparación. El Encargado del Tratamiento, asimismo, deberá responder de cualquier indemnización que a resultas de su incumplimiento tuviera que satisfacer a terceros.

d) La responsabilidad del Encargado del Tratamiento incluirá, además, el importe de cualquier sanción administrativa y/o resolución judicial condenatoria que pudiera resultar contra el Responsable del Tratamiento, como resultado del incumplimiento del Encargado del Tratamiento de la normativa y de las obligaciones exigidas en el presente contrato. La indemnización comprenderá, además del importe de la sanción y/o resolución judicial, el de los intereses de demora, costas judiciales y el importe de la defensa del Responsable del Tratamiento en cualquier proceso en el que pudiera resultar demandada por cualquiera de las causas anteriormente expuestas.

7.-Controles y auditorías.

El Responsable del Tratamiento, en su condición, se reserva el derecho de efectuar en cualquier momento los controles y auditorías que estime oportunos para comprobar el correcto cumplimiento por parte del Encargado del Tratamiento del presente contrato. Por su parte, el Encargado deberá facilitar al Responsable del Tratamiento cuantos datos o documentos le requiera para el adecuado cumplimiento de dichos controles y auditorías.

8.-Notificaciones.

a. Cualquier notificación que se efectúe entre las partes se hará por escrito y será entregada personalmente o de cualquier otra forma que certifique la recepción por la parte notificada.
b. Cualquier cambio de domicilio de una de las partes deberá ser notificado a la otra de forma inmediata y por un medio que garantice la recepción del mensaje.

9.-Cláusulas generales.

a. La no exigencia por cualquiera de las partes de cualquiera de sus derechos, de conformidad con el presente Contrato, no se considerará que constituye una renuncia a dichos derechos en el futuro.
b. La relación jurídica que se constituye entre las partes se rige por este único Contrato, siendo el único válido existente entre las partes y sustituye a cualquier tipo de acuerdo o compromiso anterior acerca del mismo objeto, ya sea escrito o verbal, y sólo podrá ser modificado por un acuerdo firmado por ambas partes.
c. Si se llegara a demostrar que alguna de las estipulaciones contenidas en este Contrato es nula, ilegal o inexigible, la validez, legalidad y exigibilidad del resto de las estipulaciones no se verán afectadas o perjudicadas por aquélla.
d. El presente Contrato y las relaciones entre el Responsable del Tratamiento y el Encargado del Tratamiento no constituyen en ningún caso sociedad, empresa conjunta, agencia o contrato de trabajo entre las partes.
e. Los encabezamientos de las distintas cláusulas son sólo a efectos informativos, y no afectarán, calificarán o ampliarán la interpretación de este Contrato.

En testimonio de lo cual formalizan el presente contrato, por duplicado, en el lugar y fecha indicados en el encabezamiento.

D:/Dña. _____
En nombre de «EL RESPONSABLE» SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

D:/Dña. _____
En nombre de «EL ENCARGADO»

4.- Evaluación de riesgos de proveedores (*Supplier Risk Evaluation*)

Es imprescindible, para verificar el grado de cumplimiento normativo en protección de datos, con base en la diligencia debida del responsable del tratamiento en la elección de sus encargados, que éstos den cumplida respuesta, y con un alto grado de satisfacción, al siguiente cuestionario que deberá ser analizado, una vez cumplimentado:

Evaluación de riesgos de proveedores (Supplier Risk Evaluation)

Encargado del tratamiento:

Finalidad de la prestación:

Fecha: __/____/20___

	Respuesta
1 Certificación GDPR	
Importante: *En caso de disponer de la certificación GDPR no será necesario completar el resto del cuestionario.*	
1.1 ¿Se han adoptado las medidas técnicas y organizativas exigibles por la normativa de protección de datos? (Serán evaluadas y vinculantes por el cuestionario)	
2 Cuestiones generales	
2.1 ¿Dispone de una política en materia de protección de datos adaptada a GDPR?, En caso afirmativa, debe ser adjuntada.	
2.2 ¿Se imparte formación en materia de protección de datos a sus empleados? En caso afirmativo, adjuntar evidencia.	
2.3 Los empleados que vayan a acceder a los datos personales del cliente, ¿firman cláusulas de confidencialidad en materia de protección de datos? En caso afirmativo, adjuntar evidencia.	
2.4 ¿Dispone de un procedimiento para gestionar solicitudes de ejercicio de derechos de interesados y/o comunicar las mismas al responsable (cliente)? En caso afirmativo, debe ser adjuntada.	
2.5 ¿Se ha designado un Delegado de Protección de Datos (DPO) o un responsable de protección de datos? En caso afirmativo, adjuntar designación formal o evidencia de designación formal.	
3 Subcontratación	
3.1 En el caso de que el servicio a prestar al responsable (cliente) vaya a ser subcontratado con un tercero en parte o en su totalidad, ¿dispone de un procedimiento de revisión y control sobre el subcontratado con el fin de verificar el cumplimiento en materia de protección de datos? En caso afirmativo, deber ser adjuntado.	
4 Transferencias internacionales de datos	
Nota*: El posible acceso del tercero proveedor del servicio a los sistemas de la compañía desde un tercer país, es considerado una transferencia internacional de datos.* ***Nota****: En todos los casos, debe contemplarse que la subcontratación de todo el servicio o parte de él en un tercero, debe regirse por los mismos requerimientos y obligaciones exigidos al proveedor.*	
4.1 ¿El servicio almacena y procesará los datos (incluso las copias de seguridad) en países del Espacio Económico Europeo* o en alguno de los siguientes países (Andorra,	

Argentina, Canadá (Sector privado), Suiza, Islas Feroe, Guernsey, Israel, Isla de Man, Jersey, Nueva Zelanda y Uruguay)? *EEE lo componen los países miembros de la UE + Islandia, Liechtenstein y Noruega)	
4.2 Responda afirmativamente si cumple alguno de los siguientes casos: **c. En el caso de que el tratamiento de los datos vaya a ser realizado por un proveedor establecido en EE.UU., Este se encuentra el mismo adherido a los Acuerdos de Privacy Shield (En caso afirmativo adjuntar evidencia de la adherencia al Privacy Shield).** **d. La transferencia internacional de datos está legitimada por el establecimiento de Binding Corporate Rules o Normas Corporativas Vinculantes entre empresas del Grupo del proveedor aprobadas por alguna Autoridad de Control (En caso afirmativo adjuntar evidencia de autorización por parte de la autoridad de control)** **e. C) La transferencia internacional de datos esta legitimada por medio de garantías adecuadas y los interesados cuentan con derechos exigibles y acciones legales efectivas.**	
5 Incidentes de seguridad	
5.1 ¿Dispone de procedimientos de actuación, de cara a informar al responsable sin dilación indebida, en caso de que se produzca un incidente de seguridad que afecte a los datos de carácter personal? En caso afirmativo, adjuntar procedimiento.	
5.2 Dentro del procedimiento de comunicación de incidentes de seguridad al responsable (cliente), ¿se describe la naturaleza de la incidencia, el número aproximado y categorías de datos, la información de contacto del DPO, la descripción de las medidas propuestas para remediar o mitigar la incidencia, así como las posibles consecuencias de dicha incidencia?	
5.3 En caso de un incidente de seguridad, ¿el proveedor dispone de un protocolo de remediación o mitigación? En caso afirmativo, adjuntar protocolo de remediación o mitigación.	
6 Evaluaciones de impacto (PIA)	
6.1 ¿Dispone de una metodología para la realización de evaluaciones de impacto (denominadas DPIAs) relativa a la protección de datos? En caso afirmativo, adjuntar la metodología utilizada.	
6.2 En caso de que exista la obligación de tener designado un Delegado de Protección de Datos, ¿la realización de las evaluaciones de impacto cuenta con el asesoramiento del DPO o el responsable de protección de datos? En caso afirmativo, adjuntar evidencia del asesoramiento del DPO o responsable de protección de datos.	

X

CLÁUSULAS Y POLÍTICAS DE SEGURIDAD PARA SUSCRIBIR POR EL PERSONAL DE

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

SUSCRIPCION DE CLÁUSULAS INFORMATIVAS POR PARTE DEL PERSONAL DE LA ORGANIZACIÓN

1.-Justificación.

La publicación y el cumplimiento de estas normas, adaptadas, en parte, al Esquema Nacional de Seguridad, contribuirá a:

- Facilitar el máximo aprovechamiento de los recursos y sistemas de información en la actuación de la entidad.
- Asegurar la protección de los derechos de los ciudadanos.
- Mejorar los servicios que las entidades del Sector Público prestan a los ciudadanos, propiciando una gestión eficiente y segura de los procesos incluidos en los sistemas de información con los que opera.
- Proteger a los sistemas de información de las entidades del Sector Público y a los datos que tratan de los riesgos que puedan deberse a la acción humana, especialmente en lo referente a conductas incorrectas, inadecuadas o ilegales.

2.-Cláusulas a suscribir por los empleados.

A) INFORMACION SOBRE PROTECCION DE DATOS

En cumplimiento de lo dispuesto en el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos le informamos de que sus datos personales recogidos con ocasión de la relación laboral que le une con la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L son objeto de tratamiento con la finalidad de gestionar correctamente la relación laboral existente, siendo cedidos, en su caso, a la correspondiente Mutua de accidentes de trabajo y enfermedades profesionales y a las Administraciones Públicas, en cumplimiento de la normativa laboral, de seguridad social y tributaria. De acuerdo con el precitado Reglamento (UE) 2016/679, la base jurídica del tratamiento se encuentra en el artículo 6.1.b del Reglamento Europeo. Los datos se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se obtuvieron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Por otro lado, le informamos de su derecho a ejercer sus derechos de acceso, rectificación o supresión, o la limitación de su tratamiento, o a oponerse al mismo. Por otro lado, le advertimos de su derecho a retirar, en cualquier momento, el consentimiento prestado para tratar sus datos, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada. Finalmente, le recordamos, por imperativo legal, su derecho a presentar una reclamación ante la Agencia Española de Protección de Datos.

He sido informado:

NOMBRE:
APELLIDOS:
FECHA: ___/____/201__

FIRMA:

B) CLAUSULA DE CONFIDENCIALIDAD

El abajo firmante, en el marco de la relación laboral que le une con SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L para el desarrollo de sus funciones en el centro de trabajo donde presta sus servicios, se da por informado y se compromete a observar la siguiente cláusula de confidencialidad en cumplimiento de la normativa que regula tanto las relaciones laborales como la protección de datos personales:

***1.** En el caso de que, por motivos relacionados con el puesto de trabajo, entre en posesión de información, de forma verbal, o a través de documentos que tenga a su alcance, que pudieran contener datos personales o información confidencial o estratégica, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le conceda derecho alguno de posesión, o titularidad o copia sobre la referida información, y sin que pueda ser comunicada a terceros. Asimismo, el empleado deberá devolver dichos materiales a VIVA inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y, en cualquier caso, a la finalización de la relación laboral. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento de VIVA no supondrá, en ningún caso, una modificación de esta cláusula. El incumplimiento de esta obligación puede constituir un delito de revelación de secretos.*

***2.** Están expresamente prohibidas las siguientes actividades:*

- *Incluir o crear ficheros paralelos, sin autorización, que contengan datos personales en el disco duro del ordenador del usuario, en la nube corporativa, en memorias USB, CD o DVD-ROM, etc., salvo autorización expresa de VIVA.*
- *Extraer del centro de trabajo, sin la correspondiente autorización, cualquier documento, en cualquier soporte.*

***3.-**El trabajador se da por informado/a de que **está expresamente prohibido utilizar los recursos informáticos y telemáticos de VIVA, incluidos Internet y el correo electrónico, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario**. En este sentido, la empresa se reserva la posibilidad de adoptar las medidas que estime más oportunas de vigilancia y control (como revisiones de los equipos o del servidor de correo electrónico) para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, con los límites establecidos por la Ley y la jurisprudencia.*

***4.-** El trabajador es informado expresamente, acerca de la existencia de un sistema de videovigilancia en las instalaciones de VIVA.*

***5.** Consecuentemente, el uso reiterado y abusivo del de los recursos de la Entidad en horario laboral, para fines particulares y ajenos a la labor profesional del empleado podrá suponer un quebranto de la buena fe contractual así como un abuso de confianza en el desempeño del trabajo, constituyendo un incumplimiento grave y culpable del contrato de trabajo.*

He sido informado:

NOMBRE:
APELLIDOS:
FECHA: ___/____/201__

FIRMA:

C) POLITICA DE PROTECCION DE DATOS DE VIVA.

La entidad SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. a través, de su gerencia y órganos de dirección mantiene la responsabilidad de determinar la estrategia y aprobar las Políticas corporativas de la organización, así como de disponer los sistemas de control interno. En el ejercicio de estas responsabilidades, y con el objeto de establecer los principios generales que deben regir el tratamiento de los datos personales en la entidad, se aprueba esta Política de protección de datos personales.

Esta Política de Protección de Datos es efectiva desde la fecha que aparece en la página anterior, y hasta que sea reemplazada por una nueva Política.

1. Finalidad

La Política de protección de datos personales establece los principios y pautas comunes de actuación que deben regir en la corporación en materia de protección de datos personales, garantizando, en todo caso, el cumplimiento de la legislación aplicable. En particular, la Política de protección de datos personales tiene la finalidad de garantizar el derecho a la protección de sus datos de todas las personas físicas que se relacionan con la entidad, asegurando el respeto del derecho al honor y a la intimidad en el tratamiento de los diferentes tipos de datos personales, procedentes de diferentes fuentes y con fines diversos en función de la actividad empresarial desarrollada por SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L., como cualquier otro organismo depende, en mayor o menor medida, de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.
El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.
Los diferentes departamentos que conforman la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

2. Ámbito de aplicación

La Política de protección de datos personales será de aplicación a la SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L., a todos los sistemas TIC, a sus administradores, directivos y empleados, así como a todas las personas que se relacionen con ellos, sin excepciones.

3. Principios del tratamiento de los datos personales

Los principios por los que se rige la Política de protección de datos personales son los siguientes:

a) Principios generales: *SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. cumplirá escrupulosamente con la legislación de su jurisdicción en materia de protección de datos, la que resulte aplicable en función del tratamiento de datos personales que se lleve a cabo y la que se determine conforme a normas o acuerdos vinculantes adoptados.*
SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. promoverá que los principios recogidos en esta Política de protección de datos personales sean tenidos en cuenta (i) en el diseño e implementación de todos los procedimientos que impliquen el tratamiento de datos personales, (ii) en los productos y servicios ofrecidos, (iii) en todos los contratos y obligaciones que formalicen con personas físicas y (iv) en la implantación de cuantos sistemas y plataformas permitan el acceso por parte de empleados o de terceros a datos personales y/o la recogida o tratamiento de dichos datos.

b) Principios relativos al tratamiento de datos personales:

(i) *Principios de legitimidad, licitud y lealtad en el tratamiento de datos personales.*
El tratamiento de datos personales será leal, legítimo y lícito conforme a la legislación aplicable. En este sentido, los datos personales deberán ser recogidos para uno o varios fines específicos y legítimos conforme a la legislación aplicable. En los casos en los que resulte obligatorio conforme a la legislación aplicable, deberá obtenerse el consentimiento de los interesados antes de recabar sus datos. Asimismo, cuando lo exija la ley, los fines del tratamiento de datos personales serán explícitos y determinados en el momento de su recogida. En particular, SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. no recabará ni tratará datos personales relativos al origen étnico o racial, a la ideología política, a las creencias, a las convicciones religiosas o filosóficas, a la vida u orientación sexual, a la afiliación sindical, a la salud, ni datos genéticos o biométricos dirigidos a identificar de manera unívoca a una persona, salvo que la recogida de los referidos datos sea necesaria, legítima y requerida o permitida por la legislación aplicable, en cuyo caso serán recabados y tratados de acuerdo con lo establecido en aquella.

(ii) *Principio de minimización.*
Solo serán objeto de tratamiento aquellos datos personales que resulten estrictamente necesarios para la finalidad para los que se recojan o traten y adecuados a tal finalidad.

(iii) *Principio de exactitud.*
Los datos personales deberán ser exactos y estar actualizados. En caso contrario, deberán suprimirse o rectificarse.

(iv) *Principio de limitación del plazo de conservación.*
Los datos personales no se conservarán más allá del plazo necesario para conseguir el fin para el cual se tratan, salvo en los supuestos previstos legalmente.

(v) *Principios de integridad y confidencialidad.*
En el tratamiento de los datos personales se deberá garantizar, mediante medidas técnicas u organizativas, una seguridad adecuada que los proteja del tratamiento no autorizado o ilícito y que evite su pérdida, su destrucción y que sufran daños accidentales. Los datos personales recabados y tratados por SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. deberán ser conservados con la máxima confidencialidad y secreto, no pudiendo ser utilizados para otros fines distintos de los que justificaron y permitieron su recogida y sin que puedan ser comunicados o cedidos a terceros fuera de los casos permitidos por la legislación aplicable.

(vi) *Principio de responsabilidad proactiva.*
SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. será responsables de cumplir con los principios estipulados en esta Política de protección de datos personales y los exigidos en la legislación aplicable y deberán ser capaces de demostrarlo, cuando así lo exija la legislación aplicable. SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. deberá realizar un análisis de necesidad de evaluación del riesgo de los tratamientos que realicen, con el fin de determinar las medidas a aplicar para garantizar que los datos personales se tratan conforme a las exigencias legales. En los casos en los que la ley lo exija, se evaluarán de forma previa los riesgos que para la protección de datos personales puedan comportar nuevos productos, servicios o sistemas de información y se adoptarán las medidas necesarias para eliminarlos o mitigarlos. SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. deberá llevar un registro de actividades en el que se describan los tratamientos de datos personales que lleven a cabo en el marco de sus actividades. En el caso de que se produzca un incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizado a dichos datos, deberán seguirse EL PROTOCOLO DE NOTIFICACION DE QUIEBRAS DE SEGURIDAD, establecido a tal efecto y, en su caso, los que establezca la legislación aplicable. Dichos incidentes deberán documentarse y se adoptarán medidas para solventar y paliar los posibles efectos negativos para los interesados. En los casos previstos en la ley, se designará a delegados de protección de datos con el fin de garantizar el cumplimiento de la normativa.

(vii) *Principios de transparencia e información.*
El tratamiento de datos personales será transparente en relación con el interesado, facilitándole la información sobre el tratamiento de sus datos de forma comprensible y accesible, cuando así lo exija la ley aplicable. A fin de garantizar un tratamiento leal y transparente, SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. en su calidad de responsable del tratamiento deberá informar a los afectados o interesados cuyos datos se pretende recabar de las circunstancias relativas al tratamiento conforme a la legislación aplicable.

(viii) *Adquisición u obtención de datos personales.*
Queda prohibida la adquisición u obtención de datos personales de fuentes ilegítimas, de fuentes que no garanticen suficientemente su legítima procedencia o de fuentes cuyos datos hayan sido recabados o cedidos contraviniendo la ley.

(ix) *Contratación de encargados del tratamiento.*
Con carácter previo a la contratación de cualquier prestador de servicios que acceda a datos personales que sean responsabilidad de SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L., así como durante la vigencia de la relación contractual, estas deberán adoptar las medidas necesarias para garantizar y, cuando sea legalmente exigible, demostrar, que el tratamiento de datos por parte del encargado se lleva a cabo conforme a la normativa aplicable.

(x) *Transferencias internacionales de datos.*
Todo tratamiento de datos personales sujeto a la normativa de la Unión Europea que implique una transferencia de datos fuera del Espacio Económico Europeo deberá llevarse a cabo con estricto cumplimiento de los requisitos establecidos en la ley aplicable en la jurisdicción de origen.

(xi) *Derechos de los interesados.*
SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. deberá permitir que los interesados puedan ejercitar los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición que sean de aplicación en cada jurisdicción, estableciendo, a tal efecto, los procedimientos internos que resulten necesarios para satisfacer, al menos, los requisitos legales aplicables en cada caso.

4.Gestión de riesgos.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá́:

- *Regularmente,*
- *Cuando cambie la información manejada o los sistemas de información,*
- *Cuando cambien los servicios prestados,*
- *Cuando ocurra un incidente grave de seguridad,*
- *Cuando se reporten o detecten vulnerabilidades graves.*

5. Implementación.

Conforme a lo dispuesto en esta Política de protección de datos personales, SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. desarrollará y mantendrán actualizada la normativa interna de gestión global de protección de datos y será de obligado cumplimiento para todos los directivos y empleados de la Sociedad.

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. dispondrá de un equipo jurídico externo responsable de reportar a la Dirección de entidad los desarrollos y novedades normativas que se produzcan en este ámbito.

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L., a través de sus técnicos (internos o externos) será la encargada de implementar en los sistemas de información de la organización, los controles y desarrollos informáticos que sean adecuados para garantizar el cumplimiento de la normativa

interna de gestión global de la protección de datos y velará por que dichos desarrollos estén actualizados en cada momento.

6. Control y evaluación

La Gerencia de SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. supervisará el cumplimiento de lo dispuesto en esta Política de protección de datos personales por parte de la Entidad. Lo anterior se entenderá, en todo caso, sin perjuicio de las responsabilidades que correspondan a otros órganos y direcciones de la corporación. Para verificar el cumplimiento de esta Política de protección de datos personales se realizarán auditorías periódicas con auditores internos o externos.

D) 50 NORMAS DE UTILIZACIÓN DE LOS SISTEMAS DE INFORMACION Y COMUNICACIONES EN VIVA.

NORMAS GENERALES.

1. *VIVA facilita a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que VIVA pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.*

2. *En general, el ordenador personal (PC) será el recurso informático que permitirá el acceso de los usuarios a los Sistemas de Información y servicios informáticos constituyendo un elemento muy importante en la cadena de seguridad de los sistemas de información, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.*

3. *Únicamente el personal autorizado por SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los Sistemas de Información. Cuando se precise instalar dispositivos no provistos por VIVA deberá solicitarse autorización previa.*

4. *Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.*

5. *Salvo autorización expresa de VIVA los usuarios no tendrán privilegio de administración sobre los equipos.*

6. *Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos aquellos. Si el personal de soporte técnico detectase cualquier anomalía que indicará una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento de la Gerencia que tomará las oportunas medidas.*

7. *Los ordenadores personales de la organización deberán mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus y cortafuegos.*

8. *Los usuarios deberán notificar a la Gerencia a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo.*

9. *Salvo aquellos ordenadores instalados en las zonas comunes de acceso a Internet, cada equipo deberá estar asignado a un usuario o grupo de usuarios concreto. Tales usuarios son responsables de su correcto uso.*

10. *El usuario deberá participar en el cuidado y mantenimiento del equipo que tiene asignado, detectando la ausencia de cables y accesorios, y dando cuenta de tales circunstancias.*

11. *El usuario debe ser consciente de las amenazas provocadas por malware. Muchos virus y troyanos requieren la participación de los usuarios para propagarse, ya sea a través de disquetes, CDs/DVDs, memorias USB, mensajes de correo electrónico o instalación de programas descargados desde Internet. Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo.*

12. *El usuario será responsable de toda la información extraída fuera de la organización a través de dispositivos tales como memorias USB, CDs, DVDs, etc., que le hayan sido asignados. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida.*

13. *En general, los equipos portátiles no deberán conectarse directamente a redes externas (incluyendo la red o el acceso a Internet del usuario en su domicilio). VIVA puede proporcionar accesos remotos autorizados y configurados a través de tarjetas móviles. Cuando este sea el caso, deberán realizar de forma obligatoria dicha conexión cuando requieran el acceso a Internet desde dichos equipos.*

14. *Los ordenadores portátiles afectados deberán tener cifrado el disco duro, disponer de software que garantice un arranque seguro, así como mecanismos de auditoría capaces de crear un registro por cada fichero extraído del sistema por cualquier medio (red, dispositivos extraíbles, impresoras, etc.).*

PROHIBICIONES

15. *Están terminantemente prohibidos los siguientes comportamientos:*

a. *Ejecución remota -salvo autorización- de archivos de tipo audiovisual (música, vídeo, animaciones, etc.)*
b. *Utilización de cualquier tipo de software dañino.*
c. *Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.*
d. *Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por VIVA, sin la previa autorización.*
e. *Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados.*
f. *Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización expresa.*
g. *Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.*

IDENTIFICACIÓN Y AUTENTICACIÓN

16. *La identificación de cada usuario ante un activo de SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. debe ser unívoca, su uso se considera personal y exclusivo, y es responsabilidad única del usuario el mantenimiento en secreto de cualquier código que posibilite el acceso a un recurso corporativo.*

17. *El proporcionar deliberadamente acceso a terceros que legítimamente no tengan acceso a los sistemas de información corporativos se considerará una falta muy grave; proporcionar o facilitar el acceso a los sistemas de forma no deliberada a terceros que legítimamente no tengan acceso a ellos se considerará una falta grave si se considera que no se ha protegido convenientemente la seguridad de dichos accesos.*

ALMACENAMIENTO DE INFORMACIÓN

18. *Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios (disco duro local, por ejemplo) no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. Por tanto, cuando tal almacenamiento esté autorizado en las normas internas correspondientes, se recomienda a los usuarios la realización periódica de copias de seguridad, especialmente de la información importante para el desarrollo de su actividad profesional.*

19. *No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales, salvo autorización previa*

NORMAS ESPECÍFICAS PARA MEMORIAS/LÁPICES USB (PENDRIVES)

20. *Con carácter general, el uso de memorias USB en VIVA no está autorizado. En su caso, la autorización deberá proporcionarla la GERENCIA.*

21. *Por razones de seguridad, los interfaces USB de los puestos de usuario estarán deshabilitados. En caso de ser necesaria su habilitación, deberá justificarse por el usuario y requerirá la previa autorización del responsable.*

22. *En el caso de que a un usuario se le autorice el uso del interfaz USB de su puesto de trabajo, las memorias USB utilizadas serán las proporcionadas por VIVA, que serán conformes a las normas de seguridad de la organización (USB CON CIFRADO Y CONTRASEÑA).*

23. *Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento.*

24. *La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento de VIVA, de forma inmediata.*

GRABACIÓN DE CDs Y DVDs

25. *Con carácter general, el uso de equipos grabadores de CDs y DVDs no está autorizado, salvo autorización expresa.*

26. *Por razones de seguridad, los equipos grabadores de CDs y DVDs de los puestos de trabajo estarán deshabilitados. En el caso de ser necesaria su habilitación, deberá justificarse por el usuario y requerirá la previa autorización del responsable.*

IMPRESORAS EN RED, FOTOCOPIADORAS Y FAXES

27. *Cuando se imprima documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.*

28. *Conviene no olvidar tomar los originales de la fotocopiadora, una vez finalizado el proceso de copia. Si se encontrase documentación sensible, confidencial o protegida abandonada en una fotocopiadora o impresora, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del responsable.*

DIGITALIZACIÓN DE DOCUMENTOS

29. *Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida.*

30. *Conviene no olvidar tomar los originales del escáner, una vez finalizado el proceso de digitalización. Si se encontrase documentación sensible, confidencial o protegida abandonada en un escáner, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente.*

CUIDADO Y PROTECCIÓN DE LA DOCUMENTACIÓN IMPRESA

31. *Se insiste en imprimir únicamente aquellos documentos que sean estrictamente necesarios. La impresión se hará, preferiblemente, a doble cara y evitando, siempre que sea posible, la impresión en color*

32. *La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios bajo llave.*

33. *Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras de VIVA de forma que no sea recuperable la información que pudieran contener.*

34. *Si, una vez impresa, es necesario almacenar tal documentación, el usuario habrá de asegurarse de proteger adecuadamente y bajo llave aquellas copias que contengan información sensible, confidencial o protegida, o crítica para su trabajo.*

PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

35. *Está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad Intelectual, sin la debida autorización.*

PROTECCIÓN DE LA DIGNIDAD DE LAS PERSONAS

36. *Está terminantemente prohibida toda transmisión, distribución o almacenamiento de cualquier material obsceno, discriminatorio o sexista, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.*

ACCESO A LOS SISTEMAS DE INFORMACIÓN Y A LOS DATOS TRATADOS

37. *Los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso, intransferibles.*

38. *Cuando un usuario deje de atender un PC durante un cierto tiempo, es necesario bloquear la sesión de usuario o activar el salvapantallas, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo.*

CONEXIÓN DE DISPOSITIVOS A LAS REDES DE COMUNICACIONES

39. *No se podrá conectar en la red de comunicaciones corporativa ningún dispositivo distinto de los admitidos, habilitados y configurados por VIVA salvo autorización previa.*

USO DEL CORREO ELECTRÓNICO

40. *Conforme a la Política de Seguridad Corporativa, la cuenta de correo electrónico que VIVA pone a disposición de sus empleados únicamente podrá ser utilizada para finalidades directamente relacionadas con el desarrollo de las funciones que les corresponden, quedando prohibido el uso de dicha cuenta para fines particulares o ajenos al objeto de su prestación laboral.*

41. *En concreto y por lo que respecta al uso del correo electrónico, además de las normas generales de seguridad, el empleado usuario de la cuenta de correo electrónico puesta a su disposición por SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. queda debidamente informado y deberá tener en cuenta lo siguiente:*

a. *El correo proporcionado por VIVA al empleado debe destinarse exclusivamente a un uso profesional, en tanto elemento de trabajo propiedad de VIVA, no pudiendo en consecuencia utilizarse para fines particulares, excepto casos puntuales justificados.*
b. *El empleado realizará en todo caso un uso adecuado, racional y leal del correo electrónico, debiendo utilizarlo en la medida en que resulte necesario para cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad con las reglas de la buena fe y diligencia.*
c. *Por motivos de seguridad, el correo electrónico no podrá ser utilizado para enviar ni para contestar mensajes o cadenas de mensajes susceptibles de provocar congestiones en los sistemas de VIVA o que puedan introducir malware o implicar cualesquiera riesgos o problemas en los sistemas y herramientas informáticas y tecnológicas de VIVA.*
d. *El correo electrónico no podrá ser utilizado con fines comerciales ni lucrativos en beneficio del empleado.*
e. *El empleado cuidará en todo momento el lenguaje utilizado en sus comunicaciones, debiendo tener presente que en cada una de ellas compromete la imagen y el nombre de VIVA.*

f. Una vez extinguida la relación contractual entre el trabajador y VIVA, el trabajador se encargará de eliminar toda aquella información que, ajena a los servicios que haya prestado en VIVA., obre por cualquier causa en su cuenta de correo.

g. Si un trabajador recibiera en su correo electrónico mensajes con contenido inadecuado deberá poner esta circunstancia en conocimiento de su superior para la adopción de las medidas que en su caso resulten pertinentes.

NORMAS GENERALES DE ACCESO A INTERNET

42. *El acceso a Internet deberá ser autorizado por VIVA, siempre que se estime necesario para el desempeño de la actividad profesional del usuario o solicitante y exista disponibilidad para ello. En otro caso, se podrá acceder a Internet desde un puesto de acceso común habilitado para ese fin.*

43. *Las conexiones que se realicen a Internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos.*

44. *Quedan prohibidas las siguientes actuaciones:*

a. La descarga de archivos muy voluminosos, especialmente en horarios coincidentes con la atención al público, salvo autorización expresa.

b. La descarga de programas informáticos sin autorización previa o ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso debe asegurarse que el sitio Web visitado es confiable.

c. El acceso a recursos y páginas-web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.

d. La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.) que no esté expresamente autorizada.

REDES SOCIALES

45. *El uso de redes sociales deberá ser autorizado por VIVA, siempre que se estime necesario para el desempeño de la actividad profesional del usuario o solicitante y exista disponibilidad para ello. En otro caso, está totalmente prohibido su uso entre el personal.*

INCIDENCIAS DE SEGURIDAD

46. *Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la Entidad o su imagen, deberá informar inmediatamente a la Gerencia.*

USO ABUSIVO DE LOS SISTEMAS DE INFORMACIÓN.

47. *El uso de Internet, del correo electrónico y el acceso al resto de los servicios y sistemas de VIVA estará debidamente controlado para todos los usuarios. Si se hiciese un uso abusivo o inapropiado de estos*

servicios, VIVA podrá adoptar las medidas disciplinarias que considere oportunas, sin perjuicio de las acciones civiles o penales a las que hubiere lugar.

48. *VIVA por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente (Artículo 23. Registro de actividad, del Esquema Nacional de Seguridad):*

a) Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
b) Monitorizará los accesos a la información contenida en sus sistemas.
c) Auditará la seguridad de las credenciales y aplicaciones.
d) Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

49. *VIVA llevará a cabo esta actividad de monitorización de manera proporcional al riesgo, con las cautelas legales pertinentes y las señaladas en la jurisprudencia y con observancia de los derechos de los usuarios*

INCUMPLIMIENTO DE LA NORMATIVA

50. *En el supuesto de que un usuario no observe alguna de los preceptos señalados en la presente Normativa General, sin perjuicio de las acciones disciplinarias que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.*

COMPROMISO DE CUMPLIMIENTO

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, como empleado de SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L. (VIVA) declara haber leído y comprendido la:

1. *La Política de Protección de Datos de la organización;*
2. *Las 50 Normas de utilización de los sistemas de información y comunicaciones.*

y se compromete, bajo su responsabilidad, a su cumplimiento.

NOMBRE:
APELLIDOS:
FECHA: ___/____/201__

FIRMA:

X

INFORME DE RIESGOS GLOBAL EN *SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.*: IDENTIFICACIÓN, EVALUACIÓN Y MEDIDAS

1.- Justificación. Análisis de riesgos global.

Cualquier tratamiento de datos personales va a implicar la necesidad de considerar la existencia de un riesgo siendo **"la aproximación basada en el riesgo"** (*risk-based approach*) el criterio esencial en torno al que gira el Reglamento General de Protección de Datos.

Este elemento es central en la regulación ya que se configura como un elemento central del principio de responsabilidad activa (*accountability*), interrelacionándose con principios como el de privacidad desde el diseño y por defecto y obligaciones como el registro de actividades de tratamiento.

El **riesgo** lo podemos definir como la contingencia o proximidad de un daño, o bien, la posibilidad de que se produzca un daño o perjuicio para una persona derivado del tratamiento de sus datos personales, que cause una afección a su derecho fundamental a la protección de datos.

El riesgo es la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas.

A diferencia de las Evaluaciones de Impacto, donde el análisis se realiza para una actividad de tratamiento específico, en un análisis de riesgos global, **las actividades de tratamiento se agrupan por procesos comunes expuestos a riesgos similares,** lo que permite establecer medidas de seguridad por defecto.

Gestión de riesgos por defecto

Los principales riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas tienen **dos dimensiones:**

- **Riesgos asociados a la protección de la información:** integridad + disponibilidad + confidencialidad.
- **Riesgos asociados al cumplimiento de los requisitos legales que afectan a los derechos de los afectados:** uso ilegítimo de datos, impedimento de ejercicio de derechos, etc.

El **proceso de gestión de riesgos** a los que está expuesta una actividad de tratamiento de datos tradicionalmente se estructura en **3 fases:**

- Identificación del riesgo
- Evaluación
- Tratamiento

El proceso de gestión de riesgos implica, como decimos, realizar inicialmente la tarea de IDENTIFICACION y de EVALUACION de los riesgos, tanto desde el punto de vista de la seguridad de los sistemas de información, como desde la perspectiva del cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados.

Partiendo de la identificación de un riesgo se aplican unas medidas de seguridad y **se obtiene un riesgo residual, un riesgo aceptable y si acaso, un riesgo inasumible.**

En un **ámbito de riesgo bajo**, el análisis puede hacerse sobre las actividades de tratamiento sin llegar a valorar los riesgos, considerando siempre que el nivel inherente de los mismos siempre será medio o bajo.

Si bien para cada riesgo identificado deben establecerse medidas de seguridad y control que reduzcan su nivel de exposición.

ASIGNACION DE VALORES A LAS ESCALAS DE PROBABILIDAD E IMPACTO	
1	DESPRECIABLE
2	LIMITADO
3	SIGNIFICATIVO
4	MÁXIMO

A

IDENTIFICACIÓN DE AMENAZAS

TRATAMIENTO	RIESGOS	AMENAZAS
T1. SOLICITANTES **T2. RECURSOS HUMANOS** **T4. CONTABILIDAD Y GESTION** **T5. VIDEOVIGILANCIA.**	RP1. La base que legitima el tratamiento no es adecuada, es ilícita o no se ha formalizado adecuadamente.	AG1. Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. AG5. Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados. AL2. Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales. AL6.-Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardas necesarias.
T1. SOLICITANTES **T2. RECURSOS HUMANOS**	RD1. En el momento de la recogida de los datos no se proporciona la información mínima prevista a la persona afectada o no se le proporciona ninguna información, cuando se obtienen derechos.	AG1. Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. AG5. Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados AL2. Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales. AL6. Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias. AL8. Utilizar cookies se seguimiento u otro mecanismo de rastreo sin obtener el consentimiento valido tras una información adecuada. AT1.-Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc.).
T1. SOLICITANTES **T2. RECURSOS HUMANOS** **T4. CONTABILIDAD Y GESTION** **T5. VIDEOVIGILANCIA.**	RD8. No hay procedimientos para dar una respuesta adecuada a los derechos.	AG5. Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados ACE2. Carencia de procedimientos y herramientas para la gestión de los derechos de los interesados. ACE3. Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales.
T1. SOLICITANTES **T2. RECURSOS HUMANOS**	RD9. La organización desconoce los procedimientos para	ACE2. Carencia de procedimientos y herramientas para la gestión de los derechos de los interesados.

T4. CONTABILIDAD Y GESTION **T5. VIDEOVIGILANCIA.**	responder el ejercicio de derechos	ACE3. Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales.
T1. SOLICITANTES	RO2. Se incumplen otras regulaciones sectoriales que inciden en la protección de los datos de carácter personal.	AG2. Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tratamiento: ES DE APLICACIÓN EL ESQUEMA NACIONAL DE SEGURIDAD.
T1. SOLICITANTES **T2. RECURSOS HUMANOS** **T4. CONTABILIDAD Y GESTION** **T5. VIDEOVIGILANCIA.**	RO5. No se puede demostrar el cumplimiento	AG1.-Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. AG5.-Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.
T1. SOLICITANTES **T2. RECURSOS HUMANOS** **T4. CONTABILIDAD Y GESTION** **T5. VIDEOVIGILANCIA.**	RO10. Los encargados de tratamiento no se han seleccionado adecuadamente	ATE2.-Falta de diligencia (o dificultad para demostrarla) en la elección de encargado de tratamiento. ATE3.-Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.
T1. SOLICITANTES **T2. RECURSOS HUMANOS** **T4. CONTABILIDAD Y GESTION** **T5. VIDEOVIGILANCIA.**	RO11. No se ha formalizado adecuadamente la relación con los encargados de tratamientos	ATE1.-Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas.
T1. SOLICITANTES **T2. RECURSOS HUMANOS** **T4. CONTABILIDAD Y GESTION** **T5. VIDEOVIGILANCIA**	RO14. No se dispone del registro de actividades de tratamiento (cuando es obligatorio)	AG1.-Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. ANR1.-Carecer de los mecanismos y procedimientos necesarios para detectar cuando debe registrarse la creación, modificación o cancelación de actividades de tratamiento
T1. SOLICITANTES **T4. CONTABILIDAD Y GESTION**	RO23-Hay incapacidad para detectar y gestionar incidentes que afectan a la seguridad de los datos	AG3.- Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de estas, en particular, cuando se producen pérdidas de datos personales. AS1.-Carencia de medidas de seguridad o aplicación deficiente las mismas. Indefinición de funciones de seguridad y de establecimiento de competencias. AS2.-Deficiencias organizativas en la gestión del control de accesos. AS3.- Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan personales. AS4.- Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información.
T1. SOLICITANTES **T2. RECURSOS HUMANOS**	R01. Se incumple la regulación general sobre el derecho a la protección	AG1.-Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales.

T4. CONTABILIDAD Y GESTION **T5. VIDEOVIGILANCIA**	de los datos de carácter personal.	AG3. Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de estas, en particular, cuando se producen pérdidas de datos personales. AG4. Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad. AG5.-Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados. ANR2.-Carecer de los mecanismos y procedimientos necesarios para detectar cuando debe realizarse análisis de impacto en protección de datos y su consulta a la autoridad de control	

VR

VALORACIÓN DEL RIESGO INHERENTE

	AMENAZA	RIESGO	PROBABILIDAD	IMPACTO	RIESGO INHERENTE
	AG1. Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. AG5. Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados. AL2. Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales. AL6.-Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardas necesarias.	RP1. La base que legitima el tratamiento no es adecuada, es ilícita o no se ha formalizado adecuadamente.	2 LIMITADO	1 DESPRECIABLE	1 DESPRECIABLE
	AG1. Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. AG5. Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados AL2. Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales. AL6. Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias.	RD1. En el momento de la recogida de los datos no se proporciona la información mínima prevista a la persona afectada o no se le proporciona ninguna información, cuando se obtienen derechos.	2 LIMITADO	2 LIMITADO	2 LIMITADO

	AL8. Utilizar cookies se seguimiento u otro mecanismo de rastreo sin obtener el consentimiento valido tras una información adecuada. AT1.-Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc.).				
	AG5. Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados ACE2. Carencia de procedimientos y herramientas para la gestión de los derechos de los interesados. ACE3. Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales.	RD8. No hay procedimientos para dar una respuesta adecuada a los derechos.	1 DESPRECIABLE	2 LIMITADO	1 DESPRECIABLE
	ACE2. Carencia de procedimientos y herramientas para la gestión de los derechos de los interesados. ACE3. Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales.	RD9. La organización desconoce los procedimientos para responder el ejercicio de derechos	3 SIGNIFICATIVO	3 SIGNIFICATIVO	3 SIGNIFICATIVO
	AG2. Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tratamiento: ES DE APLICACIÓN EL ESQUEMA NACIONAL DE SEGURIDAD.	RO2. Se incumplen otras regulaciones sectoriales que inciden en la protección de los datos de carácter personal.	2 LIMITADO	3 SIGNIFICATIVO	3 SIGNIFICATIVO
	AG1.-Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. AG5.-Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.	RO5. No se puede demostrar el cumplimiento	4 MÁXIMO	4 MÁXIMO	3 SIGNIFICATIVO
	ATE2.-Falta de diligencia (o dificultad para demostrarla) en la elección de encargado de tratamiento. ATE3.-Gestión deficiente de las subcontrataciones e insuficiente	RO10. Los encargados de tratamiento no se han seleccionado adecuadamente	3 SIGNIFICATIVO	3 SIGNIFICATIVO	3 SIGNIFICATIVO

	control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.				
	ATE1.-Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas.	RO11. No se ha formalizado adecuadamente la relación con los encargados de tratamientos	4 MÁXIMO	4 MÁXIMO	3 SIGNIFICATIVO
	AG1.-Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. ANR1.-Carecer de los mecanismos y procedimientos necesarios para detectar cuando debe registrarse la creación, modificación o cancelación de actividades de tratamiento	RO14. No se dispone del registro de actividades de tratamiento (cuando es obligatorio)	4 MÁXIMO	4 MÁXIMO	3 SIGNIFICATIVO
	AG3.- Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de estas, en particular, cuando se producen pérdidas de datos personales. AS1.-Carencia de medidas de seguridad o aplicación deficiente las mismas. Indefinición de funciones de seguridad y de establecimiento de competencias. AS2.-Deficiencias organizativas en la gestión del control de accesos. AS3.- Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan personales. AS4.- Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información.	RO23-Hay incapacidad para detectar y gestionar incidentes que afectan a la seguridad de los datos	4 MÁXIMO	4 MÁXIMO	3 SIGNIFICATIVO
	AG1.-Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. AG3. Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad	R01. Se incumple la regulación general sobre el derecho a la protección de los datos de carácter personal.	4 MÁXIMO	4 MÁXIMO	3 SIGNIFICATIVO

	adecuadas o de la ineficacia de estas, en particular, cuando se producen pérdidas de datos personales. AG4. Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad. AG5.-Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados. ANR2.-Carecer de los mecanismos y procedimientos necesarios para detectar cuando debe realizarse análisis de impacto en protección de datos y su consulta a la autoridad de control				

MC

IDENTIFICACIÓN DE MEDIDAS DE CONTROL

AMENAZA	RIESGO	MEDIDA DE CONTROL	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL
AG1. AG5. AL2. AL6	RP1. La base que legitima el tratamiento no es adecuada, es ilícita o no se ha formalizado adecuadamente.	Formación apropiada del personal sobre protección de datos. Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización, así como de las sanciones aparejadas al incumplimiento de éstas. Formación apropiada del personal sobre seguridad y uso adecuado de las TIC. Nombrar a una persona o departamento como responsable de la interlocución con los afectados en todo aquello relativo a la privacidad y la protección de datos personales, y comunicar claramente la forma de contactar con ella. Revisar las posibilidades que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales y asegurar que este encaja en alguna de ellas. Si es necesario, buscar asesoramiento experto.	1 DESPRECIABLE	1 DESPRECIABLE	1 DESPRECIABLE
AG1 AG5. AL2 AL6 AL8 AT1	RD1. En el momento de la recogida de los datos no se proporciona la información mínima prevista a la persona afectada o no se le proporciona ninguna información, cuando se obtienen derechos	Se requiere implementar clausulas informativas acordes con los art. 13 y 14 del RGPD. Deben suscribirse (para acreditar que se ha hecho) tanto por los trabajadores como por los clientes. Formación adecuada del personal sobre protección de datos, seguridad y uso adecuado de las TIC. Comunicación auditable y clara de las responsabilidades el personal en relación con el cumplimiento de las políticas de privacidad de la organización, así como de las sanciones aparejadas al incumplimiento de estas.	2 LIMITADO	1 DESPRECIABLE	1 DESPRECIABLE

		Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada. Verificar que el tratamiento de datos especialmente protegidos es absolutamente imprescindible para la finalidad o finalidades perseguidas Verificar que la información que se ofrecen en todos los lugares y situaciones es coherente y sistemática. Verificar que la información se ofrece en todos los formularios. Nombrar a una persona o departamento como responsable de la interlocución con los afectados en todo aquello relativo a la privacidad y la protección de datos personales, y comunicar claramente la forma de contactar con ella. Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas. Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada.			
AG5. ACE2. ACE3.	RD8. No hay procedimientos para dar una respuesta adecuada a los derechos	Nombrar a una persona o departamento como responsable de la interlocución con los afectados en todo aquello relativo a la privacidad y la protección de datos personales, y comunicar claramente la forma de contactar con ella. Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados. Formación de los empleados encargados de gestionar los ejercicios de derechos de los interesados. Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y	1 **DESPRECIABLE**	1 **DESPRECIABLE**	1 **DESPRECIABLE**

		oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate.			
ACE2. ACE3.	RD9. La organización desconoce los procedimientos para responder el ejercicio de derechos	Se requiere establecer un procedimiento en este sentido, formando y concienciando al personal de la empresa, y utilizando el soporte del delegado de protección de datos cuando sea requerido. Nombrar, SI SE CONSIDERA PROCEDENTE, un Delegado de Protección de Datos o (DPO) para contar con asesoramiento cualificado. Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados. Formación de los empleados encargados de gestionar los ejercicios de derechos de los interesados.	1 **DESPRECIABLE**	2 **LIMITADO**	2 **LIMITADO**
AG2	RO2. Se incumplen otras regulaciones sectoriales que inciden en la protección de los datos de carácter personal.	Formación apropiada del personal sobre protección de datos en el sector específico de que se trate. Adaptación de la entidad al Esquema Nacional de Seguridad.	2 **LIMITADO**	2 **LIMITADO**	2 **LIMITADO**
AG1 AG5	RO5. No se puede demostrar el cumplimiento	Formación apropiada del personal sobre protección de datos. Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización, así como de las sanciones aparejadas al incumplimiento de estas.	1 **DESPRECIABLE**	1 **DESPRECIABLE**	1 **DESPRECIABLE**
ATE2 ATE3	RO10. Los encargados de tratamiento no se han seleccionado adecuadamente	Seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento de los contratos y de la adopción de las medidas de seguridad estipuladas a través, por ejemplo, de su adhesión a posibles códigos de conducta o a esquemas de certificación homologados y de acreditada solvencia. Establecer contractualmente mecanismos de supervisión, verificación y auditoría de los tratamientos encargados a terceros.	1 **DESPRECIABLE**	2 **LIMITADO**	1 **DESPRECIABLE**
ATE1	RO11. No se ha formalizado adecuadamente la relación con los encargados de tratamientos	Establecer procedimientos que garanticen que siempre que se recurre a un encargado de tratamiento se firma el correspondiente contrato en los términos establecidos por la legislación de protección de datos.			
AG1 ANR1	RO14. No se dispone del registro de	Formación apropiada del personal sobre protección de datos.	1	1 **DESPRECIABLE**	1 **DESPRECIABLE**

	actividades de tratamiento	Incluir en los procesos y metodologías de desarrollo de nuevos proyectos una fase o tarea relativa a la revisión de la necesidad de cumplimiento normativo.	**DESPRECIABLE**		
AG3 AS1 AS2 AS3 AS4	RO23-Hay incapacidad para detectar y gestionar incidentes que afectan a la seguridad de los datos	Realización de informes de auditoría y verificación de medidas de seguridad. Formación apropiada del personal sobre seguridad y uso adecuado de las TIC. Formación adecuada de los empleados sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información. Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas y las medidas de seguridad, así como de las sanciones aparejadas al incumplimiento de estas. Políticas estrictas de acceso a la información y escritorios limpios de documentación para minimizar las posibilidades de acceso no autorizado a datos personales Establecer mecanismos y procedimientos de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales. Establecer sanciones disciplinarias para quienes incumplan el deber de secreto y las políticas de confidencialidad de la organización. Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales Establecer procedimientos que garanticen la revocación de permisos para acceder a datos personales cuando ya no sean necesarios (abandono de la organización, traslado, cambio de funciones…) Instalar herramientas de hardware o software que ayuden a una gestión eficaz de la seguridad y los compromisos u obligaciones legales de la organización en el área de la protección de datos personales. En el caso de que fuera necesario, instalar herramientas de detección de intrusiones o de prevención de intrusiones con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad. En su caso, implantar sistemas de prevención de pérdida de datos con la	2 **LIMITADO**	2 **LIMITADO**	2 **LIMITADO**

		necesaria información a los trabajadores sobre su instalación, características e implicaciones en la privacidad. Establecer mecanismos de registro de acciones sobre los datos personales o logging asi como herramientas fiables y flexibles de explotación de los ficheros de auditoría resultantes.			
AG1. AG3. AG4. AG5 ANR2	R01. Se incumple la regulación general sobre el derecho a la protección de los datos de carácter personal.	Formación apropiada del personal sobre protección de datos. Comunicación auditable y clara de las responsabilidades el personal en relación con el cumplimiento de las políticas de privacidad de la organización, así como de las sanciones aparejadas al incumplimiento de estas.	2 **LIMITADO**	2 **LIMITADO**	2 **LIMITADO**

R

RECOMENDACIONES COMPLEMENTARIAS

1	**Actualización de cláusulas informativas.** Se recomienda actualizar el incorporar todas las **clausulas informativas en protección de datos** en todos los formularios de recogida de datos personales, tanto en soporte papel, como a través de los formularios del sitio web.
2	**Protocolos nuevos que implementar** Prestar especial atención a la nueva **Política de Protección de Datos de VIVA**; y a las **50 Normas de utilización de los sistemas de información y comunicaciones**.
3	**Seguridad** **Se requiere que VIVA se ADAPTE a las previsiones establecidas en el Esquema Nacional de Seguridad**. Si bien en gran medida, con el cumplimiento del RGPD ya se ha avanzado enormemente en su cumplimiento, si se requiere que desde Gerencia se realicen las gestiones propias para adaptar VIVA al ENS. Entendemos que resulta de aplicación en ENS en VIVA, debido a: El RD 3/2010 es de aplicación a las entidades de derecho privado vinculadas o dependientes de la Administración de las Entidades Locales en las materias en que les sea de aplicación la normativa presupuestaria, contable, de control financiero, de control de eficacia y contratación, de acuerdo con lo dispuesto por la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, así como en el ejercicio de las funciones públicas que les hayan sido atribuidas estatutariamente, cuando se rijan por las previsiones de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas en los términos establecidos por esta.
2	**Personal.** El personal suscribir la cláusula de **política de confidencialidad** y de utilización de los medios puestos a su disposición en materia de protección de datos… (contenido en el Documento X) Realizar acciones formativas adaptadas al RGPD y dirigidas al personal, en materia de protección de datos, seguridad y uso adecuado de las TIC. Debe limitarse el acceso a Internet del personal. Únicamente permitir (con limitación informática) aquellas páginas web necesarias para el desempeño profesional, y previa solicitud motivada. Por supuesto establecer la prohibición de acceso a redes sociales.

3	**Encargados del tratamiento.** Suscribir **contratos (actualizados al RGPD) con los encargados de tratamiento** en materia de protección de datos y almacenarse, y remitirles el cuestionario de cumplimiento RGPD.
4	**Videovigilancia** Colocar **distintivos informativos** en las zonas videovigiladas, suficientemente visibles y a la altura de los ojos, tanto en espacios abiertos como cerrados, que incluya las palabras "zona videovigilada". En caso de que existan varios accesos a una misma área videovigilada deben colocarse en todos ellos.
5	**Plan de continuidad** Implantar un **plan de continuidad** de negocio **y documentarlo**. Se requiere tener un plan B ante incidencias fatales o críticas. Adjuntamos (en ANEXOS) un Protocolo de INCIBE que puede ser de ayuda en su elaboración.
6	**Equipamiento informático.** En el informe realizado por *Bitlan Asesores Informáticos* se destaca la **obsolescencia del hardware y software en la Entidad**. Debe valorarse especialmente la renovación de equipos a fin de minimizar riesgos de ciberseguridad. Especial atención a los riesgos de seguridad perimetral, que señala el citado informe, que puede comprometer la seguridad de los sistemas. Imprescindible disponer de un firewall adecuado. Todas las actualizaciones del software (antivirus, programas, etc.) deben hacerse de forma centralizada impidiendo al usuario que lo haga.
7	**Política de privilegios de acceso.** Verificar que los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. La carpeta compartida en el servidor debe analizarse a que accede cada usuario y limitarse UNICAMENTE a lo que necesitan para su trabajo.
8	**Protocolo SSL** Recomendamos implementar en la página web corporativa *http://www.smviva.com* un **certificado de seguridad** (protocolo SSL).
9	**Cifrado** Deben **cifrarse** los equipos y servidores donde se almacenen datos personales.

10	**Cambio de contraseñas.** Deben cambiarse con alguna periodicidad (al menos cada año) las **contraseñas** de acceso a los equipos.
11	**WIFI** Recomendamos proteger la red **Wifi utilizando cifrado** en las comunicaciones (WPA/WPA2), **impidiendo su conexión a los empleados**. Recomendamos modificar la contraseña de forma frecuente (cada 180 días).
12	**Red Corporativa** Debe permitirse acceder a la red únicamente a los dispositivos de trabajo (activando el filtrado de direcciones MAC).
13	**Copias de seguridad** Los procesos de copias de seguridad deben modificarse y modernizarse. Recomendamos automatizar el proceso de copias de seguridad, almacenándose en nube (con los datos cifrados) para asegurar la continuidad del negocio, llegado el caso.
14	***Software* de gestión** Recomendamos la migración a un software de gestión o ERP para la gestión de los distintos procesos que se realizan en VIVA.
15	**Control biométrico** Debe suscribirse un convenio (con el contenido establecido en este Informe y tal y como exige el RGPD entre responsables-encargados de tratamiento) con el Ayuntamiento de Valladolid, ya que está "prestando un servicio con acceso a datos personales de empleados de VIVA".
16	**Minimización de datos** Recomendamos a la Entidad que realice un análisis de proporcionalidad en los datos que trata, es decir, si puede prestar el mismo servicio, solicitando menos datos personales a los usuarios. Este juicio o análisis debería documentarse.

XII

ANÁLISIS DE NECESIDAD DE LA REALIZACIÓN DE UNA EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS EN *SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.*

Análisis de la necesidad de la realización de una Evaluación de Impacto en la Protección de Datos (EIPD).

1.-Justificación.

Una Evaluación de Impacto en la Protección de Datos Personales (EIPD) –o por sus siglas en inglés: *Privacy Impact Analysis* (PIAC) o *Privacy Impact Assessment* (PIA)– es, básicamente, un ejercicio de análisis de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho a la protección de datos de los afectados cuyos datos se tratan y, como consecuencia de ese análisis, la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminar o mitigar en lo posible aquellos que se hayan identificado.

El Reglamento Europeo (RGPD) contempla la realización de Evaluaciones de impacto en sus artículos 35 y 36.

> *Artículo 35.1.- 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.*
>
> *Por su parte, el Considerando (84) del Reglamento indica que «a fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento».*

Por todo lo anterior, se recoge acto seguido, diferente información, con la que se pretende analizar y valorar si en los tratamientos de datos de carácter personal llevados a cabo en la EMPRESA1, concurren circunstancias y situaciones que obliguen a realizar una Evaluación de Impacto en la Protección de Datos (EIPD), conforme establece el art. 35 del RGPD.

2.-Análisis de verificación de la necesidad de la realización de una Evaluación de Impacto de protección de datos.

ID	TRATAMIENTOS	FINALIDAD/ES DEL TRATAMIENTO
T1	**SOLICITANTES**	Tratamiento de datos de personas solicitantes de los distintos servicios, relacionados con la adquisición de viviendas y arrendamientos, que presta la entidad.
T2	**RECURSOS HUMANOS**	Se tratan datos personales de los trabajadores de VIVA, al igual que se almacenan curriculum de solicitantes de empleo.
T3	**CONTABILIDAD Y GESTION**	Tratamiento de datos con la finalidad de gestión y llevanza de la contabilidad de la entidad.
T4	**VIDEOVIGILANCIA**	Videovigilancia con fines de seguridad de las instalaciones, sin conexión a central de alarmas.

Tipología de datos	*SI/NO*
¿Se van a tratar (1) datos personales (2)? (SI/NO)	☑

(1) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

(2) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Finalidad del tratamiento	Detalle	*SI/NO*
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala (3)? Por favor, detalle los puntos indicados a continuación para poder analizar si se trata de un tratamiento a gran escala:		
· El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este Tratamiento)	·de 0 a 10.000	☑
	·de 10.000 a 100.000	
	·+ de 100.000	
·Las categorías de datos tratados. (Datos especialmente protegidos, Datos de carácter identificativo, Características personales, Circunstancias sociales, Datos académicos y profesionales, Detalles del empleo, Información comercial, Datos económicos, financieros y de seguro, Transacciones de bienes y servicios).	*Indicar cuántas de estas categorías aplicarían:* 1, 2, 3, 4, 5, 6, 7,8, 9	6
·La duración del tratamiento (instantáneo (I), días (D), semanas (S), meses (M),...)	Instantáneo	
	Días	
	Semanas	
	Meses	☑
· La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I)	Regional	☑
	Nacional	
	Internacional	
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? *(tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables?) Por ejemplo, uso de registro de actividad sobre clientes para detectar patrones de usuarios susceptibles de contratar un producto, perfiles comerciales, scoring, etc.*		☒
¿La recogida de los datos tiene como finalidad el tratamiento de datos especialmente protegidos?		
Datos identificativos de personas identificadas o identificables asociadas a:	*Ideología o opiniones políticas*	
	Afiliación sindical	
	Religión o opiniones religiosas	

	Creencias o creencias filosóficas	
	Origen étnico o racial	
	Datos relativos a salud	☑
	Vida sexual u orientación sexual	
	Datos de violencia de género y malos tratos	☑
	Datos biométricos	
	Datos genéticos que proporcionan una información única sobre la fisiología o la salud del identificado obtenidas del análisis de una muestra biológica	
	Datos solicitados para fines policiales sin consentimiento de las personas afectadas	
	Datos relativos a condenas y delitos penales	
¿El tratamiento involucra contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo (5) o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad (6)?		☒
5) A modo de ejemplo, las llamadas telefónicas podrían considerarse intrusivas		
6) A modo de ejemplo, la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geolocalización, Big Data o la utilización de etiquetas de radiofrecuencia o RFID10 (especialmente, si forman parte de la llamada internet de las cosas) o cualesquiera otras que puedan desarrollarse en el futuro"		
¿La finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad *(p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social, empleados...)?*		☑
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones (7)?		☒
7) A modo de ejemplo, la segmentación de clientes en base a sus datos personales con el objetivo de realizar comunicaciones comerciales		
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados (8)?		☒
8) A modo de ejemplo, autorizar o denegar un tipo de producto a un cliente mediante un algoritmo automatizado sin que ningún gestor valore el resultado para confirmar las decisiones		

¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usen las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados (9), o incluso pueda llegar a bloquear el disfrute de algún servicio?	☒
(9) A modo de ejemplo, el uso de la información contenida en ficheros externos como ASNEF o CIRBE	
¿El tratamiento implica que un elevado número de personas (más allá de las necesarias para llevar a cabo el mismo) tenga acceso a los datos personales tratados? *Por ejemplo, un departamento que no participe en el tratamiento.*	☒
¿Se van a tratar datos relativos a la observación de zonas de acceso público? *(las zonas de acceso público únicamente estarán situadas en la vía publica, excluyendo los lugares de trabajo (p.e.: oficinas comerciales)*	☒
Para llevar a cabo este tratamiento, ¿se combinan conjuntos de datos utilizados por otros responsables de tratamiento cuya finalidad diste en exceso de las expectativas del interesado (10)?	☒
10) A modo de ejemplo, utilizar el resultado de un tratamiento de análisis de datos de un cliente para realizarle ofertas comerciales en base a dichos resultados	
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?	☒

Tecnologías empleadas para el tratamiento	**Detalle**	***SI/NO***
Se señala SI/NO en función de si dichas tecnologías se usan para soportar las finalidades del tratamiento:		
¿Se prevé el uso de tecnologías que se pueden percibir como inmaduras, de reciente creación o salida al mercado, cuyo alcance no puede ser previsto por el interesado de forma clara o razonable e implique elevado riesgo para el acceso no autorizado?		☒
A modo de ejemplo, la combinación de tecnologías ya existentes, como el uso de dispositivos inteligentes de nueva creación y reconocimiento facial para aumentar la seguridad del acceso físico a las instalaciones, se considera una tecnología inmadura		

Cesiones de datos y transferencias internacionales de datos (TID)	**Detalle**	***SI/NO***
Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo?		☒

¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control (12)?

Percepción de la existencia de un riesgo elevado por parte del responsable de la actividad de tratamiento	Justificación	*SÍ/NO*
¿Es este tratamiento similar a otro para el que haya sido necesario realizar un EIPD (13)?		☒
¿Este tratamiento puede conllevar una pérdida o alteración de la información?		☒
¿Se utilizada documentación en papel para tratar datos personales?, en tal caso, indicar las medidas aplicadas:		
· **Se guarda bajo llave**	☑	
· **Se destruye de forma confidencial**	☑	
· **Se guarda con un registro de accesos**	☑	
· **Otros**		

Terceros que intervengan en el tratamiento		*SI/NO*
SOLICITANTES	— Notarías encargadas de la realización de los sorteos. — Ayuntamiento de Valladolid (publicación de listas de interesados en el sitio web de la Corporación). — Publicación, en el sitio web de la entidad (www.smviva.es), de listas de interesados, en el marco del expediente.	☑
RECURSOS HUMANOS	— Entidad a quien se encomiende la gestión en materia de riesgos laborales. — Tesorería General de la Seguridad Social. — Organizaciones sindicales. — Entidades financieras. — Agencia Estatal de Administración Tributaria.	☑
CONTABILIDAD Y GESTIÓN	— Registro público de contratos. — Entidades financieras. — Agencia Estatal de Administración Tributaria.	☑
VIDEOVIGILANCIA	— Fuerzas y Cuerpos de Seguridad del Estado. — Órganos judiciales. — Empresas de mantenimiento del sistema de videovigilancia.	☑

3.-Resultado del análisis de la necesidad y del cuestionario de evaluación objetiva

¿Se encuentran las actividades de tratamiento en los supuestos indicados como de "Riesgo alto" para los derechos y libertades de las personas o existen otros motivos que justifiquen elaborar un EIPD?

ID	TRATAMIENTOS	EVALUACION DE IMPACTO REQUERIDA
T1	SOLICITANTES	☒
T2	RECURSOS HUMANOS	☒
T3	CONTABILIDAD Y GESTION	☒
T4	VIDEOVIGILANCIA	☒

En el caso de haberse marcado cualquiera de las opciones precalificadas como de Riesgo alto [Art. 35.3 RGPD], se mantiene que el tratamiento referenciado no requiere un EIPD y se justifica, a continuación, los motivos por los cuales no es necesario realizarla.

ID	JUSTIFICACION DE NO NECESIDAD DE REALIZACION DE EIPD
T1	A priori, podría mantenerse la necesidad de contar con una Evaluación de Impacto en VIVA, para los tratamientos T1 (SOLICITANTES), con base en:

La AEPD, en su *Guía para una evaluación de impacto* relaciona una serie de situaciones para las que entiende aconsejable realizar una evaluación:

- "Cuando se vaya a llevar a cabo un tratamiento que pueda comportar un riesgo de discriminación de cualquier tipo (económica, social, política, racial, sexual, etc.) como, por ejemplo, la concesión o denegación de un determinado beneficio social (…)".

Por su parte, el Grupo de Trabajo del Artículo 29 (GT29) ha dado una serie de recomendaciones de que tipo de tratamientos pueden considerarse de alto riesgo, en su documento *WP 248 Directrices sobre Evaluaciones de Impacto, e incluye:*

- Datos relativos a las personas vulnerables: Los sujetos de datos vulnerables pueden incluir menores, segmentos más vulnerables de la población que requieren protección especial (personas con enfermedades mentales, solicitantes de asilo o ancianos, pacientes, etc.).
- Cuando el procesamiento en sí mismo "impide que los interesados ejerzan un derecho o utilicen un servicio o un contrato": Operaciones de procesamiento que tienen como objetivo permitir, modificar o rechazar el acceso de los interesados a un servicio o la entrada en un contrato.

Sin embargo, entendemos que NO SE REQUIERE UNA EVALUACION DE IMPACTO EN VIVA (tampoco en el T1) debido a:

Tal y como recuerda la AEPD, en su *"Guía práctica para las evaluaciones de impacto"* de marzo de 2018, el RGPD prevé que las EIPD se lleven a cabo "antes del tratamiento" en los casos en que sea probable que exista un alto riesgo para los derechos y libertades de los afectados. Es decir, el mandato del Reglamento NO se extiende a las operaciones de tratamiento que ya estén en curso en el momento en que comience a ser de aplicación, en mayo de 2018.

En cualquier caso, si bien, no se denomina "Evaluación de Impacto", pero en los DOCUMENTOS SOBRE PROTECCION DE DATOS DE VIVA se incluye, gran parte de la exigencia del art. 35 del RGPD.

1.-una descripción sistemática del tratamiento previsto y de la finalidad de este.
2.-una evaluación de los riesgos para los derechos y libertades de los interesados atendiendo a los tratamientos que implican alto riesgo, a la vista de la naturaleza, alcance, contexto o fines del tratamiento.
3.-las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos.

XIII

CULTURA DE PRIVACIDAD

FORMACION Y CONCIENCIACION EN

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

CULTURA DE PRIVACIDAD

La privacidad es algo que afecta a toda la organización. La política de privacidad es el procedimiento por el cual se deben tener en cuenta los términos y requisitos de Protección de Datos desde el mismo momento en que se diseña un tratamiento, producto o servicio (PRIVACIDAD DESDE EL DISEÑO) que implica tratamiento de datos personales, y también cuando se esté desarrollando. Es necesario realizar acciones de formación y concienciación, para poder evidenciar que toda la organización conoce las implicaciones en materia de privacidad.

Acciones formativas realizadas.

FECHA	ACCION FORMATIVA Y DESCRIPCION	HORAS	PERSONAL/ DEP.IMPLICADOS

Acciones de concienciación realizadas

FECHA	DESCRIPCIÓN DE LAS ACCIONES REALIZADAS	PERSONAL/ DEP.IMPLICADOS

PLAN de formación continúa en privacidad

PERIORICIDAD	PLAN DE FORMACION CONTINUA	MECANISMO DE EVALUACIÓN	PERSONAL/ DEP.IMPLICADOS

Conclusiones y resultados de las acciones de cultura de privacidad

ZONA VIDEOVIGILADA

RESPONSABLE:

SOCIEDAD MUNICIPAL DE SUELO Y VIVIENDA VALLADOLID S.L.

PUEDE EJERCITAR SUS DERECHOS DE PROTECCIÓN DE DATOS ANTE:

Plaza de la Rinconada, 5- 47001 Valladolid

MÁS INFORMACIÓN SOBRE EL TRATAMIENTO DE SUS DATOS PERSONALES:

www.smviva.com/privacidad

Informe de análisis de cookies

Resumen

Fecha del análisis: 05/07/2018
Nombre de dominio: smviva.com
Ubicación del servidor: Francia
Cookies, en total: 6

Resultado del análisis

6 cookies fueron identificadas.

Categoría: Necesario (1)

Las cookies necesarias ayudan a hacer una página web utilizable activando funciones básicas como la navegación en la página y el acceso a áreas seguras de la página web. La página web no puede funcionar adecuadamente sin estas cookies.

NOMBRE DE LA COOKIE	PROVEEDOR	TIPO	CADUCIDAD
PHPSESSID	smviva.com	HTTP	Session

Primera URL encontrada: http://smviva.com/

Descripción del objetivo de la cookie: Conserva los estados de los usuarios en todas las peticiones de la página.

Iniciador: Página número de línea fuente 12-244
Fuente: Script en línea

Datos enviados a: Francia (adecuado)

Categoría: Estadística (4)

Las cookies estadísticas ayudan a los propietarios de páginas web a comprender cómo interactúan los visitantes con las páginas web reuniendo y proporcionando información de forma anónima.

NOMBRE DE LA COOKIE	PROVEEDOR	TIPO	CADUCIDAD
_ga	smviva.com	HTTP	2 años

Primera URL encontrada: http://smviva.com/

Descripción del objetivo de la cookie: Registra una identificación única que se utiliza para generar datos estadísticos acerca de cómo utiliza el visitante el sitio web.

Iniciador: Página número de línea fuente 12-244
Fuente: Script en línea

Datos enviados a: Francia (adecuado)

Activar la previa autorización: No

_gat	smviva.com	HTTP	Session

Primera URL encontrada: http://smviva.com/

Descripción del objetivo de la cookie: Utilizado por Google Analytics para controlar la tasa de peticiones

Iniciador: Página número de línea fuente 12-244
Fuente: Script en línea

Datos enviados a: Francia (adecuado)

Activar la previa autorización: No

_gid	smviva.com	HTTP	Session

Primera URL encontrada: http://smviva.com/

Descripción del objetivo de la cookie: Registra una identificación única que se utiliza para generar datos estadísticos acerca de cómo utiliza el visitante el sitio web.

Iniciador: Página número de línea fuente 12-244
Fuente: Script en línea

Datos enviados a: Francia (adecuado)

Activar la previa autorización: No

collect	google-analytics.com	Pixel	Session

Primera URL encontrada: http://smviva.com/

Descripción del objetivo de la cookie: No clasificado

Iniciador: Etiqueta de script, página número de línea fuente 241
Fuente: http://www.google-analytics.com/collect?v=1&_v=j68&a=98562557&t=pageview&_s=2&dl=http%3A%2F%2Fsmviva.com%2F&dp=%2F%3F_escaped_fragment_%3D&ul=en-us&de=UTF-8&dt=VIVA%20Valladolid&sd=24-bit&sr=1024x768&vp=1014x722&je=0&_u=KEBAAEAB~&jid=&gjid=&cid=397900496.1530780923&tid=UA-41330133-1&_gid=742945944.1530780923&z=1234429569
mediante http://www.google-analytics.com/analytics.js

Datos enviados a: Estados Unidos (adecuado)

Categoría: Marketing (1)

Las cookies de marketing se utilizan para rastrear a los visitantes en las páginas web. La intención es mostrar anuncios relevantes y atractivos para el usuario individual, y por lo tanto, más valiosos para los editores y terceros anunciantes.

NOMBRE DE LA COOKIE	PROVEEDOR	TIPO	CADUCIDAD
r/collect	doubleclick.net	Pixel	Session

Primera URL encontrada: http://smviva.com/

Descripción del objetivo de la cookie: No clasificado

Iniciador: Script en línea, página número de línea fuente 12-244
Fuente: https://stats.g.doubleclick.net/r/collect?v=1&aip=1&t=dc&_r=3&tid=UA-41330133-1&cid=397900496.1530780923&jid=220402982&_gid=742945944.1530780923&gjid=893299704&_v=j68&z=1160209843

Datos enviados a: Estados Unidos (adecuado)

Continuidad de negocio

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. Continuidad de negocio 3

1.1. Antecedentes 3
1.2. Objetivos 3
1.3. Checklist 4
1.4. Puntos clave 5

2. Referencias 6

1. CONTINUIDAD DE NEGOCIO

1.1. Antecedentes

Es imposible garantizar la seguridad total por lo que las empresas deben estar preparadas para protegerse ante un posible **desastre** que pudiera **paralizar su actividad**. Hoy en día la información es un activo **esencial** en cualquier organización, y los sistemas de información se apoyan en **tecnologías complejas y novedosas** que también están **expuestas** a **amenazas de seguridad**. Por todo ello, es conveniente tener elaboradas unas pautas que indiquen cómo actuar en caso de que haya un fallo que comprometa la **continuidad del negocio** de nuestra empresa.

Nuestro **plan para la continuidad de negocio** [1] debe tener en cuenta las personas responsables de aplicarlo, las operativas a seguir (por ejemplo: implementar un mecanismo de respaldo para nuestra información más crítica), los activos implicados (tanto personales como físicos), indicadores, etc. Una vez que tengamos el plan de continuidad debemos **comprobar** que sabemos ponerlo en marcha.

Cuando contratemos servicios tecnológicos (en la nube o a proveedores externos) o que impliquen el tratamiento de nuestra información, debemos exigir y comprobar que tienen planes de contingencia disponibles que se adecuen a nuestra política para la continuidad del negocio [2].

1.2. Objetivos

Diseñar y probar un plan de continuidad de negocio [3] (PCN) que nos permita **recuperar** en un plazo razonable la operativa habitual de nuestra empresa para garantizar la **continuidad del negocio**.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a la **continuidad del negocio**.

Los controles se clasificarán en dos niveles de **complejidad**:

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Determinar el alcance del PCN** Analizas para que activos y procesos debes garantizar la continuidad.	☐
B	PRO	**Concretar el flujo de responsabilidades** Determinas las responsabilidades de las personas que deben llevar a cabo el plan de continuidad en caso de aparición de desastres.	☐
A	PRO/TEC	**Realización del BIA (Análisis del Impacto en el Negocio)** Elaboras detalladamente el BIA de tu empresa.	☐
B	PRO	**Definir la política de comunicación y aviso a entidades externas** Defines que tipo de mensajes debe transmitir tu empresa en caso de desastre.	☐
B	PRO	**Caducidad del PCN** Actualizas el plan de continuidad de negocio de tu empresa cada _____.	☐
A	PRO/TEC	**Elegir la estrategia de continuidad** Eliges la estrategia de continuidad óptima para tu empresa. Teniendo en cuenta si fuera preciso la implantación de un centro de respaldo.	☐
A	PRO/TEC	**Detallar la respuesta a la contingencia** Detallas los procedimientos y controles específicos a ejecutar ante la aparición de un desastre.	☐
A	PRO/TEC	**Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio** Pruebas y evalúas cada _____ el plan de continuidad de negocio de tu empresa.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Determinar el alcance del plan de continuidad del negocio.** Debemos seleccionar los activos para los cuales garantizar la continuidad. Para ello nos basaremos en los activos críticos de la clasificación de activos de información [10].
- **Concretar el flujo de responsabilidades.** Para una correcta ejecución del plan de continuidad del negocio tenemos que determinar quién(es) debe(n) hacerse cargo de la situación en caso de desastre. Definiremos las responsabilidades, la secuencia de decisiones y los canales adecuados para establecer las comunicaciones oportunas.
- **Realización del BIA (Análisis del Impacto en el Negocio)** [4] [5]**.** Para calcular el riesgo al que estamos sometidos, debemos estudiar las implicaciones de un incidente grave en los activos de información. Para ello determinaremos, entre otros:
    - cuáles son las actividades principales de la organización;
    - las dependencias, con otros procesos o proveedores, de las actividades anteriores;
    - el máximo tiempo que podemos estar sin esa actividad o actividades;
    - el tiempo mínimo de recuperación del servicio a niveles aceptables.
- **Definir la política de comunicación y aviso a entidades externas.** En ciertos casos puede ser necesario determinar qué personas deben notificar las situaciones de desastre a las autoridades pertinentes y a los medios de comunicación. Analizaremos qué tipo de mensaje se debe transmitir y cómo.
- **Caducidad del plan de continuidad del negocio.** Con el fin de mantener actualizado nuestro plan de continuidad de negocio, determinaremos la periodicidad con la cual debería revisarse. Asimismo, analizaremos la necesidad de actualizar nuestro plan tras acometer cambios importantes en nuestros sistemas de información.
- **Elegir la estrategia de continuidad.** Determinaremos que estrategia es la más adecuada para nuestra empresa. Implantaremos políticas de copias de seguridad [6], donde definiremos la información que debe incluirse en dichas copias, qué tipo de soporte se utilizará, con qué periodicidad y en qué instalaciones físicas. Asimismo, se deberían definir pruebas periódicas para verificar la integridad y la correcta recuperación de la información. Por otro lado, estudiaremos la conveniencia de implantar un centro de respaldo [7] a raíz de los resultados obtenidos durante la elaboración del BIA (Análisis del Impacto en el Negocio). Esto es especialmente importante si el alcance del Plan es el CPD [8].
- **Detallar la respuesta a la contingencia.** Se deben detallar los procedimientos y controles que aseguren el nivel de continuidad de los procesos y activos esenciales ante una situación adversa.
- **Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio** [9]**.** Para garantizar que el plan de continuidad del negocio es válido evaluaremos cada cierto tiempo todos los procedimientos y controles que lo componen, para modificarlos, eliminarlos o añadir nuevos si fuera necesario. Estas actividades se tendrán en cuenta sobre todo tras acometer cambios sustanciales en nuestros sistemas.

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – ¿Qué te interesa? – Plan de Contingencia y Continuidad de Negocio https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

[2]. Incibe – Protege tu empresa – Blog – Sube a la nube, pero no estés en «las nubes» sin continuidad de negocio https://www.incibe.es/protege-tu-empresa/blog/no-estes-en-las-nubes

[3]. Incibe – Protege tu empresa – Blog – ¿No tienes un Plan de Crisis? ¿Estás esperando al desastre? https://www.incibe.es/protege-tu-empresa/blog/plan-de-crisis

[4]. Incibe – Protege tu empresa – Blog – Pasos a seguir para realizar un análisis de impacto en nuestro negocio https://www.incibe.es/protege-tu-empresa/blog/pasos-seguir-realizar-analisis-impacto-negocio

[5]. Incibe – Protege tu empresa – ¿Qué te interesa? – Plantilla ejemplo para inventario de activos para BIA https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

[6]. Incibe – Protege tu empresa – ¿Qué te interesa? – Políticas de seguridad para la pyme – Copias de seguridad https://www.incibe.es/protege-tu-empresa/que-te-interesa

[7]. Incibe – Protege tu empresa – Blog – Frío o caliente… o quizá templado, ¿qué sitio de recuperación me conviene? https://www.incibe.es/protege-tu-empresa/blog/frio-o-caliente-que-sitio-de-recuperacion-me-conviene

[8]. Incibe – Protege tu empresa – Blog – Pon un CPD seguro en tu empresa https://www.incibe.es/protege-tu-empresa/blog/cpd-seguro-empresa

[9]. Incibe – Protege tu empresa – Blog – Las pruebas de continuidad no son una opción, sino una obligación https://www.incibe.es/protege-tu-empresa/blog/pruebas-continuidad-no-opcion-si-obligacion

[10]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Clasificación de la información https://www.incibe.es/protege-tu-empresa/herramientas/politicas

INSTITUTO NACIONAL DE CIBERSEGURIDAD