ASESORES&DATOS

DOCUMENTACIÓN PARA EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE

CLIMATIZACIÓN GUADALUPE, S.L.

ASESORES&DATOS

INDICE

ANEXOS

1. INTRODUCCIÓN

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, junto con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos; en adelante, RGPD), establece, entre otras disposiciones, los requisitos documentales necesarios para poder cumplir con el RGPD y poder ser capaz de demostrar dicho cumplimiento.

Entre la documentación mínima que debe dispone la entidad se encuentra:

- El Registro de Actividades de Tratamiento, tanto como responsable del tratamiento, como encargado del tratamiento, en su caso.
- Documentación del análisis de riesgos realizado.
- La/s Evaluación/es de Impacto relativa/s a la Protección de Datos, en su caso.
- Las medidas de seguridad implantadas.
- Las funciones y obligaciones del personal con acceso a datos personales.
- El registro de incidencias y el registro de las notificaciones de las violaciones de la seguridad a la Autoridad de Control, en su caso.
- Los protocolos de atención a los derechos de los interesados.
- Los compromisos de confidencialidad con los trabajadores.
- Los contratos de acceso a datos por cuenta de terceros.
- La documentación relativa a las transferencias internacionales de datos, así como las garantías apropiadas obtenidas o las excepciones utilizadas como base jurídica para su realización.
- Toda la documentación adicional que sea necesaria para demostrar el cumplimiento de la normativa de protección de datos en la entidad (cláusulas legales, consentimientos otorgados por los interesados, autorizaciones para la contratación de subencargados del tratamiento, ponderaciones del interés legítimo, etc.).

Esta documentación debe mantenerse en todo momento actualizada y debe ser revisada siempre que se produzcan cambios que puedan repercutir en el cumplimiento de la normativa de protección de datos o en las medidas de seguridad implantadas, como son cambios relevantes en:

- la organización
- el contenido de la información incluida en los tratamientos
- los tratamientos de datos personales realizados
- los sistemas de tratamiento empleados

Debe mantenerse adecuada, en todo momento, a las disposiciones vigentes en materia de protección de los datos de carácter personal.

2. ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento será de aplicación a los tratamientos de datos personales realizados por **CLIMATIZACIÓN GUADALUPE, S.L.**, incluyendo los sistemas de información, soportes y equipos empleados para dicho tratamiento de datos de carácter personal, las personas que intervienen en el tratamiento y los locales en los que se ubican.

En concreto, los tratamientos a los que se hace referencia en este documento, son los relacionados en el apartado 2.2.

2.1 RESPONSABLE DEL TRATAMIENTO

CLIMATIZACIÓN GUADALUPE, S.L.

B-01664382

Camino de los Raspajines 1 1F, 30107-Aljucer (Murcia)

climatizacionguadalupesl@gmail.com

2.2 TRATAMIENTOS

2.2.1 COMO RESPONSABLE DEL TRATAMIENTO

Los tratamientos que **CLIMATIZACIÓN GUADALUPE, S.L.** realiza como responsable del tratamiento, son los siguientes:

NOMBRE DEL TRATAMIENTO	FINALIDAD
GESTIÓN DE ACCIDENTES LABORALES	Gestión de los partes de accidentes laborales y su comunicación a los organismos pertinentes
GESTIÓN DE CLIENTES	Gestión fiscal, contable y administrativa de clientes, así como el envío de comunicaciones comerciales
GESTIÓN DE PERSONAL	Gestión de recursos humanos, nóminas y prevención de riesgos laborales
GESTIÓN DE POTENCIALES CLIENTES	Gestión de potenciales clientes y contactos con los que se prevé mantener una relación comercial
GESTIÓN DE PROVEEDORES	Gestión fiscal, contable y administrativa de proveedores
SELECCIÓN DE PERSONAL	Gestión de los Currículum Vitae recibidos, así como los procesos de selección de personal
VIDEOVIGILANCIA	Videovigilancia de las instalaciones y seguridad privada

En el ANEXO I se describen detalladamente cada uno de los tratamientos, junto con los detalles de cada uno de ellos.

2.2.2 COMO ENCARGADO DEL TRATAMIENTO

En anexo VII se detallan los encargados del tratamiento y se establecen los contratos.

3. ANÁLISIS DE LOS RIESGOS Y MEDIDAS DE SEGURIDAD

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

1) la seudonimización y el cifrado de datos personales;
2) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y residencia permanentes de los sistemas y servicios de tratamientos;
3) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
4) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

Para dar cumplimiento a esto, **CLIMATIZACIÓN GUADALUPE, S.L.** ha realizado un análisis de riesgos documentado, que identifica las amenazas a las que los datos están expuestos, las vulnerabilidades que pueden aprovechar dichas amenazas, así como el daño que podrían producir las distintas amenazas en caso de que se materializasen.

Con estos datos se ha realizado una estimación del nivel de riesgo, con objeto de implantar medidas de seguridad adecuadas a dicho nivel de riesgo.

Este análisis de riesgos documentado se encuentra en el ANEXO II.

Las medidas de seguridad implantadas para mitigar los riesgos identificados se encuentran en el ANEXO III.

3.1 EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

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.

El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

La evaluación de impacto relativa a la protección de los datos se requerirá en particular en caso de:

evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales; observación sistemática a gran escala de una zona de acceso público.

La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos. Dicha lista podrá consultarse en el sitio web de la Agencia Española de Protección de datos: www.agpd.es.

En el ANEXO II se encuentran las evaluaciones de impacto relativas a la protección de datos personales que, en su caso, haya sido necesario realizar.

4. PROCEDIMIENTO DE INFORMACIÓN AL PERSONAL

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas de forma general en el Capítulo siguiente y de forma específica en los ANEXOS IV y V.

CLIMATIZACIÓN GUADALUPE, S.L. debe poner en conocimiento de personal las medidas y normas que les afectan en el desarrollo de sus funciones, así como de las consecuencias de no cumplirlas. Asimismo, deberá tener a disposición del personal la parte que les afecte del presente documento.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, se pondrá a su disposición una copia de las Funciones y obligaciones del personal en materia de protección de datos personales, que se encuentran en el ANEXO IV, sin perjuicio de otras actuaciones formativas o de concienciación que pueda desarrollar en este ámbito.

5. FUNCIONES Y OBLIGACIONES DEL PERSONAL

Todo el personal que acceda a datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar a **CLIMATIZACIÓN GUADALUPE, S.L.** las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en esta documentación, y en concreto en el apartado de "Notificación, gestión y respuesta ante incidencias".

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo. Para ello, firmarán un compromiso de confidencialidad y secreto. Dichos compromisos encuentran en el ANEXO VI.

Además del responsable del tratamiento, el personal afectado por esta normativa se puede

clasificar en los siguientes perfiles genéricos:

1) **Administradores**, encargados de administrar o mantener el entorno operativo del tratamiento, así como conceder, alterar o anular el acceso autorizado a los datos. Este personal deberá estar explícitamente relacionado en el ANEXO V, ya que por sus funciones, pueden tener acceso a los datos protegidos saltándose las barreras de acceso de las aplicaciones o sistemas de información.
2) **Encargados del tratamiento**, son las personas físicas o jurídicas, autoridades públicas, servicios o cualquiera de otros organismos que sólo o con otros, traten datos personales por cuenta del responsable del tratamiento, como consecuencia de una relación jurídica de prestación de servicio. El tratamiento de los datos realizado por un encargado de tratamiento estará sometido en todo caso a las medidas de seguridad que sean necesarias para garantizar la confidencialidad, integridad y confidencialidad de los datos personales que está tratando.
3) **Usuarios del tratamiento**, o personal que usualmente accede a los datos para su tratamiento, y que debe estar explícitamente relacionado en el ANEXO V.
4) **Otras personas**, de entidades ajenas que por motivo de su desempeño profesional, puedan potencialmente tener acceso a la información de carácter personal.

Los requisitos para tratar los datos personales, tanto formales, como de seguridad, son de obligado cumplimiento para todos ellos.

Las funciones y obligaciones del personal en materia de protección de datos, están descritas en el ANEXO IV.

Los perfiles de usuario, las funciones específicas de esos perfiles dentro de la organización y los accesos autorizados a los distintos tratamientos se encuentran detallados en el ANEXO V.

5.1 EL DELEGADO DE PROTECCIÓN DE DATOS

Una figura fundamental para el correcto cumplimiento de la normativa de protección de datos personales es el Delegado de Protección de Datos.

El Delegado de Protección de Datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados en la normativa y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones propias de su puesto.

El Delegado de Protección de Datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

El Delegado de Protección de Datos tiene las siguientes funciones:

1) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben;
2) supervisar el cumplimiento de lo dispuesto en la normativa de protección de datos y de las políticas del responsable o del encargado del tratamiento en materia de

protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
3) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación;
4) cooperar con la autoridad de control;
5) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier asunto relacionado con el cumplimiento de la normativa de protección de datos.

El Delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos.

6. ENCARGADOS DEL TRATAMIENTO

Encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u organismo trate datos personales por cuenta del responsable del tratamiento.

A modo de ejemplo, la asesoría que realiza las nóminas, es encargada del tratamiento de para la empresa que manda realizar ese trabajo.

6.1 OBLIGACIONES

Cuando se vaya a realizar un tratamiento por cuenta de **CLIMATIZACIÓN GUADALUPE, S.L.**, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos del interesado.

El tratamiento por el encargado se regirá por un contrato u otro acto jurídico 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.

Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

1) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional;
2) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad;
3) tomará todas las medidas necesarias para garantizar la seguridad de los datos;
4) no recurrirá a otro encargado sin la autorización previa por escrito del responsable del tratamiento;

5) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados;
6) ayudará al responsable a garantizar el cumplimiento de las obligaciones relativas a la seguridad del tratamiento, la notificación de las violaciones de la seguridad de los datos personales, la Evaluación de Impacto relativa a la Protección de Datos y las consultas previas a la Autoridad de Control, en su caso;
7) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales;
8) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En dicho contrato se estipularán, asimismo, las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

6.2 RESPONSABLE Y ENCARGADO

Debemos tener en cuenta que, como entidad, podemos tener al mismo tiempo dos roles diferenciados: somos responsables de tratamiento de los datos propios (nuestros clientes, empleados, etc.), y al mismo tiempo, encargados del tratamiento de los clientes a los que prestamos servicios que requieran el tratamiento de datos personales de los que ellos son responsables.

6.2.1 COMO RESPONSABLE DEL TRATAMIENTO

Antes de que tenga lugar ningún tratamiento por parte del encargado del tratamiento, se debe formalizar un contrato u otro acto jurídico equivalente con el encargado en los términos descritos en el apartado 6.1.

En el ANEXO VII se recogen los contratos de acceso a datos por cuenta de terceros y otros actos jurídicos equivalentes que **CLIMATIZACIÓN GUADALUPE, S.L.** ha suscrito con los encargados del tratamiento.

6.2.2 COMO ENCARGADO DEL TRATAMIENTO

Antes de que tenga lugar ningún tratamiento por parte del encargado del tratamiento, se debe formalizar un contrato u otro acto jurídico equivalente entre el responsable y el

encargado en los términos descritos en el apartado 6.1.

En el ANEXO VIII se recogen los contratos de acceso a datos por cuenta de terceros y otros actos jurídicos equivalentes que, en su caso, **CLIMATIZACIÓN GUADALUPE, S.L.** ha suscrito con los responsables del tratamiento a los cuáles presta servicio.

Al Registro de Actividades de Tratamiento del encargado deberá añadirse la identificación de los responsables por cuenta de los cuáles actúe el encargado y los detalles de los tratamientos que se realizan así como la descripción de las medidas técnicas y organizativas de seguridad.

7. TRANSFERENCIAS INTERNACIONALES DE DATOS

Una transferencia internacional de datos, es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta de un responsable del tratamiento establecido en territorio español.

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si el responsable y el encargado del tratamiento cumplen las condiciones establecidas para su realización, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional.

Sólo podrán realizarse dichas transferencias si se cumple alguna de estas situaciones:

- Cuando la Comisión Europea haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado.
- Cuando el responsable o el encargado del tratamiento haya obtenido garantías adecuadas, y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.
- Si se cumple alguna de las condiciones siguientes:
    - Existe el consentimiento explícito del interesado a la transferencia.
    - La transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento.
    - La transferencia es necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica.
    - La transferencia es necesaria por razones importantes de interés público.
    - La transferencia es necesaria para la formulación, el ejercicio o la defensa de reclamaciones
    - Transferencia necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.

Las transferencias de datos personales a terceros países u organizaciones internacionales de cada uno de los tratamientos realizados, están detalladas en el Registro de Actividades de Tratamiento que se encuentra en el ANEXO I.

Las garantías y documentación relativa a las transferencias de datos a terceros países u organizaciones internacionales se encuentran en el ANEXO XII.

8. NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en el RGPD, así como cualquier anomalía o evento que afecte o pueda afectar a la seguridad de los datos de carácter personal en sus tres vertientes de confidencialidad, integridad y disponibilidad.

Se deberán tener en cuenta, entre otras, las siguientes incidencias:

Cualquier pérdida de información que contenga datos personales.

Modificación de datos personales por personal no autorizado o desconocido.

Existencia de sistemas de información sin las debidas medidas de seguridad.

Los intentos de acceso no autorizados a datos personales.

El conocimiento por terceros de la clave de acceso al sistema.

El intento no autorizado de salida de un soporte.

La destrucción total o parcial de un soporte que contenga datos personales.

La caída del sistema de seguridad informática, que posibilite el acceso a datos personales por personas no autorizadas.

Cualquier incidencia que pueda afectar a la confidencialidad, integridad y/o disponibilidad de los datos personales.

Todos los usuarios, administradores, responsables, así como cualquier persona que tenga acceso a datos personales, deben tener conocimiento de este procedimiento para actuar en caso de incidencia.

Este procedimiento se ha dado a conocer a todo el personal que trata con datos de carácter personal de **CLIMATIZACIÓN GUADALUPE, S.L.** y es el descrito en el documento Funciones y obligaciones del personal en materia de protección de datos personales.

8.1 REGISTRO DE INCIDENCIAS

El mantener un registro de las incidencias que comprometan la seguridad de un tratamiento es una herramienta imprescindible para aplicar las medidas correctoras necesarias, así como posibilitar la prevención de posibles ataques a esa seguridad y la persecución de los responsables de los mismos.

Cualquier usuario que tenga conocimiento de una incidencia, es responsable del registro de la misma, si el registro de incidencias está automatizado; o de la notificación por escrito al responsable del tratamiento, o la persona en quien haya delegado la gestión de las

incidencias, si el registro se realiza manualmente.

El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del tratamiento por parte de ese usuario.

En el ANEXO IX, se establece la creación de un registro de incidencias, en el que se hará constar:

- Tipo de incidencia
- Momento en que se ha producido o detectado
- La persona que realiza la notificación
- Persona a la que se comunica
- Los efectos derivados de la incidencia
- Medidas correctoras aplicadas

8.2 NOTIFICACIÓN DE LAS VIOLACIONES DE LA SEGURIDAD

Se denomina una violación de la seguridad de los datos personales a toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

8.2.1 NOTIFICACIÓN A LA AUTORIDAD DE CONTROL

En caso de violación de la seguridad de los datos personales, **CLIMATIZACIÓN GUADALUPE, S.L.** 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 violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

La notificación deberá, como mínimo:

- Describir 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;
- Comunicar 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;
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales;
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento 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 fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

Dicha comunicación se realizará de forma electrónica a la Agencia Española de Protección

de Datos través de su sitio web: www.agpd.es.

El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

CLIMATIZACIÓN GUADALUPE, S.L. documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el RGPD en este ámbito.

8.2.2 COMUNICACIÓN A LOS INTERESADOS

Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, **CLIMATIZACIÓN GUADALUPE, S.L.** la comunicará al interesado sin dilación indebida.

La comunicación al interesado describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información siguiente:

- 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;
- Una descripción de las posibles consecuencias de la violación de la seguridad de los datos personales;
- Una descripción de las medidas adoptadas o propuestas por el responsable del tratamiento 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.

La comunicación al interesado no será necesaria si se cumple alguna de las condiciones siguientes:

- El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
- El responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado;
- Suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

9. DERECHOS DE LOS INTERESADOS

Los derechos que los interesados pueden solicitar al responsable del tratamiento son los siguientes:

- Derecho de acceso.
- Derecho de rectificación.
- Derecho de supresión («el derecho al olvido»).
- Derecho a la limitación del tratamiento.
- Derecho a la portabilidad de los datos.
- Derecho de oposición.
- Derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles.

CLIMATIZACIÓN GUADALUPE, S.L. facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud de derecho por parte de un interesado, y, en cualquier caso, 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. **CLIMATIZACIÓN GUADALUPE, S.L.** informará 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.

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

Si **CLIMATIZACIÓN GUADALUPE, S.L.** no da curso a la solicitud del interesado, le informará 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.

El ejercicio de los derechos será a título gratuito para el interesado.

Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento 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 este caso, **CLIMATIZACIÓN GUADALUPE, S.L.** soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

Los protocolos para el ejercicio de los derechos de los interesados se encuentran en el ANEXO X.

10. PROCEDIMIENTOS DE REVISIÓN

10.1 REVISIÓN DE LA DOCUMENTACIÓN

La documentación necesaria para dar cumplimiento a la normativa de protección de datos deberá mantenerse en todo momento actualizada y deberá ser revisada siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los tratamientos o como consecuencia de los controles periódicos realizados. Se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos personales.

Se realizará, al menos una vez al año, la revisión completa del presente documento, así como la validez y adecuación legal de todo su contenido.

10.2 AUDITORÍA

Los tratamientos identificados en el ANEXO I deberán someterse, periódicamente, a una auditoría interna o externa, que verifique el cumplimiento de las medidas de seguridad recogidas en el ANEXO III, así como el cumplimiento de la normativa de protección de datos en todo el ciclo de vida de los datos personales.

Esta auditoría afectará tanto a los ficheros automatizados, como a los no automatizados, y abarcará tanto los sistemas de información, como las instalaciones de tratamiento y almacenamiento de los datos personales.

Con carácter extraordinario deberá realizarse cuando se lleven a cabo modificaciones tales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas, con objeto de verificar la eficacia de las mismas.

El informe analizará la adecuación de las medidas de seguridad y controles a la normativa, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias.

Los informes de las auditorías realizadas se encuentran en el ANEXO XII

ANEXO I

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

REGISTRÓ DE ACTIVIDADES DE TRATAMIENTO DEL RESPONSABLE

Datos de contacto del Responsable

CLIMATIZACIÓN GUADALUPE, S.L.

B-01664382

Camino de los Raspajines 1 1F, 30107-Aljucer (Murcia)

climatizacionguadalupesl@gmail.com

DATOS GENERALES DEL TRATAMIENTO

Nombre: *GESTIÓN DE CLIENTES*

Fines: Gestión fiscal, contable y administrativa de clientes, así como el envío de comunicaciones comerciales

CATEGORÍAS DE INTERESADOS

Personas con las que se mantiene una relación comercial

Categorías: Clientes y usuarios.

CATEGORÍAS DE DATOS PERSONALES

Identificación: CIF/DNI; Nombre y apellidos; Dirección; Teléfono; Firma; Dirección de correo electrónico.

Datos bancarios: Planes de pensiones / jubilación.

Transacciones de bienes y servicios: Bienes y servicios suministrados o recibidos por el afectado; Transacciones financieras; Compensaciones / Indemnizaciones.

CATEGORÍAS DE DESTINATARIOS

Registros públicos; Administración tributaria; Bancos/Cajas de ahorro y Cajas rurales.

TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

No existen transferencias de datos a terceros países.

PLAZOS PREVISTOS PARA LA SUPRESIÓN

Todos los datos se suprimirán cuando el cliente así lo solicite, siempre respetando los plazos previstos por la legislación fiscal respecto a la prescripción de responsabilidades.

OBSERVACIONES

DATOS GENERALES DEL TRATAMIENTO

Nombre: *GESTIÓN DE POTENCIALES CLIENTES*

Fines: Gestión de potenciales clientes y contactos con los que se prevé mantener una relación comercial

CATEGORÍAS DE INTERESADOS

Personas con las que se prevé mantener una relación comercial

Categorías: Clientes y usuarios; Personas de contacto.

CATEGORÍAS DE DATOS PERSONALES

Identificación: Nombre y apellidos; Dirección; Teléfono; Dirección de correo electrónico.

Información comercial: Actividades y negocios; Licencias comerciales; Suscripciones o publicaciones / Medios de comunicación; Creaciones artísticas, literarias, científicas o técnicas.

CATEGORÍAS DE DESTINATARIOS

TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

No existen transferencias de datos a terceros países.

PLAZOS PREVISTOS PARA LA SUPRESIÓN

Todos los datos se suprimirán cuando el cliente así lo solicite

OBSERVACIONES

DATOS GENERALES DEL TRATAMIENTO

Nombre: *GESTIÓN DE PERSONAL*

Fines: Gestión de recursos humanos, nóminas y prevención de riesgos laborales

CATEGORÍAS DE INTERESADOS

Personas con las que se mantiene tiene una relación laboral. Categorías: Empleados.

CATEGORÍAS DE DATOS PERSONALES

Identificación: CIF/DNI; Nº SS/Mutua; Nombre y apellidos; Dirección; Teléfono; Firma; Imagen/Voz; huella dactilar; dirección de correo electrónico.

Características personales: Datos de estado civil; De familia; Fecha y lugar de nacimiento; Edad; Sexo; Nacionalidad; Lengua Materna y Características física o antropométricas.

Académicos/Profesionales: Formación, titulaciones; Historial de estudiante; Experiencia profesional; Pertenencia a colegios o asociaciones profesionales.

Detalles de empleo: Profesión; Puestos de trabajo; Datos no económicos de nómina; Historial del trabajador.

Datos bancarios: Planes de pensiones / jubilación.

Datos especiales: Datos relativos a la salud.

CATEGORÍAS DE DESTINATARIOS

Organismos de la Seguridad Social; Administración tributaria; Bancos/Cajas de ahorro y Cajas rurales; Entidades aseguradoras; Entidades sanitarias.

TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

No existen transferencias de datos a terceros países.

PLAZOS PREVISTOS PARA LA SUPRESIÓN

Todos los datos se suprimirán cuando finalice la relación con el trabajador, siempre respetando los plazos previstos por la legislación laboral respecto a la prescripción de responsabilidades.

OBSERVACIONES

Los datos relativos a la salud se refieren, exclusivamente, a partes de baja, el [apto/no apto] de la prevención de riesgos laborales y el porcentaje de discapacidad, en su caso

DATOS GENERALES DEL TRATAMIENTO

Nombre: *GESTIÓN DE ACCIDENTES LABORALES*

Fines: Gestión de los partes de accidentes laborales y su comunicación a los organismos pertinentes

CATEGORÍAS DE INTERESADOS

Trabajadores con los que se mantienen una relación laboral y que han tenido un accidente laboral

Categorías: Empleados.

CATEGORÍAS DE DATOS PERSONALES

Identificación: CIF/DNI; Nº SS/Mutua; Nombre y apellidos; Dirección.

Datos especiales: Datos relativos a la salud.

CATEGORÍAS DE DESTINATARIOS

Organismos de la Seguridad Social; Entidades aseguradoras; Entidades sanitarias.

TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

No existen transferencias de datos a terceros países.

PLAZOS PREVISTOS PARA LA SUPRESIÓN

Todos los datos se suprimirán cuando finalice la relación con el trabajador, siempre respetando los plazos previstos por la legislación laboral respecto a la prescripción de responsabilidades.

OBSERVACIONES

DATOS GENERALES DEL TRATAMIENTO

Nombre: *SELECCIÓN DE PERSONAL*

Fines: Gestión de los Currículum Vitae recibidos, así como los procesos de selección de personal

CATEGORÍAS DE INTERESADOS

Personas solicitantes de empleo. Categorías: Solicitantes.

CATEGORÍAS DE DATOS PERSONALES

Identificación: CIF/DNI; Nombre y apellidos; Dirección; Teléfono; Firma; Imagen/Voz; huella dactilar; dirección de correo electrónico.

Características personales: Datos de estado civil; De familia; Fecha y lugar de nacimiento; Edad; Sexo; Nacionalidad; Lengua Materna y Características física o antropométricas.

Circunstancias sociales: Características de alojamiento y vivienda; Propiedades y posesiones; Situación militar; Aficiones y estilo de vida; Pertenencia a clubes y asociaciones; Licencias, permisos y autorizaciones.

Académicos/Profesionales: Formación, titulaciones; Historial de estudiante; Experiencia profesional; Pertenencia a colegios o asociaciones profesionales.

Detalles de empleo: Profesión; Puestos de trabajo; Datos no económicos de nómina; Historial del trabajador.

Información comercial: Actividades y negocios; Licencias comerciales; Suscripciones o publicaciones / Medios de comunicación; Creaciones artísticas, literarias, científicas o técnicas.

CATEGORÍAS DE DESTINATARIOS

TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

No existen transferencias de datos a terceros países.

PLAZOS PREVISTOS PARA LA SUPRESIÓN

Los datos se suprimirán cuando el interesado lo solicite, o a los dos años desde la última interacción con dicho interesado

OBSERVACIONES

DATOS GENERALES DEL TRATAMIENTO

Nombre: *GESTIÓN DE PROVEEDORES*

Fines: Gestión fiscal, contable y administrativa de proveedores

CATEGORÍAS DE INTERESADOS

Personas con las que se contrata una prestación de servicios

Categorías: Proveedores.

CATEGORÍAS DE DATOS PERSONALES

Identificación: CIF/DNI; Nombre y apellidos; Dirección; Teléfono; Firma; Dirección de correo electrónico.

Información comercial: Actividades y negocios; Licencias comerciales; Suscripciones o publicaciones / Medios de comunicación; Creaciones artísticas, literarias, científicas o técnicas.

Datos bancarios: Planes de pensiones / jubilación.

Transacciones de bienes y servicios: Bienes y servicios suministrados o recibidos por el afectado; Transacciones financieras; Compensaciones / Indemnizaciones.

CATEGORÍAS DE DESTINATARIOS

Registros públicos; Administración tributaria; Bancos/Cajas de ahorro y Cajas rurales.

TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

No existen transferencias de datos a terceros países.

PLAZOS PREVISTOS PARA LA SUPRESIÓN

Todos los datos se suprimirán cuando finalice la relación con el proveedor, siempre respetando los plazos previstos por la legislación fiscal respecto a la prescripción de responsabilidades.

OBSERVACIONES

DATOS GENERALES DEL TRATAMIENTO

Nombre: *VIDEOVIGILANCIA*

Legitimación: Artículo 6.1 del RGPD

Fines: Garantizar la seguridad de personas, bienes e instalaciones.

Delegado de Protección de Datos: lopd@asesoresydatos.es, con dirección en CL Antonio Machado, 51 30565 – Las Torres de Cotillas (Murcia).

CATEGORÍAS DE AFECTADOS

Personas que acceden a las instalaciones. Categorías: trabajadores, clientes, proveedores, usuarios...

CATEGORÍAS DE DATOS PERSONALES

Identificación: Imagen/Voz.

CATEGORÍAS DE DESTINATARIOS

Fuerzas y cuerpos de seguridad. Juzgados y Tribunales

TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

No existen transferencias de datos a terceros países.

PLAZOS PREVISTOS PARA LA SUPRESIÓN

Los datos se suprimirán a los 30 días, salvo que exista alguna circunstancia que exija su conservación más allá de ese tiempo para atender posibles incidentes o responsabilidades

OBSERVACIONES

ANEXO II

ANÁLISIS DE RIESGOS

1. OBJETO DEL ANÁLISIS DE RIESGOS

Tanto Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales como el Reglamento General de Protección de Datos de Europa establece que, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad apropiado al riesgo que en su caso incluya:

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

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

Para dar cumplimiento a esto, **CLIMATIZACIÓN GUADALUPE, S.L.** ha realizado un análisis de riesgos documentado.

En el análisis de riesgos se han identificado, de forma metódica, las amenazas a las que los datos personales están expuestos, así como las vulnerabilidades que pueden aprovechar dichas amenazas para tener éxito.

Se ha estimado también el daño que podrían producir las distintas amenazas en caso de que se materializasen, así como la probabilidad de su ocurrencia.

Con estos datos se ha realizado una estimación del nivel de riesgo y se han tomado las decisiones pertinentes para gestionar estos riesgos implantando medidas de seguridad que eliminen o reduzcan aquellos riesgos que se ha decidido gestionar.

2. METODOLOGÍA DEL ANÁLISIS Y GESTIÓN DE RIESGOS

Para realizar un análisis de riesgos, es preciso, en primer lugar, definir la metodología para evaluar y gestionar los riesgos a que están expuestos los tratamientos de datos personales.

La evaluación y gestión de los riesgos se aplica a todos los tratamientos de datos personales que la entidad realice y sobre todos los activos que están involucrados en los mencionados tratamientos de datos personales.

A continuación se detalla la metodología utilizada para el análisis y gestión de los riesgos.

2.1 DEFINICIONES

Para comprender la metodología del análisis y gestión de riesgos se han de tener claros los siguientes conceptos:

- Análisis de riesgos: utilización sistemática de la información disponible para identificar los peligros y estimar los riesgos.
- Confidencialidad: es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

- Integridad: propiedad de la información, por la que se garantiza que no ha sido alterada de manera no autorizada.
- Disponibilidad: propiedad de la información, por la que se garantiza que está disponible para su uso a demanda de una entidad autorizada.
- Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información.
- Activo: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la seguridad de la información (son activos los datos, los servicios, las aplicaciones, los equipos, soportes, instalaciones o el personal, entre otros).
- Amenaza: toda circunstancia, evento o persona que tiene el potencial de causar daño en forma de robo, destrucción, divulgación, modificación de datos o denegación de servicio.
- Vulnerabilidad: debilidad o necesidad de un activo a través de la cuál una amenaza puede causar un daño.
- Impacto: es el daño que se produce al materializarse una amenaza.
- Nivel de riesgo: es la combinación de las consecuencias de un suceso (impacto) y de su probabilidad. Riesgo = Impacto x Probabilidad.
- Control: medida que modifica un riesgo.

2.2 EVALUACIÓN DE RIESGOS

2.2.1 PROCESO

El análisis de riesgos se implementa a través del Cuadro de análisis de riesgos. Dicho cuadro incluye:

- Todos los activos involucrados en el tratamiento de los datos personales.
- Las distintas amenazas a que están expuestos esos activos que podrían comprometer la confidencialidad, integridad o disponibilidad de la información.
- Las distintas vulnerabilidades que pueden aprovechar las mencionadas amenazas para causar su daño.
- El daño que se podría producir en caso de que las distintas amenazas se materializasen (impacto).
- La probabilidad estimada de que las distintas amenazas se materialicen aprovechando las vulnerabilidades identificadas.
- El nivel de riesgo estimado para cada par de amenaza-vulnerabilidad. Este nivel de riesgo de calcula en base al impacto y la probabilidad.

A continuación veremos detalladamente cómo se recopila la información necesaria en cada uno de estos ámbitos.

2.2.2 IDENTIFICACIÓN DE ACTIVOS

El primer paso que se debe dar en el análisis de riesgos es identificar todos los activos que están involucrados en el tratamiento de los datos personales. Es decir, todos los activos que pueden afectar la confidencialidad, integridad y disponibilidad de los datos personales que se tratan.

Los activos pueden ser documentos en papel o en formato electrónico, equipos informáticos, aplicaciones, bases de datos, personas, infraestructura o servicios externos, entre otros.

Se debe realizar un inventario de todos los activos involucrados en los distintos tratamientos de los datos personales, así como las dependencias entre los activos.

2.2.3 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

El siguiente paso es identificar todas las amenazas y vulnerabilidades que están relacionadas con cada uno de los activos antes identificados. Hay que contemplar todas las amenazas que puedan afectar a la confidencialidad, integridad o disponibilidad de los datos personales que se están tratando.

Cada activo puede estar relacionado con varias amenazas, y cada amenaza puede estar vinculada a varias vulnerabilidades.

2.2.4 VALORACIÓN DEL IMPACTO

Una vez se han identificado las amenazas, hay que valorar el daño (impacto) que se podría producir para los interesados de cuyos datos personales se están tratando, en caso de que las amenazas identificadas en el apartado anterior tengan éxito.

Para estimar el impacto, consideramos la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Reglamento General de Protección de Datos de Europa, indica una serie de factores o supuestos asociados a riesgos para los derechos y libertades de los interesados, se detallan aquí:

- El tratamiento puede provocar daños y perjuicios físicos, materiales o inmateriales.
- El tratamiento puede dar lugar a problemas de discriminación.
- El tratamiento puede dar lugar a problemas de usurpación de identidad o fraude.
- El tratamiento puede dar lugar a problemas de pérdidas financieras.
- El tratamiento puede dar lugar a problemas de daño para la reputación.
- El tratamiento puede dar lugar a problemas de pérdida de confidencialidad de datos sujetos al secreto profesional.
- El tratamiento puede dar lugar a problemas de reversión no autorizada de la seudonimización.
- El tratamiento puede dar lugar a un perjuicio económico o social significativo.
- Existe privación a los interesados de sus derechos y libertades.
- Se impide a los interesados ejercer el control sobre sus datos personales.
- Los datos revelan el origen ético o racial.
- Los datos revelan las opiniones políticas.
- Los datos revelan la religión o las creencias filosóficas.
- Los datos revelan la militancia en sindicatos.
- Se tratan datos relativos a la salud.
- Se tratan datos genéticos.
- Se tratan datos sobre la vida sexual.
- Se tratan datos sobre condenas e infracciones penales o medidas de seguridad conexas.
- Se evalúan aspectos personales.
- Se realiza el análisis o predicción de aspectos referidos al rendimiento en el trabajo.
- Se realiza el análisis o predicción de aspectos referidos a la situación económica.
- Se realiza el análisis o predicción de aspectos referidos a la salud.
- Se realiza el análisis o predicción de aspectos referidos a preferencias o intereses personales.
- Se realiza el análisis o predicción de aspectos referidos a la fiabilidad o el comportamiento.
- Se realiza el análisis o predicción de aspectos referidos a la situación o movimientos.
- Se tratan datos de personas vulnerables (en particular niños).
- El tratamiento implica una gran cantidad de datos personales y afecta a un gran número de interesados.

A la hora de estimar el impacto de ese tratamiento se ha valorado, de forma metódica, la concurrencia de que una o varias de estas situaciones afecten a cada uno de los tratamientos que la organización realiza.

La escala utilizada para valorar el impacto es la siguiente:

IMPACTO	DESCRIPCIÓN
Muy bajo	La pérdida de la confidencialidad, disponibilidad o integridad apenas afecta a los derechos y libertades de los interesados.
Bajo	La pérdida de la confidencialidad, disponibilidad o integridad afecta de forma leve a los derechos y libertades de los interesados de forma reducida.
Medio	Se da alguno de los factores o supuestos asociados a los riesgos indicados anteriormente, pero de forma muy reducida.
Alto	Se da alguno de los factores o supuestos asociados a los riesgos indicados anteriormente.
Muy alto	Concurren dos o más de los factores o supuestos asociados a los riesgos indicados anteriormente.

Para realizar el cálculo del nivel de riesgo, se debe trasladar el impacto valorado a lo largo de todos los activos involucrados en el tratamiento objeto del análisis de riesgos.

Si un mismo activo está involucrado en varios de los tratamientos que tienen distintos impactos, deberá considerarse el impacto mayor.

2.2.5 EVALUACIÓN DE LA PROBABILIDAD

Para calcular el riesgo, es también necesario evaluar la probabilidad de que se materialice cada una de las amenazas identificadas; es decir, la probabilidad de que una amenaza aproveche una vulnerabilidad del activo en cuestión para materializarse.

Los factores que hay que tener en cuenta para estimar la probabilidad son, entre otros, los siguientes:

- El contexto del tratamiento y de los activos involucrados (personal en la organización, accesibilidad de los activos, entorno, etc.).
- La frecuencia con que se presenta la amenaza.
- La vulnerabilidad del activo frente a la amenaza.
- El grado de exposición del activo a la amenaza.
- Lo apetecible o valiosa que es la información para terceros (que puede tener, o no, relación con el impacto valorado).
- El histórico de la organización (cuántas veces se ha materializado la amenaza anteriormente).

La escala utilizada para valorar la probabilidad es la siguiente:

PROBABILIDAD	DESCRIPCIÓN
Raro	Es raro que la amenaza se materialice aunque exista la vulnerabilidad.
Poco probable	Es poco probable que la amenaza se materialice aunque exista la vulnerabilidad.
Probable	Es probable que la amenaza se materialice aprovechando la vulnerabilidad.
Muy probable	Es muy probable que la amenaza se materialice aprovechando la vulnerabilidad.
Casi seguro	Es casi seguro que la amenaza se materialice aprovechando la vulnerabilidad.

Para realizar el cálculo de la probabilidad (y en su caso, del impacto) hay que realizarlo sin considerar las medidas de seguridad existentes.

Esto arrojará el riesgo "natural" de los activos a cada amenaza y vulnerabilidad identificadas si no hay medidas de seguridad que lo mitiguen.

2.2.6 CÁLCULO DEL NIVEL DE RIESGO

Una vez obtenidos los valores de impacto y probabilidad para cada uno de los pares de amenaza-vulnerabilidad, se realiza el cálculo del riesgo en función de esos valores, tal y como se indica a continuación:

Riesgo = Probabilidad x Impacto

(Probabilidad = Frecuencia de la Amenaza x Vulnerabilidad del Activo)

Como resultado, se obtendrá una matriz de riesgos como esta:

		PROBABILIDAD				
		Raro	**Poco probable**	**Probable**	**Muy probable**	**Casi seguro**
IMPACTO	**Muy bajo**	Muy bajo	Bajo	Bajo	Medio	Medio
	Bajo	Bajo	Bajo	Medio	Medio	Alto
	Medio	Bajo	Medio	Medio	Alto	Alto
	Alto	Medio	Medio	Alto	Alto	Muy alto
	Muy alto	Medio	Alto	Alto	Muy alto	Muy alto

2.3 GESTIÓN DE LOS RIESGOS

Una vez identificados los riesgos, debemos proceder a decidir qué riesgos vamos a gestionar y cómo vamos a llevar a cabo la gestión de dichos riesgos.

2.3.1 CRITERIOS DE DECISIÓN DE LOS RIESGOS QUE SE GESTIONAN

Se debe decidir qué riesgos se van a gestionar con objeto de reducir o eliminar dichos riesgos. Los criterios de decisión que se adoptan son los siguientes:

- Los riesgos de nivel Alto y Muy alto deben gestionarse en todos los casos para reducir o eliminar ese riesgo.
- Los riesgos de nivel Medio deben gestionarse en función del coste de las medidas de seguridad y/o controles que se deben aplicar para reducir o eliminar el riesgo.
- Los riesgos de nivel Muy bajo y Bajo deben gestionarse si el coste de las medidas de seguridad y/o controles a aplicar es reducido o escaso (por ejemplo, elaborar políticas, definir procedimientos, realizar copias de respaldo, etc.).

En el Cuadro de riesgos debe indicarse si el riesgo se gestiona, o no.

2.3.2 GESTIÓN DEL RIESGO

Para los riesgos que se ha decidido gestionar, se deben seleccionar una o más medidas de seguridad, organizativas y/o técnicas, que deben aplicarse para reducir el riesgo hasta un umbral aceptable.

La gestión de riesgos relacionados con procesos externalizados deben ser atendidos por medio de contratos de acceso a datos por cuenta de terceros, en los que se indique de forma detallada las medidas de seguridad que el encargado del tratamiento debe aplicar.

2.4 MEDIDAS DE SEGURIDAD

Como resultado de este proceso de análisis y gestión de riesgos, se habrá obtenido una relación de las medidas de seguridad, técnicas y organizativas, que el responsable del tratamiento debe implantar para garantizar un nivel de seguridad apropiado al riesgo.

Las medidas de seguridad obtenidas deben documentarse de forma suficiente e implantarse en la organización. También se revisará periódicamente su eficacia.

2.5 REVISIONES PERIÓDICAS

El responsable del tratamiento debe revisar los riesgos identificados y debe actualizar periódicamente el análisis y gestión de riesgos de acuerdo con los nuevos riesgos identificados.

La revisión se realizará al menos una vez al año, o con mayor frecuencia en caso de cambios significativos en la organización, en las operaciones de tratamiento realizadas, en la tecnología o en los medios empleados.

2.6 INFORMES

El responsable del tratamiento documentará los resultados del análisis y gestión de los riesgos, y de todas las revisiones subsiguientes, en el informe de análisis de riesgos.

3. PROCESO DE ANÁLISIS Y GESTIÓN DE RIESGOS

Todo el proceso de análisis y gestión de riesgos ha sido realizado de acuerdo a la metodología de análisis y gestión de riesgos detallada en el apartado anterior.

3.1 OBJETIVO DEL ANÁLISIS Y LA GESTIÓN DE RIESGOS

El objetivo del análisis de riesgos es identificar, de forma metódica, todos los activos involucrados en el tratamiento de datos personales en la organización, así como sus vulnerabilidades y las amenazas que pueden aprovechar esas vulnerabilidades para causar un daño.

El objetivo de la gestión de riesgos es definir, a través de medios sistemáticos, las medidas de seguridad y controles que son necesarios para eliminar o mitigar los riesgos identificados.

3.2 RECOLECCIÓN DE LA INFORMACIÓN

Durante el análisis de riesgos, se obtuvo la información a través de entrevistas con las personas responsables de los activos y/o de la seguridad de los activos.

3.3 BREVE RESUMEN DE LA METODOLOGÍA APLICADA

De forma resumida, el proceso se realizó de la siguiente manera:

1. Se identificaron los tratamientos objeto del análisis, así como las categorías de datos tratadas y las finalidades de dichos tratamientos. Dicha información consta en el Registro de Actividades de Tratamiento.
2. Se identificaron los distintos activos involucrados en el tratamiento de los datos personales.
3. Se identificaron las amenazas para cada activo así como la dimensión de la seguridad (confidencialidad, integridad y disponibilidad) que podría ser afectada por cada amenaza.
4. Se identificaron las correspondientes vulnerabilidades para cada amenaza.
5. Se evaluó, con valores entre "Muy Bajo" a "Muy alto", el impacto en cada uno de los tratamientos por la pérdida de confidencialidad, integridad y disponibilidad según los criterios detallados en el punto 2.2.4.
6. Se evaluó, con valores entre "Muy bajo" a "Muy alto", la probabilidad de que se materializara cada una de las amenazas, aprovechando las vulnerabilidades existentes según los criterios detallados en el punto 2.2.5.
7. Se calculó el nivel de riesgo multiplicando el impacto por la probabilidad de su ocurrencia. El cuadro del punto 2.2.6. muestra los distintos resultados de esta operación.
8. Se decidieron los riesgos que se van a gestionar según los criterios indicados en el punto 2.3.1.
9. Para cada uno de los riesgos que se decidió gestionar, se identificaron los controles que deberían implantarse para reducir los riesgos a un umbral aceptable.
10. Los controles identificados se sustanciaron en medidas de seguridad concretas, tanto técnicas como organizativas, que es necesario implantar en la organización para lograr los objetivos de los controles.
11. Se asociaron las medidas de seguridad con los activos sobre los que debían aplicarse dichas medidas.
12. Se documentó cada una de las medidas de seguridad de forma suficiente para su implantación en la organización.

A continuación, detallamos cada una de las operaciones anteriores realizadas.

3.4 TRATAMIENTOS INCLUIDOS EN EL ANÁLISIS

El análisis y gestión de riesgos se ha realizado sobre los siguientes tratamientos:

TRATAMIENTO	FINALIDAD
GESTIÓN DE ACCIDENTES LABORALES	Gestión de los partes de accidentes laborales y su comunicación a los organismos pertinentes
GESTIÓN DE CLIENTES	Gestión fiscal, contable y administrativa de clientes, así como el envío de comunicaciones comerciales
GESTIÓN DE PERSONAL	Gestión de recursos humanos, nóminas y prevención de riesgos laborales
GESTIÓN DE POTENCIALES CLIENTES	Gestión de potenciales clientes y contactos con los que se prevé mantener una relación comercial
GESTIÓN DE PROVEEDORES	Gestión fiscal, contable y administrativa de proveedores
SELECCIÓN DE PERSONAL	Gestión de los Currículum Vitae recibidos, así como los procesos de selección de personal
VIDEOVIGILANCIA	Videovigilancia de las instalaciones y seguridad privada

El detalle de las categorías de datos personales que se tratan, las categorías de interesados y demás información sobre cada uno de los tratamientos, encuentra en el Registro de Actividades de Tratamiento.

3.5 ACTIVOS INVOLUCRADOS EN LOS TRATAMIENTOS

Los activos involucrados en los tratamientos de datos personales identificados en el punto anterior son los siguientes:

ACTIVO	TIPO	DESCRIPCIÓN	TRATAMIENTOS
APLICACIONES	Aplicaciones (software)	Software	GESTIÓN DE CLIENTES, GESTIÓN DE PERSONAL, GESTIÓN DE PROVEEDORES,
COMUNICACIONES	Comunicaciones (routers ADSL, fibra, ...)	Comunicaciones	GESTIÓN DE CLIENTES, GESTIÓN DE PERSONAL, GESTIÓN DE PROVEEDORES,
DATOS	Datos / Información	Tratamiento de la información	GESTIÓN DE CLIENTES, GESTIÓN DE PERSONAL, GESTIÓN DE PROVEEDORES,
DOCUMENTOS	Documentación (papel)	Documentos(archivadores en estanterías o armarios)	GESTIÓN DE CLIENTES, GESTIÓN DE PERSONAL, GESTIÓN DE PROVEEDORES,
EQUIPAMIENTO	Equipamiento auxiliar (Impresora, destructora, ...)	Equipos, impresoras...	GESTIÓN DE CLIENTES, GESTIÓN DE PERSONAL, GESTIÓN DE PROVEEDORES,
EQUIPOS	Equipos (hardware)	Equipos	GESTIÓN DE CLIENTES, GESTIÓN DE PERSONAL, GESTIÓN DE PROVEEDORES,
INSTALACIONES	Instalaciones / Recintos	Instalaciones	GESTIÓN DE ACCIDENTES LABORALES, GESTIÓN DE CLIENTES, GESTIÓN DE PERSONAL, GESTIÓN DE POTENCIALES CLIENTES, GESTIÓN DE PROVEEDORES, SELECCIÓN DE PERSONAL, VIDEOVIGILANCIA
INTERNET	Servicios externos (hosting, mail, SaaS, ...)	Internet	GESTIÓN DE CLIENTES, GESTIÓN DE PERSONAL, GESTIÓN DE POTENCIALES CLIENTES, GESTIÓN DE PROVEEDORES,
PERSONAL	Personas / Usuarios	Personas y usuarios	GESTIÓN DE PERSONAL,
SOPORTES	Soportes (digitales)	Soporte de almacenamiento de datos o medio de almacenamiento físico	INFORMACIÓN CON DATOS
VIDEOVIGILANCIA	Cámaras de videovigilancia	Videovigilancia y seguridad	VIDEOVIGILANCIA

Dichos activos se encuentran en las siguientes sedes:

SEDE DE LA EMPRESA, **Camino de los Raspajines 1 1F, 30107-Aljucer (Murcia)** (ESPAÑA).

3.6 IDENTIFICACIÓN DE LAS AMENAZAS

Las amenazas que afectan a cada uno de los activos identificados en el punto anterior, así como las dimensiones de la seguridad de la información que podrían resultar afectadas si la amenaza se materializa, son las siguientes:

ACTIVO	AMENAZAS	DIMENSIONES AFECTADAS
APLICACIONES Aplicaciones (software)	Acceso no autorizado	C | I | D
	Destrucción de información por avería o accidente	D
	Vulnerabilidades en equipos, programas y dispositivos	C | I | D
	Acceso excesivo a la información	C | I | D
	Intentos reiterados de acceso no autorizado	C | I | D
	Errores de los usuarios	C | I | D
	Errores de los administradores	C | I | D
COMUNICACIONES Comunicaciones (routers ADSL, fibra, ...)	Vulnerabilidades en equipos, programas y dispositivos	C | I | D
	Acceso no autorizado a la red WIFI	C | I | D
	Acceso no autorizado al dispositivo	C
ACTIVO	AMENAZAS	DIMENSIONES AFECTADAS
DATOS Datos / Información	Acceso no autorizado	C | I | D
	Destrucción de información por avería o accidente	D
	Acceso no autorizado a la información almacenada o transmitida	C | I
	Acceso excesivo a la información	C | I | D
	Errores de los usuarios	C | I | D
	Errores de los administradores	C | I | D
DOCUMENTOS Documentación (papel)	Acceso no autorizado	C | I | D
	Destrucción no segura de documentación	C
	Robo	C | I | D
EQUIPAMIENTO Equipamiento auxiliar (Impresora, destructora, ...)	Robo	C | I | D
EQUIPOS Equipos (hardware)	Acceso no autorizado	C | I | D
	Destrucción de información por avería o accidente	D
	Destrucción no segura o reutilización de equipos y soportes	C
	Robo	C | I | D
	Ejecución de software malicioso (malware)	C | I | D
	Vulnerabilidades en equipos, programas y dispositivos	C | I | D
	Acceso no autorizado a la información almacenada o transmitida	C | I
	Acceso remoto no autorizado	C | I | D
INSTALACIONES Instalaciones / Recintos	Daños por fuego	D
	Daños por agua	D
	Tratamiento no seguro fuera de los locales	C | I | D
	Desastres (incendio, inundación, terremoto, ...)	C | I | D
	Acceso no autorizado	C | I | D
	AMENAZAS	DIMENSIONES AFECTADAS
INTERNET Servicios externos (hosting, mail, SaaS, ...)	Acceso no autorizado	C | I | D
	Errores de los usuarios	C | I | D
	Errores de los administradores	C | I | D
PERSONAL Personas / Usuarios	Descontrol en el acceso a datos personales	C | I | D
	Incumplimiento de la normativa de protección de datos	C

ACTIVO	AMENAZAS	DIMENSIONES AFECTADAS
	Revelación de información	C
SOPORTES Soportes (digitales)	Destrucción de información por avería o accidente	D
	Destrucción no segura o reutilización de equipos y soportes	C
	Robo	C | I | D
	Acceso no autorizado	C | I | D
	Descontrol en la gestión de soportes	C | I | D
	Acceso no autorizado a la información almacenada o transmitida	C | I
	Errores de los usuarios	C | I | D
	Errores de los administradores	C | I | D
	Degradación de los soportes	D
VIDEOVIGILANCIA Cámaras de videovigilancia	Acceso no autorizado a las cámaras de videovigilancia	C
	Uso inadecuado de cámaras de videovigilancia	C

(C: Confidencialidad; D: Disponibilidad; I: Integridad)

3.7 IDENTIFICACIÓN DE LAS VULNERABILIDADES

Las vulnerabilidades que afectan a cada uno de los activos identificados en el punto anterior, son las siguientes:

ACTIVO	AMENAZAS	VULNERABILIDADES
APLICACIONES Aplicaciones (software)	Acceso excesivo a la información	No se registran los accesos a la información
	Acceso no autorizado	Deficiente política de contraseñas
		Ausencia o deficiente sistema de autenticación
		No se limita el número de intentos de acceso no autorizado
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente
	Errores de los administradores	Deficiencias en la formación del personal
	Errores de los usuarios	Deficiencias en la formación del personal
	Intentos reiterados de acceso no autorizado	No se registran los accesos a la información
	Vulnerabilidades en equipos, programas y dispositivos	Deficiente actualización de equipos
COMUNICACIONES Comunicaciones (routers ADSL, fibra, ...)	Acceso no autorizado a la red WIFI	Red WIFI no segura
	Acceso no autorizado al dispositivo	Deficiente política de contraseñas
		Ausencia o deficiente sistema de autenticación
	Vulnerabilidades en equipos, programas y dispositivos	Deficiente actualización de equipos
DATOS Datos / Información	Acceso excesivo a la información	No se registran los accesos a la información
	Acceso no autorizado	Deficiente política de contraseñas
		Ausencia o deficiente sistema de autenticación
		No se limita el número de intentos de acceso no autorizado
	Acceso no autorizado a la información almacenada o transmitida	Ausencia de cifrado
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente
	Errores de los administradores	Deficiencias en la formación del personal
	Errores de los usuarios	Deficiencias en la formación del personal
DOCUMENTOS Documentación (papel)	Acceso no autorizado	Copia o reproducción sin control
		Almacenamiento en dispositivos no seguros
		Ausencia de protocolos para el traslado seguro de soportes y documentos
		Inadecuada protección física del área
	Destrucción no segura de documentación	Ausencia de protocolos para la destrucción de documentación
	Robo	Deficiencias en la seguridad física
EQUIPAMIENTO Equipamiento auxiliar (Impresora, destructora, ...) EQUIPOS Equipos (hardware)	Robo	Deficiencias en la seguridad física
	Acceso no autorizado	Deficiente política de contraseñas
		Ausencia o deficiente sistema de autenticación
		No se limita el número de intentos de acceso no autorizado
	Acceso no autorizado a la información almacenada o transmitida	Ausencia de cifrado
	Acceso remoto no autorizado	Deficiencias en la seguridad del acceso remoto
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente
	Destrucción no segura o reutilización de equipos y soportes	Ausencia de protocolos para la destrucción y reutilización de equipos y soportes
	Ejecución de software malicioso (malware)	Ausencia de software anti-malware
	Robo	Deficiencias en la seguridad física
	Vulnerabilidades en equipos, programas y dispositivos	Deficiente actualización de equipos
INSTALACIONES Instalaciones / Recintos	Acceso no autorizado	No se restringe el acceso (no hay cerradura)
	Daños por agua	Ubicación no preparada para inundaciones o fugas de agua
	Daños por fuego	Ausencia de extintores o sistema anti-incendios
	Desastres (incendio, inundación, terremoto, ...)	Ausencia de copia de copia de respaldo remota
	Tratamiento no seguro fuera de los locales	Ausencia de política de trabajo fuera de los locales

INTERNET Servicios externos (hosting, mail, SaaS, ...)	Acceso no autorizado	Deficiente política de contraseñas
		Ausencia o deficiente sistema de autenticación
		No se limita el número de intentos de acceso no autorizado
	Errores de los administradores	Deficiencias en la formación del personal
	Errores de los usuarios	Deficiencias en la formación del personal
PERSONAL Personas / Usuarios	Descontrol en el acceso a datos personales	Ausencia de Política de control de acceso
		Falta de definición sobre quién debe acceder a qué
	Incumplimiento de la normativa de protección de datos	Deficiencias en la formación del personal
	Revelación de información	Ausencia de compromiso de confidencialidad y deber de secreto
SOPORTES Soportes (digitales)	Acceso no autorizado	Almacenamiento en dispositivos no seguros
		Ausencia de protocolos para el traslado seguro de soportes y documentos
		Inadecuada protección física del área
	Acceso no autorizado a la información almacenada o transmitida	Ausencia de cifrado
	Degradación de los soportes	Deficiente control de la degradación de los soportes
	Descontrol en la gestión de soportes	Ausencia de un inventario de soportes
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente
	Destrucción no segura o reutilización de equipos y soportes	Ausencia de protocolos para la destrucción y reutilización de equipos y soportes
	Errores de los administradores	Deficiencias en la formación del personal
	Errores de los usuarios	Deficiencias en la formación del personal
	Robo	Deficiencias en la seguridad física
VIDEOVIGILANCIA Cámaras de videovigilancia	Acceso no autorizado a las cámaras de videovigilancia	Deficiente política de contraseñas
		Ausencia o deficiente sistema de autenticación
	Uso inadecuado de cámaras de videovigilancia	Desconocimiento del uso adecuado de las cámaras

ACTIVO	AMENAZAS	VULNERABILIDADES
SOPORTES Soportes (digitales)	Acceso no autorizado	Almacenamiento en dispositivos no seguros
		Ausencia de protocolos para el traslado seguro de soportes y documentos
		Inadecuada protección física del área
	Acceso no autorizado a la información almacenada o transmitida	Ausencia de cifrado
	Degradación de los soportes	Deficiente control de la degradación de los soportes
	Descontrol en la gestión de soportes	Ausencia de un inventario de soportes
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente
	Destrucción no segura o reutilización de equipos y soportes	Ausencia de protocolos para la destrucción y reutilización de equipos y soportes
	Errores de los administradores	Deficiencias en la formación del personal
	Errores de los usuarios	Deficiencias en la formación del personal
	Robo	Deficiencias en la seguridad física
VIDEOVIGILANCIA Cámaras de videovigilancia	Acceso no autorizado a las cámaras de videovigilancia	Deficiente política de contraseñas
		Ausencia o deficiente sistema de autenticación

	Uso inadecuado de cámaras de videovigilancia	Desconocimiento del uso adecuado de las cámaras

3.8 VALORACIÓN DEL IMPACTO

El impacto que se podría producir en los distintos tratamientos de datos personales en caso de que se materializase alguna de las amenazas detalladas en el apartado anterior, así como los factores o supuestos asociados a riesgos para los derechos y libertades de los interesados, indicados en el apartado 2.2.4., se detallan a continuación:

TRATAMIENTO	IMPACTO	Factores o supuestos asociados a riesgos
GESTIÓN DE ACCIDENTES LABORALES	Bajo	No existen
GESTIÓN DE CLIENTES	Bajo	No existen
GESTIÓN DE PERSONAL	Bajo	No existen
GESTIÓN DE POTENCIALES CLIENTES	Bajo	No existen
GESTIÓN DE PROVEEDORES	Bajo	No existen
SELECCIÓN DE PERSONAL	Bajo	No existen
VIDEOVIGILANCIA	Medio	No existen

3.9 EVALUACIÓN DE LA PROBABILIDAD

La probabilidad estimada de que cada una de las amenazas identificadas en el apartado 3.6., aproveche la correspondiente vulnerabilidad del activo en cuestión para materializarse, se detalla a continuación:

ACTIVO	AMENAZAS	VULNERABILIDADES	PROB.
APLICACIONES Aplicaciones (software)	Acceso excesivo a la información	No se registran los accesos a la información	Probable
	Acceso no autorizado	Deficiente política de contraseñas	Probable
		Ausencia o deficiente sistema de autenticación	Probable
		No se limita el número de intentos de acceso no autorizado	Probable
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente	Probable
	Errores de los administradores	Deficiencias en la formación del personal	Probable
	Errores de los usuarios	Deficiencias en la formación del personal	Probable
	Intentos reiterados de acceso no autorizado	No se registran los accesos a la información	Probable
	Vulnerabilidades en equipos, programas y dispositivos	Deficiente actualización de equipos	Probable

ACTIVO	AMENAZAS	VULNERABILIDADES	PROB.
COMUNICACIONES Comunicaciones (routers ADSL, fibra, ...)	Acceso no autorizado a la red WIFI	Red WIFI no segura	Probable
	Acceso no autorizado al dispositivo	Deficiente política de contraseñas	Probable
		Ausencia o deficiente sistema de autenticación	Probable
	Vulnerabilidades en equipos, programas y dispositivos	Deficiente actualización de equipos	Probable
DATOS Datos / Información	Acceso excesivo a la información	No se registran los accesos a la información	Probable
	Acceso no autorizado	Deficiente política de contraseñas	Probable
		Ausencia o deficiente sistema de autenticación	Probable
		No se limita el número de intentos de acceso no autorizado	Probable
	Acceso no autorizado a la información almacenada o transmitida	Ausencia de cifrado	Probable
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente	Probable
	Errores de los administradores	Deficiencias en la formación del personal	Probable
	Errores de los usuarios	Deficiencias en la formación del personal	Probable
DOCUMENTOS Documentación (papel)	Acceso no autorizado	Copia o reproducción sin control	Probable
		Almacenamiento en dispositivos no seguros	Probable
		Ausencia de protocolos para el traslado seguro de soportes y documentos	Probable
		Inadecuada protección física del área	Probable
	Destrucción no segura de documentación	Ausencia de protocolos para la destrucción de documentación	Probable
	Robo	Deficiencias en la seguridad física	Probable
EQUIPAMIENTO Equipamiento auxiliar (Impresora, destructora, ...)	Robo	Deficiencias en la seguridad física	Probable
EQUIPOS Equipos (hardware)	Acceso no autorizado	Deficiente política de contraseñas	Probable
		Ausencia o deficiente sistema de autenticación	Probable
		No se limita el número de intentos de acceso no autorizado	Probable
	Acceso no autorizado a la información almacenada o transmitida	Ausencia de cifrado	Probable
	Acceso remoto no autorizado	Deficiencias en la seguridad del acceso remoto	Probable
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente	Probable
	Destrucción no segura o reutilización de equipos y soportes	Ausencia de protocolos para la destrucción y reutilización de equipos y soportes	Probable
	Ejecución de software malicioso (malware)	Ausencia de software anti-malware	Probable
	Robo	Deficiencias en la seguridad física	Probable
	Vulnerabilidades en equipos, programas y dispositivos	Deficiente actualización de equipos	Probable
INSTALACIONES	Acceso no autorizado	No se restringe el acceso (no hay	Probable

ACTIVO	AMENAZAS	VULNERABILIDADES	PROB.
Instalaciones / Recintos		cerradura)	
	Daños por agua	Ubicación no preparada para inundaciones o fugas de agua	Probable
	Daños por fuego	Ausencia de extintores o sistema anti-incendios	Probable
	Desastres (incendio, inundación, terremoto, ...)	Ausencia de copia de copia de respaldo remota	Probable
	Tratamiento no seguro fuera de los locales	Ausencia de política de trabajo fuera de los locales	Probable
INTERNET Servicios externos (hosting, mail, SaaS, ...)	Acceso no autorizado	Deficiente política de contraseñas	Probable
		Ausencia o deficiente sistema de autenticación	Probable
		No se limita el número de intentos de acceso no autorizado	Probable
	Errores de los administradores	Deficiencias en la formación del personal	Probable
	Errores de los usuarios	Deficiencias en la formación del personal	Probable
PERSONAL Personas / Usuarios	Descontrol en el acceso a datos personales	Ausencia de Política de control de acceso	Probable
		Falta de definición sobre quién debe acceder a qué	Probable
	Incumplimiento de la normativa de protección de datos	Deficiencias en la formación del personal	Probable
	Revelación de información	Ausencia de compromiso de confidencialidad y deber de secreto	Probable
SOPORTES Soportes (digitales)	Acceso no autorizado	Almacenamiento en dispositivos no seguros	Probable
		Ausencia de protocolos para el traslado seguro de soportes y documentos	Probable
		Inadecuada protección física del área	Probable
	Acceso no autorizado a la información almacenada o transmitida	Ausencia de cifrado	Probable
	Degradación de los soportes	Deficiente control de la degradación de los soportes	Probable
	Descontrol en la gestión de soportes	Ausencia de un inventario de soportes	Probable
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente	Probable
	Destrucción no segura o reutilización de equipos y soportes	Ausencia de protocolos para la destrucción y reutilización de equipos y soportes	Probable
	Errores de los administradores	Deficiencias en la formación del personal	Probable
	Errores de los usuarios	Deficiencias en la formación del personal	Probable
	Robo	Deficiencias en la seguridad física	Probable
VIDEOVIGILANCIA Cámaras de videovigilancia	Acceso no autorizado a las cámaras de videovigilancia	Deficiente política de contraseñas	Probable
		Ausencia o deficiente sistema de autenticación	Probable
	Uso inadecuado de cámaras de videovigilancia	Desconocimiento del uso adecuado de las cámaras	Probable

3.10 CÁLCULO DEL NIVEL DE RIESGO

El nivel de riesgo para cada uno de los activos es el resultado del impacto (en función de los tratamientos en los que está involucrado) por la probabilidad de que las amenazas aprovechen las vulnerabilidades para materializarse.

Para realizar el cálculo del nivel de riesgo, se ha trasladado el impacto valorado en el punto 3.8, a lo largo de todos los activos involucrados en esos tratamientos (que están descritos en el punto 3.5).

Si un mismo activo está involucrado en varios tratamientos que tienen distintos impactos, se ha trasladado el impacto mayor de los tratamientos en los que está involucrado el activo en cuestión.

El resultado el siguiente Cuadro de riesgos:

ACTIVO	AMENAZAS	VULNERABILIDADES	IMPA.	PROB.	RIES.
APLICACIONES Aplicaciones (software)	Acceso excesivo a la información	No se registran los accesos a la información	Medio	Probable	Medio
	Acceso no autorizado	Ausencia o deficiente sistema de autenticación		Probable	Medio
		Deficiente política de contraseñas		Probable	Medio
		No se limita el número de intentos de acceso no autorizado		Probable	Medio
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente		Probable	Medio
	Errores de los administradores	Deficiencias en la formación del personal		Probable	Medio
	Errores de los usuarios	Deficiencias en la formación del personal		Probable	Medio
	Intentos reiterados de acceso no autorizado	No se registran los accesos a la información		Probable	Medio
	Vulnerabilidades en equipos, programas y dispositivos	Deficiente actualización de equipos		Probable	Medio
COMUNICACIONES Comunicaciones (routers ADSL, fibra, ...)	Acceso no autorizado a la red WIFI	Red WIFI no segura	Medio	Probable	Medio
	Acceso no autorizado al dispositivo	Ausencia o deficiente sistema de autenticación		Probable	Medio
		Deficiente política de contraseñas		Probable	Medio
	Vulnerabilidades en equipos, programas y dispositivos	Deficiente actualización de equipos		Probable	Medio
DATOS Datos / Información	Acceso excesivo a la información	No se registran los accesos a la información	Medio	Probable	Medio
	Acceso no autorizado	Ausencia o deficiente sistema de autenticación		Probable	Medio
		Deficiente política de contraseñas		Probable	Medio
		No se limita el número de intentos de acceso no autorizado		Probable	Medio
	Acceso no autorizado a la información almacenada o transmitida	Ausencia de cifrado		Probable	Medio
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente		Probable	Medio
	Errores de los	Deficiencias en la formación del		Probable	Medio

ACTIVO	AMENAZAS	VULNERABILIDADES	IMPA.	PROB.	RIES.
	administradores	personal			
	Errores de los usuarios	Deficiencias en la formación del personal		Probable	Medio
DOCUMENTOS Documentación (papel)	Acceso no autorizado	Almacenamiento en dispositivos no seguros	Medio	Probable	Medio
		Ausencia de protocolos para el traslado seguro de soportes y documentos		Probable	Medio
		Copia o reproducción sin control		Probable	Medio
		Inadecuada protección física del área		Probable	Medio
	Destrucción no segura de documentación	Ausencia de protocolos para la destrucción de documentación		Probable	Medio
	Robo	Deficiencias en la seguridad física		Probable	Medio
EQUIPAMIENTO Equipamiento auxiliar (Impresora, destructora, ...)	Robo	Deficiencias en la seguridad física	Medio	Probable	Medio
EQUIPOS Equipos (hardware)	Acceso no autorizado	Ausencia o deficiente sistema de autenticación	Medio	Probable	Medio
		Deficiente política de contraseñas		Probable	Medio
		No se limita el número de intentos de acceso no autorizado		Probable	Medio
	Acceso no autorizado a la información almacenada o transmitida	Ausencia de cifrado		Probable	Medio
	Acceso remoto no autorizado	Deficiencias en la seguridad del acceso remoto		Probable	Medio
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente		Probable	Medio
	Destrucción no segura o reutilización de equipos y soportes	Ausencia de protocolos para la destrucción y reutilización de equipos y soportes		Probable	Medio
	Ejecución de software malicioso (malware)	Ausencia de software anti-malware		Probable	Medio
	Robo	Deficiencias en la seguridad física		Probable	Medio
	Vulnerabilidades en equipos, programas y dispositivos	Deficiente actualización de equipos		Probable	Medio
INSTALACIONES Instalaciones / Recintos	Acceso no autorizado	No se restringe el acceso (no hay cerradura)	Medio	Probable	Medio
	Daños por agua	Ubicación no preparada para inundaciones o fugas de agua		Probable	Medio
	Daños por fuego	Ausencia de extintores o sistema anti-incendios		Probable	Medio
	Desastres (incendio, inundación, terremoto, ...)	Ausencia de copia de copia de respaldo remota		Probable	Medio
	Tratamiento no seguro fuera de los locales	Ausencia de política de trabajo fuera de los locales		Probable	Medio
INTERNET Servicios externos (hosting, mail, SaaS, ...)	Acceso no autorizado	Ausencia o deficiente sistema de autenticación	Medio	Probable	Medio
		Deficiente política de contraseñas		Probable	Medio

ACTIVO	AMENAZAS	VULNERABILIDADES	IMPA.	PROB.	RIES.
		No se limita el número de intentos de acceso no autorizado		Probable	Medio
	Errores de los administradores	Deficiencias en la formación del personal		Probable	Medio
	Errores de los usuarios	Deficiencias en la formación del personal		Probable	Medio
PERSONAL Personas / Usuarios	Descontrol en el acceso a datos personales	Ausencia de Política de control de acceso	Bajo	Probable	Medio
		Falta de definición sobre quién debe acceder a qué		Probable	Medio
	Incumplimiento de la normativa de protección de datos	Deficiencias en la formación del personal		Probable	Medio
	Revelación de información	Ausencia de compromiso de confidencialidad y deber de secreto		Probable	Medio
SOPORTES Soportes (digitales)	Acceso no autorizado	Almacenamiento en dispositivos no seguros	Medio	Probable	Medio
		Ausencia de protocolos para el traslado seguro de soportes y documentos		Probable	Medio
		Inadecuada protección física del área		Probable	Medio
	Acceso no autorizado a la información almacenada o transmitida	Ausencia de cifrado		Probable	Medio
	Degradación de los soportes	Deficiente control de la degradación de los soportes		Probable	Medio
	Descontrol en la gestión de soportes	Ausencia de un inventario de soportes		Probable	Medio
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente		Probable	Medio
	Destrucción no segura o reutilización de equipos y soportes	Ausencia de protocolos para la destrucción y reutilización de equipos y soportes		Probable	Medio
	Errores de los administradores	Deficiencias en la formación del personal		Probable	Medio
	Errores de los usuarios	Deficiencias en la formación del personal		Probable	Medio
	Robo	Deficiencias en la seguridad física		Probable	Medio
VIDEOVIGILANCIA Cámaras de videovigilancia	Acceso no autorizado a las cámaras de videovigilancia	Ausencia o deficiente sistema de autenticación	Medio	Probable	Medio
		Deficiente política de contraseñas		Probable	Medio
	Uso inadecuado de cámaras de videovigilancia	Desconocimiento del uso adecuado de las cámaras		Probable	Medio

3.11 RIESGOS QUE SE VAN A GESTIONAR

Según los criterios indicados en el punto 2.3.1. se ha decidido gestionar los siguientes riesgos:

ACTIVO	AMENAZAS	VULNERABILIDADES	IMPA.	PROB.	RIES.
APLICACIONES Aplicaciones (software)	Acceso no autorizado	Ausencia o deficiente sistema de autenticación	Medio	Probable	Medio
		Deficiente política de contraseñas		Probable	Medio

ACTIVO	AMENAZAS	VULNERABILIDADES	IMPA.	PROB.	RIES.
	Destrucción de información por avería o accidente	Ausencia de copia de respaldo reciente		Probable	Medio
		Deficiencias en la formación del personal		Probable	Medio
		Deficiencias en la formación del personal		Probable	Medio
		Deficiente actualización de equipos		Probable	Medio
COMUNICACIONES Comunicaciones (routers ADSL, fibra, ...)		Red WIFI no segura	Medio	Probable	Medio
	Acceso no autorizado al dispositivo	Ausencia o deficiente sistema de autenticación		Probable	Medio
		Deficiente política de contraseñas		Probable	Medio
		Deficiente actualización de equipos		Probable	Medio
DATOS Datos / Información	Acceso no autorizado	Ausencia o deficiente sistema de autenticación	Medio	Probable	Medio
		Deficiente política de contraseñas		Probable	Medio
		Ausencia de copia de respaldo reciente		Probable	Medio
		Deficiencias en la formación del personal		Probable	Medio
		Deficiencias en la formación del personal		Probable	Medio
DOCUMENTOS Documentación (papel)	Acceso no autorizado	Almacenamiento en dispositivos no seguros	Medio	Probable	Medio
		Ausencia de protocolos para el traslado seguro de soportes y documentos		Probable	Medio
		Ausencia de protocolos para la destrucción de documentación		Probable	Medio
		Deficiencias en la seguridad física		Probable	Medio
		Deficiencias en la seguridad física		Probable	Medio
EQUIPOS Equipos (hardware)	Acceso no autorizado	Ausencia o deficiente sistema de autenticación	Medio	Probable	Medio
		Deficiente política de contraseñas		Probable	Medio
		Deficiencias en la seguridad del acceso remoto		Probable	Medio
		Ausencia de copia de respaldo reciente		Probable	Medio
		Ausencia de protocolos para la destrucción y reutilización de equipos y soportes		Probable	Medio
		Ausencia de software anti-malware		Probable	Medio
		Deficiencias en la seguridad física		Probable	Medio
		Deficiente actualización de equipos		Probable	Medio
INSTALACIONES Instalaciones / Recintos		Ubicación no preparada para inundaciones o fugas de agua	Medio	Probable	Medio
		Ausencia de extintores o sistema		Probable	Medio

ACTIVO	AMENAZAS	VULNERABILIDADES	IMPA.	PROB.	RIES.
		anti-incendios			
		Ausencia de política de trabajo fuera de los locales		Probable	Medio
INTERNET Servicios externos (hosting, mail, SaaS, ...)	Acceso no autorizado	Ausencia o deficiente sistema de autenticación	Medio	Probable	Medio
		Deficiente política de contraseñas		Probable	Medio
		Deficiencias en la formación del personal		Probable	Medio
		Deficiencias en la formación del personal		Probable	Medio
PERSONAL Personas / Usuarios	Descontrol en el acceso a datos personales	Ausencia de Política de control de acceso	Bajo	Probable	Medio
		Falta de definición sobre quién debe acceder a qué		Probable	Medio
		Deficiencias en la formación del personal		Probable	Medio
		Ausencia de compromiso de confidencialidad y deber de secreto		Probable	Medio
SOPORTES Soportes (digitales)	Acceso no autorizado	Almacenamiento en dispositivos no seguros	Medio	Probable	Medio
		Ausencia de protocolos para el traslado seguro de soportes y documentos		Probable	Medio
		Ausencia de copia de respaldo reciente		Probable	Medio
		Ausencia de protocolos para la destrucción y reutilización de equipos y soportes		Probable	Medio
		Deficiencias en la formación del personal		Probable	Medio
		Deficiencias en la formación del personal		Probable	Medio
		Deficiencias en la seguridad física		Probable	Medio
VIDEOVIGILANCIA Cámaras de videovigilancia	Acceso no autorizado a las cámaras de videovigilancia	Ausencia o deficiente sistema de autenticación	Medio	Probable	Medio
		Deficiente política de contraseñas		Probable	Medio
	Uso inadecuado de cámaras de videovigilancia	Desconocimiento del uso adecuado de las cámaras		Probable	Medio

3.12 IDENTIFICACIÓN DE LOS CONTROLES A IMPLANTAR

Una vez que se han seleccionado los riesgos que se van a gestionar (punto 3.11), se han identificado los controles apropiados para mitigar las vulnerabilidades asociadas a las correspondientes amenazas y riesgos.

Los controles identificados son los siguientes:

VULNERABILIDAD	CONTROL
Almacenamiento en dispositivos no seguros	Los dispositivos de almacenamiento deben tener el acceso restringido
Ausencia de compromiso de confidencialidad y deber de secreto	Compromiso de confidencialidad y deber de secreto

VULNERABILIDAD	CONTROL
Ausencia de copia de respaldo reciente	Disponer de una política de copias de respaldo y recuperación
Ausencia de extintores o sistema anti-incendios	Colocar extintores o sistema anti-incendios
Ausencia de Política de control de acceso	Disponer de una política de control de acceso
Ausencia de política de trabajo fuera de los locales	Disponer de una política de trabajo fuera de los locales
Ausencia de protocolos para el traslado seguro de soportes y documentos	Definir protocolos para el traslado seguro de soportes y documentos
Ausencia de protocolos para la destrucción de documentación	Disponer de protocolos para la destrucción de documentación
Ausencia de protocolos para la destrucción y reutilización de equipos y soportes	Disponer de protocolos para la destrucción y reutilización de equipos y soportes
Ausencia de software anti-malware	Los equipos deben tener instalados un software anti-malware
Ausencia o deficiente sistema de autenticación	Implantar un sistema de identificación y autenticación seguro
Deficiencias en la formación del personal	Formación del personal
Deficiencias en la seguridad del acceso remoto	Acceso remoto seguro
Deficiencias en la seguridad física	Disponer de un entorno de trabajo seguro
Deficiente actualización de equipos	Instalación periódica de actualizaciones
Deficiente política de contraseñas	Política de contraseñas eficaz
Desconocimiento del uso adecuado de las cámaras	Política de videovigilancia
Falta de definición sobre quién debe acceder a qué	Disponer de una relación de usuarios, perfiles y accesos autorizados
Red WIFI no segura	Seguridad de la red WIFI
Ubicación no preparada para inundaciones o fugas de agua	Establecer los equipos, soportes y sistemas seguros ante inundaciones o fugas de agua

3.13 IDENTIFICACIÓN DE LAS MEDIDAS DE SEGURIDAD

Los controles identificados en el apartado anterior se han sustanciado en una serie de medidas de seguridad, técnicas y organizativas, que deben ser implantadas en la organización para reducir los riesgos identificados hasta un umbral aceptable.

Las medidas de seguridad, resultantes de los controles, son las siguientes:

CONTROL	MEDIDA DE SEGURIDAD
Los dispositivos de almacenamiento deben tener el acceso restringido	Almacenamiento seguro de soportes y documentos
Compromiso de confidencialidad y deber de secreto	Compromiso de confidencialidad y deber de secreto
Disponer de una política de copias de respaldo y recuperación	Copias de respaldo y recuperación
Colocar extintores o sistema anti-incendios	Entorno de trabajo seguro
Disponer de una política de control de acceso	Control de acceso

Disponer de una política de trabajo fuera de los locales	Política de trabajo fuera de los locales
Definir protocolos para el traslado seguro de soportes y documentos	Protocolos para el traslado seguro de soportes y documentos
Disponer de protocolos para la destrucción de documentación	Protocolos para la destrucción de documentación
Disponer de protocolos para la destrucción y reutilización de equipos y soportes	Protocolos para la destrucción y reutilización de equipos y soportes
Los equipos deben tener instalados un software anti-malware	Software anti-malware
CONTROL	MEDIDA DE SEGURIDAD
Implantar un sistema de identificación y autenticación seguro	Sistema seguro de identificación y autenticación
Formación del personal	Formación del personal
Acceso remoto seguro	Acceso remoto seguro
Disponer de un entorno de trabajo seguro	Entorno de trabajo seguro
Instalación periódica de actualizaciones	Actualización de programas, equipos y dispositivos
Política de contraseñas eficaz	Sistema seguro de identificación y autenticación
Política de videovigilancia	Política de videovigilancia
Disponer de una relación de usuarios, perfiles y accesos autorizados	Control de acceso
Seguridad de la red WIFI	Seguridad de la red WIFI
Establecer los equipos, soportes y sistemas seguros ante inundaciones o fugas de agua	Entorno de trabajo seguro

3.14 VINCULACIÓN ENTRE MEDIDAS DE SEGURIDAD Y ACTIVOS

Las medidas de seguridad identificadas en el punto anterior, deben implantarse sobre los activos que estén relacionados con los riesgos que se desean reducir.

Las medidas de seguridad, así como los activos a los que deben aplicarse, se indican en el siguiente cuadro:

MEDIDA DE SEGURIDAD	ACTIVOS
Almacenamiento seguro de soportes y documentos	SOPORTES, DOCUMENTOS
Compromiso de confidencialidad y deber de secreto	PERSONAL
Copias de respaldo y recuperación	EQUIPOS, APLICACIONES, DATOS, SOPORTES
Entorno de trabajo seguro	INSTALACIONES, EQUIPOS, SOPORTES, DOCUMENTOS, EQUIPAMIENTO
Control de acceso	PERSONAL
Política de trabajo fuera de los locales	INSTALACIONES
Protocolos para el traslado seguro de soportes y documentos	SOPORTES, DOCUMENTOS
Protocolos para la destrucción de documentación	DOCUMENTOS
Protocolos para la destrucción y reutilización de equipos y soportes	EQUIPOS, SOPORTES

MEDIDA DE SEGURIDAD	ACTIVOS
Almacenamiento seguro de soportes y documentos	SOPORTES, DOCUMENTOS
Compromiso de confidencialidad y deber de secreto	PERSONAL
Copias de respaldo y recuperación	EQUIPOS, APLICACIONES, DATOS, SOPORTES
Entorno de trabajo seguro	INSTALACIONES, EQUIPOS, SOPORTES, DOCUMENTOS, EQUIPAMIENTO
Control de acceso	PERSONAL
Política de trabajo fuera de los locales	INSTALACIONES
Protocolos para el traslado seguro de soportes y documentos	SOPORTES, DOCUMENTOS
Protocolos para la destrucción de documentación	DOCUMENTOS
Software anti-malware	EQUIPOS
Sistema seguro de identificación y autenticación	EQUIPOS, APLICACIONES, DATOS, COMUNICACIONES, VIDEOVIGILANCIA, INTERNET
Formación del personal	PERSONAL, APLICACIONES, DATOS, SOPORTES, INTERNET
Acceso remoto seguro	EQUIPOS
Entorno de trabajo seguro	INSTALACIONES, EQUIPOS, SOPORTES, DOCUMENTOS, EQUIPAMIENTO
Actualización de programas, equipos y dispositivos	EQUIPOS, APLICACIONES, COMUNICACIONES
Sistema seguro de identificación y autenticación	EQUIPOS, APLICACIONES, DATOS, COMUNICACIONES, VIDEOVIGILANCIA, INTERNET
Política de videovigilancia	VIDEOVIGILANCIA
Control de acceso	PERSONAL
Seguridad de la red WIFI	COMUNICACIONES
Entorno de trabajo seguro	INSTALACIONES, EQUIPOS, SOPORTES, DOCUMENTOS, EQUIPAMIENTO

3.15 DOCUMENTACIÓN DE LAS MEDIDAS DE SEGURIDAD

Las medidas de seguridad deben estar documentadas de forma suficiente para su implantación en la organización.

El detalle de las medidas de seguridad se encuentra en el punto 4.

4. MEDIDAS DE SEGURIDAD

Como resultado del Análisis de Riesgos realizado por **CLIMATIZACIÓN GUADALUPE, S.L.**, las medidas de seguridad que deben implantase en la organización son las que a continuación se enumeran.

4.1. ACCESO REMOTO SEGURO

Cuando se realicen conexiones remotas a equipos o servidores de la organización, dicha conexión a la red corporativa debe realizarse siempre mediante VPN o sistema equivalente, que garantice la seguridad de la conexión, la identidad de la persona que se conecta y la confidencialidad de los datos transmitidos.

Para ello, la conexión ha de realizarse siempre según los procedimientos establecidos por la organización, cada persona que accede de forma remota ha de estar identificada de forma única e inequívoca y dicha conexión debe siempre establecerse de forma cifrada.

En ningún caso debe conectarse a la red corporativa a través de redes o WIFIs públicas o desconocidas.

En la medida de lo posible, se debe guardar un log de los accesos que han tenido lugar para poder detectar accesos fraudulentos, así como restringir dicho acceso en los horarios que no sean adecuados. Dicho log debe revisarse de forma periódica para detectar posibles accesos indebidos o en horas sospechosas.

Cuando una persona deja de pertenecer a la organización, debe existir un procedimiento para suprimir el acceso remoto que pudiera tener, así como una verificación periódica de los usuarios que lo tienen habilitado para detectar posibles accesos indebidos.

4.2. ACTUALIZACIÓN DE EQUIPOS Y DISPOSITIVOS

Los ordenadores, portátiles, tabletas, smartphones y demás dispositivos utilizados para el almacenamiento, tratamiento o transmisión de datos personales, deberán mantenerse actualizados en la medida de lo posible.

Sistemas operativos: deben estar instaladas las últimas versiones estables, y las actualizaciones han de ser provistas directamente por el fabricante.

Programas: deben estar instaladas las últimas versiones estables, y las actualizaciones han de ser provistas directamente por el fabricante.

Dispositivos (routers, firewalls, videocámaras, etc.): se ha de mantener el firmware actualizado a la última versión estable proporcionada por el fabricante.

4.3. ALMACENAMIENTO DE SOPORTES Y DOCUMENTOS

Los dispositivos de almacenamiento de los soportes y documentos que contengan datos de carácter personal, deberán disponer de mecanismos que obstaculicen su apertura, mediante llaves u otros medios que realicen la misma función.

Solo los usuarios autorizados deberán disponer de las llaves y medios que facilitan la apertura de dichos dispositivos.

Cuando las características físicas no permitan adoptar esta medida, se deberán adoptar las medidas necesarias para impedir el acceso de personas no autorizadas.

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamiento indicados anteriormente, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso de personas no autorizadas.

4.4. COMPROMISO DE CONFIDENCIALIDAD Y DEBER DE SECRETO

Todo el personal involucrado en el tratamiento de datos personales debe firmar un compromiso de confidencialidad y deber de secreto.

En dicho compromiso se estipulará que los datos a los que tenga acceso esa persona, en el ejercicio de sus funciones son confidenciales y tiene el deber de guardar secreto profesional respecto a ellos. Dicho deber de secreto subsistirá aún después de terminada la relación con el responsable del tratamiento.

4.5. CONTROL DE ACCESO

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. Se deberán establecer mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

Dichos mecanismos, en el caso de soportes informáticos, podrán consistir en la asignación de contraseñas para el acceso a los mismos, u otros dispositivos más sofisticados: biométricos, llaves USB, etc.; y en el caso de documentos en papel, en la entrega de llaves que facilitan la apertura de los dispositivos de almacenamiento donde se recopila la información.

Deberá existir también una relación actualizada de perfiles, usuarios y accesos autorizados.

Exclusivamente el Administrador de cada fichero está autorizado para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el Responsable del

Tratamiento.

Asimismo, deberán existir procedimientos para efectuar el alta, modificación y baja de las autorizaciones de acceso a los datos, así como los controles de acceso a los sistemas de información y las ubicaciones donde se almacenan datos personales.

De existir personal ajeno al responsable del tratamiento con acceso a los recursos, deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

4.6. COPIAS DE RESPALDO Y RECUPERACIÓN

La seguridad de los datos personales no solo supone la confidencialidad de los mismos, sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y recuperación, de forma, que ante un fallo informático, permitan reconstruir el fichero en el estado que se encontraba antes de la pérdida.

Se realizarán copias de respaldo periódicamente, en función del volumen y de la frecuencia de actualización de los datos.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos, quedando constancia motivada de este hecho en el Registro de Incidencias.

Se verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información que traten con datos de carácter personal no se realizarán con datos reales, salvo que se asegure la seguridad correspondiente al tratamiento realizado y se registre su realización. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

4.7. CENTROS DE TRATAMIENTO Y LOCALES

Los locales donde se realizan los tratamientos de datos personales deben ser objeto especial de protección que garanticen la confidencialidad, integridad y disponibilidad de los datos protegidos, así como la adecuada protección del equipamiento utilizado para el tratamiento. A tal efecto, la documentación, los soportes y el equipamiento informático deberán ser protegidos frente robo o acceso no autorizado.

Para ello, los locales deberán contar con los medios mínimos de seguridad siendo conveniente que dispongan de dispositivos extintores de incendios, alarmas, etc.

Asimismo, los equipos, soportes y sistemas estarán ubicados en sitios seguros frente a inundaciones o fugas de agua.

Los puntos de red no utilizados deben encontrarse desactivados para evitar un posible acceso no autorizado a la red interna de la entidad.

Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall o cortafuegos activados en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales que tengan conexión a Internet.

4.8. FORMACIÓN DEL PERSONAL

Para que el tratamiento de los datos personales se realice en todo momento según los requisitos

legales y de seguridad que marca la normativa, todo el personal involucrado en el tratamiento (recogida, registro, utilización, destrucción, etc.), sea externo o interno, debe recibir formación apropiada a las funciones realice, tanto en materia de protección de datos personales como en materia de seguridad y ciberseguridad.

El personal que realice tareas de administración de sistemas debe recibir formación apropiada en relación a los sistemas que gestiona, de forma que no se produzcan omisiones o errores accidentales que afecten, o puedan afectar, a la confidencialidad, integridad y disponibilidad de los datos personales.

Las personas (o persona) que actúe como Delegado de Protección de Datos y/o Responsable de Seguridad debe disponer de la formación y las competencias necesarias para desempeñar sus funciones con rigor y solvencia.

4.9. TRABAJO FUERA DE LOS LOCALES

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable del tratamiento, o del encargado del tratamiento, será preciso que exista una autorización previa, y en todo caso, deberán garantizarse los requisitos de seguridad correspondientes al tipo de tratamiento realizado.

4.10. CÁMARAS DE VIDEOVIGILANCIA

Los sistemas de videovigilancia pueden ser instalados con fines de seguridad o para control empresarial.

Los sistemas de videovigilancia para control empresarial sólo se adoptarán cuando exista una relación de proporcionalidad entre la finalidad perseguida y el modo en que se traten las imágenes y no haya otra medida más idónea.

En todo caso, se deberán tener en cuenta los siguientes aspectos:

1. Ubicación de las cámaras: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores, vestuarios, baños y la vía pública.

2. Ubicación de los monitores: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros. A las imágenes grabadas solo accederá el personal autorizado.

3. Conservación de imágenes: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.

4. Deber de información: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto informativo.

5. Control laboral: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representantes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.

6. Derecho de acceso a las imágenes: Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso. No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado

sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

7. Cesión a las Fuerzas y Cuerpos de Seguridad: La petición de imágenes por las Fuerzas y Cuerpos de Seguridad se realizará en el marco de actuaciones judiciales o policiales. El requerimiento al titular será el documento que ampare a éste para ceder datos a las mismas o a los Juzgados y Tribunales que los requieran.

8. Acceso a través de Internet: Si el acceso se realiza a través de Internet, dicho acceso se restringirá con un código de usuario y una contraseña (o cualquier otro medio que garantice la identificación y autenticación unívoca), que sólo serán conocidos por las personas autorizadas a acceder a dichas imágenes. Una vez colocada la cámara, debe cambiarse la contraseña de fábrica por otra que siga las pautas de complejidad establecidas por la entidad.

4.11. TRASLADO DE SOPORTES Y DOCUMENTOS

Cuando los soportes y/o documentos vayan a salir fuera de los locales en que se encuentran ubicados los tratamientos, se adoptarán las medidas necesarias para impedir la sustracción, pérdida o acceso indebido a la información durante el transporte.

Para ello, el traslado de soportes y documentos fuera de las instalaciones se realizará en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.

En todo momento el maletín o contenedor debe estar controlado, bajo supervisión de la persona que lo custodia.

En el caso de los soportes digitales, siempre que sea posible, se debe cifrar la información que contiene o bien utilizar otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

4.12. DESTRUCCIÓN DE DOCUMENTACIÓN

Uno de los mayores peligros para la confidencialidad de los datos son los documentos desechados.

Todos los documentos en papel desechados que contengan datos de carácter personal, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

- Como norma general ningún documento debe ser nunca dejado para retirar sin ser destruido o depositado en un contenedor de la empresa encargada de la destrucción de los datos si la hubiera, o destruido por otros medios que impidan la recuperación de la información.

- Aquellos soportes en papel o material blando, y que no sean demasiado voluminosos, deberán ser destruidos en una destructora de papel.

- En caso de no existir máquina destructora de papel o en el caso de que los listados o documentos sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una empresa encargada de la destrucción de los datos, que garantice mediante contrato la destrucción de los mismos.

- El Responsable del Fichero deberá exigir a la empresa encargada de la destrucción de los datos un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

4.13. DESTRUCCIÓN Y REUTILIZACIÓN DE EQUIPOS Y SOPORTES

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados.

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter

personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

Todos los desechos informáticos de cualquier tipo que puedan contener información de carácter personal, como CDs, cintas, discos removibles, o incluso los propios ordenadores, tabletas o smartphone obsoletos que contengan discos o memorias de almacenamiento, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

1. Como norma general, ningún desecho informático debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.

2. Aquellos CDs que contengan datos de carácter personal deberán ser destruidos en una destructora o por cualquier otro medio que haga imposible extraer ningún dato posteriormente.

3. Todos los disquetes y otros soportes removibles desechados deberán ser eliminados sus datos previamente con alguna aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos y entregados para su reutilización al Responsable de Seguridad o al Delegado de Protección de Datos.

4. Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras organizaciones, deberá comunicarse al Responsable de Seguridad o al Delegado de Protección de Datos para que pase una aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y proceder a su destrucción o encomendar a una empresa de reciclaje especializada la destrucción de los mismos.

5. El Responsable del tratamiento deberá exigir a la empresa de reciclaje un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

4.14. SEGURIDAD DE LA RED WIFI

Los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio. Las ondas de radio pueden viajar más allá de las paredes y filtrarse en habitaciones contiguas o llegar hasta la calle.

La infiltración no autorizada en redes inalámbricas es una tarea muy sencilla si la red WIFI no está adecuadamente configurada y protegida.

Para evitar esto, se debe proteger la red WIFI de las siguientes formas:

1. Cambiar la contraseña de acceso al WIFI que viene por defecto siguiendo el procedimiento establecido por la entidad para la construcción de contraseñas seguras.

2. Activar el cifrado WPA2 (en ningún caso dejarla en abierto o con cifrado WEP).

3. Cambiar el SSID de fábrica. En ningún caso debe identificar a la entidad.

4. Valorar la activación del filtrado por MAC.

5. Cambiar la clave de acceso regularmente.

6. Cuando sea posible, aislar la red WIFI de la red interna

4.15. IDENTIFICACIÓN Y AUTENTICACIÓN

Se establecerán las medidas de seguridad necesarias en los sistemas informáticos de forma que se garantice que únicamente accederá a los tratamientos el personal autorizado para ello.

Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.

Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.

De la misma forma, se establecerá un sistema que permita la identificación inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información, y la debida autenticación para verificar la identidad del usuario que intenta acceder.

Aunque ya existen procedimientos de identificación basados en certificado electrónico, o incluso en datos biométricos, como huellas dactilares, las contraseñas personales constituyen todavía hoy en día uno de los métodos más usados para proteger el acceso a los datos, y por tanto, deben estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

La periodicidad máxima con la que tienen que ser cambiadas las contraseñas no debe ser superior a un año. Se almacenarán de forma ininteligible en los sistemas informáticos mientras estén vigentes.

Las contraseñas deberán ser suficientemente complejas y difícilmente adivinables por terceros, evitando el uso del propio identificador como contraseña o palabras sencillas, como "casa", el nombre propio, etc. Para ello se seguirán las siguientes pautas en la construcción de contraseñas: longitud de al menos 8 caracteres, mezcla de números y letras; no deberán coincidir, ni siquiera en parte, con el código del usuario; y no deberán estar basadas en cadenas de caracteres que sean fácilmente asociadas al usuario (nombre, apellidos, ciudad y fecha de nacimiento, nombres de familiares, matrícula del coche, etc.).

En el caso de dispositivos que no permitan varios nombres de usuario (como routers, firewalls, cámaras, etc.), el responsable de seguridad establecerá la contraseña de dicho dispositivo según las pautas indicadas anteriormente y la almacenará de forma que se garantice su confidencialidad e integridad.

Antes de colocar cualquier dispositivo en la red o para su uso, debe cambiarse la contraseña de fábrica por otra que siga las pautas antes indicadas.

4.16. SOFTWARE ANTI-MALWARE

En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema anti-malware que evite, en la medida de lo posible, el robo y la destrucción de la información y datos personales. El sistema anti-malware deberá ser actualizado de forma periódica.

ANEXO III

MEDIDAS DE SEGURIDAD

MEDIDAS DE SEGURIDAD

Como resultado de la Evaluación de Riesgos realizada, las medidas de seguridad que deben implantase en la organización son las que a continuación se enumeran.

1. ACCESO REMOTO SEGURO

Cuando se realicen conexiones remotas a equipos o servidores de la organización, dicha conexión a la red corporativa debe realizarse siempre mediante VPN o sistema equivalente, que garantice la seguridad de la conexión, la identidad de la persona que se conecta y la confidencialidad de los datos transmitidos.

Para ello, la conexión ha de realizarse siempre según los procedimientos establecidos por la organización, cada persona que accede de forma remota ha de estar identificada de forma única e inequívoca y dicha conexión debe siempre establecerse de forma cifrada.

En ningún caso debe conectarse a la red corporativa a través de redes o WIFIs públicas o desconocidas.

En la medida de lo posible, se debe guardar un log de los accesos que han tenido lugar para poder detectar accesos fraudulentos, así como restringir dicho acceso en los horarios que no sean adecuados. Dicho log debe revisarse de forma periódica para detectar posibles accesos indebidos o en horas sospechosas.

Cuando una persona deja de pertenecer a la organización, debe existir un procedimiento para suprimir el acceso remoto que pudiera tener, así como una verificación periódica de los usuarios que lo tienen habilitado para detectar posibles accesos indebidos.

Activos afectados

Los activos afectados por esta medida son los siguientes:

EQUIPOS:

2. ACTUALIZACIÓN DE EQUIPOS Y DISPOSITIVOS

Los ordenadores, portátiles, tabletas, Smartphone y demás dispositivos utilizados para el almacenamiento, tratamiento o transmisión de datos personales, deberán mantenerse actualizados en la medida de lo posible.

Sistemas operativos: deben estar instaladas las últimas versiones estables, y las actualizaciones han de ser provistas directamente por el fabricante.

Programas: deben estar instaladas las últimas versiones estables, y las actualizaciones han de ser provistas directamente por el fabricante.

Dispositivos (routers, firewalls, videocámaras, etc.): se ha de mantener el firmware actualizado a la última versión estable proporcionada por el fabricante.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- EQUIPOS:
- APLICACIONES:
- COMUNICACIONES:

3. ALMACENAMIENTO DE SOPORTES Y DOCUMENTOS

Los dispositivos de almacenamiento de los soportes y documentos que contengan datos de carácter personal, deberán disponer de mecanismos que obstaculicen su apertura,

mediante llaves u otros medios que realicen la misma función.

Solo los usuarios autorizados deberán disponer de las llaves y medios que facilitan la apertura de dichos dispositivos.

Cuando las características físicas no permitan adoptar esta medida, se deberán adoptar las medidas necesarias para impedir el acceso de personas no autorizadas.

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamiento indicados anteriormente, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso de personas no autorizadas.

Implementación

Todos los soportes y documentos con datos personales se almacenan en dispositivos que disponen de mecanismos que obstaculizan su apertura mediante llave.

Siempre que una persona no autorizada pueda tener acceso a soportes o documentos con datos personales, está en todo momento supervisada por alguien autorizado para acceder a dichos documentos, no dejándola sola con ellos bajo ninguna circunstancia.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- SOPORTES
- DOCUMENTOS

4. COMPROMISO DE CONFIDENCIALIDAD Y DEBER DE SECRETO

Todo el personal involucrado en el tratamiento de datos personales debe firmar un compromiso de confidencialidad y deber de secreto.

En dicho compromiso se estipulará que los datos a los que tenga acceso esa persona, en el ejercicio de sus funciones son confidenciales y tiene el deber de guardar secreto profesional respecto a ellos. Dicho deber de secreto subsistirá aún después de terminada la relación con el responsable del tratamiento.

Implementación

Todo el personal, antes de iniciar su actividad, firma el Compromiso de Confidencialidad y Deber de Secreto estipulado por la organización.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- PERSONAL

5. CONTROL DE ACCESO

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. Se deberán establecer mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

Dichos mecanismos, en el caso de soportes informáticos, podrán consistir en la asignación de contraseñas para el acceso a los mismos, u otros dispositivos más sofisticados: biométricos, llaves USB, etc.; y en el caso de documentos en papel, en la entrega de llaves que facilitan la apertura de los dispositivos de almacenamiento donde se recopila la información.

Deberá existir también una relación actualizada de perfiles, usuarios y accesos autorizados.

Exclusivamente el Administrador de cada fichero está autorizado para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el Responsable del Tratamiento.

Asimismo, deberán existir procedimientos para efectuar el alta, modificación y baja de las autorizaciones de acceso a los datos, así como los controles de acceso a los sistemas de información y las ubicaciones donde se almacenan datos personales.

De existir personal ajeno al responsable del tratamiento con acceso a los recursos, deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Implementación

Los procedimientos para dar de alta, baja o modificación de acceso autorizado a los tratamientos son los siguientes:

1. Alta: cuanto un nuevo empleado se incorpora, el administrador de ese tratamiento construye un identificador único para ese usuario según el procedimiento establecido y le asigna privilegios en función del perfil al que pertenece. Asimismo, el administrador del fichero le asigna una contraseña provisional que el usuario deberá cambiar en el primer acceso al sistema.

2. Baja: en caso de que la baja sea temporal, el administrador procederá a bloquear la identificación del usuario, y en caso de que sea definitiva, procederá a la eliminación inmediata de todos sus derechos de acceso.

3. Modificación: cuando un usuario desempeñe distintas funciones en la empresa, o tenga que acceder a datos a los que anteriormente no accedía, al administrador del fichero deberá cambiar sus privilegios de acceso en función al nuevo perfil al que pertenece.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- PERSONAL

6. COPIAS DE RESPALDO Y RECUPERACIÓN

La seguridad de los datos personales no solo supone la confidencialidad de los mismos, sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y recuperación, de forma, que ante un fallo informático, permitan reconstruir el fichero en el estado que se encontraba antes de la pérdida.

Se realizarán copias de respaldo periódicamente, en función del volumen y de la frecuencia de actualización de los datos.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar

manualmente los datos, quedando constancia motivada de este hecho en el Registro de Incidencias.

Se verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información que traten con datos de carácter personal no se realizarán con datos reales, salvo que se asegure la seguridad correspondiente al tratamiento realizado y se registre su realización. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Implementación

Las copias de respaldo se realizan semanalmente a un disco duro externo.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- EQUIPOS
- APLICACIONES
- DATOS
- SOPORTES

7. CENTROS DE TRATAMIENTO Y LOCALES

Los locales donde se realizan los tratamientos de datos personales deben ser objeto especial de protección que garanticen la confidencialidad, integridad y disponibilidad de los datos protegidos, así como la adecuada protección del equipamiento utilizado para el tratamiento. A tal efecto, la documentación, los soportes y el equipamiento informático deberán ser protegidos frente robo o acceso no autorizado.

Para ello, los locales deberán contar con los medios mínimos de seguridad siendo conveniente que dispongan de dispositivos extintores de incendios, alarmas, etc.

Asimismo, los equipos, soportes y sistemas estarán ubicados en sitios seguros frente a inundaciones o fugas de agua.

Los puntos de red no utilizados deben encontrarse desactivados para evitar un posible acceso no autorizado a la red interna de la entidad.

Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall o cortafuegos activados en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales que tengan conexión a Internet.

Implementación

Se dispone de extintores, así como de firewall activado.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- INSTALACIONES
- EQUIPOS
- SOPORTES
- DOCUMENTOS

- EQUIPAMIENTO

8. FORMACIÓN DEL PERSONAL

Para que el tratamiento de los datos personales se realice en todo momento según los requisitos legales y de seguridad que marca la normativa, todo el personal involucrado en el tratamiento (recogida, registro, utilización, destrucción, etc.), sea externo o interno, debe recibir formación apropiada a las funciones realice, tanto en materia de protección de datos personales como en materia de seguridad y ciberseguridad.

El personal que realice tareas de administración de sistemas debe recibir formación apropiada en relación a los sistemas que gestiona, de forma que no se produzcan omisiones o errores accidentales que afecten, o puedan afectar, a la confidencialidad, integridad y disponibilidad de los datos personales.

Las personas (o persona) que actúe como Delegado de Protección de Datos y/o Responsable de Seguridad debe disponer de la formación y las competencias necesarias para desempeñar sus funciones con rigor y solvencia.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- PERSONAL
- APLICACIONES
- DATOS
- SOPORTES
- INTERNET

9. TRABAJO FUERA DE LOS LOCALES

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable del tratamiento, o del encargado del tratamiento, será preciso que exista una autorización previa, y en todo caso, deberán garantizarse los requisitos de seguridad correspondientes al tipo de tratamiento realizado.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- INSTALACIONES

10. CÁMARAS DE VIDEOVIGILANCIA

Los sistemas de videovigilancia pueden ser instalados con fines de seguridad o para control empresarial.

Los sistemas de videovigilancia para control empresarial sólo se adoptarán cuando exista una relación de proporcionalidad entre la finalidad perseguida y el modo en que se traten las imágenes y no haya otra medida más idónea.

En todo caso, se deberán tener en cuenta los siguientes aspectos:

1. Ubicación de las cámaras: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores, vestuarios, baños y la vía pública.

2. Ubicación de los monitores: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros. A las imágenes grabadas solo accederá el personal autorizado.

3. Conservación de imágenes: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.

4. Deber de información: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto informativo.

5. Control laboral: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representantes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.

6. Derecho de acceso a las imágenes: Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso. No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

7. Cesión a las Fuerzas y Cuerpos de Seguridad: La petición de imágenes por las Fuerzas y Cuerpos de Seguridad se realizará en el marco de actuaciones judiciales o policiales. El requerimiento al titular será el documento que ampare a éste para ceder datos a las mismas o a los Juzgados y Tribunales que los requieran.

8. Acceso a través de Internet: Si el acceso se realiza a través de Internet, dicho acceso se restringirá con un código de usuario y una contraseña (o cualquier otro medio que garantice la identificación y autenticación unívoca), que sólo serán conocidos por las personas autorizadas a acceder a dichas imágenes. Una vez colocada la cámara, debe cambiarse la contraseña de fábrica por otra que siga las pautas de complejidad establecidas por la entidad.

Implementación

Las cámaras están situadas en lugares adecuados, sin captar en ningún caso, la vía pública.

La longitud y contenido de las contraseñas de las cámaras: deben tener una longitud mínima de 8 caracteres y contener mezcla de números y letras.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- VIDEOVIGILANCIA

11. TRASLADO DE SOPORTES Y DOCUMENTOS

Cuando los soportes y/o documentos vayan a salir fuera de los locales en que se encuentran ubicados los tratamientos, se adoptarán las medidas necesarias para impedir la sustracción, pérdida o acceso indebido a la información durante el transporte.

Para ello, el traslado de soportes y documentos fuera de las instalaciones se realizará en un maletín o contenedor similar y que disponga de mecanismo que para su apertura

precise de una llave o el conocimiento de una combinación.

En todo momento el maletín o contenedor debe estar controlado, bajo supervisión de la persona que lo custodia.

En el caso de los soportes digitales, siempre que sea posible, se debe cifrar la información que contiene o bien utilizar otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- SOPORTES
- DOCUMENTOS

12. DESTRUCCIÓN DE DOCUMENTACIÓN

Uno de los mayores peligros para la confidencialidad de los datos son los documentos desechados.

Todos los documentos en papel desechados que contengan datos de carácter personal, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

- Como norma general ningún documento debe ser nunca dejado para retirar sin ser destruido o depositado en un contenedor de la empresa encargada de la destrucción de los datos si la hubiera, o destruido por otros medios que impidan la recuperación de la información.

- Aquellos soportes en papel o material blando, y que no sean demasiado voluminosos, deberán ser destruidos en una destructora de papel.

- En caso de no existir máquina destructora de papel o en el caso de que los listados o documentos sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una empresa encargada de la destrucción de los datos, que garantice mediante contrato la destrucción de los mismos.

- El Responsable del Fichero deberá exigir a la empresa encargada de la destrucción de los datos un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- DOCUMENTOS

13. DESTRUCCIÓN Y REUTILIZACIÓN DE EQUIPOS Y SOPORTES

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados.

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

Todos los desechos informáticos de cualquier tipo que puedan contener información de carácter personal, como CDs, cintas, discos removibles, o incluso los propios ordenadores, tabletas o smartphone obsoletos que contengan discos o memorias de almacenamiento,

deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

1. Como norma general, ningún desecho informático debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.

2. Aquellos CDs que contengan datos de carácter personal deberán ser destruidos en una destructora o por cualquier otro medio que haga imposible extraer ningún dato posteriormente.

3. Todos los disquetes y otros soportes removibles desechados deberán ser eliminados sus datos previamente con alguna aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos y entregados para su reutilización al Responsable de Seguridad o al Delegado de Protección de Datos.

4. Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras organizaciones, deberá comunicarse al Responsable de Seguridad o al Delegado de Protección de Datos para que pase una aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y proceder a su destrucción o encomendar a una empresa de reciclaje especializada la destrucción de los mismos.

5. El Responsable del tratamiento deberá exigir a la empresa de reciclaje un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- EQUIPOS
- SOPORTES

14. SEGURIDAD DE LA RED WIFI

Los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio. Las ondas de radio pueden viajar más allá de las paredes y filtrarse en habitaciones contiguas o llegar hasta la calle.

La infiltración no autorizada en redes inalámbricas es una tarea muy sencilla si la red WIFI no está adecuadamente configurada y protegida.

Para evitar esto, se debe proteger la red WIFI de las siguientes formas:

1. Cambiar la contraseña de acceso al WIFI que viene por defecto siguiendo el procedimiento establecido por la entidad para la construcción de contraseñas seguras.

2. Activar el cifrado WPA2 (en ningún caso dejarla en abierto o con cifrado WEP).

3. Cambiar el SSID de fábrica. En ningún caso debe identificar a la entidad.

4. Valorar la activación del filtrado por MAC.

5. Cambiar la clave de acceso regularmente.

6. Cuando sea posible, aislar la red WIFI de la red interna

Activos afectados

Los activos afectados por esta medida son los siguientes:

- COMUNICACIONES

15. IDENTIFICACIÓN Y AUTENTICACIÓN

Se establecerán las medidas de seguridad necesarias en los sistemas informáticos de forma que se garantice que únicamente accederá a los tratamientos el personal autorizado para ello.

Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.

Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.

De la misma forma, se establecerá un sistema que permita la identificación inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información, y la debida autenticación para verificar la identidad del usuario que intenta acceder.

Aunque ya existen procedimientos de identificación basados en certificado electrónico, o incluso en datos biométricos, como huellas dactilares, las contraseñas personales constituyen todavía hoy en día uno de los métodos más usados para proteger el acceso a los datos, y por tanto, deben estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

La periodicidad máxima con la que tienen que ser cambiadas las contraseñas no debe ser superior a un año. Se almacenarán de forma ininteligible en los sistemas informáticos mientras estén vigentes.

Las contraseñas deberán ser suficientemente complejas y difícilmente adivinables por terceros, evitando el uso del propio identificador como contraseña o palabras sencillas, como "casa", el nombre propio, etc. Para ello se seguirán las siguientes pautas en la construcción de contraseñas: longitud de al menos 8 caracteres, mezcla de números y letras; no deberán coincidir, ni siquiera en parte, con el código del usuario; y no deberán estar basadas en cadenas de caracteres que sean fácilmente asociadas al usuario (nombre, apellidos, ciudad y fecha de nacimiento, nombres de familiares, matrícula del coche, etc.).

En el caso de dispositivos que no permitan varios nombres de usuario (como routers, firewalls, cámaras, etc.), el responsable de seguridad establecerá la contraseña de dicho dispositivo según las pautas indicadas anteriormente y la almacenará de forma que se garantice su confidencialidad e integridad.

Antes de colocar cualquier dispositivo en la red o para su uso, debe cambiarse la contraseña de fábrica por otra que siga las pautas antes indicadas.

Implementación

El sistema de identificación y autenticación que da acceso a los ficheros automatizados,

dispone de las siguientes características:

1. Identificación: inicial del nombre más el apellido.

2. Autenticación: contraseña escogida por el usuario.

3. Longitud y contenido de las contraseñas: deben tener una longitud mínima de 8 caracteres y contener mezcla de números y letras.

4. Periodicidad de cambio: el cambio de las contraseñas es cada 365 días.

5. Acceso al sistema por primera vez: el administrador asignará una contraseña provisional al nuevo usuario, que deberá ser cambiada en su primer acceso al sistema por una que sólo conozca el usuario y en base a las características definidas anteriormente.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- EQUIPOS
- APLICACIONES
- DATOS
- COMUNICACIONES
- VIDEOVIGILANCIA
- INTERNET

16. SOFTWARE ANTI-MALWARE

En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema anti-malware que evite, en la medida de lo posible, el robo y la destrucción de la información y datos personales. El sistema anti-malware deberá ser actualizado de forma periódica.

Activos afectados

Los activos afectados por esta medida son los siguientes:

- EQUIPOS

ANEXO IV

FUNCIONES Y OBLIGACIONES DEL PERSONAL EN MATERIA DE PROTECCIÓN DE DATO

1. INTRODUCCIÓN

1.1 ¿QUÉ ES LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES?

Es la normativa que regula la recogida y el tratamiento de los datos personales (dichos datos pueden ser de clientes, trabajadores, solicitantes de empleo, usuarios, etc.).

1.2 ¿QUÉ OBJETO TIENE?

Establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

Es decir, limitar el grado de intrusión en nuestra intimidad que pueden generar las nuevas tecnologías, así como el tráfico indiscriminado de datos personales.

1.3 ¿A QUIEN INCUMBE LA LEY?

La ley obliga a su cumplimiento a todos los profesionales, empresas, organismos públicos y privados que traten con datos personales registrados en soporte físico (soporte papel o informático).

1.4 ¿QUÉ SON LOS DATOS PERSONALES?

Es 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.

Son datos de carácter personal:

- El nombre y apellidos de una persona.
- Teléfono fijo o móvil.
- Dirección postal.
- Correo electrónico.
- DNI / CIF.
- Dirección IP.
- Una fotografía.
- Una grabación de vídeo.
- Cualquier otra información de la que se desprendan datos personales.

1.5 CLASIFICACIÓN DE LOS DATOS PERSONALES

Los datos de carácter personal se pueden clasificar en:

- Datos identificativos: nombre y apellidos, dirección postal, dirección electrónica, teléfono, DNI/CIF, SS/mutualidad, imagen, voz, firma o huella digitalizada, firma electrónica, etc.
- Datos de características personales: estado civil, familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna, características físicas o antropométricas.
- Datos de circunstancias sociales: características de alojamiento, vivienda, situación militar, propiedades y posesiones, aficiones y estilo de vida, pertenencia a clubes y asociaciones, licencias, permisos y autorizaciones.

- Datos académicos y profesionales: formación y titulaciones, historial del estudiante, experiencia profesional, pertenencia a colegios o a asociaciones profesionales.
- Datos de empleo: profesión, puestos de trabajo, datos no económicos de nómina, historial del trabajador.
- Datos de información comercial: actividades y negocios, licencias comerciales, suscripciones a publicaciones y medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.
- Datos económicos, financieros y de seguros: ingresos y rentas, inversiones y bienes patrimoniales, créditos, préstamos y avales, datos bancarios, planes de pensiones, jubilación, datos económicos de nómina, deducciones impositivas, impuestos, seguros, hipotecas, subsidios y beneficios, historial de créditos, tarjetas de crédito.
- Datos de transacciones de bienes y servicios: bienes y servicios suministrados por el afectado, bienes y servicios recibidos por el afectado, transacciones financieras, compensaciones, indemnizaciones.
- Categorías especiales de datos personales: son aquellos datos que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como los datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

1.6 MEDIDAS DE SEGURIDAD

No es lo mismo tratar datos meramente identificativos para, por ejemplo, realizar la facturación de un servicio, que tratar el historial médico, o la vida sexual de una persona.

Hay datos mucho más sensibles que otros, y que necesitan de una mayor protección para garantizar la confidencialidad e integridad de los mismos.

En particular, los datos más sensibles (y que deben ser objeto de una mayor protección) son los detallados como categorías especiales de datos personales del apartado anterior.

Deben implantarse medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

1.7 ¿QUÉ ES UN TRATAMIENTO DE DATOS PERSONALES?

Es 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.

1.8 ¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO?

Es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

1.9 ¿QUIÉN ES EL ENCARGADO DEL TRATAMIENTO?

La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Por ejemplo, la asesoría laboral del responsable, que realiza las nóminas de sus trabajadores, es un encargado del tratamiento.

1.10 OBLIGACIONES DEL RESPONSABLE Y DEL ENCARGADO DEL TRATAMIENTO

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

La normativa también establece los requisitos documentales necesarios para poder cumplir con la citada normativa y poder ser capaz de demostrar dicho cumplimiento

Entre la documentación mínima que debe dispone la entidad se encuentra:

- El Registro de Actividades de Tratamiento, tanto como responsable del tratamiento, como encargado del tratamiento, en su caso.
- Documentación del análisis de riesgos realizado.
- La/s Evaluación/es de Impacto relativa/s a la Protección de Datos, en su caso.
- Las medidas de seguridad implantadas.
- Las funciones y obligaciones del personal con acceso a datos personales.
- El registro de incidencias y el registro de las notificaciones de las violaciones de la seguridad a la Autoridad de Control, en su caso.
- Los protocolos de atención a los derechos de los interesados.
- Los compromisos de confidencialidad con los trabajadores.
- Los contratos de acceso a datos por cuenta de terceros.
- La documentación relativa a las transferencias internacionales de datos, así como las garantías apropiadas obtenidas o las excepciones utilizadas como base jurídica para su realización.
- Toda la documentación adicional que sea necesaria para demostrar el cumplimiento de la normativa de protección de datos en la entidad (cláusulas legales, consentimientos otorgados por los interesados, autorizaciones para la contratación de subencargados del tratamiento, ponderaciones del interés legítimo, etc.).

Esta documentación debe mantenerse en todo momento actualizada y debe ser revisada siempre que se produzcan cambios que puedan repercutir en el cumplimiento de la normativa de protección de datos o en las medidas de seguridad implantadas, como son cambios relevantes en:

- la organización
- el contenido de la información incluida en los tratamientos
- los tratamientos de datos personales realizados
- los sistemas de tratamiento empleados

Debe mantenerse adecuada, en todo momento, a las disposiciones vigentes en materia de protección de los datos de carácter personal.

1.11 LOS DERECHOS DE LOS INTERESADOS

Los derechos que los interesados pueden solicitar al responsable del tratamiento son los siguientes:

- Derecho de acceso.
- Derecho de rectificación.
- Derecho de supresión («el derecho al olvido»).

- Derecho a la limitación del tratamiento.
- Derecho a la portabilidad de los datos.
- Derecho de oposición.
- Derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles.

El protocolo, los plazos y la forma de actuación está detallada en el ANEXO IX, "Protocolos de atención a los derechos". El personal podrá solicitar una copia del mismo en cualquier momento.

Cualquier usuario que reciba una solicitud por parte de un interesado, deberá rellenar el formulario "GESTIÓN DE SOLICITUDES DE DERECHOS DE LOS INTERESADOS", que se encuentra en el APÉNDICE II, y remitirlo cuanto antes al Delegado de Protección de Datos o al responsable de gestionar los derechos de los interesados.

2. FUNCIONES Y OBLIGACIONES DE LOS USUARIOS

Usuario es todo el personal autorizado que accede a los datos de carácter personal para el desempeño de las funciones propias de su puesto de trabajo.

Todos los usuarios tienen la obligación de colaborar con el responsable del tratamiento para velar por el cumplimiento de la legislación vigente sobre protección de datos personales.

Los usuarios deben respetar los procedimientos definidos para gestionar la seguridad de la información personal que se detallan a continuación.

2.1 OBLIGACIONES GENERALES

- Guardar secreto y confidencialidad de la información tratada. Quienes intervienen en cualquier fase del tratamiento de los datos personales, está obligado al secreto profesional respecto a los datos y al deber de guardarlos, obligaciones que continúan incluso después de finalizar las relaciones con el responsable del tratamiento.
- La vulneración del deber de secreto respecto a los datos personales tratados, será considerado una falta grave, lo cual dará lugar al inicio de acciones disciplinarias, si proceden.
- Proteger los datos personales que esté tratando y custodiarlos para que personal no autorizado no tenga acceso a ellos.
- Los sistemas de información, recursos, y la información personal a la que se accede, sólo se debe utilizar para las labores estrictamente profesionales que el usuario tiene asignadas.
- Facilitar a los interesados el ejercicio de sus derechos. Para ello, recogerá la solicitud escrita y la trasladará al responsable correspondiente para su atención según el protocolo establecido.

2.2 PUESTOS DE TRABAJO

- Cada usuario es responsable de la confidencialidad de la contraseña que tiene para acceder a los sistemas de información. En caso que de forma accidental o intencionada esta contraseña sea conocida por personas no autorizadas, deberá registrarlo como incidencia y proceder al cambio de la misma.
- El usuario deberá cambiar la contraseña inicial asignada en el primer acceso que realice al sistema, o tras el desbloqueo de su contraseña cuando haya sido necesaria

la intervención de una tercera persona para realizar el proceso. Las contraseñas deberán ser lo suficientemente complejas para no ser adivinadas de forma sencilla por un tercero. Para ello, se deberán seguir las siguientes normas para elegir la contraseña:

- Deberán tener una longitud mínima de 8 caracteres alfanuméricos.
- No deberán coincidir, ni siquiera en parte, con el código de usuario.
- No deberán estar basados en cadenas de caracteres que sean fácilmente asociadas al usuario (nombre, apellidos, ciudad y fecha de nacimiento, nombres de familiares, matrícula del coche, etc.).
- El usuario deberá aplicar las reglas nemotécnicas para poder construir una contraseña lo suficientemente compleja como para que no pueda ser adivinada por terceros y a la vez sean muy fáciles de recordar por él.
- Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible a personas no autorizadas.
- Los puestos de trabajo deberán estar físicamente ubicados en lugares que garanticen la confidencialidad, así como las pantallas, impresoras y cualquier otro dispositivo conectado al puesto de trabajo y desde el que sea posible tener acceso a datos de carácter personal.
- Cuando el responsable del puesto de trabajo lo abandone, bien temporalmente, o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. Para reanudar el trabajo será necesaria la introducción de una contraseña que desactive el protector de pantalla. Deberá retirar también cualquier soporte, como documentos, fichas, discos, u otros que contengan datos del fichero, y proceder a guardarlos en su ubicación protegida habitual.
- En el caso de las impresoras, deberá asegurarse que no quedan documentos con datos personales en la bandeja de salida. Si las impresoras son compartidas, el usuario que ha mandado la impresión deberá retirar los documentos conforme vayan siendo impresos.
- Queda expresamente prohibido cualquier cambio de la configuración de la conexión de los puestos de trabajo a sistemas o redes exteriores, que no esté autorizada previamente por el responsable del tratamiento.
- Se deberá evitar el guardar copias de los datos personales en ficheros temporales. En caso de que el tratamiento haga imprescindible realizar dichas copias, se deberán adoptar las siguientes precauciones: realizar siempre las copias sobre un mismo directorio de nombre TEMP o similar, de forma que no queden dispersas por el disco duro, y siempre sea posible conocer dónde están los datos temporales. Tras realizar el tratamiento que ha requerido estos datos temporales, proceder a su inmediata eliminación.
- Los ficheros temporales creados exclusivamente para la realización de trabajos temporales o auxiliares, deberán cumplir las medidas de seguridad que les corresponda en función de los datos que contienen.

- El trabajo fuera de los locales del responsable del tratamiento, solo se podrá realizar cuando exista una autorización previa del responsable del tratamiento o del encargado del tratamiento, en todo caso, deberá garantizarse la seguridad de esos datos.
- No deberá copiarse, ni transportar información en portátiles, o equipos que se encuentren fuera de las oficinas sin la correspondiente autorización del responsable del tratamiento. Especial consideración deberán tener los puestos de trabajo portátiles, como ordenadores portátiles o PDA. Estos dispositivos portátiles, cuando puedan almacenar datos personales, deberán contar con una autorización especial por parte del responsable del tratamiento.

2.3 GESTIÓN DE SOPORTES

Se entiende por soporte todo objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Ejemplos de soportes: disquetes, cd-rom, dvd-rom, memoria usb, disco duro, etc.

Los usuarios deben observar las siguientes medidas de seguridad en relación con los soportes que contengan datos de carácter personal:

- Los usuarios que traten los soportes o documentos con datos de carácter personal, son los encargados de custodiarlos y vigilar para que personas no autorizadas no accedan al soporte físico o documentos a su cargo.
- Cuando un usuario gestione o produzca soportes que contengan datos de carácter personal, estos deberán estar claramente identificados con una etiqueta externa y, en su caso, inventariados según el protocolo establecido.
- Los soportes que contengan datos personales, deberán ser almacenados en lugares a los que no tenga acceso el personal no autorizado.
- La salida de soportes que contengan datos de carácter personal de las instalaciones bajo control del responsable del tratamiento, deberá ser autorizada previamente.
- La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o añejos a un correo electrónico, fuera de los locales bajo el control del responsable fichero o tratamiento, deberá ser autorizada previamente.
- El traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.
- Cuando deban ser enviados datos personales sensibles fuera de las ubicaciones del responsable del tratamiento, ya sea mediante soporte físico de grabación de datos o bien a través de correo electrónico o FTP, deberán ir cifrados o utilizar cualquier otro mecanismo que asegure que la información no es accesible ni manipulada durante su transporte.

2.3.1 DESTRUCCIÓN Y REUTILIZACIÓN DE SOPORTES

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados.

Todos los desechos informáticos de cualquier tipo que puedan contener información de carácter

personal, como CDs, cintas, discos removibles, o incluso los propios ordenadores obsoletos que contengan discos de almacenamiento, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

- Como norma general, ningún desecho informático debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.
- Aquellos CDs que contengan datos de carácter personal deberán ser destruidos en una destructora o por cualquier otro medio que haga imposible extraer ningún dato posteriormente.
- Todos los disquetes y otros soportes removibles desechados deberán ser eliminados sus datos previamente con alguna aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos y entregados para su reutilización al responsable del tratamiento.
- Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras organizaciones, deberá comunicarse al responsable del tratamiento para que pase una aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y proceder a su destrucción o encomendar a una empresa de reciclaje especializada la destrucción de los mismos.

2.4 FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

- Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir las medidas de seguridad que les corresponda y serán borrados o destruidos una vez hayan dejado de ser necesarios para los fines que motivaron su creación.

2.5 DOCUMENTACIÓN EN PAPEL (NO AUTOMATIZADA)

- En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamiento indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso de personas no autorizadas.
- Siempre que se proceda al traslado físico de documentación que contenga datos personales (especialmente si son sensibles), deberán adoptarse las medidas que impidan el acceso indebido, manipulación, sustracción o pérdida de la información objeto del traslado durante el transporte de la misma. Para ello, el traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación y en todo momento el maletín o contenedor debe estar controlado, bajo supervisión de la persona que lo custodia.

2.5.1 DESTRUCCIÓN DE DOCUMENTACIÓN

Uno de los mayores peligros para la confidencialidad de los datos son los documentos desechados.

Todos los documentos en papel desechados que contengan datos de carácter personal, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

- Como norma general ningún documento debe ser nunca dejado para retirar sin ser destruido o depositado en un contenedor de la empresa encargada de la destrucción de los datos si la hubiera, o destruido por otros medios que impidan la recuperación de la información.
- Aquellos soportes en papel o material blando, y que no sean demasiado voluminosos, deberán ser destruidos en una destructora de papel.
- En caso de no existir máquina destructora de papel o en el caso de que los listados o documentos sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una empresa encargada de la destrucción de los datos, que garantice mediante contrato la destrucción de los mismos.
- El responsable del tratamiento deberá exigir a la empresa encargada de la destrucción de los datos un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

2.6 GESTIÓN DE INCIDENCIAS

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa de protección de datos personales, así como cualquier anomalía o evento que afecte o pueda afectar a la seguridad de los datos personales en sus tres vertientes de confidencialidad, integridad y disponibilidad.

Se deberán tener en cuenta, entre otras, las siguientes incidencias:

- Pérdida de información personal.
- Modificación de datos personales por personal no autorizado o desconocido.
- Existencia de sistemas de información sin las debidas medidas de seguridad.
- Los intentos de acceso no autorizados a ficheros de carácter personal.
- El conocimiento por terceros de la clave de acceso al sistema.
- El intento no autorizado de salida de un soporte.
- La existencia de soportes sin control que contengan datos personales.
- La destrucción total o parcial de un soporte que contenga datos de carácter personal.
- La caída del sistema de seguridad informática, que posibilite el acceso a datos personales por personas no autorizadas.
- Cualquier incidencia que pueda afectar a la confidencialidad, integridad y/o disponibilidad de los datos personales.

Todos los usuarios, administradores, responsables, así como cualquier persona que tenga acceso a datos de carácter personal, deben tener conocimiento de este procedimiento para actuar en caso de incidencia que se detalla a continuación:

Cuando una persona tenga conocimiento de una incidencia que afecte, o pueda afectar, a la confidencialidad o integridad de los datos contenidos en los ficheros de la organización, deberá comunicarla inmediatamente al responsable del registro de incidencias a través del formulario GESTIÓN DE INCIDENCIAS, del que se le ha hecho entrega a cada trabajador. Deberá especificar el tipo de incidencia producida y su descripción detallada, indicando las intervenciones de las personas que hayan podido tener relación con la producción de la incidencia, así como la fecha y hora en que se ha producido o detectado, la persona que realiza la notificación, a quién se comunica

y los efectos que se pueden haber derivado de la incidencia.

Una vez rellena la plantilla, se obtendrán 2 copias y se entregarán inmediatamente al responsable del tratamiento, Delegado de Protección de Datos, o a la persona en quien haya delegado la gestión de las incidencias, solicitándole el acuse de recibo en una de las copias. Esta copia se guardará como resguardo de la notificación.

El responsable del tratamiento, Delegado de Protección de Datos, o a la persona en quien haya delegado la gestión de las incidencias, quedará encargo de la gestión, coordinación y resolución de la misma, así como al registro de la incidencia en el registro habilitado para ello.

El conocimiento y no notificación de una incidencia por parte de un usuario, será considerado como una falta de seguridad por parte de ese usuario.

3. FUNCIONES Y OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. Deberá:

- Elaborar el Registro de Actividades de Tratamiento.
- Realizar el análisis de los riesgos y guardar la documentación del mismo, así como, en su caso, la evaluación de impacto relativa a la protección de datos.
- Implantar y hacer cumplir las medidas de seguridad establecidas.
- Garantizar la difusión y formación al personal que trate con datos personales de las medidas de seguridad y requisitos que deben cumplir para realizar el tratamiento de datos personales.
- Mantener actualizada la documentación siempre que se produzcan cambios relevantes en:
- El sistema de información.
- Es sistema de tratamiento.
- La organización.
- El contenido de la información incluida en los tratamientos.
- Como consecuencia de los controles periódicos realizados.
- Se considera que un cambio es relevante cuando pueda afectar al cumplimiento de las medidas de seguridad implantadas.
- Nombrar uno o varios responsables delegados para el correcto cumplimiento de la normativa de protección de datos.
- Verificar periódicamente la eficacia de las medidas de seguridad establecidas.
- Analizar las incidencias registradas e implantará las medidas correctivas necesarias para evitar ese tipo de incidencias en el futuro.

4. FUNCIONES Y OBLIGACIONES DEL DELEGADO DE PROTECCIÓN DE DATOS O FIGURA EQUIVALENTE

El Delegado de Protección de Datos tiene las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben;
b) supervisar el cumplimiento de lo dispuesto en la normativa de protección de datos y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación;
d) cooperar con la autoridad de control;
    a. actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier asunto relacionado con el cumplimiento de la normativa de protección de datos. Para ello:
    b. Coordinará la puesta en marcha de las medidas de seguridad, colaborará con el responsable del tratamiento en su difusión y cooperará con el responsable del tratamiento controlando el cumplimiento de las mismas.
    c. Analizará las incidencias registradas, tomando las medidas oportunas en colaboración con el responsable del tratamiento.
    d. Comprobará, periódicamente, la existencia de copias de respaldo que permitan la recuperación de los datos, realizando una prueba de restaurado que verifique la correcta definición de los procedimiento y proceso de recuperación, y enviando evidencias de esta comprobación al responsable del tratamiento.
    e. A su vez, también periódicamente, comunicará el responsable del fichero cualquier cambio que se haya realizado en los sistemas de información, como cambios en el hardware o software, bases de datos, aplicaciones de acceso al fichero, etc., procediendo a la actualización de la documentación pertinente.
    f. Verificará, periódicamente, la veracidad del inventario de soportes.
    g. Tendrá el control directo de los mecanismos que permiten el registro de accesos, sin que se deba permitir, en ningún caso, la desactivación de los mismos.
    h. Se encargará de revisar, en su caso y de forma periódica, la información de control registrada en el registro de accesos y elaborará un informe que entregará al responsable del tratamiento para su revisión y archivo.
    i. Periódicamente realizará una auditoría de la eficacia de las medidas de seguridad implantadas.
    j. Los resultados de los controles periódicos, así como de las auditorías, serán adjuntados a la documentación acreditativa del cumplimiento de la normativa de protección de datos.

APÉNDICE I

GESTIÓN DE INCIDENCIAS			
FECHA:		**HORA:**	
TIPO DE INCIDENCIA:			
DESCRIPCIÓN:			
EFECTOS DERIVADOS:			
PERSONA QUE COMUNICA LA INCIDENCIA:			
PERSONA QUE RECIBE LA NOTIFICACIÓN:			
ACUSE DE RECIBO			
FECHA:		**HORA:**	
FIRMA:			

APÉNDICE II

GESTIÓN DE SOLICITUDES DE DERECHOS DE LOS INTERESADOS			
FECHA:		**HORA:**	
NOMBRE DEL SOLICITANTE			
APELLIDOS DEL SOLICITANTE:			
CIF DEL SOLICITANTE:			
DOMICILIO DEL SOLICITANTE:			
DERECHO QUE DESEA EJERCER	**[ ] ACCESO**	**[ ] RECTIFICACIÓN**	
	[ ] SUPRESIÓN	**[ ] LIMITACIÓN DEL TTO**	
	[ ] OPOSICIÓN	**[ ] PORTABILIDAD**	
	[ ] DECISIONES INDIVIDUALES AUTOMATIZADAS		
OBSERVACIONES:			
[ ] FOTOCOPIA DEL CIF INCLUIDA			
[ ] OTROS DOCUMENTOS APORTADOS:			
PERSONA QUE RECIBE LA SOLICITUD:			

ANEXO V

PERFILES DE USUARIO Y ACCESOS AUTORIZADOS

1. USUARIOS, PERFILES Y ACCESOS AUTORIZADOS

Una de las medidas principales en la gestión la seguridad de la información es la definición, por parte de la organización, de los distintos perfiles de usuario que existen en la misma y la información a la que puede acceder cada uno de dichos perfiles según sus funciones dentro de la organización.

Un perfil de usuario es, entonces, un conjunto de usuarios que acceden a los mismos tratamientos y realizan actividades comunes respecto al tratamiento de los datos personales dentro de la organización.

2. PERFILES DEFINIDOS EN LA ORGANIZACIÓN

Los perfiles de usuario, sus funciones dentro de la organización y los tratamientos a los que tiene acceso cada uno de los perfiles, se detallan a continuación:

PERFILES	FUNCIONES Y TRATAMIENTOS
GERENTE	GESTIÓN DE LA EMPRESA Este perfil es responsable de autorizar el acceso a otros. GESTIÓN DE PERSONAL (Mixto) (Administrador) GESTIÓN DE PROVEEDORES (Mixto) (Administrador) GESTIÓN DE CLIENTES (Mixto) (Administrador)
ADMINISTRATIVO	TAREAS DE ADMINISTRACION GESTIÓN DE PERSONAL (Mixto) GESTIÓN DE PROVEEDORES (Mixto) GESTIÓN DE CLIENTES (Mixto)
COMERCIAL	VENTA Y COMERCIALIZACIÓN DE PRODUCTOS Y SERVICIOS GESTIÓN DE CLIENTES (Mixto)
VENTAS	GESTION DE VENTAS
ALBAÑIL	TRABAJADOR ESPECIALIZADO EN ALBAÑILERIA
LIMPIADORA	TRABAJOS DE LIMPIEZA
MOZO INST. AIRE ACON.	INSTALADOR

Debido a su especial relevancia y privilegios, en la tabla se ha realizado especial indicación a

aquellos perfiles que son responsables de autorizar el acceso a otros y a aquellos que son administradores de cada tratamiento (es decir, aquellos que proporcionan las credenciales de acceso a la información digital o las llaves de acceso a los lugares donde se almacena la información en formato papel).

3. USUARIOS

A continuación se detallan los usuarios que pertenecen a cada uno de los perfiles definidos anteriormente:

PERFIL	USUARIOS
GERENTE	JOSE DAVID ESTEBAN MANZANO
ADMINISTRATIVO	CRISTIAN STIVEN OSORIO MONTOYA MARIA DOLORES VIVO JIMENEZ
COMERCIAL	DANNY ROBERTO TERAN ABRIL
VENTAS	DANNY ROBERTO TERAN ABRIL
ALBAÑIL	RAMON UTRERAS ESCUDERO TEJANI KHARBOUCSE
LIMPIADORA	MARIA DOLORES MANZANO GARCIA
MOZO INST. AIRE ACON.	JULIO ALBERTO NICOLAS BO JOAQUIN ALBERTO ANDREU BERANDO LAMINE TOURE LUIS ERNESTO ESCOBAR UARGAS VICTOR GUILLAMON BASTIDA DANIEL FERNANDEZ DURAN LUIS LOPEZ PUIGCERVER ENTIQUE COTTER ROS JOSE ENRIQUE MUÑOZ SRERANO

ANEXO VI

COMPROMISOS DE CONFIDENCIALIDAD

COMPROMISO DE CONFIDENCIALIDAD Y SECRETO

En _____, a _____ de _____ de _____.

REUNIDOS

De una parte, **CLIMATIZACIÓN GUADALUPE, S.L.**, con CIF/DNI: **B-01664382** y domicilio social en **Camino de los Raspajines 1 1F, 30107-Aljucer (Murcia)** (en adelante, el RESPONSABLE DEL TRATAMIENTO).

Y de otra parte, **xxNOMBRExEMPLEADOxx**, mayor de edad, actuando en su propio nombre y representación (en adelante, el USUARIO).

EXPONEN

1. Ambas partes se reconocen capacidad legal suficiente para suscribir el presente Compromiso.

2. Debido al desempeño de las funciones que el USUARIO realiza a favor del RESPONSABLE DEL TRATAMIENTO, tendrá acceso a sistemas y soportes en los que se contiene información relativa a datos de carácter personal.

3. El USUARIO es consciente de su obligación al secreto profesional respecto a los datos de carácter personal que trate y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el RESPONSABLE DEL TRATAMIENTO.

4. Ambos suscriben el presente COMPROMISO DE CONFIDENCIALIDAD Y SECRETO, el cual aceptan expresamente y de acuerdo a las siguientes:

CLÁUSULAS

- El RESPONSABLE DEL TRATAMIENTO es el único competente para establecer las políticas, reglas, normas y procedimientos para el tratamiento de la información, debiendo el USUARIO atenerse a los mismos de forma estricta. Respetará y cumplirá las medidas de seguridad implantadas para garantizar la confidencialidad y secreto de toda la información que sea considerada "confidencial". A estos efectos, será considerada información confidencial:
  ii) Cualquier información concerniente a una persona física identificada o identificable, es decir, datos de carácter personal.
  iii) Cualquier información interna de la organización, como por ejemplo, desarrollos, ideas, invenciones, dibujos, diseños, procedimientos, fórmulas, datos, programas, descubrimientos, secretos comerciales, listas de precios, información financiera, plantillas, presupuestos, nombres de clientes y/o proveedores, estadísticas, objetivos, etc.
- El USUARIO observará el más estricto secreto profesional respecto a toda información confidencial a la que tenga acceso en el desempeño de sus funciones, comprometiéndose a no divulgarla ni cederla, por cualquier medio, a Terceros u otras personas dentro de la organización del RESPONSABLE DEL TRATAMIENTO que no estén autorizadas para acceder a dicha información.
- El USUARIO solo accederá a la información confidencial que sea estrictamente necesaria para el desempeño de sus funciones, utilizando los datos exclusivamente para los fines y funciones que fueron recabados, y no para cualquier otra finalidad.
- El USUARIO comunicará todas aquellas incidencias que se produzcan en la organización y que afecten o puedan afectar a la seguridad de la información confidencial.
- El USUARIO cumplirá con las funciones y obligaciones que están recogidas en el documento "Funciones y obligaciones del personal en materia de protección de datos", que el USUARIO ha recibido o tiene a su disposición.

- Las obligaciones contenidas en este Compromiso subsistirán aún después de finalizar la relación laboral o profesional entre el USUARIO y el RESPONSABLE DEL TRATAMIENTO.
- El incumplimiento de las obligaciones estipuladas en este Compromiso por una actuación negligente del USUARIO, que genere un daño, sanción o indemnización tanto para el RESPONSABLE DEL TRATAMIENTO como para Terceros, será sancionado de conformidad con el régimen disciplinario aplicable. En el supuesto de que la actuación negligente del USUARIO exceda, por su especial gravedad, de tal ámbito disciplinario, se le podrán reclamar las indemnizaciones por incumplimiento que procedan.
- Información básica sobre protección de datos del RESPONSABLE DEL TRATAMIENTO: utilizamos sus datos personales para gestionar la relación laboral, así como los compromisos y obligaciones derivadas de ella. La legitimación en base a la cuál tratamos sus datos es: ejecución de contrato. No se cederán datos a terceros salvo obligación legal. Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, indicados en la información adicional, que puede ejercer dirigiéndose a la dirección del RESPONSABLE DEL TRATAMIENTO. Puede consultar información adicional y detallada sobre protección de datos dirigiéndose al RESPONSABLE DEL TRATAMIENTO.

Y en prueba de aceptación y conformidad con todas y cada una de las cláusulas estipuladas, obligándose al cumplimiento de todo lo acordado, lo firman por duplicado en el lugar y fecha del encabezamiento del presente documento.

Fdo. **CLIMATIZACIÓN GUADALUPE, S.L.**

Fdo. **xxNOMBRExEMPLEADOxx**

ANEXO VII

CONTRATOS DE ACCESO A DATOS CON ENCARGADOS

ANEXO VIII

CONTRATOS DE ACCESO A DATOS CON RESPONSABLES

ANEXO IX

REGISTRO DE INCIDENCIAS

REGISTRO DE INCIDENCIAS	
FECHA	
TIPO DE INCIDENCIA:	
DESCRIPCIÓN:	
EFECTOS DERIVADOS:	
MEDIDAS CORRECTORAS:	
PERSONA QUE COMUNICA LA INCIDENCIA	
PERSONA QUE RECIBE LA NOTIFICACIÓN	
PERSONA QUE EJECUTÓ EL PROCESO DE RECUPERACIÓN	
DATOS RESTAURADOS	
DATOS GRABADOS MANUALMENTE	

ANEXO X

PROTOCOLOS DE ATENCIÓN

A LOS DERECHOS DE LOS INTERESADOS

1. LOS DERECHOS DE LOS INTERESADOS

Los derechos que los interesados pueden solicitar al responsable del tratamiento son los siguientes:

- Derecho de acceso.
- Derecho de rectificación.
- Derecho de supresión («el derecho al olvido»).
- Derecho a la limitación del tratamiento.
- Derecho a la portabilidad de los datos.
- Derecho de oposición.
- Derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles.

Hay que tener especial cuidado y diligencia en la resolución satisfactoria del ejercicio de estos derechos en plazo y forma, ya que de su omisión pueden derivarse cuantiosas sanciones.

CLIMATIZACIÓN GUADALUPE, S.L., deberá informar al personal que tiene acceso a datos personales del procedimiento a seguir para facilitar a los interesados o afectados el ejercicio de sus derechos.

1.1 QUIÉN PUEDE SOLICITAR LOS DERECHOS

Los derechos son personalísimos y serán ejecutados por el afectado.

Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad.
b) Por su representante legal (acreditado), cuando el afectado se encuentre en situación de discapacidad o minoría de edad que el imposibilite el ejercicio personal de estos derechos.
c) Por un representante voluntario, expresamente designado para el ejercicio del derecho. En este caso, deberá constar claramente acreditada la identidad del representado, mediante DNI o documento equivalente, y la representación conferida por aquél.

Los derechos serán denegados cuando la solicitud sea formulada por una persona distinta del afectado y no se acredita que actúa en representación de aquél.

1.2 GRATUIDAD DEL EJERCICIO DE LOS DERECHOS

Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos. El ejercicio de los derechos también será gratuito para el interesado.

No se considerarán conformes los supuestos siguientes:

- El envío de cartas certificadas o semejantes.
- La utilización de servicios de telecomunicaciones que impliquen tarificación adicional.
- Cualquier medio que implique un coste excesivo para el interesado.

Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

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

CLIMATIZACIÓN GUADALUPE, S.L. soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

1.3 PROCEDIMIENTO

Deberá dirigirse una comunicación a **CLIMATIZACIÓN GUADALUPE, S.L.** en la que conste:

- Nombre y apellidos del interesado.
- Fotocopia del DNI/CIF del interesado, y en su caso, de la persona que lo representa, así como el documento que acredita tal representación.
- Petición en que se concreta la solicitud.
- Dirección a efectos de notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición que formula, en su caso.

CLIMATIZACIÓN GUADALUPE, S.L. deberá contestar la solicitud que se le dirija en todo caso, teniendo en cuenta que:

- Deberá responder incluso si no figuran los datos personales del afectado en sus ficheros.
- En caso de que la solicitud no reúna los requisitos, solicitar la subsanación de los mismos.
- Deberá guardar prueba del cumplimiento del deber, conservando la acreditación del mismo.
- Deberá adoptar las medidas oportunas para garantizar que el personal que tenga acceso a datos, pueda informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

En el supuesto de no contestar dentro de los plazos establecidos, o hacerlo de forma incompleta, el afectado podrá ponerlo en conocimiento de la AEPD, pudiendo abrir la misma un expediente sancionador y pudiendo derivarse del mismo una sanción.

Cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud para que se atiendan sus derechos, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

1.4 PLAZOS DE TIEMPO

CLIMATIZACIÓN GUADALUPE, S.L. facilitará al interesado la información relativa a sus actuaciones en un plazo máximo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso de ser necesario, teniendo en cuenta la complejidad y el número de solicitudes.

CLIMATIZACIÓN GUADALUPE, S.L. informará 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.

1.5 FORMA DE FACILITAR LA INFORMACIÓN

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

1.6 LOS DERECHOS ANTE UN ENCARGADO DEL TRATAMIENTO

Cuando los afectados ejerciten sus derechos ante un encargado del tratamiento, el encargado deberá trasladar la solicitud **CLIMATIZACIÓN GUADALUPE, S.L.** para que proceda a su resolución, salvo que en el contrato de encargo se haya pactado que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio de derechos de los afectados.

1.7 DENEGACIÓN DE LOS DERECHOS

Si **CLIMATIZACIÓN GUADALUPE, S.L.** no da curso a la solicitud del interesado, le informará 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.

2. DERECHO DE ACCESO

El derecho de acceso es el derecho del interesado a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;
b) Las categorías de datos personales de que se trate;
c) Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
d) De ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
e) La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
f) El derecho a presentar una reclamación ante una autoridad de control;
g) Cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
h) La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas relativas a la transferencia.

2.1 EJERCICIO DEL DERECHO DE ACCESO

Al ejercitar el derecho de acceso un interesado, **CLIMATIZACIÓN GUADALUPE, S.L.** facilitará una copia de los datos personales objeto de tratamiento.

El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon

razonable basado en los costes administrativos.

Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

El derecho a obtener copia mencionada de los datos no afectará negativamente a los derechos y libertades de otros (es decir, que no haya datos de otros interesados en dicha copia).

2.2 DENEGACIÓN DEL ACCESO

CLIMATIZACIÓN GUADALUPE, S.L. podrá denegar el acceso en estos casos:

Cuando la solicitud sea formulada por una persona distinta del afectado y no se acredita que actúa en representación de aquél.

Cuando lo prevea una Ley o una norma de derecho comunitario.

3. DERECHO DE RECTIFICACIÓN

El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan.

Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

CLIMATIZACIÓN GUADALUPE, S.L. comunicará cualquier rectificación de datos personales a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. También informará al interesado acerca de dichos destinatarios, si este así lo solicita.

3.1 EJERCICIO DEL DERECHO DE RECTIFICACIÓN

El afectado podrá ejercer el derecho de rectificación ante **CLIMATIZACIÓN GUADALUPE, S.L.** a través de la solicitud correspondiente, que deberá tener:

Los datos en que se concreta la solicitud y expuestos en el apartado 1.3.

La corrección a realizar (en caso de rectificación) o los datos que deban ser completados.

La documentación justificativa de lo solicitado.

4. DERECHO DE SUPRESIÓN ("EL DERECHO AL OLVIDO")

El interesado tendrá derecho a obtener sin dilación indebida de **CLIMATIZACIÓN GUADALUPE, S.L.** la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de sus datos personales, y dicho tratamiento no se base en otro fundamento jurídico;
c) El interesado se oponga al tratamiento realizado por un responsable en base al interés legítimo, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento de sus datos personales con fines de mercadotecnia directa;
d) Los datos personales hayan sido tratados ilícitamente;
e) Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
f) Los datos personales se hayan obtenido en base al consentimiento, en relación con una oferta de servicios de la sociedad de la información dirigida a niños.

Cuando haya hecho públicos los datos personales y esté obligado a suprimir dichos datos, **CLIMATIZACIÓN GUADALUPE, S.L.**, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

CLIMATIZACIÓN GUADALUPE, S.L. comunicará cualquier supresión de datos personales a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. También informará al interesado acerca de dichos destinatarios, si este así lo solicita.

4.1 DENEGACIÓN DEL DERECHO DE SUPRESIÓN

La supresión de los datos no se aplicará cuando el tratamiento sea necesario:

a) Para ejercer el derecho a la libertad de expresión e información;
b) 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;
c) Por razones de interés público en el ámbito de la salud pública;
d) Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
e) Para la formulación, el ejercicio o la defensa de reclamaciones.

5. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
b) El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
d) El interesado se haya opuesto al tratamiento en base al interés legítimo, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Cuando el tratamiento de datos personales se haya limitado, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

Todo interesado que haya obtenido la limitación del tratamiento será informado por el responsable antes del levantamiento de dicha limitación.

CLIMATIZACIÓN GUADALUPE, S.L. comunicará cualquier limitación del tratamiento de datos a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. También informará al interesado acerca de dichos destinatarios, si este así lo solicita.

6. DERECHO DE PORTABILIDAD DE LOS DATOS

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a **CLIMATIZACIÓN GUADALUPE, S.L.**, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) El tratamiento esté basado en el consentimiento, o en un contrato en el que el interesado es parte, y
b) El tratamiento se efectúe por medios automatizados.

Al ejercer su derecho a la portabilidad de los datos, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

El derecho de portabilidad de los datos no afectará negativamente a los derechos y libertades de otros.

7. DERECHO DE OPOSICIÓN

El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en:

a) Que es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, o
b) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

Incluida la elaboración de perfiles sobre la base de dichas disposiciones.

a) El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

7.1 OPOSICIÓN PARA FINES DE MERCADOTECNIA DIRECTA

a) Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.
b) Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

7.2 INFORMACIÓN DEL DERECHO DE OPOSICIÓN

A más tardar en el momento de la primera comunicación con el interesado, el derecho de oposición indicado en los apartados anteriores será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

7.3 EJERCICIO DEL DERECHO POR MEDIOS AUTOMATIZADOS

En el contexto de la utilización de servicios de la sociedad de la información, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

8. DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES

Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Lo anterior no se aplicará si la decisión:

a) Es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
b) Está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
c) Se basa en el consentimiento explícito del interesado.

En los casos a que se refieren las letras a) y c), **CLIMATIZACIÓN GUADALUPE, S.L.** adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

Las decisiones anteriores no se basarán en las categorías especiales de datos personales, salvo que haya obtenido el consentimiento explícito del interesado o sea necesario por razones de interés público esencial, y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

9. DERECHO A INDEMNIZACIÓN Y RESPONSABILIDAD

Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción de la normativa de protección de datos, tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro en el que el responsable o encargado tenga establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

ANEXO XI

CLÁUSULAS LEGALES

Tratamiento de los datos de clientes - Capa 1

Información básica sobre Protección de datos	
Responsable:	**CLIMATIZACIÓN GUADALUPE, S.L.**
Finalidad:	Prestar los servicios solicitados y enviar comunicaciones comerciales
Legitimación:	Ejecución de un contrato. Interés legítimo del Responsable.
Destinatarios:	Están previstas cesiones de datos a: Agencia Tributaria; Entidades financieras.
Derechos:	Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, indicados en la información adicional, que puede ejercer dirigiéndose a la dirección del responsable del tratamiento
Procedencia:	El propio interesado.
Información adicional:	

Esta cláusula se deberá incorporar en los formularios donde se recojan datos personales de clientes. Ej. hojas de pedido, formularios, contratos, etc.

Fecha:

Nombre y apellidos:

_____

Firma:

1. ¿Quién es el responsable del tratamiento de sus datos?

CLIMATIZACIÓN GUADALUPE, S.L.

B-01664382

Camino de los Raspajines 1 1F, 30107-Aljucer (Murcia)

2. ¿Con qué finalidad tratamos sus datos personales?

En **CLIMATIZACIÓN GUADALUPE, S.L.** tratamos la información que nos

facilitan las personas interesadas con el fin de Realizar la gestión administrativa, contable y fiscal de los servicios solicitados, así como enviar comunicaciones comerciales sobre nuestros productos y servicios.

3. ¿Por cuánto tiempo conservaremos sus datos?

Los datos se conservarán mientras el interesado no solicite su supresión, y en su caso, durante los años necesarios para cumplir con las obligaciones legales.

4. ¿Cuál es la legitimación para el tratamiento de sus datos?

Le indicamos la base legal para el tratamiento de sus datos:

- Ejecución de un contrato: Prestación de los servicios solicitados
- Interés legítimo del responsable: Envío de comunicaciones comerciales

5. ¿A qué destinatarios se comunicarán sus datos?

Los datos se comunicarán a los siguientes destinatarios:

- Agencia Tributaria, con la finalidad de Cumplir con las obligaciones legales
- Entidades financieras, con la finalidad de Girar los recibos correspondientes

6. Transferencias de datos a terceros países

No están previstas transferencias de datos a terceros países.

7. ¿Cuáles son sus derechos cuando nos facilita sus datos?

Cualquier persona tiene derecho a obtener confirmación sobre si en **CLIMATIZACIÓN GUADALUPE, S.L.** estamos tratando datos personales que les conciernan, o no.

Las personas interesadas tienen derecho a 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. En

este caso, **CLIMATIZACIÓN GUADALUPE, S.L.** dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.

Podrá ejercitar materialmente sus derechos de la siguiente forma: dirigiéndose a la dirección del responsable del tratamiento

Si ha otorgado su consentimiento para alguna finalidad concreta, tiene derecho a retirar el consentimiento otorgado en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

En caso de que sienta vulnerados sus derechos en lo concerniente a la protección de sus datos personales, especialmente cuando no haya obtenido satisfacción en el ejercicio de sus derechos, puede presentar una reclamación ante la Autoridad de Control en materia de Protección de Datos competente a través de su sitio web: www.agpd.es.

8. ¿Cómo hemos obtenido sus datos?

Los datos personales que tratamos en **CLIMATIZACIÓN GUADALUPE, S.L.** proceden del propio interesado.

Las categorías de datos que se tratan son:

- Datos identificativos
- Direcciones postales y electrónicas
- Información comercial

No se tratan categorías especiales de datos personales (son aquellos datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física).

Tratamiento de los datos de potenciales clientes - Capa 1

Información básica sobre Protección de datos	
Responsable:	**CLIMATIZACIÓN GUADALUPE, S.L.**
Finalidad:	Atender su solicitud y enviarle comunicaciones comerciales
Legitimación:	Ejecución de un contrato. Consentimiento del interesado.
Destinatarios:	No se cederán datos a terceros, salvo obligación legal.
Derechos:	Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, indicados en la información adicional, que puede ejercer Puede ejercer sus derechos enviando un correo electrónico al responsable
Procedencia:	El propio interesado.
Información adicional:	

Esta cláusula debe incluirse en los formularios de contacto de la web o de otros lugares donde se recojan datos de potenciales clientes

Fecha:

Nombre y apellidos:

Firma:

1. ¿Quién es el responsable del tratamiento de sus datos?

CLIMATIZACIÓN GUADALUPE, S.L.

B-01664382

Camino de los Raspajines 1 1F, 30107-Aljucer (Murcia)

2. ¿Con qué finalidad tratamos sus datos personales?

En **CLIMATIZACIÓN GUADALUPE, S.L.** tratamos la información que nos facilitan las personas interesadas con el fin de Atender su solicitud y enviarle comunicaciones comerciales, inclusive por vía electrónica

3. ¿Por cuánto tiempo conservaremos sus datos?

Los datos se conservarán mientras el interesado no solicite su supresión

4. ¿Cuál es la legitimación para el tratamiento de sus datos?

Le indicamos la base legal para el tratamiento de sus datos:

- Ejecución de un contrato: Atender su solicitud
- Consentimiento del interesado: Enviarle comunicaciones comerciales

5. ¿A qué destinatarios se comunicarán sus datos?

No se cederán datos a terceros, salvo obligación legal.

6. Transferencias de datos a terceros países

No están previstas transferencias de datos a terceros países.

7. ¿Cuáles son sus derechos cuando nos facilita sus datos?

Cualquier persona tiene derecho a obtener confirmación sobre si en **CLIMATIZACIÓN GUADALUPE, S.L.** estamos tratando datos personales que les conciernan, o no.

Las personas interesadas tienen derecho a 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. En este caso, **CLIMATIZACIÓN GUADALUPE, S.L.** dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.

Podrá ejercitar materialmente sus derechos de la siguiente forma: Puede ejercer sus derechos enviando un correo electrónico al responsable

Si ha otorgado su consentimiento para alguna finalidad concreta, tiene derecho a retirar el consentimiento otorgado en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

En caso de que sienta vulnerados sus derechos en lo concerniente a la protección de sus datos personales, especialmente cuando no haya obtenido satisfacción en el ejercicio de sus derechos, puede presentar una reclamación ante la Autoridad de Control en materia de Protección de Datos competente a través de su sitio web: www.agpd.es.

8. ¿Cómo hemos obtenido sus datos?

Los datos personales que tratamos en **CLIMATIZACIÓN GUADALUPE, S.L.**

proceden del propio interesado.

Las categorías de datos que se tratan son:

- Datos identificativos
- Direcciones postales y electrónicas

No se tratan categorías especiales de datos personales (son aquellos datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física).

Tratamiento de los datos de candidatos a un puesto de trabajo - Capa 1

Información básica sobre Protección de datos	
Responsable:	**CLIMATIZACIÓN GUADALUPE, S.L.**
Finalidad:	Realizar los procesos de selección de personal
Legitimación:	Consentimiento del interesado.
Destinatarios:	No se cederán datos a terceros, salvo obligación legal.
Derechos:	Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, indicados en la información adicional, que puede ejercer dirigiéndose a la dirección del responsable del tratamiento
Procedencia:	El propio interesado.
Información adicional:	

En el acuse de recibo a la recepción de Curriculum Vitae o en los formularios utilizados en los procesos de selección de personal

Fecha:

Nombre y apellidos: _____

Firma:

1. ¿Quién es el responsable del tratamiento de sus datos?

CLIMATIZACIÓN GUADALUPE, S.L.

B-01664382

Camino de los Raspajines 1 1F, 30107-Aljucer (Murcia)

2. ¿Con qué finalidad tratamos sus datos personales?

En **CLIMATIZACIÓN GUADALUPE, S.L.** tratamos la información que nos facilitan las personas interesadas con el fin de Gestionar los currículos Vitae recibidos y realizar los procesos de selección de personal

3. ¿Por cuánto tiempo conservaremos sus datos?

Dos años desde la última interacción

4. ¿Cuál es la legitimación para el tratamiento de sus datos?

Le indicamos la base legal para el tratamiento de sus datos:

Consentimiento del interesado: Gestionar los Currículos Vitae recibidos y realizar los procesos de selección de personal

5. ¿A qué destinatarios se comunicarán sus datos?

No se cederán datos a terceros, salvo obligación legal.

6. Transferencias de datos a terceros países

No están previstas transferencias de datos a terceros países.

7. ¿Cuáles son sus derechos cuando nos facilita sus datos?

Cualquier persona tiene derecho a obtener confirmación sobre si en **CLIMATIZACIÓN GUADALUPE, S.L.** estamos tratando datos personales que les conciernan, o no.

Las personas interesadas tienen derecho a 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. En este caso, **CLIMATIZACIÓN GUADALUPE, S.L.** dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.

Podrá ejercitar materialmente sus derechos de la siguiente forma: dirigiéndose a la dirección del responsable del tratamiento

Si ha otorgado su consentimiento para alguna finalidad concreta, tiene derecho a retirar el consentimiento otorgado en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

En caso de que sienta vulnerados sus derechos en lo concerniente a la protección de sus datos personales, especialmente cuando no haya obtenido satisfacción en el ejercicio de sus derechos, puede presentar una reclamación ante la Autoridad de Control en materia de Protección de Datos competente a través de su sitio web: www.agpd.es.

8. ¿Cómo hemos obtenido sus datos?

Los datos personales que tratamos en **CLIMATIZACIÓN GUADALUPE, S.L.** proceden del propio interesado.

Las categorías de datos que se tratan son:

- Datos identificativos
- Direcciones postales y electrónicas

No se tratan categorías especiales de datos personales (son aquellos datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física).

ASESORES&DATOS

Tratamiento de los datos del personal - Capa 1

Información básica sobre Protección de datos	
Responsable:	**CLIMATIZACIÓN GUADALUPE, S.L.**
Finalidad:	Gestionar la relación laboral
Legitimación:	Ejecución de un contrato.
Destinatarios:	Están previstas cesiones de datos a: Agencia Tributaria, Seguridad Social y Mutua.
Derechos:	Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, indicados en la información adicional, que puede ejercer dirigiéndose a la dirección del responsable del tratamiento
Procedencia:	El propio interesado.
Información adicional:	

Esta cláusula se deberá incorporar en los documentos que recojan datos personales de los trabajadores. Ej. Contratos, nóminas, circulares a trabajadores, etc.

Fecha:

Nombre y apellidos: _____

Firma:

1. ¿Quién es el responsable del tratamiento de sus datos?

CLIMATIZACIÓN GUADALUPE, S.L.

B-01664382

Camino de los Raspajines 1 1F, 30107-Aljucer (Murcia)

2. ¿Con qué finalidad tratamos sus datos personales?

En **CLIMATIZACIÓN GUADALUPE, S.L.** tratamos la información que nos facilitan las personas interesadas con el fin de Elaborar el contrato de trabajo, nóminas y seguros sociales, así como realizar la prevención de riesgos laborales y la vigilancia de la salud.

3. ¿Por cuánto tiempo conservaremos sus datos?

Mientras se mantenga la relación laboral con la entidad y durante los años necesarios para cumplir con las obligaciones legales.

4. ¿Cuál es la legitimación para el tratamiento de sus datos?

Le indicamos la base legal para el tratamiento de sus datos:

Ejecución de un contrato: Mantenimiento de la relación laboral

5. ¿A qué destinatarios se comunicarán sus datos?

Los datos se comunicarán a los siguientes destinatarios:

Agencia Tributaria, Seguridad Social y Mutua, con la finalidad de Cumplimiento de las obligaciones legales

6. Transferencias de datos a terceros países

No están previstas transferencias de datos a terceros países.

7. ¿Cuáles son sus derechos cuando nos facilita sus datos?

Cualquier persona tiene derecho a obtener confirmación sobre si en **CLIMATIZACIÓN GUADALUPE, S.L.** estamos tratando datos personales que les conciernan, o no.

Las personas interesadas tienen derecho a 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. En este caso, **CLIMATIZACIÓN GUADALUPE, S.L.** dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.

Podrá ejercitar materialmente sus derechos de la siguiente forma: dirigiéndose a la dirección del responsable del tratamiento

Si ha otorgado su consentimiento para alguna finalidad concreta, tiene derecho a retirar el consentimiento otorgado en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

En caso de que sienta vulnerados sus derechos en lo concerniente a la protección de sus datos personales, especialmente cuando no haya obtenido satisfacción en el ejercicio de sus derechos, puede presentar una reclamación ante la Autoridad de Control en materia de Protección de Datos competente a través de su sitio web: www.agpd.es.

8. ¿Cómo hemos obtenido sus datos?

Los datos personales que tratamos en **CLIMATIZACIÓN GUADALUPE, S.L.** proceden del propio interesado.

Las categorías de datos que se tratan son:

- Datos identificativos
- Información comercial
- Datos económicos

Se tratan las siguientes categorías de datos especiales: salud

1. OBJETO

El presente aviso legal regula el uso y utilización del sitio web [DOMINIOWEB], del que es titular **CLIMATIZACIÓN GUADALUPE, S.L.** (en adelante, EL PROPIETARIO DE LA WEB).

La navegación por el sitio web de EL PROPIETARIO DE LA WEB le atribuye la condición de USUARIO del mismo y conlleva su aceptación plena y sin reservas de todas y cada una de las condiciones publicadas en este aviso legal, advirtiendo de que dichas condiciones podrán ser modificadas sin notificación previa por parte de EL PROPIETARIO DE LA WEB, en cuyo caso se procederá a su publicación y aviso con la máxima antelación posible.

Por ello es recomendable leer atentamente su contenido en caso de desear acceder y hacer uso de la información y de los servicios ofrecidos desde este sitio web.

El usuario además, se obliga a hacer un uso correcto del sitio web de conformidad con las leyes, la buena fe, el orden público, los usos del tráfico y el presente Aviso Legal, y responderá frente a EL PROPIETARIO DE LA WEB o frente a terceros, de cualesquiera daños y perjuicios que pudieran causarse como consecuencia del incumplimiento de dicha obligación.

Cualquier utilización distinta a la autorizada está expresamente prohibida, pudiendo EL PROPIETARIO DE LA WEB denegar o retirar el acceso y su uso en cualquier momento.

2. IDENTIFICACIÓN

EL PROPIETARIO DE LA WEB, en cumplimiento de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, le informa de que:

- Su denominación social es: **CLIMATIZACIÓN GUADALUPE, S.L.**
- Su CIF/DNI es: **B-01664382**
- Su domicilio social está en: **Camino de los Raspajines 1 1F, 30107-Aljucer (Murcia)**
- [DATOS DE INSCRIPCIÓN EN EL REGISTRO MERCANTIL, EN SU CASO]

3. COMUNICACIONES

Para comunicarse con nosotros, ponemos a su disposición diferentes medios de contacto que detallamos a continuación:

Todas las notificaciones y comunicaciones entre los usuarios y PROPIETARIO DE LA WEB se considerarán eficaces, a todos los efectos, cuando se realicen a través de cualquier medio de los detallados anteriormente.

4. CONDICIONES DE ACCESO Y UTILIZACIÓN

El sitio web y sus servicios son de acceso libre y gratuito. No obstante, PROPIETARIO DE LA WEB puede condicionar la utilización de algunos de los servicios ofrecidos en su web a la previa cumplimentación del correspondiente formulario.

El usuario garantiza la autenticidad y actualidad de todos aquellos datos que comunique a PROPIETARIO DE LA WEB y será el único responsable de las manifestaciones falsas o inexactas que realice.

El usuario se compromete expresamente a hacer un uso adecuado de los contenidos y servicios de PROPIETARIO DE LA WEB y a no emplearlos para, entre otros:

a) Difundir contenidos delictivos, violentos, pornográficos, racistas, xenófobos, ofensivos, de apología del terrorismo o, en general, contrarios a la ley o al orden público.
b) Introducir en la red virus informáticos o realizar actuaciones susceptibles de alterar, estropear, interrumpir o generar errores o daños en los documentos electrónicos, datos o sistemas físicos y lógicos de PROPIETARIO DE LA WEB o de terceras personas; así como obstaculizar el acceso de otros usuarios al sitio web y a sus servicios mediante el consumo masivo de los recursos informáticos a través de los cuales PROPIETARIO DE LA WEB presta sus servicios.
c) Intentar acceder a las cuentas de correo electrónico de otros usuarios o a áreas restringidas de los sistemas informáticos de PROPIETARIO DE LA WEB o de terceros y, en su caso, extraer información.
d) Vulnerar los derechos de propiedad intelectual o industrial, así como violar la confidencialidad de la información de PROPIETARIO DE LA WEB o de terceros.
e) Suplantar la identidad de cualquier otro usuario.
f) Reproducir, copiar, distribuir, poner a disposición de, o cualquier otra forma de comunicación pública, transformar o modificar los contenidos, a menos que se cuente con la autorización del titular de los correspondientes derechos o ello resulte legalmente permitido.
g) Recabar datos con finalidad publicitaria y de remitir publicidad de cualquier clase y comunicaciones con fines de venta u otras de naturaleza comercial sin que medie su previa solicitud o consentimiento.

Todos los contenidos del sitio web, como textos, fotografías, gráficos, imágenes, iconos, tecnología, software, así como su diseño gráfico y códigos fuente, constituyen una obra cuya propiedad pertenece a PROPIETARIO DE LA WEB, sin que puedan entenderse cedidos al usuario ninguno de los derechos de explotación sobre los mismos más allá de lo estrictamente necesario para el correcto uso de la web.

En definitiva, los usuarios que accedan a este sitio web pueden visualizar los contenidos y efectuar, en su caso, copias privadas autorizadas siempre que los elementos reproducidos no sean cedidos posteriormente a terceros, ni se instalen a servidores conectados a redes, ni sean objeto de ningún tipo de explotación.

Asimismo, todas las marcas, nombres comerciales o signos distintivos de cualquier clase que aparecen en el sitio web son propiedad de PROPIETARIO DE LA WEB, sin que pueda entenderse que el uso o acceso al mismo atribuya al usuario derecho alguno sobre los mismos.

La distribución, modificación, cesión o comunicación pública de los contenidos y cualquier otro acto que no haya sido expresamente autorizado por el titular de los derechos de explotación quedan prohibidos.

El establecimiento de un hiperenlace no implica en ningún caso la existencia de relaciones entre PROPIETARIO DE LA WEB y el propietario del sitio web en la que se establezca, ni la aceptación y aprobación por parte de PROPIETARIO DE LA WEB de sus contenidos o servicios.

PROPIETARIO DE LA WEB no se responsabiliza del uso que cada usuario le dé a los

materiales puestos a disposición en este sitio web ni de las actuaciones que realice en base a los mismos.

4.1 EXCLUSIÓN DE GARANTÍAS Y DE RESPONSABILIDAD EN EL ACCESO Y LA UTILIZACIÓN

El contenido del presente sitio web es de carácter general y tiene una finalidad meramente informativa, sin que se garantice plenamente el acceso a todos los contenidos, ni su exhaustividad, corrección, vigencia o actualidad, ni su idoneidad o utilidad para un objetivo específico.

PROPIETARIO DE LA WEB excluye, hasta donde permite el ordenamiento jurídico, cualquier responsabilidad por los daños y perjuicios de toda naturaleza derivados de:

a) La imposibilidad de acceso al sitio web o la falta de veracidad, exactitud, exhaustividad y/o actualidad de los contenidos, así como la existencia de vicios y defectos de toda clase de los contenidos transmitidos, difundidos, almacenados, puestos a disposición, a los que se haya accedido a través del sitio web o de los servicios que se ofrecen.
b) La presencia de virus o de otros elementos en los contenidos que puedan producir alteraciones en los sistemas informáticos, documentos electrónicos o datos de los usuarios.
c) El incumplimiento de las leyes, la buena fe, el orden público, los usos del tráfico y el presente aviso legal como consecuencia del uso incorrecto del sitio web. En particular, y a modo ejemplificativo, PROPIETARIO DE LA WEB no se hace responsable de las actuaciones de terceros que vulneren derechos de propiedad intelectual e industrial, secretos empresariales, derechos al honor, a la intimidad personal y familiar y a la propia imagen, así como la normativa en materia de competencia desleal y publicidad ilícita.

Asimismo, PROPIETARIO DE LA WEB declina cualquier responsabilidad respecto a la información que se halle fuera de esta web y no sea gestionada directamente por nuestro webmaster. La función de los links que aparecen en esta web es exclusivamente la de informar al usuario sobre la existencia de otras fuentes susceptibles de ampliar los contenidos que ofrece este sitio web. PROPIETARIO DE LA WEB no garantiza ni se responsabiliza del funcionamiento o accesibilidad de los sitios enlazados; ni sugiere, invita o recomienda la visita a los mismos, por lo que tampoco será responsable del resultado obtenido. PROPIETARIO DE LA WEB no se responsabiliza del establecimiento de hipervínculos por parte de terceros.

4.2 PROCEDIMIENTO EN CASO DE REALIZACIÓN DE ACTIVIDADES DE CARÁCTER ILÍCITO

En el caso de que cualquier usuario o un tercero considere que existen hechos o circunstancias que revelen el carácter ilícito de la utilización de cualquier contenido y/o de la realización de cualquier actividad en las páginas web incluidas o accesibles a través del sitio web, deberá enviar una notificación a PROPIETARIO DE LA WEB identificándose debidamente y especificando las supuestas infracciones.

4.3 PUBLICACIONES

La información administrativa facilitada a través del sitio web no sustituye la publicidad

legal de las leyes, normativas, planes, disposiciones generales y actos que tengan que ser publicados formalmente a los diarios oficiales de las administraciones públicas, que constituyen el único instrumento que da fe de su autenticidad y contenido. La información disponible en este sitio web debe entenderse como una guía sin propósito de validez legal.

5. LEGISLACIÓN APLICABLE

Las condiciones presentes se regirán por la legislación española vigente.

La lengua utilizada será el castellano.

CLÁUSULA PARA EL CORREO ELECTRÓNICO

Información Básica de Protección de Datos. Responsable: **CLIMATIZACIÓN GUADALUPE, S.L.**; Finalidad: prestarle los servicios que nos ha solicitado, atender sus solicitudes de información y enviarle comunicaciones comerciales. Legitimación: Ejecución de contrato, Interés legítimo del responsable o Consentimiento del Interesado. Cesiones: No se cederán sus datos a terceros salvo obligación legal.

Derechos: Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, Vd. dispone de 30 días para manifestar su oposición al tratamiento y cesiones antes descritas. Pasado dicho plazo y de no pronunciarse a tal efecto entenderemos que acepta las presentes cláusulas.

Este mensaje y sus archivos adjuntos van dirigidos exclusivamente a su destinatario, pudiendo contener información confidencial sometida a secreto profesional. No está permitida su reproducción o distribución sin nuestra autorización expresa. Si usted no es el destinatario final por favor elimínelo e infórmenos por esta vía. Puede ejercer los derechos de Acceso, Cancelación, Rectificación u Oposición dirigiéndose a **Camino de los Raspajines 1 1F, 30107-Aljucer (Murcia)** o enviando un email a **climatizacionguadalupesl@gmail.com** .

ANEXO XII

DOCUMENTACIÓN ADICIONAL