DOCUMENTO DE SEGURIDAD

ASISTIA GRAN CANARIA SL

21 de septiembre de 2020

Contenido del documento de seguridad

ANEXOS:

1.- Definiciones

Para una mejor comprensión del contenido y comprensión de los procedimientos descritos en el presente Documento de Seguridad, cabe tener presente las definiciones previstas en la normativa de protección de datos:

- Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

- **Persona identificable:** Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

- **Fichero:** Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

- **Fichero no automatizado:** Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

- **Tratamiento de datos:** Cualquier operación o procedimiento técnico, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

- Responsable del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

- **Afectado o interesado:** Persona física titular de los datos que sean objeto del tratamiento.

- **Encargado del tratamiento:** La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del tratamiento, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

- **Cesión o comunicación de datos:** Tratamiento de datos que supone su revelación a una persona distinta del interesado.

- **Destinatario o cesionario:** La persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

- **Consentimiento del interesado:** Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

- **Dato disociado:** Aquél que no permite la identificación de un afectado o interesado.

- **Procedimiento de disociación:** Todo tratamiento de datos personales que permita la obtención de datos disociados.

- **Transferencia internacional de datos:** Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del tratamiento establecido en territorio español.

- **Exportador de datos personales:** La persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice una transferencia de datos de carácter personal a un país tercero.

- **Importador de datos personales:** La persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

- **Fuentes accesibles al público:** Aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, las guías de servicios de comunicaciones electrónicas y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

- **Sistemas de información:** Conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

- **Usuario:** Sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

- **Perfil de usuario:** Accesos autorizados a un grupo de usuarios.

- **Accesos autorizados:** Autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del tratamiento.

- **Recurso:** Cualquier parte componente de un sistema de información.

- **Identificación:** Procedimiento de reconocimiento de la identidad de un usuario.

- **Autenticación:** Procedimiento de comprobación de la identidad de un usuario.

- **Control de acceso:** Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

- **Contraseña:** Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

- **Incidencia:** Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

- **Soporte:** 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.

- **Documento:** Todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

- **Ficheros temporales:** Ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

- **Transmisión de documentos:** Cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

- **Copia del respaldo:** Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación

2.- OBJETO DEL DOCUMENTO

En virtud de lo establecido en la normativa de Protección de Datos de Carácter Personal, el Responsable del Tratamiento y, en su caso, el Encargado del Tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal, a los efectos de evitar e impedir su alteración, pérdida, tratamiento o acceso no autorizados teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Ésta obligación de garantizar la seguridad de los datos de carácter personal obliga a ASISTIA GRAN CANARIA SL, a aplicar medidas que ofrezcan un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

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

El presente manual de procedimientos de seguridad (en adelante “Documento de Seguridad”) responde a esa obligación, recogiendo las medidas de índole técnica y organizativas necesarias para garantizar los ficheros que contienen datos de carácter personal correspondientes a ASISTIA GRAN CANARIA SL.

El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados siempre con el prisma de aplicar el principio de responsabilidad activa marcado por la legislación así como ofrecer una protección de datos desde el diseño.

Por tanto, el contenido del Documento de Seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal así como a la realidad de la ASISTIA GRAN CANARIA SL Siendo responsabilidad de la empresa, como responsable del tratamiento, adoptar las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

3.- ÁMBITO DE APLICACIÓN

El presente Documento de Seguridad será de aplicación sobre los tratamientos que contienen datos de carácter personal que se hallan bajo la responsabilidad de ASISTIA GRAN CANARIA SL incluyendo los sistemas de información, soportes y equipos informáticos empleados para el tratamiento de datos de carácter personal, aplicando las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

I.- Establecimiento de las medidas de seguridad e identificación de los tratamientos.

En base a lo anterior, se han establecido diferentes medidas de seguridad clasificadas en tres niveles acumulativos, con carácter de mínimos exigibles, atendiendo a la naturaleza de los datos objeto de tratamiento, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información. Estos niveles son los siguientes:

1) Nivel básico: Cualquier fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros.
- Se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero.
- En los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

2) Nivel medio: Ficheros o tratamientos con datos que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas.

3) Nivel alto: Ficheros o tratamientos con datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico.

Los tratamientos sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondientes son los siguientes:

Nombre del Tratamiento	Tipología de datos	Tratamiento
CONTABILIDAD Y ADMINISTRACIÓN	Básico	Interno/Externo
HISTORIAL CLINICO	Alto	Interno
RECURSOS HUMANOS	Básico	Interno/Externo
PACIENTES	Alto	Interno
USUARIOS WEB	Básico	Interno/Externo
CLIENTES	Básico	Interno/Externo
VIDEOVIGILANCIA	Básico	Interno/Externo

En el **Anexo I** se describen detalladamente cada uno de los tratamientos y ofrece la posibilidad de llevar a cabo el Registro de Actividades de tratamiento.

II.- Centros de tratamiento

A continuación se detallan los centros propios donde se realiza el tratamiento de los datos personales:

RAZÓN SOCIAL: ASISTIA GRAN CANARIA SL		CIF: B76195908
CENTRO DE TRATAMIENTO: CLÍNICA		TEL:
DIRECCIÓN: AVENIDA PRIMERO DE MAYO 9 LOCAL	CP: 35002	POBLACIÓN: LAS PALMAS DE GRAN CANARIA

Por otra parte, se adjunta en el **Anexo VIII** la relación de los centros de aquellos proveedores que tienen la consideración de Encargados de Tratamiento

III.- Inventario de recursos informáticos

ASISTIA GRAN CANARIA SL dispone de varios equipos y programas informáticos mediante los cuales se tratan o almacenan datos de carácter personal. La relación de dichos equipos utilizados por ASISTIA GRAN CANARIA SL que tratan o almacenan datos de carácter personal se adjunta como **Anexo II**

El Responsable de seguridad del fichero deberá mantener actualizado el inventario de recursos protegidos en todo momento.

IV.- Personal

Las medidas de seguridad contenidas en el presente Documento de Seguridad son de aplicación a todo el personal involucrado en el tratamiento de datos de carácter personal, que deberá observar lo prevenido en este Documento de Seguridad. La relación de personal autorizado se recoge en el **Anexo III.**

4.- PROTOCOLO PARA EL TRATAMIENTO DE DATOS PERSONALES

I.- PRINCIPIO DE FINALIDAD Y ADECUACIÓN DE LOS TRATAMIENTOS.

La recogida y tratamiento de datos de carácter personal debe efectuarse desde su subordinación a los principios de calidad de los datos y proporcionalidad que establece la Ley.

No puede obviarse que estamos tratando de un auténtico derecho fundamental, cuyo contenido el Tribunal Constitucional ha terminado de perfilar en la Sentencia 292/2000, de 30 de noviembre, denominándolo derecho de autodeterminación informativa o de libre disponibilidad de los datos de carácter personal. Así, en dicha sentencia se indica que este derecho fundamental '*persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado', estableciendo, en cuanto a su ámbito, que 'el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18. 1 CE otorga, sino los datos de carácter personal'.*

Aún concretando más el contenido del derecho, se establece que el poder de disposición y control sobre los datos personales que tal derecho implica '*se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos*'.

- **Calidad de los datos:** Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

  Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

  Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

  Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados.

  Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

  Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Por todo lo expuesto, el tratamiento de los datos de carácter personal realizado por ASISTIA GRAN CANARIA SL deberá adecuarse, de conformidad a los principios de la normativa en materia de protección de datos y **sólo podrá recoger los datos de carácter personal para su tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.**

Se deberá determinar con claridad la finalidad y el contenido de los tratamientos de datos que se efectúen y se comunicará al cliente, en cada una de las relaciones que sean mantenidas con el mismo. ASISTIA GRAN CANARIA SL concretará todas las finalidades que sean necesarias para el desarrollo de su función, finalidades sobre las que deberá informar al afectado por el tratamiento teniendo en cuenta que para fines compatibles con la relación contractual no será necesario el consentimiento. Los datos podrán ser utilizados y mantenidos también con fines históricos y estadísticos, siempre que se conserven de forma anónima o previo procedimiento de disociación. Para ello no se conservarán los nombres de las personas físicas a que se refieren ni cualquier otro dato que permita su identificación. **Y se cancelarán cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron recogidos, manteniendo sólo aquellos que puedan ser necesarios para hacer frente a las obligaciones legales y sólo durante el tiempo en que legalmente deban ser conservados.**

II.- DERECHO DE INFORMACIÓN Y PRINCIPIO DE CONSENTIMIENTO DEL CLIENTE PARA EL TRATAMIENTO DE SUS DATOS PERSONALES

Respecto al deber de información a las personas de las cuales se vaya a obtener cualquier tipo de datos personales, se ha de mostrar la siguiente información:

- La existencia del fichero o tratamiento, su finalidad y destinatarios

- El carácter obligatorio o no de la respuesta, así como de sus consecuencias.

- La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

- La identidad y datos de contacto del responsable del tratamiento

- Los datos de contacto del Delegado de Protección de Datos, en su caso.

- La base jurídica o legitimación para el tratamiento.

- El plazo o los criterios de conservación de la información,

- La existencia de decisiones automatizadas o elaboración de perfiles,

- La previsión de transferencias a Terceros Países

- El derecho a presentar una reclamación ante las Autoridades de Control

Y además, en el caso de que los datos no se obtengan del propio interesado:

- El origen de los datos

- Las categorías de los datos

Pero además de otorgar la información sobre los aspectos señalados, para el tratamiento de datos de carácter personal, de acuerdo con el principio general, ASISTIA GRAN CANARIA SL requerirá el consentimiento del cliente titular de los datos objeto de tratamiento. Este consentimiento deberá ser libre, inequívoco, específico e informado, debiendo en consecuencia aparecer vinculado a las finalidades determinadas, específicas y legítimas que justifican el tratamiento de los datos. Asimismo, será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar. Por todo lo manifestado ASISTIA GRAN CANARIA SL utilizará los métodos adecuados que en cada caso permitan dejar prueba y constancia de que el afectado ha recibido la información a la que se refiere este apartado incluyendo las siguientes cláusulas:

- ***Para realizar procesos de selección:***

A) *Si se presentó en un mostrador u oficina* se le informará allí mediante la cumplimentación de un formulario donde se recoja el siguiente texto:

Responsable del tratamiento	Sus datos formarán parte de los ficheros y tratamientos de ASISTIA GRAN CANARIA SL .
Finalidad:	Con la finalidad de gestionar la selección de candidatos que la empresa considere de interés en base a las vacantes existentes o puestos a cubrir. A tales efectos se requerirá a los candidatos el envío de su currículum, lo cual conlleva facilitar datos de carácter personal tales como: nombre, dirección, teléfono, e-mail, estudios, profesión y otros necesarios para la correcta selección de personal que desempeñamos. Su tratamiento estará enfocado únicamente a la consecución de estos fines.
Plazo de conservación	La empresa se reserva el poder conservar el curriculum del candidato para futuros procesos de selección durante un periodo máximo de un año.
Legitimación:	Por otra parte, le informamos que los datos serán tratados con la legitimidad que otorga con su consentimiento. El candidato garantiza a la empresa que toda la información de carácter personal y empresarial que facilite es exacta y está puesta al día de forma que responde con veracidad a la situación actual del candidato. Corresponde y es obligación del candidato mantener, en todo momento, sus datos actualizados, siendo el candidato el único responsable de la inexactitud o falsedad de los datos facilitados a la empresa y de los perjuicios que pueda causar por ello a ASISTIA GRAN CANARIA SL.
Derechos:	En cualquier momento puede revocar el consentimiento prestado para el tratamiento de su información, sin que ello afecte a la licitud del tratamiento efectuado hasta esa fecha, así como para ejercer los derechos de acceso, rectificación, supresión, limitación y oposición del tratamiento y portabilidad de los datos que le conciernen dirigiéndose mediante comunicación fehaciente por escrito, acreditando su identidad, en nuestro domicilio social o bien dirigiendo su solicitud a nuestro delegado de protección de datos a la siguiente dirección de correo electrónico: ADMINISTRACION@ASISTIACANARIAS.COM, adjuntando fotocopia del DNI. Y en el caso de que lo considere oportuno, podrá presentar una reclamación ante la Agencia Española de Protección de Datos para solicitar la tutela de sus derechos.

B) *Si el interesado remite por correo postal o electrónico.* En esta situación y puesto que se cuenta con una dirección electrónica facilitada por el propio interesado puede remitírsele información por ese medio solicitando confirmación de la recepción y condicionando el tratamiento de los datos al acuse de recibo. Es decir, se le responderá por el mismo medio que el candidato envío el currículo adjuntando el texto anterior. **Queda totalmente prohibida la cesión de currículums a otras empresas sin contar con el consentimiento expreso del candidato para tal fin.**

- ***En las facturas y formularios de la empresa***

En virtud de lo dispuesto en la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales y el nuevo Reglamento General de Protección de Datos Personales 2016/679 del Parlamento Europeo y del Consejo le informamos que sus datos formarán parte de los ficheros y tratamientos de ASISTIA GRAN CANARIA SL, sita en AVENIDA PRIMERO DE MAYO 9 LOCAL CP 35002 DE LAS PALMAS DE GRAN CANARIA), con la finalidad de gestionar nuestra relación comercial y remitirle información sobre nuestra actividad empresarial. La base jurídica que legitima este tratamiento será su consentimiento, el interés legítimo o la necesidad de gestionar nuestra relación. Sus datos serán conservados en nuestros ficheros durante todo el tiempo que sea necesario para cumplir con nuestras obligaciones legales. Podrá ejercer los derechos de acceso, rectificación, supresión, limitación y oposición del tratamiento y portabilidad de los datos que le conciernen dirigiéndose mediante comunicación fehaciente por escrito, acreditando su identidad, en el domicilio indicado o bien dirigiendo su solicitud a nuestro delegado de protección de datos a la siguiente dirección de correo electrónico: ADMINISTRACION@ASISTIACANARIAS.COM adjuntando fotocopia del DNI. Y en el caso de que lo considere oportuno, podrá presentar una reclamación ante la Agencia Española de Protección de Datos para solicitar la tutela de sus derechos.

- ***Firma a adjuntar en el correo electrónico enviados desde la empresa.***

CONFIDENCIALIDAD: El contenido de esta comunicación, así como el de toda la documentación anexa, es confidencial y va dirigido únicamente al destinatario del mismo. En el supuesto de que usted no fuera el destinatario, le solicitamos que nos lo indique y no comunique su contenido a terceros, procediendo a su destrucción. PRIVACIDAD: En virtud de lo dispuesto en 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 Personales 2016/679 del Parlamento Europeo y del Consejo le informamos que sus datos formarán parte de los ficheros y tratamiento de ASISTIA GRAN CANARIA SL, sita en AVENIDA PRIMERO DE MAYO 9 LOCAL CP 35002 DE LAS PALMAS DE GRAN CANARIA) para poder mantener el contacto con usted, prestarle el servicio que nos ha solicitado y remitirle información sobre nuestra entidad a través de medios electrónicos. La base jurídica que legitima este tratamiento será su consentimiento, el interés legítimo o la necesidad de gestionar nuestra relación. Sus datos serán conservados en nuestros ficheros durante todo el tiempo que sea necesario para cumplir con nuestras obligaciones o hasta cumplir con los requisitos legales, por ejemplo en materia fiscal. Una vez cumplidas las obligaciones legales oportunas, serán suprimidos por completo. Podrá ejercer los derechos de acceso, rectificación, supresión, limitación y oposición del tratamiento y portabilidad de los datos que le conciernen dirigiéndose mediante comunicación fehaciente por escrito, acreditando su identidad, en el domicilio indicado o bien dirigiendo su solicitud a nuestro delegado de protección de datos a la siguiente dirección de correo electrónico: ADMINISTRACION@ASISTIACANARIAS.COM adjuntando fotocopia del DNI. Y en el caso de que lo considere oportuno, podrá presentar una reclamación ante la Agencia Española de Protección de Datos para solicitar la tutela de sus derechos.

Información en caso de uso de datos con fines de publicidad y marketing.

Cuando se pretenda utilizar los datos del cliente con la finalidad de enviarle publicidad, promociones de cualquier tipo, etc. será necesario suministrar información clara e inequívoca para utilizar sus datos con ese propósito.

Cuando los datos del afectado sean extraídos de fuentes accesibles al público (por ejemplo, las páginas blancas), y se destinen a la actividad de publicidad o prospección comercial, en cada comunicación que se dirija al interesado se le informará del origen de los datos, de la identidad del responsable del tratamiento así como de los derechos que le asisten.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de **oponerse** al tratamiento de sus datos con fines promocionales **mediante un procedimiento sencillo y gratuito**, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija. Por tanto, el destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

5.- DERECHOS DE LOS TITULARES DE LOS DATOS

ASISTIA GRAN CANARIA SL posibilitará en todo momento el ejercicio de los derechos fundamentales de acceso, rectificación, cancelación y oposición sobre los datos objeto de tratamiento.

Para cumplir con dichos derechos ASISTIA GRAN CANARIA SL seguirá las siguientes normas:

a) Los derechos de acceso, rectificación, cancelación y oposición del cliente, son derechos personalísimos, que como tales sólo podrá ejercitar él mismo o persona expresamente autorizada por aquél para ello. La autorización deberá ser expresa e incluir la petición en la que se concreta la solicitud.

b) Los derechos de acceso, rectificación cancelación y oposición se refieren tanto a los datos informatizados como a los que se guarden en expedientes y archivos en papel.

c) Se deberá tener establecido en todo momento un procedimiento para el cumplimiento con los derechos de acceso, rectificación, cancelación y oposición de datos en los plazos legalmente establecidos.

Normas de aplicación común para el ejercicio de cualquiera de los derechos señalados

La solicitud para el ejercicio de estos derechos por el cliente deberá dirigirse al responsable del tratamiento (la empresa), conteniendo los aspectos que en cada caso sean necesarios según se indica más adelante en las presentes recomendaciones.

Asimismo, y en interés del afectado, será recomendable utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

El cliente tiene derecho a que ASISTIA GRAN CANARIA SL conteste siempre a la solicitud que se le formule, con independencia de que figuren o no datos personales del mismo en sus ficheros.

ASISTIA GRAN CANARIA SL adoptará las medidas necesarias para que todo su personal con acceso a datos de pueda informar del procedimiento a seguir por el cliente para el ejercicio de sus derechos. El conocimiento de este procedimiento será una de las obligaciones que todo el personal de la entidad deberá cumplir, con independencia de sus funciones.

Normas de aplicación específica para el Derecho de Acceso

De acuerdo con el art. 15 del nuevo Reglamento Europeo de Protección de Datos, el interesado tendrá derecho 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, a que se refiere el artículo 22, apartados 1 y 4, 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.

Además, 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 en virtud del artículo 46 relativas a la transferencia.

Esto significa que el cliente tendrá derecho a solicitar y obtener información gratuita de sus datos personales del origen de dichos datos, así como de las comunicaciones realizadas o que se prevean hacer de los mismos. Por su parte, El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento

Por ello, ASISTIA GRAN CANARIA SL facilitará al cliente la posibilidad de acceder a sus datos por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración del mismo lo permita:

a) visualización en pantalla;

b) indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

ASISTIA GRAN CANARIA SL se obligará a resolver sobre las solicitudes de acceso en el plazo máximo de un mes, a contar desde la recepción de las mismas, resolución que deberá producirse, aunque no disponga de datos personales de los afectados, en cuyo caso, deberá contemplar esta única circunstancia en la misma. Si la resolución de acceso fuese afirmativa, dicho acceso se concederá en un plazo máximo de 10 días.

Podrá denegarse el acceso a los datos personales cuando el derecho se haya ejercitado en un intervalo inferior a doce meses y el interesado no acredite un interés legítimo al efecto, así como cuando la solicitud la formule persona distinta al afectado sin acreditación de personalidad o representación.

Normas de aplicación específica a los derechos de rectificación y cancelación de datos (este último denominado derecho de supresión tras la entrada en vigor del Reglamento europeo 2016/679 del Parlamento Europeo y del Consejo)

En relación al **derecho de rectificación**, el art. 16 del nuevo Reglamento europeo, prevé que el interesado pueda 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.

Por su parte, **el derecho de supresión**, en el art. 17, implica que el interesado tenga derecho a obtener sin dilación indebida del responsable del tratamiento 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 conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
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 relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

Se exceptúa el tratamiento que 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 de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;
d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 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.

Cuando haya hecho públicos los datos personales y el responsable esté obligado a suprimir dichos datos, ASISTIA GRAN CANARIA SL , 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.

ASISTIA GRAN CANARIA SL se obliga a hacer efectivos los derechos de rectificación y cancelación de datos en el plazo máximo de 10 días desde su solicitud por el cliente.

ASISTIA GRAN CANARIA SL comunicará cualquier rectificación o supresión a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. Informará también al interesado acerca de dichos destinatarios, si este así lo solicita.

La cancelación (rectificación) dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Normas de aplicación específica al derecho de oposición

En la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, se preveía que, en los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del tratamiento excluirá del tratamiento los datos relativos al afectado. Además, debía ofrecerse al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines de comunicaciones comerciales mediante un procedimiento sencillo y gratuito.

Actualmente, en el art. 21 del nuevo Reglamento europeo, se establece en relación con ese derecho que el interesado tenga 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 lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. En estos casos, ASISTIA GRAN CANARIA SL, deberá dejar 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.

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. En estos casos, los datos personales dejarán de ser tratados para dichos fines.

Desde el momento de la primera comunicación con el interesado, este derecho será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información (lo que se cumple con las leyendas a incluir en formularios, hojas de encargo, mails…)

Procedimiento general para facilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Los documentos que se adjuntan en el **Anexo XIII** conforman el procedimiento de cumplimiento con los derechos del cliente y tienen por finalidad no sólo fijar las pautas internas de ASISTIA GRAN CANARIA SL para el cumplimiento de los derechos reseñados, sino también constituirse como elemento de conocimiento y consulta para cualquiera de los empleados de la empresa.

Será necesario que el titular de los datos acredite su identidad frente a al responsable del tratamiento presentando una copia del D.N.I.

También se admitirá que este derecho sea ejercitado por tercero que acredite actuar en representación del interesado a través de autorización expresa, a la que se adjunte copia del D.N.I. del interesado y en la que se incluya de forma clara el alcance de la autorización y el dato o datos a los que se concreta la solicitud de acceso.

Se pondrá en conocimiento y a disposición de todo el personal el presente procedimiento. Todos los empleados o personal autónomo con vinculación con la misma habrán de tener conocimiento de las medidas aquí indicadas. Asimismo, la empresa establecerá de forma expresa el personal que tiene funciones activas en el cumplimiento de las exigencias legales.

La solicitud de acceso a presentar por el cliente habrá de contener como mínimo las siguientes menciones (un modelo de solicitud estará siempre a disposición del cliente en la empresa)

- Nombre, apellidos del cliente y fotocopia del documento nacional de identidad del mismo y, en su caso, de la persona que lo represente, así como el documento acreditativo de tal representación. También se admitirán otros medios válidos en derecho (Sentencia firme de incapacitación, ...)
- Petición en que se concreta la solicitud.
- Domicilio a efectos de notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición que formula, en su caso.

La información incluirá los datos que en el fichero o ficheros concreto de nuestra empresa constan sobre el cliente, procedan de él de forma directa o de procesos informáticos o repertorios públicos, señalando el origen de los mismos, las empresas o terceros a quién se hayan entregado y los usos y finalidades para los que se almacenaron los datos.

Si ASISTIA GRAN CANARIA SL considera que la solicitud de rectificación no se puede cumplir por los motivos señalados en los párrafos anteriores, lo comunicará al cliente motivadamente y dentro del plazo de diez días, para que el cliente proceda a subsanar los defectos de su solicitud o, en su caso lleve a cabo las actuaciones de reclamación que considere oportunas al amparo de la normativa. En todo caso denegará dicha rectificación de forma motivada, por escrito y con constancia de la recepción por parte del interesado, a través de un medio que deje constancia de la firma de recepción por el interesado, sea entrega física o por correo certificado o burofax con acuse de recibo.

Transcurrido el plazo previsto por la normativa sin que hayamos contestado de forma expresa, el cliente podrá entender desestimada su solicitud a los efectos de interponer la reclamación

que corresponda. La solicitud de rectificación deberá acreditar la personalidad del cliente solicitante o su representante y señalar expresamente el dato o datos que considera erróneos, justificando con documentación dicho cambio, salvo que el mismo dependa únicamente de la voluntad del propio interesado, en cuyo caso se hará constar este hecho. ASISTIA GRAN CANARIA SL también cancelará los datos del interesado cuando los mismos hayan dejado de ser necesarios para la finalidad con la cual fueron recogidos y sobre la cual recae el consentimiento del interesado. En estos supuestos, cuando después de la cancelación se reciba una solicitud del interesado, se dará una respuesta en la cual se pondrá en conocimiento del interesado que los mismos fueron cancelados y si se conserva el motivo de la cancelación dicho motivo (por ejemplo, haber concluido la finalidad, terminado el plazo de vigencia de una relación jurídica etc.).

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 virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Así, cuando se haya producido esta limitación del tratamiento, ASISTIA GRAN CANARIA SL sólo podrá tratarlos, a 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 con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación. ASISTIA GRAN CANARIA SL comunicará esta limitación del tratamiento a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. Informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Derecho a la portabilidad de los datos

El interesado, dice el art. 20 del Reglamento Europeo, tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento (en este caso, a ASISTIA GRAN CANARIA SL), en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el primero, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
b) el tratamiento se efectúe por medios automatizados.

Al ejercer su derecho a la portabilidad, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. El ejercicio de este derecho se entiende sin perjuicio del derecho de supresión, pero no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. El ejercicio de este derecho no podrá afectar negativamente a los derechos y libertades de otros.

6.- RELACIÓN CON ENTIDADES EXTERNAS

I.- CESIÓN DE DATOS

ASISTIA GRAN CANARIA SL no realizará comunicaciones de datos que no estén estrictamente justificadas por su relación con el cliente o el trabajador. Dichas comunicaciones sólo se podrán realizar en cumplimiento de fines directamente relacionados con la finalidad legítima del tratamiento de datos y con el previo consentimiento del afectado o cuando una Ley así lo establezca. Será necesario el consentimiento del afectado en aquellas cesiones que no estén relacionadas con los fines directos de la relación contractual. Este consentimiento debe contener una información clara y detallada de los términos de la cesión, no siendo admisibles términos genéricos de información tales como: finalidad de cesión “a otras empresas del grupo”, “empresas de publicidad” “remitirle ofertas comerciales”, etc.

Serán cesionarios legítimos todos aquellos a los que sea necesario transmitir la información para concretar el servicio solicitado por el cliente. Para cesiones ajenas a dicha relación será necesario concretar destinatario y finalidad del tratamiento, dejando opción al cliente para que se oponga a dicha cesión.

La normativa establece las siguientes excepciones para realizar cesiones sin consentimiento del cliente:

a) Cuando la cesión esté autorizada en una Ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con los ficheros de terceros. En este caso, la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

II.- LOS ENCARGADOS DE TRATAMIENTO

ASISTIA GRAN CANARIA SL se obligará a estipular mediante contratos, aquellas relaciones con terceras empresas que le presten un servicio en las que se vea implicada la entrega, transmisión o acceso a los datos de carácter personal objeto de tratamiento, por la prestadora del servicio. Debiendo reflejar copia del contrato de acceso a datos en el **Anexo VIII** del presente documento de seguridad.

En estos contratos se marcará las obligaciones de la empresa prestadora del servicio, con respecto a los datos objeto de tratamiento, distinguiéndose así de una cesión de datos.

En estos casos, los contratos, que deberán constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, establecerán expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones de ASISTIA GRAN CANARIA SL, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

Asimismo, en el contrato se estipularán las medidas de seguridad a que se refiere el art. 9 de la LOPD, y descritas en el presente documento de seguridad, y que el encargado de tratamiento está obligado a implementar. Por tanto, el personal de cualquier Encargado de Tratamiento siempre deberá cumplir con las medidas de seguridad previstas en el presente Documento de Seguridad, por lo que la empresa deberá facilitar a los trabajadores de los Encargados una copia del documento Funciones y Obligaciones del Personal de la empresa.

Una vez cumplida la prestación contractual, el encargado de tratamiento deberá destruir los datos de carácter personal o devolverlos a ASISTIA GRAN CANARIA SL , al igual que cualquier soporte o documento en el que conste algún dato de carácter personal.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en este caso, el encargado del tratamiento deberá conservar los datos debidamente bloqueados, en tanto que pudieran derivarse responsabilidades de su relación con el responsable.

Por otro lado, en los supuestos en que se prevea por parte el prestador del servicio una subcontratación que implique tratamiento de datos personales, deberán reflejarse en el contrato los requisitos exigidos por la normativa de protección de datos, haciendo constar expresamente que, o bien el contratista del servicio actúa en nombre y por cuenta de la empresa o, alternativamente, se especifiquen los siguientes requisitos acumulativos, que deberán figurar en el contrato:

a) Que los servicios a subcontratar se hayan previsto expresamente en la oferta o contrato celebrado entre la empresa y el prestador del servicio.
b) Que el contenido concreto del servicio subcontratado y la empresa subcontratista consta en la oferta o en el contrato.
c) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones de la empresa.

El incumplimiento de la obligación de firmar un contrato de este tipo entre ASISTIA GRAN CANARIA SL y los distintos Encargados del Tratamiento será considerado como una cesión ilegal de datos pudiendo derivar en alguna sanción económica.

Por otra parte, cuando ASISTIA GRAN CANARIA SL, contrate la prestación de un servicio que comporte un tratamiento de datos personales, deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de la normativa de protección de datos haciendo el examen de responsabilidad activa adjunto en el Anexo VIII.

III.- PRESTACIONES DE SERVICIOS SIN ACCESO A DATOS PERSONALES

Cuando ASISTIA GRAN CANARIA SL contrate con algún proveedor que deba realizar tareas en las oficinas o instalaciones de la empresa, pero sin que sea necesario acceder a datos personales (por ejemplo, una empresa de limpieza, etc.), deberá proceder a la firma de un contrato que prohíba a dicha empresa el acceso a los datos personales, y la obligue a guardar secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

7.- NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

Para garantizar la seguridad de los sistemas de información de ASISTIA GRAN CANARIA SL y de cada uno de sus recursos, se establecen las siguientes medidas, normas, procedimientos, reglas y estándares de seguridad para los siguientes tratamientos:

Nombre del Tratamiento
CONTABILIDAD Y ADMINISTRACIÓN
RECURSOS HUMANOS
PACIENTES
HISTORIAL CLINICO
VIDEOVIGILANCIA
USUARIOS WEB
CLIENTES

La empresa procederá en todo momento siguiendo las medidas que a continuación se detallan y, en su caso, deberá informar al personal de ASISTIA GRAN CANARIA SL sobre su cumplimiento:

I.- PUESTOS DE TRABAJO:

Puesto de trabajo es todo ordenador personal, terminal u otro dispositivo desde el que se pueda acceder a los datos del fichero. En los ficheros manuales, puesto de trabajo se asimila a la concepción clásica de ubicación donde desempeña su labor el usuario con acceso autorizado al fichero.

Cada una de las personas autorizadas tendrá asignado un puesto de trabajo desde el que acceder a los datos del fichero. El usuario asignado al puesto de trabajo será responsable de garantizar que la información a la que accede no podrá ser visualizada o comunicada a personas no autorizadas. Cualquier dispositivo conectado al puesto de trabajo tales como impresoras o pantallas deberán de estar ubicadas de forma que se garantice la confidencialidad de la información y que ésta no pueda ser visualizada o comunicada a personas no autorizadas.

El usuario responsable del puesto de trabajo, cuando finalice su turno o cuando se ausente temporalmente, deberá dejar los equipos y dispositivos en un estado que impida el acceso o la visualización de los datos protegidos a personas no autorizadas. Esto se podrá realizar mediante un protector de pantalla, la suspensión de la sesión de trabajo o la salida del sistema y apagado del equipo. La reanudación del trabajo implicará la desactivación de la pantalla protectora, el reinicio de la sesión o el encendido del equipo con la introducción del nombre de usuario y contraseña correspondiente en cada caso.

No deberá dejar en la impresora documentos impresos en la bandeja de salida que contengan datos de carácter personal. Si la impresora es compartida con otros usuarios no autorizados para acceder a los datos del Fichero, el responsable de cada puesto de trabajo deberá retirar los documentos conforme vayan siendo impresos.

La configuración de los puestos de trabajo desde los que se tiene acceso al fichero sólo podrá ser cambiada con la autorización de la dirección de la empresa, el responsable de seguridad o el administrador del sistema designado.

Con respecto a ficheros manuales, los documentos, carpetas y expedientes quedarán debidamente archivados cuando el usuario responsable del puesto de trabajo se ausente temporalmente o finalice su turno de trabajo.

II.- IDENTIFICACIÓN Y AUTENTICACIÓN DEL PERSONAL AUTORIZADO

Se establecerá un procedimiento que garantice la correcta identificación y autenticación de los usuarios autorizados a acceder a los sistemas de información.

Los accesos a los sistemas de información se realizarán mediante un mecanismo que permita la identificación de forma inequívoca y personalizada del usuario. Por lo que cada identificación deberá pertenecer a un único usuario.

Todos los usuarios autorizados para acceder al Fichero, relacionados en el **Anexo III.** Relación de personal autorizado, deberán tener un código o nombre de usuario que será único, y que estará asociado a una contraseña que sólo será conocida por el propio usuario.

Procedimiento de asignación y cambio de contraseñas

La dirección de la empresa, el administrador del sistema o la persona con autorización delegada, asignará un nombre de usuario y propondrá una contraseña para cada uno de los usuarios que, tras el primer acceso, vendrán obligados a cambiarlas.

Las contraseñas deberán constar de un mínimo de dígitos seis caracteres combinando letras mayúsculas y minúsculas junto con cifras, (como, por ejemplo: Uk7N1s) que no sean fácilmente deducibles. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

Las contraseñas son de carácter personal e intransferible y no serán visibles en pantalla cuando son introducidas. Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder inmediatamente a su cambio.

Con una periodicidad de seis meses y de forma automática, se propondrá a los usuarios, que cambien su contraseña por una nueva, volviendo a quedar almacenada de forma segura. Procediendo anotar dicho cambio en el documento de seguridad en el Anexo II b sobre cambios de contraseñas.

La dirección de la empresa, el Administrador del sistema o la persona con autorización delegada, en su caso, podrá cambiar los requisitos de acceso, las condiciones, modos, sistemas y formas de tratamiento o de lectura cuando lo crea oportuno, notificando la decisión a los usuarios y dejando constancia de tal modificación en el presente Documento de seguridad.

Las contraseñas son personales e intransferibles y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada a la dirección de la empresa, el administrador del sistema o la persona con autorización delegada o a la persona con autorización delegada y subsanada en el menor plazo de tiempo posible.

Medidas de seguridad específicas para los tratamientos de nivel medio y alto:

Nombre del Tratamiento
PACIENTES
HISTORIAL CLINICO

Quedará limitado el número de intentos para el acceso no autorizado al sistema de información donde contengan datos. Tras varios intentos fallidos de acceso quedará bloqueada la contraseña, por lo que el sistema no permitirá más de **TRES** intentos de acceso fallidos, siendo el usuario posteriormente bloqueado.

III.- CONTROL DE ACCESO LÓGICO

Los usuarios de los sistemas de información tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. Por tanto, queda prohibido que un usuario acceda a recursos con derechos distintos de los que ha sido autorizado.

En el **Anexo III** donde se detalla la relación del personal autorizado incluyendo una relación actualizada de usuarios, perfiles de usuarios y los accesos autorizados para cada uno de ellos.

Si la aplicación informática o programa informático que permite el acceso al Fichero donde se encuentran los datos personales no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta el programa informático, el que impida el acceso no autorizado, mediante la restricción y disponibilidad de recursos en la sesión del usuario con el control de acceso lógico mediante usuario y contraseña.

En el caso de personal ajeno a la empresa (como, por ejemplo, la persona designada por una empresa externa para el mantenimiento informático) que tenga acceso a los recursos estará sometido a las mismas condiciones y obligaciones de seguridad que el personal propio de la empresa.

Exclusivamente la dirección de la empresa, el administrador del sistema o la persona con autorización delegada, podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por ASISTIA GRAN CANARIA SL

Para crear nuevas altas de accesos, se comunicará a la persona autorizada por la empresa la propuesta de acceso, código de acceso y listado de las funciones del nuevo autorizado. De todo ello se deberá dejar constancia en este Documento de Seguridad en el **Anexo III** donde consta la relación de personal autorizado.

IV.- CONTROL DE ACCESO FÍSICO

Exclusivamente el personal autorizado en este Documento de Seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información correspondientes a los ficheros objeto de esta medida.

El personal autorizado consta relacionado en el **Anexo III,** Relación de personal autorizado como personal afecto a los citados ficheros.

El personal de la empresa con acceso a los sistemas de información pero que no tengan un perfil de usuario, como pueden ser de mantenimiento, limpieza, seguridad, etc., serán autorizados por el responsable de seguridad, quien expedirá autorización o credencial que acredite su acceso autorizado.

El personal ajeno a la empresa, que le presta servicios sin acceso a datos personales, en el contrato de prestación de servicios deberá constar expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que pueda conocer con motivo de la prestación del servicio.

Medidas de seguridad específicas para los tratamientos de nivel alto:

Nombre del Tratamiento
PACIENTES
HISTORIAL CLINICO

Exclusivamente el personal autorizado en el presente Documento de Seguridad tendrá acceso físico a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información que traten datos de carácter personal de nivel medio y/o alto. En el Anexo III del presente Documento de Seguridad se establece la relación de usuarios, y se definen quiénes son los usuarios autorizados a acceder a los lugares donde se encuentran ubicados los sistemas de información con datos de nivel medio y/o alto.

V.- GESTION Y DISTRIBUCIÓN DE SOPORTES Y DOCUMENTOS

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los documentos adjuntos en los correos electrónicos, fuera de los locales bajo el control de la empresa, deberá ser autorizada por la dirección de la empresa, el administrador del sistema o la persona con autorización delegada.

Con respecto a los documentos, también se consideran incluidos en la salida de documentos los siguientes supuestos:

1) Envío por correo electrónico en el cuerpo del mensaje o como adjuntos datos de un fichero o tratamiento.

2) Los faxes cuando incorporan datos de un fichero o tratamiento.

3) Cualquier otro procedimiento electrónico como ftp, descargas desde la web o carpetas compartidas, etc.

Los ordenadores portátiles y los dispositivos móviles que contengan datos personales deberán de ser sometidos al mismo procedimiento de autorización para su salida de los locales en los que está ubicado el fichero.

En el caso del correo electrónico, para garantizar la trazabilidad de los datos que salen materialmente del sistema de información, puede servir como registro el propio sistema de indexación del gestor del correo electrónico.

Los soportes y documentos de ASISTIA GRAN CANARIA SL que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen. Asimismo, serán inventariados y almacenados en un lugar con acceso restringido al personal autorizado en el presente Documento de Seguridad.

Cuando por las características físicas del soporte no sea posible el cumplimiento de las anteriores obligaciones, se dejará constancia motivada de ello en el propio Inventario de Soportes. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control de la empresa deberá encontrarse debidamente autorizada en el presente Documento de Seguridad o bien ser autorizada por las personas habilitadas para ello en el **Anexo V**, incluyéndose dicha autorización en el **Libro Registro de Autorizaciones** de la empresa.

Asimismo, en el traslado de la documentación se adoptarán las medidas oportunas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte, utilizando para ello dispositivos de transporte con mecanismos que obstaculicen su apertura.

Cuando un soporte o documento vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el Inventario de soportes.

La identificación de los soportes que contengan datos de carácter personal considerados por parte de la empresa como especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Medidas de seguridad específicas para los tratamientos de nivel alto:

Nombre del Tratamiento
PACIENTES
HISTORIAL CLINICO

Para los supuestos de entrada y salida de soportes que contengan datos de carácter personal de nivel medio o alto, se establece un sistema de registro de entrada de soportes que permite conocer el tipo de documento o soporte, la fecha y hora de entrada, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

A estos efectos, ASISTIA GRAN CANARIA SL dispone de sendos **Registros de Entrada y Salida de Soportes**. Dichos registros incluirán, en cada caso, las preceptivas autorizaciones a que se refieren los párrafos anteriores, que serán emitidas por las personas designadas en el **Anexo VI** al presente Documento de Seguridad.

La identificación de los soportes con datos personales de nivel alto se realizará siempre utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido pero que a su vez imposibiliten la identificación de la información al resto de personas.

La distribución de los soportes que contengan datos personales de nivel alto se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

VI.- ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Si el ordenador en el que se ubica el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso al Fichero, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

VII.- RÉGIMEN DE TRABAJO FUERA DE LAS OFICINAS

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de la empresa, deberá estar autorizado expresamente por la misma, garantizándose el nivel de seguridad correspondiente al tipo de fichero tratado.

En relación con la necesaria autorización indicada en el párrafo anterior, se incluye en el **Anexo V** la relación de las personas habilitadas para otorgar dichas autorizaciones.

Asimismo, en el **Libro Registro de Autorizaciones** de la empresa deberán constar las autorizaciones otorgadas, que podrán establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

También deberán constar en el **Libro Registro de Autorizaciones** las autorizaciones otorgadas a los Encargados del Tratamiento que, para la prestación del servicio contratado, requieran trabajar con los datos personales fuera de los locales del propio Encargado del Tratamiento.

Lo expresado en los párrafos anteriores se aplica a todas aquellas personas que precisen acceder y trabajar con datos de carácter personal a través de ordenadores portátiles o agendas electrónicas. El uso de ordenadores portátiles y agendas electrónicas con datos de carácter personal fuera de las instalaciones de la empresa, deberá ser previamente autorizada, incluyéndose dicha autorización en el mencionado **Libro Registro de Autorizaciones**.

Medidas de seguridad específicas para los tratamientos de nivel alto:

Nombre del Tratamiento
PACIENTES
HISTORIAL CLINICO

La presente medida de seguridad única y exclusivamente será de aplicación para aquellos ficheros con datos de carácter personal que requieran un nivel alto de seguridad.

Se cifrarán todos los datos que contengan los dispositivos portátiles cuando salgan de las instalaciones de la empresa, evitando el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado.

Cuando no pudiera cifrarse el dispositivo, pero fuera necesario el tratamiento de los datos contenidos en él, se hará constar tal circunstancia de forma motivada mediante un Anexo específico al presente Documento de Seguridad en el que se especificarán las medidas necesarias para tener en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

VIII.- FICHEROS TEMPORALES O COPIAS DE TRABAJO

Los ficheros temporales o copias de documentos que se creen con la finalidad de realizar trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda.
Todos los ficheros temporales o copias de documentos así creados serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

Las copias de trabajo de documentos en formato papel, deberán procederse a su destrucción mediante la trituradora de papel. Quedando prohibida la reutilización de documentos o copias de trabajo en formato papel.
Se deberá asegurar de que los ficheros temporales o copias de trabajo de documentos no son accesibles por personal no autorizado.

8.- FUNCIONES Y OBLIGACIONES DEL PERSONAL

Todo el personal de la empresa deberá suscribir el pertinente acuerdo de confidencialidad, el cual se adjuntará en el Anexo IV, además de conocer las funciones y obligaciones de su puesto de trabajo respecto al acceso a los datos de carácter personal y a los sistemas de información.

ASISTIA GRAN CANARIA SL adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento. Asimismo, establecerá las medidas necesarias para que periódicamente se revise el nivel de conocimiento de dichas funciones y obligaciones. En todo caso, en el momento en que una persona entre a trabajar en ASISTIA GRAN CANARIA SL se le facilitará por escrito una copia de dichas funciones y obligaciones del personal. Las funciones y obligaciones del personal en relación con el acceso a los sistemas de información de la empresa y el tratamiento de los datos de carácter personal se detallan en el **Anexo III** junto con la formación recibida para la concienciación de aplicar los principios de seguridad descritos en el presente Documento de Seguridad.

Las funciones y obligaciones de cada una de las personas que forman parte de ASISTIA GRAN CANARIA SL y que tienen acceso a los datos de carácter personal y a los sistemas de información son las que se relacionan a continuación. En todo caso, el personal de la empresa se obliga al cumplimiento íntegro de todas las previsiones establecidas en el Documento de Seguridad de la empresa. En caso de incumplimiento de las presentes funciones y obligaciones por parte de cualquier trabajador de ASISTIA GRAN CANARIA SL , la dirección de la empresa, de conformidad con la legislación vigente, podrá adoptar las sanciones que tenga estipuladas, así como reclamar las responsabilidades civiles y penales que legalmente correspondan.

1. PERSONAL DE ASISTIA GRAN CANARIA SL

Datos de carácter personal

- El personal de ASISTIA GRAN CANARIA SL únicamente tiene acceso autorizado a los datos de carácter personal y a los sistemas de información cuando lo precisen para el desarrollo de sus funciones.

- Las personas con acceso autorizado a los ficheros de ASISTIA GRAN CANARIA SL a través de su puesto de trabajo no podrán modificar la configuración de las aplicaciones ni del sistema operativo, salvo autorización expresa de la empresa.

- El personal de ASISTIA GRAN CANARIA SL única y exclusivamente podrá utilizar aquellos datos de carácter personal a los que tenga acceso en virtud de sus funciones para dar cumplimiento a sus obligaciones laborales, quedando expresa y completamente prohibida cualquier otra utilización.

- El personal de ASISTIA GRAN CANARIA SL no podrá borrar, destruir, dañar, alterar o modificar cualquiera de los datos de carácter personal que contengan las bases de datos de ASISTIA GRAN CANARIA SL sin la autorización expresa de la empresa, siempre y cuando no sea en ejercicio de las funciones que le han sido encomendadas.

- Cada trabajador de ASISTIA GRAN CANARIA SL que, por razón del ejercicio de sus funciones, tenga acceso a los datos deberá observar la debida reserva, confidencialidad y sigilo en relación con los mismos. Esta obligación perdurará incluso tras finalizar su vinculación con la empresa.

- El personal de ASISTIA GRAN CANARIA SL no podrá realizar copias, transmisiones, comunicaciones o cesiones de los datos de carácter personal tratados por ASISTIA GRAN CANARIA SL sin la autorización expresa de la empresa, siempre y cuando no sea en ejercicio de las funciones que le han sido encomendadas.

- El personal de ASISTIA GRAN CANARIA SL tendrá la obligación de comunicar cualquier incidencia, anomalía, error o fallo que detectara en los ficheros o sistemas de información propiedad de ASISTIA GRAN CANARIA SL

- El uso de ordenadores y soportes portátiles que contengan datos de carácter personal fuera de las instalaciones de la empresa deberá ser previamente autorizada por escrito por parte de ésta.

- Todo fichero temporal (como aquellas hojas donde se dejan anotados recados recogidos de las llamadas o post-it's) copia de trabajo será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

- Está estrictamente prohibido copiar información de carácter personal incluida en los ficheros de ASISTIA GRAN CANARIA SL en cualquier tipo de soporte informático (DVD, Memorias USB's, etc.) sin la autorización previa y expresa de la empresa. En caso de haber sido autorizada la utilización de cualquier soporte informático, el usuario deberá comunicarlo inmediatamente a la empresa para su inventario y etiquetado.

- Cualquier salida de soportes informáticos que contengan datos de carácter personal (DVD, Memorias USB's, etc.) fuera de las instalaciones de ASISTIA GRAN CANARIA SL deberá ser autorizada de forma previa y expresa por parte de la empresa.

- En el supuesto de recibir cualquier soporte informático que contenga datos de carácter personal procedente del exterior de la empresa, el usuario deberá comunicarlo a la empresa a los efectos de poder anotarlo en el Registro de Entrada de Soportes.

- Cuando un soporte deba ser desechado, se deberá entregar a los responsables de Área o Departamento para que se pueda proceder a su destrucción y baja en el Inventario de Soportes.

- El personal de ASISTIA GRAN CANARIA SL deberá comunicar a los Responsables de Área cualquier solicitud de acceso, rectificación, cancelación u oposición de datos de carácter personal presentada por parte de algún afectado. Dicha comunicación deberá realizarse en el plazo máximo de 3 horas desde la recepción de la solicitud.

Claves de acceso o identificadores de usuario

- Cada trabajador de ASISTIA GRAN CANARIA SL que en el desarrollo de sus funciones laborales realice actividades en las cuales sea necesario acceder a los ficheros de datos de carácter personal propiedad de ASISTIA GRAN CANARIA SL , dispondrá de un nombre de usuario que le identifique única y exclusivamente a él y de una clave o contraseña personal que le permita, durante el proceso de acceso a los datos, autenticarse como usuario autorizado.

- Dicho nombre de usuario o identificador así como la correspondiente contraseña, será personal e intransferible. Queda absolutamente prohibida su revelación a cualquier otra persona sin la autorización expresa de la empresa.

- En los supuestos en los que la aplicación informática lo permita, el usuario deberá modificar su contraseña de acceso la primera vez que acceda a la aplicación.

- La contraseña deberá cambiarse de manera obligatoria, como mínimo anualmente, aún en el caso de que la aplicación no obligue a ello. Esto es aplicable a todas las aplicaciones informáticas utilizadas en la empresa, así como a todos aquellos recursos informáticos que requieran identificación previa y permitan el cambio de la clave de acceso.

- Cada trabajador será responsable de conservar de forma confidencial y segura su nombre de usuario (identificador único) y su contraseña personal. En los supuestos que el trabajador tuviera la certeza o sospechara que alguien está utilizando dichos identificadores o contraseñas, podrá solicitar a la empresa que le asigne un identificador y contraseña nuevos.

- Dicho identificador único y la contraseña sólo podrán utilizarse dentro de los locales de ASISTIA GRAN CANARIA SL Queda expresamente prohibido el acceso desde fuera de los locales de ASISTIA GRAN CANARIA SL sin la autorización expresa de la empresa.

- Cada trabajador deberá evitar que los datos contenidos en los ficheros sean visibles a través de sus puestos de trabajo por personas no autorizadas: apagando el equipo o utilizando un protector de pantalla con la contraseña correspondiente.

Sistemas de comunicación

- En caso de tener que enviar correos electrónicos a más de un destinatario a la vez, es obligatorio utilizar la opción de copia oculta (CCO). En caso de duda sobre dicha funcionalidad, puede consultarse con cualquier Responsable de Área.

- El personal de ASISTIA GRAN CANARIA SL no podrá utilizar sistemas de comunicación para transmitir datos de carácter personal si éstos no han sido expresamente autorizados por la empresa. En cualquier caso, queda expresamente prohibida la transmisión de datos de carácter personal de nivel alto (ideología, afiliación sindical, creencias, religión, origen racial, salud, vida sexual, violencia de género, etc.) si no es mediante sistemas de transmisión seguros, en los cuales los datos sean cifrados durante su transmisión.

Tratamiento de los datos en servidor

- Todos los datos de carácter personal que sean objeto de tratamiento por parte de los trabajadores, deberán ubicarse y/o tratarse en los servidores de la empresa. El personal de ASISTIA GRAN CANARIA SL no podrá alojar ningún tipo de dato de carácter personal en el disco duro de sus ordenadores personales.

Copias de seguridad

- Cada trabajador de la empresa que, en el desarrollo de sus funciones laborales y con autorización de la empresa, aloje datos de carácter personal en su equipo de trabajo, deberá realizar copias de seguridad de la información almacenada en el mismo con una periodicidad, al menos, semanal.

Tratamiento de documentación en papel

- Los documentos que contengan datos de carácter personal deberán almacenarse siempre en los armarios y archivadores establecidos al efecto y que dispondrán de los oportunos mecanismos de cierre que obstaculicen su apertura.
- Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento previstos por la empresa, por estar en proceso de revisión o tramitación, el trabajador que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada. Para ello, se deberán guardar los documentos que contengan datos personales protegidos en un sitio que no pueda ser visible para terceros.

- Cada trabajador será responsable de proceder a la destrucción de las copias o reproducciones desechadas, de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior. Se recomienda la utilización de destructoras de papel.

- Siempre que se proceda al traslado físico de la documentación contenida en un fichero, se deberán adoptar medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

- En el uso de impresoras, faxes y fotocopiadoras se debe retirar la documentación relativa a los datos personales inmediatamente después de su impresión, envío o copia evitando el acceso por parte de personas no autorizadas.

2. PERSONAL DE ENCARGADOS DEL TRATAMIENTO

- El personal de cualquier Encargado del Tratamiento contratado por ASISTIA GRAN CANARIA SL que preste servicios en las oficinas o instalaciones de la empresa o que acceda a los ficheros de ASISTIA GRAN CANARIA SL de forma remota, deberá

cumplir con las mismas medidas de seguridad previstas en el apartado anterior para el personal en plantilla.

3. RESPONSABLE DE SEGURIDAD

Datos de carácter personal

- El Responsable de Seguridad se encargará de coordinar y controlar las medidas de seguridad aplicables a los ficheros de ASISTIA GRAN CANARIA SL que contengan datos de carácter personal.

- Deberá mantener el Documento de Seguridad y sus Anexos actualizado.

- El Responsable de Seguridad será la persona encargada de otorgar, en los casos en que procedan, las autorizaciones previstas en el presente Documento de Seguridad.

- Deberá comprobar, al menos semestralmente, los procedimientos de realización de copias de seguridad y de recuperación de los datos. Asimismo será el encargado de su realización o, en su caso, determinar la persona encargada de dichas funciones.

- Será el responsable de la llevanza de los registros de Incidencias, Entrada de Soportes, Salida de Soportes y demás registros de la empresa previstos en el Documento de Seguridad.

- El Responsable de Seguridad deberá analizar los informes de auditoría que se realicen, en los casos que sea necesario en virtud del nivel de seguridad de los datos y deberá elevar las conclusiones a la dirección de la empresa.

- Se encargará de revisar periódicamente la información de control registrada en las aplicaciones o entornos que manejen información de nivel alto y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

- El Responsable de Seguridad será el encargado de coordinar y analizar los resultados de los controles periódicos semestrales previstos en el Documento de Seguridad.

Claves de acceso o identificadores de usuario

- El Responsable de Seguridad deberá comprobar que efectivamente se aplican los mecanismos de identificación y autenticación.

- Deberá comprobar que los usuarios tengan acceso únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

- El Responsable de Seguridad se encargará de conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por la dirección de la empresa.

Sistemas de comunicación

- El Responsable de Seguridad, en aquellos casos en que sea necesario, se encargará de autorizar la transmisión de datos de carácter personal mediante sistemas de comunicación. En cada caso determinará la pertinencia o no de los sistemas de comunicación propuestos atendiendo a la naturaleza de la información transmitida.

- Deberá controlar los mecanismos de encriptación o cifrado necesarios para la transmisión de datos de carácter personal de nivel alto.

- Deberá establecer las medidas de seguridad necesarias para evitar accesos a los ficheros no autorizados mediante la utilización de cualquier sistema de comunicación por acceso remoto.

4. DELEGADO DE PROTECCIÓN DE DATOS

- El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar a ASISTIA GRAN CANARIA SL o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud de la normativa y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de la normativa y de las políticas del presente manual 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;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto.

- 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.

9.- COPIAS DE SEGURIDAD

ASISTIA GRAN CANARIA SL implantará un sistema de copias de respaldo y de recuperación de los datos que permita su fácil ejecución, y deberá ser realizado con una periodicidad semanal, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. Dicho procedimiento garantizará la reconstrucción de los datos en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Corresponde a la empresa verificar la definición y la correcta aplicación de los procedimientos de realización de copias de respaldo, así como la recuperación de los datos. Asimismo, deberá responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo de los ficheros, de forma que ninguna persona no autorizada tenga acceso a las copias. La copia de respaldo debe conservarse en un lugar diferente de los equipos informáticos que los tratan para obtener la mayor eficiencia de las copias de seguridad.

Existirá una persona, bien sea el administrador de los sistemas o bien otro usuario expresamente designado por el responsable, que será responsable de obtener periódicamente una copia de seguridad de los ficheros, a efectos de respaldo y posible recuperación en caso de fallo. «G_Copias»Será necesaria la autorización de la dirección, el administrador del sistema o de la persona debidamente delegada para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación

La dirección de la empresa, el administrador del sistema o la persona con autorización delegada verificará, cada seis meses, la correcta definición, funcionamiento y aplicación de los siguientes procedimientos de realización de copias de respaldo y recuperación de los datos:

PROCEDIMIENTO DE REALIZACIÓN DE COPIAS DE RESPALDO DE LOS SITEMAS DE INFORMACIÓN DE LA EMPRESA

Se harán copias de respaldo completas de todos los sistemas de información donde se almacenen datos con una periodicidad mínima semanal. Esta copia de seguridad semanal se establece como criterio de mínimos.

En cualquier caso, la empresa intentará dotarse de los recursos necesarios que le permitan disponer de una copia de seguridad diaria de lunes a viernes o el último día laborable de la semana, debiendo conservarse la copia del último día, a modo de respaldo semanal.

Antes de guardar los soportes que contengan las copias semanales en los dispositivos de almacenamiento previstos por la empresa, se procederá a comprobar que dichos soportes se pueden leer correctamente y restaurarse sin problemas. Para ello se restaurará en una carpeta temporal la copia de seguridad completa, comprobándose que el procedimiento de restauración y los datos del fichero son correctos. En caso de que el soporte fuera erróneo se sustituiría por el soporte del día anterior, siempre y cuando éste superara con éxito la correspondiente comprobación.

Todos los soportes utilizados por la empresa para la realización de las copias de seguridad se etiquetarán debidamente de conformidad con lo previsto en el presente Documento de Seguridad.

Todos los soportes se guardarán en dispositivitos de almacenamiento con mecanismos que obstaculicen su apertura, permitiéndose únicamente el acceso al personal autorizado en el presente Documento de Seguridad. Debiendo guardarse la copia de seguridad en sitio diferente donde se encuentren los sistemas de información para evitar su perdida total en caso de incendio o robo.

Respecto a las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado. Cuando esté previsto realizar este tipo de pruebas con datos reales, será obligatorio realizar con carácter previo una copia de seguridad específica de los datos y deberá anotarse en el Libro Registro de Autorizaciones.

PROCEDIMIENTO DE RECUPERACIÓN DE LAS COPIAS DE RESPALDO

El procedimiento para la recuperación de los datos debe garantizar en todo momento su reconstrucción en el estado en que se encontraba al tiempo de producirse la pérdida o destrucción. En caso de fallo del sistema con pérdida total o parcial de los datos de los ficheros existirá un procedimiento, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos perdidos al estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Para realizar adecuadamente la recuperación de datos vista en los párrafos anteriores se procederá a observar las siguientes etapas o actividades:

Detección de la pérdida de datos

En cualquiera de las fases del tratamiento de los datos de carácter personal puede existir una incidencia que ocasione una pérdida de datos. Todo aquel usuario que detecte una incidencia tiene la obligación de comunicarlo a la dirección de la empresa, el administrador del sistema o la persona con autorización delegada, para que se proceda al registro de la incidencia y se adopten las medidas de restauración de los datos oportunas.

Aprobación de la recuperación de datos

Las personas designadas por la empresa para la gestión de las copias de respaldo y de recuperación de datos comprobarán la pérdida de los datos y, en su caso, aprobarán el procedimiento de restauración de los mismos.

Respecto de los ficheros parcialmente automatizados, (es decir que tengan un tratamiento mixto por tratarse tanto en soporte papel como informático) y siempre que exista documentación que permita alcanzar la recuperación de los datos al estado en que se encontraban al tiempo de producirse la pérdida o destrucción, se procederá a grabar manualmente los datos quedando constancia motivada de este hecho en el Registro de incidencias.

Recuperación de los datos

Las personas designadas por la empresa para la gestión de las copias de respaldo y de recuperación de datos identificarán el día a restaurar, en función de las copias de respaldo disponibles con fecha anterior a la incidencia. Una vez identificado el soporte o cinta a restaurar, se realizará la recuperación de los datos.

Registro de la incidencia

Las personas designadas por la empresa para la gestión de las copias de respaldo y de recuperación de datos deberán siempre comunicar la incidencia por los canales establecidos, a los efectos de que dicha incidencia se registre según el Procedimiento de Gestión de Incidencias.

10.- VIOLACIONES DE SEGURIDAD

Una incidencia es cualquier violación de la seguridad que afecte o pudiera afectar a la integridad de los datos, es decir, a la confidencialidad y disponibilidad de los datos de los ficheros. Cualquier incumplimiento de la normativa del presente Documento de Seguridad se considera una incidencia y por tanto violación de seguridad.

Asimismo, para la gestión de dichas situaciones la empresa dispone en el **Anexo VII** de un Libro Registro de Incidencias en el que se hace constar el tipo de incidencia o quiebra de seguridad, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

El objeto del presente protocolo de actuación es establecer y describir un procedimiento de notificación y gestión de las violaciones de seguridad siendo aplicable a todas las personas vinculadas con la empresa y que traten datos de carácter personal incluidos en todos los ficheros y tratamientos que sean responsabilidad de la empresa.

1.- Detección: Una incidencia puede ser detectada en cualquiera de las fases del tratamiento de los datos de carácter personal incluidos en los ficheros que sean responsabilidad de la empresa ya sea en calidad de Responsable o de Encargado del Tratamiento. **Una vez detectada, la persona que detectó la incidencia deberá notificarlo, a la junta de gobierno, o en su caso al delegado de protección de datos.**

2.- Comunicación: Aquella persona que detectó la incidencia utilizará los medios oportunos que faciliten el aviso de la misma tan pronto como se haya detectado. En dicha comunicación se procederá a realizar una descripción de la incidencia y como mínimo deberá de:
a) 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;
b) 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;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) 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.

Además de internamente, la violación de seguridad se deberá notificar a la autoridad de control competente a más tardar 72 horas después de que la empresa 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. En este último caso, la empresa también informará a los interesados afectados por la violación de seguridad.

3.- Resolución de la incidencia: Si en el proceso de resolución de la incidencia hubiera una pérdida de integridad, confidencialidad o disponibilidad de los datos afectados, antes de realizar cualquier operación se deberá pedir la autorización de las personas designadas en el **Anexo IV** del presente Documento de Seguridad para proceder a la gestión de la incidencia. Excepcionalmente podrá prescindirse de autorización previa cuando concurran circunstancias de fuerza mayor o ante posibilidad cierta de degradación del servicio que se presta sobre la base del fichero afectado.

4.- Finalización de la incidencia: La incidencia tendrá la consideración de finalizada cuando toda persona implicada en cualquiera de las anteriores fases esté conforme con la solución, quedando fechada y anotada en el Registro de Incidencias.

5.- Registro de la incidencia: Tras la resolución de la incidencia se deberá anotarla en el Registro de Incidencias, manteniendo un histórico durante, al menos, los dos últimos años. El

Registro de Incidencias de la ASISTIA GRAN CANARIA SL consta en el **Anexo VII** junto al modelo de hoja de dicho Registro de Incidencias.

EVENTOS MÁS COMUNES QUE DEBERÍAN SER CONSIDERADOS COMO VIOLACIONES DE SEGURIDAD

El siguiente listado muestra las situaciones más comunes que tienen la consideración de incidencia debiéndose comunicar y gestionar según el procedimiento establecido en los apartados anteriores. Cabe tener presente que el listado no es excluyente sino informativo debido a que pudiera ocurrir cualquier otra situación que comprometa la información contenida en los ficheros y no esté reflejada en las situaciones detalladas:

1. Pérdida, robo o extravío de equipos portátiles (ordenadores, PDA's, etc.)
2. Pérdida, robo o extravío de documentación en papel.
3. Pérdida, robo o extravío de soportes informáticos (dispositivos USB, DVD, etc.)
4. Contraseñas de acceso a los sistemas informáticos que hayan visto comprometida su confidencialidad.
5. Fallos en los procesos de copias de seguridad o de restauración de datos.
6. Comportamientos anómalos/errores de sistemas, aplicaciones y bases de datos que manejen datos de carácter personal y que puedan afectar a la seguridad de la información.
7. Accesos no autorizados a los sistemas de información de la empresa.
8. Accesos físicos no autorizados a las instalaciones de la empresa, especialmente a la sala de servidores o CPU's.
9. Desaparición o alteración de ficheros informáticos.

11.- ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

El Documento de Seguridad ha de mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

El contenido del Documento de Seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.
Por tanto, cualquier instalación de nuevos sistemas que impliquen un tratamiento de datos como puede ser cámaras de seguridad, dispositivos de geolocalización, sistemas que verifiquen el cumplimiento de la jornada laboral, etc… deberán hacerse bajo el procedimiento oportuno que respete y se adapte a la legislación vigente en materia de protección de datos.

La dirección de la empresa, el administrador del sistema o la persona con autorización delegada, junto con el responsable de seguridad o los delegados de protección de datos, tanto propios como de proveedores, si es el caso, mantendrán una reunión con carácter extraordinario cada vez que se produzcan cambios relevantes que impliquen la realización de una evaluación de impacto a la privacidad donde se vean afectados los ficheros o tratamientos de los datos de carácter personal, con el objetivo de coordinar las medidas de seguridad a implantar. Dejando constancia de las modificaciones en el Registro de Actualizaciones dispuesto en el **Anexo X** del presente Documento de Seguridad.

12- CONTROLES PERIÓDICOS

Para la verificación periódica sobre la aplicación de las medidas de seguridad y la correcta actualización del presente Documento de Seguridad se establecen los siguientes controles periódicos:

A) IMPLANTACIÓN DE LAS MEDIDAS DE SEGURIDAD

En referencia a la implantación de las medidas de seguridad en los ficheros que contengan datos de carácter personal, la empresa deberá analizar su actual situación y adoptar las medidas necesarias para que todas y cada una de las normas establecidas en el presente Documento de Seguridad sean implantadas en todos sus aspectos siguiendo las presentes fases:

I.- Análisis de las medidas de seguridad actuales para asegurar su adecuación al Documento de Seguridad.

II.- Implantación de las medidas o correcciones necesarias.

III.- Difusión entre el personal de la empresa de sus obligaciones y deberes en materia de tratamiento de datos de carácter personal, en función de sus responsabilidades.

En el caso que alguna de las normas o procedimientos establecidos en el presente Documento de Seguridad no se estuvieran aplicando o lo estuvieran de forma inadecuada, se establecerá un plan y un calendario para su correcta implantación, donde se adoptarán las medidas de urgencia necesarias para que no exista riesgo alguno para los datos de carácter personal contenidos en los Ficheros. Si durante el proceso de implementación se realizasen pruebas para verificar la implantación de las medidas de seguridad, éstas no se realizarán con datos reales. Pero, llegado el caso se tuvieran que realizar con datos reales, en todo momento se garantizaría el nivel de seguridad correspondiente al tratamiento realizado dejando constancia de su realización en el Libro Registro de Autorizaciones de la empresa. Asimismo, en tales casos, será estrictamente necesario realizar con carácter previo una copia de seguridad de los datos.

B) EJECUCIÓN DE LOS CONTROLES PERIÓDICOS

El procedimiento de ejecución de los controles periódicos de verificación se efectuará con periodicidad, al menos, semestral (recomendándose realizarlas de forma mensual) con la finalidad de comprobar el adecuado cumplimiento de las normas y procedimientos establecidos en el presente Documento de Seguridad y velar por su correcta actualización sobre los siguientes aspectos:

Documento de Seguridad

- Comprobar que la descripción de los sistemas de información, la estructura básica de los ficheros está actualizado. Asimismo, se comprobará que el inventario de los equipos informáticos, los programas informáticos y soportes utilizados en la empresa para el tratamiento de datos refleja la situación actual de la empresa.
- Se analizará la vigencia de los ficheros tratados por la empresa, haciendo especial atención en comprobar que los datos se tratan según el principio de calidad, es decir, verificando que los datos de carácter personal de clientes o trabajadores son actuales.
- Se comprobará la identificación de los Encargados del Tratamiento que acceden a los ficheros de la empresa.
- Comprobar que las autorizaciones previstas en el presente Documento de Seguridad se encuentran actualizadas.

Personal de la empresa

- Se comprobará que la lista de usuarios autorizados del Anexo II se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al personal designado al efecto. El personal responsable de las altas, bajas o modificaciones de usuarios

comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.
- Difusión de las funciones y obligaciones del personal entre los trabajadores de la empresa. Prestando especial atención en recabar las firmas de los últimos trabajadores incorporados a la empresa dejando constancia de que han recibido por escrito sus funciones y obligaciones.
- Se comprobará la designación del cargo de Responsable de Seguridad.

Identificación y autenticación
- Se procederá a un cambio de contraseñas semestralmente en los distintos entornos o aplicaciones informáticas, verificando que limitan el número de intentos de acceso fallido, en los términos previstos por este documento, verificándose asimismo su correcta aplicación.

Gestión de Incidencias
- Comprobar que se emplea el canal y protocolo definido para la comunicación de incidencias y que en las mismas se incluye la información exigible.
- Analizar las incidencias registradas en el anexo correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.

Copias de Respaldo y Recuperación
- Se comprobará la existencia de copias de respaldo y el funcionamiento de los procedimientos que permitan la recuperación de los ficheros, así como su debida anotación en el inventario de soportes.

Ficheros temporales o copias de trabajo de documentos
- Seleccionar un número aleatorio de puestos de trabajo y comprobar la posible existencia de ficheros temporales con datos de carácter personal en el disco local o en el escritorio y la adecuada seguridad de los mismos.

Gestión de Soportes
- El Responsable de Seguridad, verificará el cumplimiento de lo previsto en este documento en relación con las entradas y salidas de datos, sean por red o en soporte portátil. Asimismo, velará por el adecuado cumplimiento de lo referido al inventario y al registro de entrada y salida de soportes, analizando, en su caso, los sistemas de cifrado de los soportes que sean objeto de traslado fuera de las oficinas de la empresa.
- Comprobar que los soportes están etiquetados e inventariados acorde a lo descrito en el presente Documento de Seguridad, almacenados físicamente en los lugares oportunos, y que su identificador coincide con lo indicado en el Inventario de soportes.

Telecomunicaciones
- Comprobar que los sistemas de cifrado cumplen con los requisitos de impedir que el personal no autorizado acceda a los datos de nivel alto que se transmitan a través de redes de comunicaciones electrónicas.

Ficheros no automatizados
- Comprobar los procedimientos de archivo, custodia y tratamiento de los ficheros en soporte papel.

Siguiendo con el procedimiento de los controles periódicos tras la verificación de los aspectos vistos, el Responsable de Seguridad o la persona habilitada por la empresa para llevar a cabo el control periódico, recopilará todas las pruebas efectuadas y analizará, conjuntamente con los responsables pertinentes, los resultados obtenidos y las acciones correctivas o de mejora a ejecutar, si hubiese lugar. La documentación asociada a los controles ejecutados y los resultados obtenidos deberán mantenerse, al menos, durante dos años en el **Anexo X** del presente Documento de Seguridad.

13.- EVALUACIONES DE IMPACTO A LA PRIVACIDAD

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, ASISTIA GRAN CANARIA SL realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

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

a) 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;

b) tratamiento a gran escala de las categorías especiales de datos, entendiéndose estos como datos de salud, afiliación política, etc.

c) observación sistemática a gran escala de una zona de acceso público.

La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por ASISTIA GRAN CANARIA SL ;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Los informes de las evaluaciones de impacto quedarán acompañados al presente documento de Documento de Seguridad en el **Anexo IX.**

14.- SANCIONES

Las sanciones introducidas por el nuevo Reglamento se articulan de la siguiente manera:

En el apartado 4 del art. 83 se prevé que se sancionen, de acuerdo con el apartado 2, con **multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente** al **2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior**, **optándose por la de mayor cuantía:**

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.

Por su parte, el apartado 5 del mismo artículo establece que se sancionarán, de acuerdo con el apartado 2, con multas administrativas de **20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía**:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

En el supuesto específico de incumplir las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Por otra parte, debe tenerse en cuenta que, sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

Ahora bien, el ejercicio por una autoridad de control de sus poderes en virtud del artículo 83, estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el contenido del art. 83 podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control.

En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

En cuanto a las condiciones generales para la imposición de estas multas, han de tenerse en cuenta los apartados 1, 2 y 3 del mentado artículo 83, que prevé cada autoridad de control garantizará que la imposición

de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

Concretamente, las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

> a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
>
> b) la intencionalidad o negligencia en la infracción; c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
>
> d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
>
> e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
>
> f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
>
> g) las categorías de los datos de carácter personal afectados por la infracción;
>
> h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
>
> i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
>
> j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
>
> k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

Pero debe tenerse en cuenta que, si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

Finalmente, poner de manifiesto que, según el art. 84, relativo a las sanciones, los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias.

Además, cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que les sea aplicable.

ANEXO I:

DESCRIPCIÓN DE LOS TRATAMIENTOS Y REGISTRO DE LAS ACTIVIDADES DEL TRATAMIENTO

Nombre del Tratamiento	Recursos Humanos	Contabilidad y administración	Pacientes	Historial Clínico	Usuarios web
Finalidades	Gestión integral del área de recursos humanos, emisión de nóminas, altas y bajas en la seguridad social, gestión de la prevención de riesgos laborales, realización de cursos formativas, control de la jornada laboral.	Gestionar el área financiera y económica de la empresa, controlando cobros y gastos, así como la llevanza de la contabilidad, la liquidación de impuestos y tareas administrativas.	Gestionar la relación comercial con los pacientes del centro, y prestarle los servicios y los cuidados solicitados.	Gestionar la relación comercial con los pacientes de la clínica. Establecer un informe histórico de sus visitas y los tratamientos efectuados.	Gestionar de consultas realizadas por usuarios mediante la página web
Categoría de datos	Nombre, Apellidos, DNI, número de seguridad social, tarjeta sanitaria, imágenes, firma, correo electrónico, teléfono.	Apellidos, DNI, firma, correo electrónico, teléfono, datos financieros y de transacciones bancarias.	Nombre, Apellidos, Dni, firma, correo electrónico, teléfono, datos de salud.	Nombre, Apellidos, Dni, firma, correo electrónico, teléfono, datos de salud.	Nombre, apellidos, número de teléfono, correo electrónico
Interesados	Empleados, ex empleados, colaboradores	Empleados, clientes y proveedores	Pacientes, Pacientes potenciales, Personas de contacto, representantes legales.	Pacientes, Pacientes potenciales, Personas de contacto, representantes legales.	Usuarios web
Cesiones previstas	Organismos de la Seguridad Social, Bancos y cajas Rurales, Aseguradoras, Empresas de formación, Servicios de Prevención de Riesgos Laborales.	Bancos y cajas Rurales, Aseguradoras, Agencia Tributaria	No existen	No existen	No existen
Transferencias internacionales	No existen	No existen	No existen	No existen	No se realizan transferencias internacionales de datos
Plazos de conservación	Durante la vigencia del contrato de trabajo y posteriormente el máximo establecido en la correspondiente normativa.	Durante el máximo establecido en la correspondiente normativa.	No existe	No existe	Hasta que decidan revocar el consentimiento de pertenecer a las listas de distribución (newsletter)
Medidas de seguridad aplicadas	Las medidas de seguridad descritas en el documento de seguridad.	Las medidas de seguridad descritas en el documento de seguridad.	Las medidas de seguridad descritas en el documento de seguridad.	Las medidas de seguridad descritas en el documento de seguridad.	Las medidas de seguridad descritas en el documento de seguridad
Ejercicio de los derechos	En las dependencias centrales de la organización	En las dependencias centrales de la organización	En las dependencias centrales de la organización	En las dependencias centrales de la organización	En las dependencias centrales de la organización

Nombre del Tratamiento	Videovigilancia	Clientes			
Finalidades	Controlar las instalaciones con el fin de mantener la seguridad de las mismas así como prevenir robos.	Gestionar la relación comercial, precontractual y contractual con los clientes de la empresa, así como prestar los servicios solicitados. Remitirles información comercial sobre los servicios de la empresa			
Categoría de datos	Imágenes	Nombre, Apellidos, Dni, firma, correo electrónico, teléfono, imagen.			
Interesados	Personas que acceden al portal y al interior de la oficina	Clientes, Personas de contacto, representantes legales,			
Cesiones previstas	Fuerzas Y Cuerpos De Seguridad Del Estado	No existen			
Transferencias internacionales	No existen	No existen			
Plazos de conservación	1 mes	No existe			
Medidas de seguridad aplicadas	Las medidas de seguridad descritas en el documento de seguridad.	Las medidas de seguridad de nivel alto descritas en el documento de seguridad.			
Ejercicio de los derechos	En las dependencias centrales de la empresa de seguridad privada	En las dependencias centrales de la organización			

ANEXO II:

INVENTARIO DE SOPORTES Y PROGRAMAS INFORMÁTICOS

ANEXO II- CAMBIO DE CONTRASEÑAS

Número de serie del recurso informático	Fecha del cambio de contraseña	Usuario que efectúa el cambio
TODOS LOS RECURSOS INFORMATICOS	**06/08/2020**	Héctor Hernández González

Inventario de equipos

Tipo hardware	Nº de serie	Ubicación	Usuario
DESKTOP-6SLLRE0	AEE3AF2D-0A3A-4052-A9DF-046FC4BB06D2		Fernando Miguel Pérez Valdivia
DESKTOP-CSG5HN9	4BD46F41-DF19-4B8D-B7C2-C137C5C33BA1		Eduvigis Gil Suárez
DESKTOP-ERIBE3Q	45FB1501-378D-4A94-8FD1-691851A1314A		Tania Fleitas Sauco
DESKTOP-HMTPTCJ	B5AF5069-B446-42A4-9CE5-A6AF73A189C5		Leticia González Verona

Inventario de software

Aplicación	Versión	Uso	Usuario	Acceso remoto

ANEXO III:
RELACIÓN DEL PERSONAL

Nombre y apellidos	Puesto	Descripción	Carta firmada
VALERIO HIDALGO MARTEL	GERENTE	GERENTE	

LETICIA GONZALEZ VERONA	DIRECTORA	DIRECTORA	
EDUVIGIS GIL SUAREZ	AUXILIAR ADMINISTRATIVO	AUXILIAR ADMINISTRATIVO	
TANIA FLEITAS SAUCO	TRABAJADORA SOCIAL	TRABAJADORA SOCIAL	
FERNANDO MIGUEL PEREZ VALDIVIA	AUX ADMINISTRATIVO	AUX ADMINISTRATIVO	
HECTOR HERNANDEZ GONZALEZ	AUX ADMINISTRATIVO	AUX ADMINISTRATIVO	

ANEXO IV:

OBLIGACIONES DEL PERSONAL

COMPROMISO DE CONFIDENCIALIDAD

ANEXO V:

DESIGNACIONES / AUTORIZACIONES

LIBRO REGISTRO DE AUTORIZACIONES

DESIGNACIÓN DEL RESPONSABLE DE SEGURIDAD

Mediante el presente escrito, D. Fernando Miguel Pérez Valdivia asume formalmente las funciones de coordinar y controlar las medidas de seguridad establecidas en el presente Documento de Seguridad en relación con todos los ficheros o tratamientos de datos de carácter personal de la empresa, en particular para desarrollar las funciones de:

1. Cooperar en el registro y análisis de cualquier incidencia que pueda suponer un peligro para la seguridad de los ficheros tomando las medidas oportunas en colaboración con el responsable de los ficheros.

2. Responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo de los ficheros, de forma que ninguna persona no autorizada tenga acceso a las mismas.

3. Realizar controles periódicos de verificación del cumplimiento, comprobando cada tres meses:

a) Que la lista de usuarios autorizados del Anexo III se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al personal informático designado al efecto.

b) La existencia de copias de respaldo que permitan la recuperación de Fichero.

c) Cualquier cambio que se haya realizado en los datos técnicos de los anexos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos anexos.

d) El cumplimiento de lo previsto en este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.

e) Analizar, junto con el responsable de los ficheros las incidencias registradas en el libro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, proponer las medidas correctoras que limiten esas incidencias en el futuro.

f) Revisar la información de control de accesos registrada y elaborará un informe de las revisiones realizadas y los problemas detectados, al menos una vez al mes.

g) Supervisar la aplicación de las medidas previstas para el entorno de sistema operativo y de comunicaciones de los ficheros.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al Responsable de los Ficheros, de conformidad con lo dispuesto en 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 Personales 2016/679 del Parlamento Europeo y del Consejo.

Responsable de los tratamientos

Responsable de Seguridad
DNI: 78765653-Z
Firma:

DESIGNACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS

Mediante el presente escrito, ASISTIA GRAN CANARIA SL nombra delegado de protección de datos a D…… al amparo del artículo 38 y 39 del Reglamento Europeo de Protección de datos, quien asume formalmente las funciones coordinar y controlar las medidas de seguridad establecidas en el presente Documento de Seguridad en relación con todos los ficheros o tratamientos de datos de carácter personal de la empresa, en particular para desarrollar las funciones de:

a) informar y asesorar a ASISTIA GRAN CANARIA SL o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud de la normativa y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de la normativa y de las políticas del presente manual 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;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto.

ASISTIA GRAN CANARIA SL

Responsable de los Tratamientos **Responsable de Seguridad**

Firma y DNI: Firma y DNI:

:

NOMBRAMIENTO DEL ADMINISTRADOR DE LOS SISTEMAS INFORMATICOS

ASISTIA GRAN CANARIA SL , autoriza a:
D. Fernando Miguel Pérez Valdivia

X Trabajador de esta empresa
___ Informático externo

a desarrollar la Administración del Sistema Informático de la empresa, teniendo autoridad para realizar todas las acciones necesarias que garanticen el óptimo funcionamiento y el cumplimiento de todas las normativas vigentes en materia de seguridad informática y protección de datos de carácter personal exigen por Ley y demás medidas complementarias.

De la misma forma el Administrador del Sistema Informático deberá velar el total cumplimiento de las medidas y acciones que se establecen en el Documento de Seguridad que la empresa dispone en cumplimiento con la LOPD, absteniéndose de realizar acciones no autorizadas en el mismo.

Toda acción que sea necesario realizar y no esté contemplada en el Manual de Seguridad, al igual que cualquier incidencia que pueda poner en peligro la integridad de la red y los datos que contiene, deberá ser informada con urgencia al Responsable de Seguridad de la empresa y tomarse todas las medidas necesarias para minimizar los riesgos que se pueden derivar de esa incidencia.

La persona designada, mediante la firma de este documento, acepta las funciones y obligaciones que se desprenden del desarrollo de esta labor, responsabilizándose por garantizar que en todo momento las mismas se hagan en correspondencia con las medidas de seguridad establecidas en la empresa.

En ningún caso esta designación supone la delegación de la responsabilidad que corresponde a ASISTIA GRAN CANARIA SL como Responsable de los Tratamientos, tal y como estipula la normativa de protección de datos.

Y para que así conste firmo la presente,

En Avenida Primero de Mayo nº9

Responsable de los Tratamientos	**Administrador del sistema informático**
Firma y DNI:	Firma y DNI: 78765653-Z

AUTORIZACION PARA LA REALIZACION Y CONSERVACION DE LAS COPIAS DE SEGURIDAD

ASISTIA GRAN CANARIA SL como Responsable de los Tratamientos, autoriza a D. Fernando Miguel Pérez Valdivia a realizar las copias de seguridad con la frecuencia que se indica en el Documento de Seguridad por el cual se rigen las actuaciones en materia de Protección de Datos que se llevan a cabo en la gestión interna de esta entidad.

En consecuencia, el encargado de esta actividad procederá a realizar dichas acciones en las fechas que corresponda, siendo además el encargado de conservarlas bajo las siguientes condiciones generales:

- Las copias de seguridad sólo se podrán realizar en el soporte a continuación descrito ……. que la empresa ha facilitado al encargado de realizar las copias.
- Las copias de seguridad en todos los casos se deberán realizar únicamente de los ficheros que se autorizan en anexo a este documento.
- Se deberá tener especial cuidado en que todos los ficheros a los que se realice copias de seguridad se hagan encriptándolos y en caso de no ser posible compactándolos y colocándole una contraseña que será acordada con el responsable de seguridad de la empresa.
- Las copias de seguridad se deberán conservar en un lugar protegido con llave y que además no corra peligro ante posibles desastres como inundaciones, fuegos, etc., pues su pérdida implicaría que toda la información atesorada por la empresa desaparecería creando serios problemas de gestión.
- Se recomienda que al menos las copias mensuales y anuales se conserven además de en la empresa en un lugar fuera de la misma que se especifica en anexo a este documento.
- Ante cualquier incidencia con las copias de seguridad que puedan poner en peligro su integridad o seguridad, el encargado de protegerlas deberá informar a la empresa y tomar las medidas necesarias para salvaguardarlas, generándose una incidencia en cada caso que deberá ser registrada en el manual de seguridad.

La persona designada, mediante la firma de este documento, acepta las funciones y obligaciones que se desprenden del desarrollo de esta labor, responsabilizándose por garantizar que en todo momento las mismas se hagan en correspondencia con las medidas de seguridad establecidas en la empresa.

En ningún caso esta designación supone la delegación de la responsabilidad que corresponde al Responsable de los Tratamientos, tal y como estipula la normativa de protección de datos.

Y para que así conste firmo la presente,

En Avenida Primero de Mayo 9

Responsable de los Tratamientos	**Encargado de las Copias de Seguridad**
Firma y DNI: 78765653 Z	Firma y DNI: 78765653 Z

LIBRO DE REGISTRO DE AUTORIZACIONES

FUNCION: conceder, alterar o anular el acceso a los distintos recursos de los sistemas de información y para gestionar las contraseñas de acceso.

NOMBRE	CARGO	FICHERO AFECTADO	FECHA Y FIRMA
EDUVIGIS GIL SUAREZ	AUXILIAR ADMINISTRATIVO	**TODOS**	**06/10/2020**
TANIA FLEITAS SAUCO	TRABAJADORA SOCIAL	**TODOS**	**06/10/2020**
FERNANDO MIGUEL PEREZ VALDIVIA	AUX ADMINISTRATIVO	**TODOS**	**06/10/2020**
HECTOR HERNANDEZ GONZALEZ	AUX ADMINISTRATIVO	**TODOS**	**06/10/2020**

FUNCIÓN: sacar soportes y documentos que contengan datos de carácter personal fuera de los locales bajo el control de la empresa:

NOMBRE	CARGO	FICHERO AFECTADO	FECHA Y FIRMA
EDUVIGIS GIL SUAREZ	AUXILIAR ADMINISTRATIVO	**TODOS**	**06/10/2020**
TANIA FLEITAS SAUCO	TRABAJADORA SOCIAL	**TODOS**	**06/10/2020**
FERNANDO MIGUEL PEREZ VALDIVIA	AUX ADMINISTRATIVO	**TODOS**	**06/10/2020**
HECTOR HERNANDEZ GONZALEZ	AUX ADMINISTRATIVO	**TODOS**	**06/10/2020**

FUNCIÓN: Autorización para ejecutar, controlar y supervisar el procedimiento de gestión de incidencias por persona distinta al Responsable de Seguridad:

NOMBRE	CARGO	FICHERO AFECTADO	FECHA Y FIRMA
EDUVIGIS GIL SUAREZ	AUXILIAR ADMINISTRATIVO	**TODOS**	**06/10/2020**
TANIA FLEITAS SAUCO	TRABAJADORA SOCIAL	**TODOS**	**06/10/2020**
HECTOR HERNANDEZ GONZALEZ	AUX ADMINISTRATIVO	**TODOS**	**06/10/2020**

FUNCION: Realizar, con datos reales, pruebas anteriores a la implantación o modificación de los sistemas de información.

NOMBRE	CARGO	FICHERO AFECTADO	FECHA Y FIRMA
EDUVIGIS GIL SUAREZ	AUXILIAR ADMINISTRATIVO	**TODOS**	**06/10/2020**
TANIA FLEITAS SAUCO	TRABAJADORA SOCIAL	**TODOS**	**06/10/2020**
FERNANDO MIGUEL PEREZ VALDIVIA	AUX ADMINISTRATIVO	**TODOS**	**06/10/2020**
HECTOR HERNANDEZ GONZALEZ	AUX ADMINISTRATIVO	**TODOS**	**06/10/2020**

FUNCION:

NOMBRE	CARGO	FICHERO AFECTADO	FECHA Y FIRMA

FUNCION:

NOMBRE	CARGO	FICHERO AFECTADO	FECHA Y FIRMA

ANEXO VI:

REGISTROS DE ENTRADA Y SALIDAS DE SOPORTES

Tipo de documento y soporte	Fecha y hora de salida	Fecha y hora de entrada	Información que contiene	Persona encargada de la recepción / envío	Firma Persona encargada de la recepción / envío	Firma del Responsable de Seguridad

Tipo de documento y soporte	Fecha y hora de salida	Fecha y hora de entrada	Información que contiene	Persona encargada de la recepción / envío	Firma Persona encargada de la recepción / envío	Firma del Responsable de Seguridad

ANEXO VII:

REGISTRO DE VIOLACIONES DE SEGURIDAD

Incidencia Número: |_____|	
Fecha de notificación: /__/__/____/	Fecha y hora en que se produjo la incidencia: /__/__/____/
Tipo de incidencia:	
Descripción detallada de la incidencia:	
Medidas correctoras aplicadas:	
Persona(s) a quien(es) se comunica:	
Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella)	
Recuperación de Datos :(A rellenar sólo si la incidencia es de este tipo) Procedimiento realizado: Datos restaurados: Datos grabados manualmente: Persona que ejecutó el proceso: Firma del Responsable del Tratamiento: Fdo _____	
Persona que realiza la comunicación: Fdo.:_____	

Incidencia Número: |_____|	
Fecha de notificación: /__/__/____/	Fecha y hora en que se produjo la incidencia: /__/__/____/
Tipo de incidencia:	
Descripción detallada de la incidencia:	
Medidas correctoras aplicadas:	
Persona(s) a quien(es) se comunica:	
Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella)	
Recuperación de Datos :(A rellenar sólo si la incidencia es de este tipo) Procedimiento realizado: Datos restaurados: Datos grabados manualmente: Persona que ejecutó el proceso: Firma del Responsable del Tratamiento: Fdo _____	
Persona que realiza la comunicación: Fdo.:_____	

Nº de Incidencia	Tipo de Incidencia	Fecha de notificación	Fecha de resolución	Persona encargada	Efectos derivados

ANEXO VIII:
ENCARGADOS DE TRATAMIENTO

ANTES DE CONTRATAR CON UN PROVEEDOR

1 Política de seguridad y de protección de datos personales

1.1 Su compañía, incluyendo todas sus filiales ¿Tiene una Política de Seguridad y Privacidad de datos adaptada a la legislación aplicable y estándares en todas las jurisdicciones donde opera?

SI		NO	

En caso negativo, le rogamos facilite detalles sobre otros procedimientos internos de la empresa para la protección de datos y las jurisdicciones donde no se encuentran adaptados:

1.2 ¿Dispone de un plan de emergencia en el caso de que descubran una brecha de seguridad de sistemas o brecha de privacidad/seguridad de datos?

SI		NO	

En caso afirmativo, por favor facilite detalles a continuación:.

1.3 ¿Su compañía informa y facilita a todos sus empleados los procedimientos y políticas internas de protección de datos así como sus actualizaciones y les requiere la confirmación de su cumplimiento?

SI		NO	

En caso negativo, le rogamos facilite explicación del motivo:

1.4 ¿Cuándo y por parte de quién fueron revisados por última vez los procedimiento internos de protección de datos?

1.5 ¿Dispone su compañía de certificados relacionadas con la gestión de los sistemas de información (por ejemplo, ISO9001, ISO27001; ISO20000-1, CMMI, PCI DSS, etc.)?

SI		NO	

En caso afirmativo, le rogamos indique cuáles:

1.6 ¿Su compañía tiene alguna filial en los Estados Unidos de América?

SI		NO	

En caso afirmativo, ¿se ha registrado su compañía y da cumplimiento al Programa "*Privacy Shield*" firmado entre la Unión Europea y los Estados Unidos de América?

SI		NO	

En caso negativo, rogamos facilite detalles en relación a la falta de cumplimiento con dicho programa:

1.7 ¿Tiene su compañía un Responsable de seguridad, un Responsable de protección de los datos, un asesor legal interno o cualquier otra persona formalmente responsable de la protección y seguridad de los datos?

SI		NO	

En caso negativo, ¿quién es responsable de la gestión y cumplimiento de lo relativo a la seguridad y protección de los datos?:

2 Protección de los sistemas y antivirus

2.1 Su compañía, utiliza procesos y sistemas de protección anti-virus actualizado en sus equipos, sistemas de comunicación y servidores para servicios básicos y de misión crítica para protegerlos contra código malicioso (incluyendo pero no limitando, virus, troyanos/gusanos, spyware, malware y root-kits?

SI		NO	

En caso afirmativo, ¿cada cuanto tiempo actualizan estos procedimientos y sistemas de protección? ¿Se actualiza automáticamente?:

2.2 ¿Dispone de un programa de evaluación de vulnerabilidades proactivo que monitoriza las brechas y asegura un tiempo de actualización en los parches de seguridad críticos, vulnerabilidades conocidas?

SI		NO	

3 Seguridad y funcionamiento de red

3.1 Su compañía ¿utiliza sistemas de protección con el fin de evitar accesos no autorizados o daños a sus sistemas informáticos, redes, o sistemas de almacenamiento de datos e información (tales como IPS, "firewalls", autentificación de usuarios en remoto, etc.)?

SI		NO	

En caso afirmativo, ¿están todos los ordenadores, dispositivos móviles y sitios web protegidos con "firewalls" o tienen sistemas de prevención de intrusión/acceso en los mismos?

SI		NO	

3.2 ¿Tiene su compañía procesos instaurados de identificación y detección de debilidades en sus sistemas/redes?

SI		NO	

En caso negativo, motive la decisión:

3.3 Su compañía, ¿monitoriza sus redes y sistemas informáticos buscando violaciones de seguridad?

SI		NO	

En caso negativo, motive la decisión:

3.4 Su compañía, ¿Realiza con regularidad auditorias y revisiones de la arquitectura de seguridad de la red?

SI		NO	

En caso afirmativo, ¿se ha implantado un plan correctivo?

SI		NO	

3.5 ¿Tiene su compañía requerimientos de cifrado para datos en tránsito y datos en depósito que protejan la integridad de la información confidencial, incluidos los datos contenidos en dispositivos o tecnología móvil (por ejemplo, portátiles, grabaciones de backup en DVD, drivers, dispositivos USB…etc.?

SI		NO	

4 Copias de seguridad y Plan de continuidad

4.1 Su compañía mantiene mecanismos de copias de seguridad y procesos de recuperación para todos:

SI		NO	

i) los sistemas de misión crítica

SI		NO	

ii) los datos y activos informáticos

4.2 ¿Dispone de un plan de continuidad del negocio (BCP) y plan de recuperación ante desastres (DRP) de trabajo para evitar la Interrupción del negocio a causa de problemas informáticos o acelerar su recuperación?

SI		NO	

En caso afirmativo, ¿Cuánto tiempo le llevaría restablecer las operaciones después de un ataque cibernético u otra pérdida/corrupción de datos?

En caso negativo, ¿tiene previsto establecer un plan de continuidad? ¿Cuándo? Rogamos facilite detalle:

5 Seguridad física de la sala de ordenadores

5.1 Su compañía ¿Ha realizado un inventario de los sistemas críticos?

SI		NO	

5.2 Su compañía, ¿Tiene establecidos controles físicos de seguridad para la detección y detención de accesos no autorizados a los sistemas informáticos y centros de datos?

SI		NO	

6 Actividades de Outsourcing (Servicios de Externalización)

6.1 Su compañía, ¿externaliza alguna parte de sus redes, sistemas informáticos o funciones de seguridad de la información?

SI		NO	

En caso afirmativo, ¿Audita su compañía periódicamente las funciones del al subcontratista (también denominado "prestador de servicios") para asegurarse de que cumplen con las políticas de seguridad del solicitante?:

¿Quién se encarga de la externalización de la seguridad?:

6.2 ¿Su compañía, requiere al subcontratista que dé cumplimiento con los términos de la política de protección de datos de su compañía?

SI		NO	

6.3 ¿Se han suscrito Acuerdos de Nivel de Servicio (SLAs) con el subcontratista y/o acuerdos de encargado de tratamiento?

SI		NO	

6.4 ¿Se exige al subcontratista la contratación de póliza de RC Profesional y/o protección de datos?

SI		NO	

En caso afirmativo, especificar cual de ellas:

6.5 Su compañía, ¿dispone de servicios en nube o *cloud computing*?

SI		NO	

En caso afirmativo:

¿Dispone de una política de seguridad cloud? Si No

SI		NO	

En caso negativo, le rogamos facilite detalles sobre otros procedimientos internos para asegurar los datos personales y corporativos:

Proveedor:	
CIF:	

Nombre y Apellidos	
Número de Identificación Fiscal	
Cargo en la empresa	
Lugar y fecha	

Firma

Los datos personales que puedan constar en este documento se incorporarán en los ficheros propiedad de ASISTIA GRAN CANARIA SL con la finalidad de llevar a cabo la gestión contractual con ustedes. Puede ejercitar sus derechos de acceso, supresión, rectificación y oposición, dirigiendo un escrito a nuestro domicilio social adjuntando fotocopia del DNI.

RELACIÓN DE PROVEEDORES CON ACCESO A DATOS

RAZÓN SOCIAL: JD ASESORIA JOSE DAMASO SL		CIF: B35776921
CENTRO DE TRATAMIENTO: ASESORIA INTEGRAL		TEL:
DIRECCIÓN: CALLE LEON Y CASTILLO 36, 1º PLANTA EDIF. CENTRO DE NEGOCIOS JD 36	CP: 35200	POBLACION: TELDE – LAS PALMAS DE GRAN CANARIA

RAZÓN SOCIAL: TYCO ADT CANARIAS ALARMAS SL		CIF: B82115577
CENTRO DE TRATAMIENTO: VIDEOVIGILANCIA		TEL:
DIRECCIÓN: CARRETERA DE LA CORUÑA KM 23, 500	CP: 28290	POBLACION: LAS ROZAS - MADRID

RAZÓN SOCIAL: JUAN MANUEL GONZALEZ SANTANA		CIF: 42804677K
CENTRO DE TRATAMIENTO: INFORMATICO WEB		TEL:
DIRECCIÓN: C/ MALAGA 45-5ºA	CP: 35016	POBLACION: LAS PALMAS DE GRAN CANARIA

RAZÓN SOCIAL: SOLUCIONES AVANZADAS EN TECNOLOGIA INTEGRAL SL	CIF: B35704642

CENTRO DE TRATAMIENTO: INFORMATICO DE SISTEMAS		TEL:
DIRECCIÓN: C/ RUIZ MUÑIZ 20 LOCAL	CP: 35200	POBLACION: TELDE – LAS PALMAS DE GRAN CANARIA

RAZÓN SOCIAL:		CIF:
CENTRO DE TRATAMIENTO:		TEL:
DIRECCIÓN:	CP:	POBLACION:

ANEXO IX:

EVALUACIONES DE IMPACTO A LA PRIVACIDAD

Fecha	Descripción del tratamiento a realizar	Resumen de las soluciones adoptadas

ANEXO X:

CONTROLES PERIÓDICOS Y ACTUALIZACIONES

Fecha en que comienza la revisión	Persona que realiza la revisión	Medidas realizadas en el Control o Actualización	Fecha en que termina la actualización	Observaciones
06/10/2020	Fernando Miguel Pérez Valdivia	Control que se llevan a cabo todas las medidas	06/10/2020	

ANEXO XI:

FORMULARIOS Y OTROS DOCUMENTOS

ANEXO XII:

EJERCICIO DE LOS DERECHOS OTORGADOS POR LA NORMATIVA DE PROTECCIÓN DE DATOS

A) EJERCICIO DEL DERECHO DE ACCESO

IDENTIFICACIÓN DE LA EMPRESA RESPONSABLE DEL TRATAMIENTO

ASISTIA GRAN CANARIA SL como responsable del tratamiento;

DATOS DEL SOLICITANTE O REPRESENTANTE LEGAL:

D./Dª. _____, mayor de edad, con domicilio en la calle _____, número_____, Localidad_____, Código Postal _____, Provincia con D.N.I. _____, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con el artículo 15 del Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo,

SOLICITA

1. Que se le facilite el derecho de acceso a los ficheros de la **ASISTIA GRAN CANARIA SL** , en el plazo máximo de **un mes** a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se considerará denegada.

2. Que esta información comprenda, de modo legible e inteligible, los datos de base que sobre mi persona están incluidos en sus ficheros, los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los mismos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

3. Que, si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada.

En …….., a ....., de.....de 202..

Fdo.

Modelo carta contestación al Derecho de acceso

En ……., a ....., de.....de 202...

Apreciado/a Sr./a

Por la presente, y en virtud de la solicitud que Usted nos remitió en fecha ___de _____ de 202__, relativa al ejercicio de su derecho de acceso en virtud de lo establecido en el artículo 15 del Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo,
, tenemos el agrado de comunicarle:

1.- Que ASISTIA GRAN CANARIA SL ha tenido acceso únicamente a sus datos (relacionar los datos) para _____.
2.- Que ASISTIA GRAN CANARIA SL tuvo conocimiento de dichos datos a través de la información facilitada por usted.
3.- Que sus datos no han sido comunicados ni cedidos a terceros.

Dando cumplimiento al deber establecido en la normativa vigente en materia de protección de datos de carácter personal, se da por ejercitado el derecho de acceso solicitado por usted, quedando a su disposición para cualquier duda que tenga al respecto.
Reciba un cordial saludo.

Fdo: _____

B) EJERCICIO DEL DERECHO DE RECTIFICACIÓN

IDENTIFICACIÓN DE LA EMPRESA RESPONSABLE DEL TRATAMIENTO

ASISTIA GRAN CANARIA SL como responsable del tratamiento;

DATOS DEL SOLICITANTE O REPRESENTANTE LEGAL:

D./Dª. _____,
mayor de edad, con domicilio en la calle _____, número_____, Localidad_____, Código Postal _____, Provincia _____con D.N.I. _____, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer derecho de rectificación, de conformidad con los artículos 16 15 del Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo,

EXPONE

1. Que se proceda a la efectiva rectificación en el plazo de **diez 10 días** desde la recepción de esta solicitud, de los datos inexactos relativos a mi persona que se encuentren en los ficheros de **ASISTIA GRAN CANARIA SL** ,
2. Los datos que hay que rectificar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan en esta solicitud para acreditar la veracidad de los nuevos datos.
3. Que en el caso de que el responsable del tratamiento considere que la rectificación no procede lo comunique en el plazo de diez días señalado.
4. Que, si los datos rectificados hubieran sido comunicados previamente a un tercero, se notifique al mismo la rectificación practicada, con el fin de que éste proceda también a realizar las modificaciones oportunas.
5. Que cualquier comunicación que hubiere lugar se realice a la dirección arriba indicada.

En ……., a , de.....de 202....

Fdo.

Modelo carta contestación al Derecho de rectificación

En …….., a , de.....de 201....

Apreciado/a Sr./a
Por la presente, y en virtud de la solicitud que Usted nos remitió en fecha ___ de _____ de 201__, relativa al ejercicio de su derecho de rectificación en virtud de lo establecido en el artículo 16 del Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo, tenemos el agrado de comunicarle:

1.- Que ASISTIA GRAN CANARIA SL ha procedido a rectificar los datos relativos a su persona de los que disponía, conforme a su petición.

Dando cumplimiento al deber establecido en la normativa vigente en materia de protección de datos de carácter personal, se da por ejercitado el derecho de rectificación solicitado por usted, quedando a su disposición para cualquier duda que tenga al respecto.
Reciba un cordial saludo.

Fdo: _____

C) EJERCICIO DEL DERECHO DE SUPRESIÓN

IDENTIFICACIÓN DE LA EMPRESA RESPONSABLE DEL TRATAMIENTO

ASISTIA GRAN CANARIA SL como responsable del tratamiento;

DATOS DEL SOLICITANTE O REPRESENTANTE LEGAL:

D./Dª. _____,
mayor de edad, con domicilio en la calle _____,
número_____, Localidad_____, Código Postal _____, Provincia _____con D.N.I. _____, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer derecho de cancelación, de conformidad con el art. 17 de la 15 del Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo,

EXPONE

1. Que se proceda a la efectiva cancelación en el plazo de **diez 10 días** desde la recepción de esta solicitud, de los datos relativos a mi persona que se encuentren en los ficheros de **ASISTIA GRAN CANARIA SL** que relaciono a continuación, al no existir vinculación jurídica o disposición legal que justifique su mantenimiento.
2. Los datos que hay que cancelar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan en esta solicitud para acreditar la procedencia de la misma.
3. Que en el caso de que el responsable del tratamiento considere que la cancelación no procede lo comunique en el plazo de diez días señalado.
4. Que, si los datos cancelados hubieran sido comunicados previamente a un tercero, se notifique al mismo la operación practicada, con el fin de que éste proceda también a realizar las cancelaciones oportunas.
5. Que cualquier comunicación que hubiere lugar se realice a la dirección arriba indicada.

En ……., a , de.....de 201....

Fdo.

Modelo carta contestación al Derecho de Supresión

En ……., a , de.....de 201....

Apreciado/a Sr./a

Por la presente, y en virtud de la solicitud que Usted nos remitió en fecha ___ de _____ de 201__, relativa al ejercicio de su derecho de cancelación en virtud de lo establecido en el artículo 17 15 del Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo, tenemos el agrado de comunicarle:

1.- Que ASISTIA GRAN CANARIA SL ha procedido a bloquear sus datos personales, conservándose a disposición de las Administraciones públicas, Jueces y Tribunales y durante los plazos previstos en las disposiciones aplicables.

Dando cumplimiento al deber establecido en la normativa vigente en materia de protección de datos de carácter personal, se da por ejercitado el derecho de cancelación solicitado por usted, quedando a su disposición para cualquier duda que tenga al respecto.

Reciba un cordial saludo.

Fdo: _____

D) EJERCICIO DEL DERECHO DE OPOSICIÓN

IDENTIFICACIÓN DE LA EMPRESA RESPONSABLE DEL TRATAMIENTO

ASISTIA GRAN CANARIA SL como responsable del tratamiento;
DATOS DEL SOLICITANTE O REPRESENTANTE LEGAL:
D./Dª. _____,
mayor de edad, con domicilio en la calle _____,
número_____, Localidad_____, Código Postal
_____, Provincia _____con D.N.I. _____,
del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer derecho de oposición, de conformidad con el art. 21 del Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo,

EXPONE

1. Que se proceda a la efectiva oposición en el plazo de **diez 10 días** desde la recepción de esta solicitud, del tratamiento de los datos relativos a mi persona que se encuentren en los ficheros de **ASISTIA GRAN CANARIA SL** que relaciono a continuación, al no existir vinculación jurídica o disposición legal que justifique su mantenimiento.
2. Los datos que hay que oponerse se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan en esta solicitud para acreditar la procedencia de la misma.
3. Que en el caso de que el responsable del tratamiento considere que la oposición no procede lo comunique en el plazo de diez días señalado.
4. Que si los datos personales hubieran sido comunicados previamente a un tercero, se notifique al mismo la operación practicada, con el fin de que éste proceda también a realizar las oposiciones oportunas.
5. Que cualquier comunicación que hubiere lugar se realice a la dirección arriba indicada.

En ……., a , de.....de 201....

Fdo.

Modelo carta contestación al Derecho de oposición

En ……., a , de.....de 201....

Apreciado/a Sr./a

Por la presente, y en virtud de la solicitud que Usted nos remitió en fecha ___ de _____ de 201__, relativa al ejercicio de su derecho de oposición en virtud de lo establecido por el Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo,
tenemos el agrado de comunicarle:

1.- Que ASISTIA GRAN CANARIA SL ha cesado en el tratamiento de sus datos conforme a la petición.

Dando cumplimiento al deber establecido en la normativa vigente en materia de protección de datos de carácter personal, se da por ejercitado el derecho de oposición solicitado por usted, quedando a su disposición para cualquier duda que tenga al respecto.

Reciba un cordial saludo.

Fdo: _____