REGLAMENTO GENERAL PROTECCIÓN DE DATOS
UE 679/2016

ENTREGA DE DOCUMENTACIÓN

NUEVA ANDALUCÍA a de de 201

Con el presente documento se formaliza la entrega del siguiente material para el cumplimiento del RGPD UE 679/2016
Carpeta para guardar toda la documentación relacionada con dicho Reglamento.

ALFONSO GONZÁLEZ BUENO con DNI 25077065G como representante legal de la empresa INVERSIONES BARUTA 2002, S.L., con CIF B92332337, hace constar que **safedata®** nos ha informado, de conformidad con el Reglamento UE 679/2016, de los siguientes puntos:
Obligación de incluir las cláusulas legales de consentimiento en los correspondientes formularios e informar a los empleados sobre el ejercicio de los derechos.
Obligación de entregar y guardar copia firmada del compromiso de confidencialidad por parte de los empleados que tengan acceso a datos de carácter personal.
Obligación de entregar a todos los empleados el comunicado interno para el tratamiento de datos de carácter personal.
Obligación de firmar por las partes implicadas los contratos de tratamiento de datos por cuenta de terceros.
Obligación de notificar a **safedata®** nuevos medios para recoger datos, así como otros destinatarios para las cesiones o encargados del tratamiento que no hayan estado comunicados en la consultoría inicial.
La cesión de bases de datos en las cuales aparezcan datos de carácter personal de personas físicas, sin el consentimiento previo de estas, comporta una vulneración del Reglamento y como consecuencia una sanción por parte de la Agencia Española de Protección de Datos.
Todos los documentos entregados son propiedad de **safedata®** y están protegidos por los derechos de Propiedad Intelectual e Industrial. El destinatario de estos documentos, únicamente tiene derecho a un uso privado de los mismos y necesita autorización expresa y por escrito de **safedata®** para reproducirlos, explotarlos y especialmente comercializarlos, o hacer uso de cualquier derecho que pertenezca al titular.
El cliente únicamente podrá distribuir los documentos entregados por **safedata®** a sus empleados o a quien le indique expresamente, siguiendo los estándares de confidencialidad que determine la normativa legal vigente, así como a requerimiento de los organismos públicos competentes y se responsabilizarán de la custodia de los mismos.

Firma de conformidad:

INVERSIONES BARUTA 2002, S.L. **safedata@**

OBJETO DEL DOCUMENTO

El objeto del presente documento es recopilar la normativa referente a las medidas de seguridad de obligado cumplimiento para todo el personal con acceso a los datos automatizados o no automatizados de carácter personal y a los sistemas de información.
Debido a la continua evolución y cambios intrínsecos de los sistemas de información y a la propia complejidad de la organización, el documento intentará ser un marco estable y, al mismo tiempo, flexible, en lugar de una descripción estática, por la que se vería sometido a continuas actualizaciones.
En esta línea, el documento incluye referencias a otros documentos que conforman la política de seguridad establecida en la organización y, en ocasiones, en lugar de incluir relaciones estáticas se describe el procedimiento para obtener las citadas relaciones en el momento en que sean necesarias.
El presente documento se mantendrá en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
Del mismo modo se adaptará, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

ÁMBITO DE APLICACIÓN DEL DOCUMENTO

Las medidas de seguridad definidas en el presente documento van encaminadas a proteger todos los ficheros, aplicaciones, herramientas de actualización y consulta, recursos del sistema operativo, redes de telecomunicaciones, soportes y equipos informáticos que pueden ser gestionados por INVERSIONES BARUTA 2002, S.L., o por cualquier otra empresa con la cual se haya subscrito un contrato de prestación de servicios que comporte el tratamiento de datos de carácter personal.
En consecuencia, los recursos comprendidos dentro del ámbito de aplicación de este documento serán todos los datos de carácter personal que componen el registro de actividades, así como las aplicaciones y sistemas que los tratan, los equipos informáticos que los soportan y los locales donde se ubican.

ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

En INVERSIONES BARUTA 2002, S.L. NO existe acceso remoto.

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE UBICACIÓN DEL FICHERO

En INVERSIONES BARUTA 2002, S.L. NO existen ordenadores portátiles, autorizados previamente siguiendo la política mencionada a continuación y relacionados en el ANEXO ”Tratamiento de datos en los portátiles”.
Los empleados de INVERSIONES BARUTA 2002, S.L. que disponen de ordenador portátil, son informados de la prohibición, salvo excepciones autorizadas, de almacenar datos de carácter personal en el disco duro de los ordenadores portátiles y de la obligación de trabajar con datos de carácter personal únicamente sobre las unidades lógicas definidas en el servidor de aplicaciones.
Además, tendrán que cumplir con las medidas de seguridad implementadas en INVERSIONES BARUTA 2002, S.L. que quedan definidas en este documento.
Será obligatorio que en los ordenadores portátiles se habiliten los mismos criterios establecidos sobre identificación, autentificación y control de accesos definidos en este documento de seguridad, siempre que se conecten a la red local o accedan de manera remota.

FICHEROS TEMPORALES
Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los datos tratados.
Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

IDENTIFICACIÓN Y AUTENTICACIÓN
El procedimiento seguido en INVERSIONES BARUTA 2002, S.L. para la identificación y autenticación de los usuarios cuando intentan acceder al sistema, la red o las aplicaciones, está basado en la combinación de un código de identificación de usuario y una contraseña. A cada usuario le ha sido asignada una identificación única tanto para el acceso al sistema como para el acceso a las aplicaciones.
En el anexo de Medidas Técnicas se describen los procedimientos establecidos en INVERSIONES BARUTA 2002, S.L. referentes a las contraseñas.

CONTROL DE ACCESO
Los usuarios recibirán sus derechos de acceso siguiendo la política de mínimo privilegio, asignándoles un único código de identificación. Es decir, únicamente accederán a aquellos datos y recursos informáticos que precisan para el desarrollo de sus funciones.
En el anexo Usuarios del sistema, se indica el procedimiento a seguir para obtener la relación de usuarios con acceso autorizado a la red y a las aplicaciones; así como los derechos que tienen concedidos.
En el anexo Relación de usuarios, se incluye la relación de usuarios con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos.
Esta lista se actualizará cada vez que un usuario reciba nuevos privilegios o cada vez que se dé de alta un nuevo usuario con acceso a datos de carácter personal.

GESTIÓN DE SOPORTES
Los soportes que contengan datos de carácter personal serán etiquetados permitiendo su identificación; del mismo modo serán inventariados y almacenados en las instalaciones dónde se ubican los sistemas de información y solo deberán ser accesibles por el personal autorizado para ello. No está permitido enviar ningún soporte fuera de la organización, sin antes cumplir con las siguientes directivas. La salida debe ser previamente autorizada y la información no podrá ser manipulada ni accesible por ningún medio. El procedimiento de autorización de salida de soportes fuera de INVERSIONES BARUTA 2002, S.L. está regulado en el procedimiento descrito en el siguiente apartado del presente informe.
En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte. Siempre que se vaya a desecharse cualquier documento o soporte que contengan datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

PROCEDIMIENTO PARA OBTENER LA AUTORIZACIÓN DE SALIDA DE SOPORTES FUERA DE LA ENTIDAD

La Dirección ha aprobado una relación de salidas habituales que han sido debidamente autorizadas.

Esta relación, que se incorpora como anexo Salidas de soportes autorizados. En el caso de necesitar una autorización para algún soporte que no figure a esta relación, tendrán que seguirse inexcusablemente los siguientes pasos:

Petición

Cumplimentación de una solicitud por parte del peticionario que deberá contar con autorización.

Aprobación

Se dará traslado a la Dirección que deberá dar la aprobación o denegación de la solicitud.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

OBLIGACIONES DEL PERSONAL

INVERSIONES BARUTA 2002, S.L. emitirá una Circular Interna dónde se establecerán las directrices para el tratamiento, por parte del personal, de los datos conocidos como consecuencia del desarrollo de su tarea dentro de la empresa.

En este Comunicado se recogerán las principales obligaciones en materia de seguridad sobre datos de carácter personal incluyendo la prohibición expresa de instalar cualquier tipo de aplicación en los equipos informáticos y la utilización de los recursos informáticos para otras finalidades diferentes de las estrictamente derivadas del desarrollo de su actividad laboral; así como la obligación de mantener el deber de secreto sobre todos los datos tratados con motivo del desarrollo de su puesto de trabajo y de no comunicar estos datos a ninguna persona o entidad sin la autorización pertinente.

Se incorporará al documento una copia del citado comunicado como Anexo Comunicado Interno sobre Protección de Datos de Carácter Personal.

COMUNICACIÓN AL PERSONAL

INVERSIONES BARUTA 2002, S.L. ha editado el Comunicado Interno mencionado en el apartado anterior y lo ha comunicado a todo el personal de la entidad.

PROCEDIMIENTOS DE COPIAS DE SEGURIDAD Y RECUPERACIÓN

Copias de Seguridad

EL SISTEMA realiza copias de seguridad de los datos de carácter personal DIARIAMENTE en DISCO DURO EXTERNO. EL SISTEMA almacena las copias EN LA OFICINA.

8.2. Procedimientos de recuperación

En el resto de situaciones que no supongan un riesgo para la disponibilidad de las aplicaciones, se tendrá que seguir inexcusablemente los siguientes pasos:

Cumplimentación de una solicitud por parte del peticionario que tendrá que contar con el beneplácito del Responsable de Seguridad.

Se procederá a trasladar el orden de recuperación al personal autorizado, enviando copia al solicitante indicando la aprobación o denegación.

Acto seguido, el Responsable de Seguridad anotará el hecho en el registro de incidencias.

Toda la documentación original será archivada por el Responsable de Seguridad.

Inventario de aplicaciones por entorno
En este anexo se recoge una relación exhaustiva de las aplicaciones existentes que tratan datos de carácter personal en cada uno de los diferentes equipos informáticos existentes.

FINALIDAD	NOMBRE APLICACIÓN
FACTURACIÓN Y GESTIÓN	OFFICE

Apéndice A

Usuarios del sistema

Con la intención de evitar efectuar modificaciones al Documento de Seguridad y para mantener su actualización, se describirá el procedimiento a seguir para la obtención de la relación de los usuarios con acceso autorizado a los sistemas; así como los derechos que tienen concedidos.

Este procedimiento se basa en la asignación del identificador de usuario que se compone del nombre del mismo usuario. En el caso de encontrar otro usuario con el mismo identificador se establecerán otras combinaciones aleatorias.

Para la contraseña de cada usuario se establecerá una aleatoria que podrá ser cambiada por el usuario cuando crea conveniente. Se debe tener en cuenta que en caso alguno la contraseña podrá ser utilizada por un plazo superior a 180 días, pasado el cual se deberá cambiar obligatoriamente.

Apéndice B
Relación de usuarios

IDENTIFICADOR	NOMBRE	DNI	APLICACIÓN

Apéndice C

Contratos de prestación de servicios

En el presente anexo se recoge una relación de los datos tratados por terceros como consecuencia de un contrato de prestación de servicios en el que INVERSIONES BARUTA 2002, S.L. es Responsable del Fichero. En la siguiente tabla se recoge esta información:

PRESTADOR DEL SERVICIO	DATOS FACILITADOS	FINALIDADES
MORENO ABOGADOS MARBELLA, S.L.	Datos empresa y personal	Asesoramiento laboral
CARLOS VIÑADO PÉREZ	Datos empresa, personal y clientes	Obligaciones tributarias
JOSÉ CARLOS MOLINA CERVÁN	Datos empresa y clientes	Mant. Web
SERVITEL MARBELLA, S.L.	Datos empresa y clientes	Videovigilancia
SERVICIO DE PREVENCIÓN ANTEA, S.A.	Datos empresa y personal	Prevención de Riesgos Laborales

Apéndice D

Tratamiento de datos en los portátiles

A continuación se relacionan los portátiles existentes en INVERSIONES BARUTA 2002, S.L..
En la columna autorización encontramos la firma del Responsable del fichero para el tratamiento de los datos fuera de los locales de ubicación del fichero, siempre que los portátiles salgan de la empresa y no se haya manifestado en otro documento.

TIPO PORTATIL
TERMINAL
UBICACIÓN
USUARIOS:

SALE DE LA EMPRESA

AUTORIZACIÓN

Apéndice E

Salidas de soportes autorizados

La Dirección de INVERSIONES BARUTA 2002, S.L. ha aprobado la relación de salidas periódicas de soportes que contienen datos de carácter personal que han sido autorizadas por la Entidad. A continuación se presenta la relación que será actualizada cada vez que se produzcan modificaciones al respecto.

DATOS ENVIADOS	DESTINATARIOS	PERIODICIDAD

Apéndice F

Gestión de usuarios

Alta de usuarios

Únicamente el Responsable del fichero tiene competencias para dar de alta los identificadores de usuarios y asociarlos a los perfiles definidos por los diferentes niveles de acceso a las aplicaciones y ficheros.

Los Responsables directos de los usuarios que tengan que dar de alta a uno nuevo al sistema o a las aplicaciones, lo tendrán que notificar al Responsable del fichero utilizando el modelo establecido al efecto indicando en la solicitud los derechos de acceso deseados. Será la Dirección de la empresa quien tenga la última decisión sobre los derechos de acceso de los usuarios.

Una vez realizada el alta, el Responsable del fichero la comunicará al nuevo usuario y al Responsable que autorizó la solicitud indicando los datos de éste y el identificador de usuario asignado.

Para el primer acceso del usuario al sistema, el Responsable del fichero le deberá comunicar de forma confidencial su identificador y su contraseña de acceso inicial, según las indicaciones en la norma sobre gestión de contraseñas. Se tendrán en cuenta las siguientes normas en la asignación de identificadores:

No se reutilizará nunca un identificador.

Utilizar al menos cuatro caracteres en la composición del identificador del usuario.

Se tienen que mantener únicamente aquellos nombres de usuario propios de los sistemas operativos y de las aplicaciones de software que no puedan ser modificadas.

Baja de un usuario

INVERSIONES BARUTA 2002, S.L. se encargará de cancelar el usuario y sus derechos de acceso. El Responsable del fichero almacenará información descriptiva sobre los perfiles de acceso de los usuarios que se den de baja durante el tiempo requerido para el cumplimiento de las obligaciones legales y por la auditoria.

Modificación de permisos de un usuario

La modificación de los derechos o permisos de acceso de un usuario requerirá de la misma autorización jerárquica, diferenciada para cada tipología de usuarios, ya descrita en el protocolo de alta. Por esto, el procedimiento enunciado en el apartado de alta será extensible a este punto de modificación de permisos.

Reactivación de usuarios

La reactivación de usuarios exige un procedimiento diferenciado respecto al resto de protocolos enunciados anteriormente puesto que parte de la premisa de la existencia de un alta previa no requiere un cambio de permisos del usuario en el sistema.

En aquellos casos en los que el acceso del usuario al sistema se haya revocado por causas accidentales, como el olvido de la contraseña, un periodo prolongado de inactividad o un excesivo número de intentos fallidos, la reactivación del usuario exigirá su comunicación al Responsable del fichero para resolver la situación.

Registros

El Responsable del fichero mantendrá actualizada la documentación en lo referente a perfiles de acceso e identificadores asociados por el usuario, altas, bajas, revocación y modificación de usuario por fechas.

Datos sobre usuarios:

Nombre y apellidos completos.

Empresa, en el caso de tratarse de personal externo.

Área, Departamento y servicio.

Cualquiera de estos datos se podrá utilizar en la localización de usuarios y en la reactivación de usuarios revocados, para su control, uso o modificación.

Apéndice G

Gestión de contraseñas

Generación

Cada usuario tiene un identificador que se autentifica mediante contraseña. Los identificadores de usuario y las contraseñas de acceso asociadas son de uso personal e intransferible y no pueden ser compartidas.

Privacidad

Las contraseñas tienen que ser conocidas exclusivamente por el usuario propietario de ésta y tratadas como información personal e intransferible. Es responsabilidad del usuario asegurar la confidencialidad y custodia de la contraseña.

INVERSIONES BARUTA 2002, S.L. ha establecido ciertas consideraciones en el momento de escoger una contraseña que deberá ser aplicada por todos los usuarios del sistema:

Se evitarán nombres comunes o cualquier otra combinación que pueda identificar al usuario, fecha de nacimiento, matrículas de vehículos, etc.

La contraseña contendrá un mínimo de cinco caracteres alfanuméricos.

Deberá cambiarse al menos una vez cada 180 días.

Los sistemas o aplicaciones de INVERSIONES BARUTA 2002, S.L. que realizan la autentificación del usuario, permiten la limitación del número de intentos fallidos para accesos de usuarios no autorizados.

Se evitará la comunicación escrita que revele la contraseña de cualquier usuario.

Almacenamiento
Las contraseñas se almacenarán cifradas y solo el Responsable del fichero tendrá acceso a su descodificación.
Mantenimiento
Todas las contraseñas tienen que ser modificadas por el usuario al menos con la frecuencia establecida en el apartado de periodicidad. En los entornos en los que sea posible se automatizará este requerimiento de caducidad. Cuando no sea posible, el usuario será responsable del cambio sistemático.
En caso de olvido o cualquier dificultad relacionada con contraseñas, los usuarios contarán con la asistencia del Responsable del fichero.
Distribución
La comunicación de contraseñas siempre se realizará por parte del Responsable del fichero al usuario, ya sea personalmente o vía telefónica.

Apéndice H
FICHEROS NO AUTOMATIZADOS
Por fichero no automatizado se entiende todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado, repartido de forma funcional o geográfica.
Por tanto entenderemos como fichero no automatizado de modo genérico todo documento en el que se encuentren datos de carácter personal en formato no informático. Entre otros, facturas, presupuestos, albaranes, contratos, currículum vitae, etc.

H.1.1. Criterios de Archivo
El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos.
En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban de seguirse para el archivo.
Los contratos, albaranes, presupuestos, facturas, currículum vitae o cualesquiera otros documentos que contengan datos de carácter personal se archivarán en compartimentos cerrados con llave a los que sólo tenga acceso personal autorizado y que permitan a su vez su fácil y pronta recuperación para el caso en que se requiera.
H.1.2. Dispositivos de almacenamiento
Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizada.

Este documento contiene las cláusulas informativas que debe incluir en los formularios de solicitud de información, el documento a anexar en cada uno de los contratos de prestación de servicios, el registro de actividades de tratamiento y un anexo con recomendaciones sobre medidas de seguridad y tratamientos de datos personales (imágenes) captados por cámaras de videovigilancia, las cuales debe implantar en su organización.

TRATAMIENTO DE DATOS DE CLIENTES

Clausula informativa:

El texto que se muestra a continuación deberá incluirlo en todos aquellos formularios que utilice para recabar datos personales de sus clientes, tanto si se realiza en soporte papel como si los recoge a través de un formulario web:

Responsable: Identidad: D. ALFONSO GONZÁLEZ BUENO con NIF 25077065G como representante legal de la empresa INVERSIONES BARUTA 2002, S.L. - CIF: B92332337 Dir. postal: POL. IND. NUEVA CAMPANA NAVE 90 29660 NUEVA ANDALUCÍA Teléfono: 952929811 Correo electrónico: ino@camuri.es

"En nombre de la empresa tratamos la información que nos facilita con el fin de prestarles el servicio solicitado, realizar la facturación del mismo. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener confirmación sobre si en INVERSIONES BARUTA 2002, S.L. estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios.

Asimismo solicito su autorización para ofrecerle productos y servicios relacionados con los solicitados y fidelizarle como cliente."

SI ☐

NO ☐

AVISO: Debe tener en cuenta que si su cliente marca la opción NO, en ningún caso podrá enviarle publicidad

TRATAMIENTO DE DATOS DE POTENCIALES CLIENTES

Clausula informativa:

El texto que se muestra a continuación deberá incluirlo en todos aquellos formularios que utilice para recabar datos personales de sus potenciales clientes, tanto si se realiza en soporte papel como si los recoge a través de un formulario web.

Responsable: Identidad: INVERSIONES BARUTA 2002, S.L. - CIF: B92332337 Dir. postal: POL. IND. NUEVA CAMPANA NAVE 90 29660 NUEVA ANDALUCÍA, Teléfono: 952929811, Correo electrónico: ino@camuri.es

"En nombre de la empresa tratamos la información que nos facilita con el fin de enviarle publicidad relacionada con nuestros productos y servicios por cualquier medio (postal, email o teléfono) e invitarle a eventos organizados por la empresa. Los datos proporcionados se conservarán mientras no solicite el cese de la actividad. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener confirmación sobre si en INVERSIONES BARUTA 2002, S.L. estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexacto o solicitar su supresión cuando los datos ya no sean necesarios para los fines que fueron recogidos"

AVISO: Si compra datos personales a terceros para realizar publicidad de sus productos y servicios, debe tener en cuenta que los mismos proceden de fuentes accesibles al público y que están contrastados con la lista Robinson.

AVISO: Recuerde que debe borrar los datos cuando haya trascurrido un tiempo sin hacer uso de los mismos.

TRATAMIENTO DE DATOS DE CANDIDATOS

Clausula informativa:

El texto que se muestra a continuación deberá incluirlo en todos aquellos formularios que utilice para recabar datos personales de los candidatos a un puesto de trabajo, tanto si se realiza en soporte papel como si los recoge a través de un formulario web:

Responsable: Identidad: INVERSIONES BARUTA 2002, S.L. - CIF: B92332337 Dir. postal: POL. IND. NUEVA CAMPANA NAVE 90 29660 NUEVA ANDALUCÍA, Teléfono: 952929811, Correo electrónico: ino@camuri.es

"En nombre de la empresa tratamos la información que nos facilita con el fin de mantenerle informado de las distintas vacantes a un puesto de trabajo que se produzcan en nuestra organización. Los datos proporcionados se conservarán hasta la adjudicación de un puesto de trabajo o hasta que usted ejerza su derecho de cancelación por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios. Los datos no se cederán a terceros."

Si los candidatos aportan su CV en papel normal, sin formulario, se les pedirá que firmen un formulario fechado en que figure al información antes citada.

TRATAMIENTO DE DATOS DE PROVEEDORES

Clausula informativa:

El texto que se muestra a continuación deberá incluirlo en todos aquellos formularios que utilice para recabar datos personales de los proveedores como por ejemplo en facturas:

Responsable: Identidad: INVERSIONES BARUTA 2002, S.L. - CIF: B92332337 Dir. postal: POL. IND. NUEVA CAMPANA NAVE 90 29660 NUEVA ANDALUCÍA, Teléfono: 952929811, Correo electrónico: ino@camuri.es

"En nombre de la empresa tratamos la información que nos facilita con el fin de realizar pedido y facturar los servicios. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener confirmación sobre si en INVERSIONES BARUTA 2002, S.L. estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios."

Si los proveedores aportan sus datos mediante otro sistema, se les pedirá que firmen un formulario fechado en que figure la información antes citada.

CORREO ELECTRÓNICO

Responsable: INVERSIONES BARUTA 2002, S.L. **CIF:** B92332337

Le informamos que sus datos identificativos y los contenidos en los correos electrónicos y ficheros adjuntos pueden ser incorporados a nuestras bases de datos con la finalidad de mantener relaciones profesionales y/o comerciales y, que serán conservados mientras se mantenga la relación. Si lo desea, puede ejercer su derecho a acceder, rectificar y suprimir sus datos y demás reconocidos normativamente dirigiéndose al correo emisor o en los datos del responsable.

Este mensaje y cualquier documento que lleve adjunto, en su caso, puede ser confidencial y destinado únicamente a la persona o entidad a quien ha sido enviado.

CLÁUSULA FACTURAS

Responsable: INVERSIONES BARUTA 2002, S.L. **CIF:** B92332337

Los datos personales tratados para gestionar la relación contractual y, en su caso, remitirle información comercial por medios electrónicos, se conservarán hasta el fin de la relación, baja comercial o los plazos de retención legales. Puede ejercer sus derechos en la dirección indicada del responsable o en ino@camuri.es.

INFORMACIÓN SOBRE PROTECCIÓN DE DATOS CLIENTES

A. RESPONSABLE:

- INVERSIONES BARUTA 2002, S.L. CIF: B92332337
- POL. IND. NUEVA CAMPANA NAVE 90 29660 NUEVA ANDALUCÍA
- ino@camuri.es

B. FINALIDADES:

- Prestar el servicio contratado y gestionar las tareas administrativas derivadas.
- Mantenerle informado de nuestros productos y servicios por medios electrónicos.

C. LEGITIMACIÓN:

- Ejecución de contrato de prestación de servicios.
- Interés legítimo en mantenerle informado de nuestros productos y servicios como cliente.

D. DESTINATARIO:

- Cesiones necesarias para la prestación del servicio (entidades bancarias y Administración Pública).
- Cesiones legalmente previstas.

E. CONSERVACIÓN:

- Durante la relación contractual.
- Solicitud de baja comercial.
- Durante los plazos exigidos por ley para atender eventuales responsabilidades, finalizada la relación.

F. DERECHOS:

- Tiene derecho a:
  - Solicitar el acceso, rectificación, supresión, y/o portabilidad de sus datos.
  - Solicitar la oposición y/o limitación de su tratamiento.
- Dónde y cómo solicitarlos: Mediante un escrito dirigiéndose a los datos de responsable, indicando el tratamiento concreto y el derecho que quiere ejercitar.
- En caso de divergencias en relación con el tratamiento de sus datos, puede presentar una reclamación ante la Agencia de Protección de Datos (www.agpd.es).

□ **NO DESEO RECIBIR INFORMACIONES COMERCIALES**

Fecha

Nombre y Apellidos

Fdo.

AVISO LEGAL

Esta página Web es propiedad de INVERSIONES BARUTA 2002, S.L. con CIF B92332337 y domicilio en POL. IND. NUEVA CAMPANA NAVE 90 NUEVA ANDALUCÍA 29660 e Inscrita en el Registro Mercantil de …….. con los siguientes datos en el tomo….., libro ……., folio ……, hoja……, inscripción…..

Para cualquier consulta o propuesta, contáctenos en el e-mail: ino@camuri.es

Esta página Web se rige por la normativa exclusivamente aplicable en España, quedando sometida a ella, tanto nacionales como extranjeros que utilicen esta Web.

El acceso a nuestra página Web por parte del USUARIO es gratuito y está condicionado a la previa lectura y aceptación integra, expresa y sin reservas de las presentes CONDICIONES GENERALES DE USO vigentes en el momento del acceso, que rogamos lea detenidamente. El USUARIO en el momento que utiliza nuestro portal, sus contenidos o servicios, acepta y se somete expresamente a las condiciones generales de uso del mismo. Si el usuario no estuviere de acuerdo con las presentes condiciones de uso, deberá abstenerse de utilizar este portal y operar por medio del mismo.

En cualquier momento podremos modificar la presentación y configuración de nuestra Web, ampliar o reducir servicios, e incluso suprimirla de la Red, así como los servicios y contenidos prestados, todo ello de forma unilateral y sin previo aviso.

A. PROPIEDAD INTELECTUAL

Todos los contenidos, textos, imágenes, marcas y códigos fuente son de nuestra propiedad o de terceros a los que se han adquirido sus derechos de explotación, y están protegidos por los derechos de Propiedad Intelectual e Industrial.

El usuario únicamente tiene derecho a un uso privado de los mismos, sin ánimo de lucro, y necesita autorización expresa para modificarlos, reproducirlos, explotarlos, distribuirlos o ejercer cualquier derecho perteneciente a su titular.

B. CONDICIONES DE ACCESO

El acceso a nuestra página Web es gratuito y no exige previa suscripción o registro.

El envío de datos personales implica la aceptación expresa por parte del USUARIO de nuestra política de privacidad.

El usuario debe acceder a nuestra página Web conforme a la buena fe, las normas de orden público y a las presentes Condiciones Generales de uso. El acceso a nuestro sitio Web se realiza bajo la propia y exclusiva responsabilidad del usuario, que responderá en todo caso de los daños y perjuicios que pueda causar a terceros o a nosotros mismos.

Teniendo en cuenta la imposibilidad de control respecto a la información, contenidos y servicios que contengan otras páginas web a los que se pueda acceder a través de los enlaces que nuestra página web pueda poner a su disposición, le comunicamos que quedamos eximidos de cualquier responsabilidad por los daños y perjuicios de toda clase que pudiesen derivar por la utilización de esas páginas web, ajenas a nuestra empresa, por parte del usuario.

C. POLÍTICA DE PRIVACIDAD

La confidencialidad y la seguridad son valores primordiales de INVERSIONES BARUTA 2002, S.L. y, en consecuencia, asumimos el compromiso de garantizar la privacidad del Usuario en todo momento y de no recabar información innecesaria. A continuación, le proporcionamos toda la información necesaria sobre nuestra Política de Privacidad en relación con los datos personales que recabamos, explicándole:

- Quién es el responsable del tratamiento de sus datos.
- Para qué finalidades recabamos los datos que le solicitamos.
- Cuál es la legitimación para su tratamiento.
- Durante cuánto tiempo los conservamos.
- A qué destinatarios se comunican sus datos.
- Cuáles son sus derechos.

RESPONSABLE: ver datos en el encabezamiento.

2. FINALIDADES, LEGITIMACIÓN Y CONSERVACIÓN y conservación de los tratamientos de los datos enviados a través de:

- Formulario de Contacto.

  Finalidad: Facilitarle un medio para que pueda ponerse en contacto con nosotros y contestar a sus solicitudes de información, así como enviarle comunicaciones de nuestros productos, servicios y actividades, inclusive por medios electrónicos (correo electrónico), si marca la casilla de aceptación.

  Legitimación: El consentimiento del usuario al solicitarnos información a través de nuestro formulario de contactos y al marcar la casilla de aceptación de envío de información.

  Conservación: Una vez resuelta su solicitud por medio de nuestro formulario o contestada por correo electrónico, si no ha generado un nuevo tratamiento, y en caso de haber aceptado recibir envíos comerciales, hasta que solicite la baja de los mismos.

- Envío de correos electrónicos.

  Finalidad: Contestar a sus solicitudes de información, atender sus peticiones y responder sus consultas o dudas. En caso de recibir su Currículum Vitae, sus datos personales y curriculares podrán formar parte de nuestras bases de datos para participar en nuestros procesos de selección presentes y futuros.

  Legitimación: El consentimiento del usuario al solicitarnos información a través de la dirección de correo electrónico o enviarnos sus datos y CV para participar en nuestros procesos de selección.

  Conservación: Una vez resulta contestada su petición por correo electrónico, si no ha generado un nuevo tratamiento. En el caso de recibir su CV, sus datos podrán ser conservados durante un año máximo para futuros procesos de selección.

Obligación de facilitarnos sus datos personales y consecuencias de no hacerlo.

El suministro de datos personales requiere una edad mínima de 14 años, o en su caso, disponer de capacidad jurídica suficiente para contratar.

Los datos personales solicitados son necesarios para gestionar sus solicitudes, darle de alta como usuario y/o prestarle los servicios que pueda contratar, por lo que, si no nos los facilita, no podremos atenderle correctamente ni prestarle el servicio que ha solicitado.

En todo caso, nos reservamos el derecho de decidir sobre la incorporación o no de sus datos personales y demás información a nuestras bases de datos.

3. DESTINATARIOS DE SUS DATOS.

Sus datos son confidenciales y no se cederán a terceros, salvo que exista obligación legal.

4. DERECHOS EN RELACIÓN CON SUS DATOS PERSONALES.

Cualquier persona puede retirar su consentimiento en cualquier momento, cuando el mismo se haya otorgado para el tratamiento de sus datos. En ningún caso, la retirada de este consentimiento condiciona la ejecución del contrato de suscripción o las relaciones generadas con anterioridad.

Igualmente, puede ejercer los siguientes derechos:

- Solicitar el acceso a sus datos personales o su rectificación cuando sean inexactos.
- Solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.
- Solicitar la limitación de su tratamiento en determinadas circunstancias.
- Solicitar la oposición al tratamiento de sus datos por motivos relacionados con su situación particular.
- Solicitar la portabilidad de los datos en los casos previstos en la normativa.
- Otros derechos reconocidos en las normativas aplicables.

Dónde y cómo solicitar sus Derechos: Mediante un escrito dirigido al responsable a su dirección postal o electrónica (indicadas en el apartado A), indicando la referencia "Datos Personales", especificando el derecho que se quiere ejercer y respecto a qué datos personales.

En caso de divergencias con la empresa en relación con el tratamiento de sus datos, puede presentar una reclamación ante la Agencia de Protección de Datos (www.agpd.es).

5. SEGURIDAD DE SUS DATOS PERSONALES

Con el objetivo de salvaguardar la seguridad de sus datos personales, le informamos que hemos adoptado todas las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos personales suministrados de su alteración, pérdida y tratamientos o accesos no autorizados.

6. ACTUALIZACIÓN DE SUS DATOS

Es importante que para que podamos mantener sus datos personales actualizados, nos informe siempre que haya habido alguna modificación en ellos, en caso contrario, no respondemos de la veracidad de los mismos.

No nos hacemos responsables de la política de privacidad respecto a los datos personales que pueda facilitar a terceros por medio de los enlaces disponibles en nuestra página web.

La presente Política de Privacidad puede ser modificada para adaptarlas a los cambios que se produzca en nuestra web, así como modificaciones legislativas o jurisprudenciales sobre datos personales que vayan apareciendo, por lo que exige su lectura, cada vez que nos facilite sus datos a través de esta Web.

D. RESPONSABILIDADES

Al poner a disposición del usuario esta página Web queremos ofrecerle un servicio de calidad, utilizando la máxima diligencia en la prestación del mismo, así como en los medios tecnológicos utilizados. No obstante, no responderemos de la presencia de virus y otros elementos que de algún modo puedan dañar el sistema informático del usuario.

No garantizamos que la disponibilidad del servicio sea continua e ininterrumpida.

El USUARIO tiene prohibido cualquier tipo de acción sobre nuestro portal que origine una excesiva sobrecarga de funcionamiento a nuestros sistemas informáticos, así como la introducción de virus, o instalación de robots, o software que altere el normal funcionamiento de nuestra web, o en definitiva pueda causar daños a nuestros sistemas informáticos.

El USUARIO asume toda la responsabilidad derivada del uso de nuestra página web.

El USUARIO reconoce que ha entendido toda la información respecto a las condiciones de uso de nuestro portal, y reconoce que son suficientes para la exclusión del error en las mismas, y por lo tanto, las acepta integra y expresamente.

FORMULARIO DE CONTACTO

INFORMACIÓN PROTECCIÓN DE DATOS DE INVERSIONES BARUTA 2002, S.L.

Finalidades: Responder a sus solicitudes y remitirle información comercial de nuestros productos y servicios, incluso por correo electrónico. **Legitimación:** Consentimiento del interesado. **Destinatarios:** No están previstas cesiones de datos. **Derechos:** Puede retirar su consentimiento en cualquier momento, así como acceder, rectificar, suprimir sus datos y demás derechos en ino@camuri.es.

□ Acepto recibir información comercial, incluso por correo electrónico.

□ He leído y acepto la Política de Privacidad.

RESPONSABLE: **INVERSIONES BARUTA 2002, S.L.**
POL. IND. NUEVA CAMPANA NAVE 90
29660 NUEVA ANDALUCÍA

FINALIDAD: **Utilización de sistemas de videovigilancia**

LEGITIMACIÓN: Seguridad de las instalaciones

DESTINATARIOS: Fuerzas de seguridad del Estado

DERECHOS:

- **Puede solicitar el acceso, rectificación, supresión, oposición y la limitación de su tratamiento al responsable**
- **En caso de divergencias, puede dirigirse a la Agencia de Protección de Datos: www.agpd.es**

CONSENTIMIENTO EMPLEADOS

A. RESPONSABLE:

INVERSIONES BARUTA 2002, S.L.

POL. IND. NUEVA CAMPANA NAVE 90 29660 NUEVA ANDALUCÍA

ino@camuri.es

B. FINALIDADES:

- Gestión de la relación laboral con el trabajador y el pago de nóminas.

- Prevención de riesgos laborales.

- Formación.

- Evaluación, seguimiento y control del desarrollo de las actividades profesionales.

- Controles de acceso y presenciales.

C. LEGITIMACIÓN:

- Convenio Colectivo y Estatuto de los Trabajadores (Real Decreto Legislativo 2/2015, de 23 de octubre)

- Ejecución de contrato laboral.

D. DESTINATARIOS:

- Administraciones Públicas y entidades bancarias para la gestión laboral y el pago de nóminas.

- Mutuas laborales y empresas de prevención de riesgos laborales.

- Aquellas entidades, clientes y proveedores ante las cuales sea necesario identificar a los empleados, inclusive, en su caso, para temas de coordinación empresarial (Cto., TC's, ...).

- Empresas de formación y tramitación de bonificaciones ante la Fundación Estatal para el Empleo.

E. CONSERVACIÓN DE LOS DATOS:

- Serán conservados durante la vigencia del contrato laboral y, finalizada este, los datos laborales se conservarán bloqueados durante los plazos exigidos legalmente para atender eventuales responsabilidades.

- La empresa conservará, en base a un interés legítimo, el nombre y apellidos, puesto de trabajo y fechas como registro histórico de trabajadores con carácter indefinido.

F. DERECHOS:

- Todo trabajador tiene derecho a solicitar el acceso, rectificación, supresión, oposición, limitación y portabilidad de sus datos.

Dónde y cómo solicitarlos: Mediante un escrito dirigido a su responsable de recursos humanos indicando el tratamiento concreto y el derecho que quiere ejercitar.

En caso de divergencias con la empresa en relación con el tratamiento de sus datos, puede presentar una reclamación ante la Agencia de Protección de Datos (www.agpd.es).

Fecha

Nombre y Apellidos

Fdo. Trabajador

CIRCULAR SOBRE LAS FUNCIONES Y OBLIGACIONES QUE AFECTAN A

TODOS LOS EMPLEADOS/USUARIOS CON ACCESO A DATOS PERSONALES

El cumplimiento del Reglamento General de Protección de Datos 2016/679, implica que todo el personal y demás usuarios con acceso a datos personales conozca las normas de seguridad que afecten al desarrollo de sus funciones.

En este documento, se recogen las principales funciones y obligaciones en materia de seguridad sobre los datos personales que debe acatar cualquier usuario de la empresa que acceda a los mismos.

Obligaciones comunes que afectan al personal

1. **Confidencialidad**	Todo el personal y demás usuarios están obligados al secreto profesional, inclusive finalizada la relación laboral o con la entidad. La confidencialidad es extensible a los datos personales, documentación, procedimientos técnicos, especificaciones, parámetros, procesos, programas, datos o información técnica, comercial o financiera que tenga este carácter confidencial.
2. **Acceso a datos personales**	Solamente se podrá acceder a los datos de carácter personal a los que se esté autorizado y, exclusivamente para el desarrollo de sus funciones laborales, quedando expresamente prohibido su uso para fines privados.
3. **Medidas de seguridad**	Todo usuario está obligado a adoptar las medidas de seguridad que la empresa le indique.
4. **Cesión de datos**	Está absolutamente prohibida la comunicación de datos personales a terceros no autorizados, externos o internos a la entidad, excepto en los casos legalmente previstos, y en aquellos supuestos que sea necesario para el desarrollo de la actividad laboral.
5. **Uso de periféricos**	En el uso de impresoras, fotocopiadoras, escáner y fax, se deberá tener la precaución de que en la bandeja de salida no quede ningún documento que contenga datos personales. La documentación de las bandejas de salida que no le pertenezca, es confidencial.
6. **Puestos de trabajo**	Los usuarios son responsables de su puesto de trabajo y, deberán garantizar, en la medida de lo posible, que ninguna otra persona no autorizada pueda ver la información sobre datos personales que muestran sus equipos informáticos o documentación en soporte papel.
7. **Derechos de los ciudadanos**	Todo el personal está obligado a atender los derechos solicitados por terceros (acceso, rectificación, cancelación, oposición, limitación y portabilidad) y, a ponerlo en conocimiento de su responsable inmediatamente.

8. **Incidencias de seguridad**	Cualquier incidencia que afecte a la seguridad de los datos deberá ser comunicada a su responsable. Su conocimiento y no comunicación puede ser considerada como una falta contra la seguridad de los datos personales por parte del usuario.
9. **Dudas seguridad**	Cualquier duda con relación a la confidencialidad y seguridad en el tratamiento de datos personales se debe poner en conocimiento de sus responsables.

Funciones y Obligaciones del personal con acceso informático

10. **Contraseñas**	Todos los usuarios de los sistemas informáticos deberán cumplir con la política de identificación (nombres de usuario y contraseñas), indicada por su organización. En caso de elección libre de la contraseña por parte del usuario, queda absolutamente prohibida la utilización de contraseñas fácilmente identificables.
11. **Confidencialidad contraseñas**	Cada usuario es responsable de la confidencialidad y salvaguarda de su propia contraseña, que no podrá ser comunicada a terceros ajenos o no a la entidad, salvo autorización expresa de la empresa.
12. **Uso sistemas informáticos**	Está prohibido el uso de los sistemas informáticos para fines privados, salvo autorización de sus responsables.
13. **Sistemas informáticos**	Los terminales y sistemas informáticos solo podrán ser modificados o manipulados por el personal expresamente autorizado. Está prohibido instalar programas informáticos sin la autorización previa de la empresa.
14. **Almacenamiento de información**	Los usuarios deberán guardar la información y documentos generados en el servidor de la empresa y, salvo autorización expresa o que no se disponga de servidores, no se podrán utilizar los discos duros locales de los ordenadores para el tratamiento de datos personales.
15. **Puesto de trabajo**	Cuando se abandone el puesto de trabajo, ya sea temporalmente o por terminar su jornada laboral, deberá apagar o bloquear su ordenador.
16. **Uso de soportes informáticos**	Salvo autorización expresa, está prohibido la realización de copias de datos personales, en cualquier tipo de soporte informático (DVD, cintas, Pen Drives, discos duros externos, u otros).

17. **Uso de dispositivos portátiles**	El uso externo de ordenadores portátiles, Smartphones, tabletas o similares que contengan datos personales titularidad de su empresa, requerirá la autorización de sus responsables.
18. **Accesos remotos o teletrabajo**	Todas las medidas descritas serán igualmente aplicables cuando el acceso se produzca en la modalidad de acceso remoto, fuera del centro de trabajo.
19. **Almacenamiento en la nube (Cloud)**	Está prohibido la utilización se sistemas de almacenamiento en la nube (Dropbox, Google Drive…), plataformas de envíos de correos electrónicos (Mailchimp…), cuentas de correo electrónico no corporativas (Gmail, Hotmail...) o el uso de cualquier software que no se aloje en el servidor u ordenador de la empresa, sin disponer previamente de la autorización expresa y por escrito de la empresa.

Funciones y Obligaciones del personal por medio de soporte papel

20. **Custodia y archivo**	La documentación debe ser custodiada y archivada de manera que no sea accesible por personas no autorizadas, tanto externas como de la propia organización, y procurando no dejar documentación encima de las mesas, sobre todo cuando el trabajador se encuentre ausente de su lugar de trabajo.
21. **Destrucción de documentación**	No está permitido tirar documentos y papeles que contengan datos personales sin adoptar las medidas necesarias que impidan su posterior visualización, inclusive en las cajas de reciclaje que pueda habilitar la empresa.
22. **Reutilización de documentación**	No se podrá reutilizar la documentación que contenga datos personales.
23. **Salida de documentación**	Queda totalmente prohibido extraer documentación que contenga datos personales de las instalaciones de la entidad sin la debida autorización.

Obligaciones que afectan al uso de los sistemas informáticos, correo electrónico e Internet

24. **Uso de Sistemas informáti-cos**	Los sistemas informáticos son puestos a disposición del usuario para el desarrollo de sus obligaciones laborales exclusivamente, y deben ser utilizados de forma adecuada.
25. **Uso del correo electrónico**	El uso del correo electrónico es estrictamente profesional, no permitiéndose ningún uso personal de los recursos técnicos e informáticos facilitados por la entidad, excepto en aquellos casos en los que se cuente con el consentimiento expreso del responsable encargado de la seguridad de la información.
26. **Normas de uso del correo electrónico**	El uso del correo electrónico se debe realizar tomando las debidas precauciones que impidan el envío a destinatarios erróneos, no abriendo enlaces de cuyo origen no estemos seguros y utilizando los sistemas de copia oculta (CCO) cuando se envíe el correo a varios destinatarios no relacionados entre sí. Está prohibido almacenar o guardar correos electrónicos privados o de contenido personal en los gestores de correo de la entidad.
27. **Acceso a Inter-net**	El acceso a Internet mediante el uso de los equipos informáticos facilitados se limitará a temas estrictamente laborales. En concreto, el acceso a Internet queda prohibido, salvo autorización expresa del responsable de la entidad para acceso a Chats, páginas de intercambio de datos (música, juegos, etc.), redes sociales (Facebook, Twitter, etc.) y descargarse programas sin consentimiento.
28. **Controles de la empresa**	El correo electrónico e Internet pueden ser controlados por la empresa, de manera que se informa que los correos electrónicos podrán ser consultados por el responsable con fines profesionales (vacaciones, bajas, suplencias de los trabajadores, finalización de contrato laboral, …) y al objeto de controlar el buen uso de los recursos proporcionados, la comisión de actos ilícitos, así como el control técnico en el envío de correos electrónicos a través de la red de la entidad de determinado volumen.

Fdo.

Nombre y Apellidos
Fecha

El incumplimiento de cualquiera de las obligaciones que afectan a los usuarios comportará las consecuencias jurídicas y/o laborales que pudieran derivarse frente a su empresa/organización, así como frente a cualquier tercero afectado como consecuencia del incumplimiento.

En a de de

CONTRATO DE PRESTACIÓN DE SERVICIOS ASESORÍA FISCAL

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a CARLOS VIÑADO PÉREZ, con dirección en JARDINES SIERRA BLANCA B1 BH 29602 MARBELLA y CIF 25381858R como encargado del tratamiento para tratar por cuenta de INVERSIONES BARUTA 2002, S.L., en calidad de responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio que en adelante se especifica.

El tratamiento consistirá en ASESORÍA FISCAL

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad INVERSIONES BARUTA 2002, S.L. como responsable del tratamiento, pone a disposición de la entidad CARLOS VIÑADO PÉREZ, los datos de identificación y bancarios de sus clientes.

3. Duración

El presente acuerdo tiene una duración de , siendo renovado automáticamente salvo decisión en contra por alguna de las partes. Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable o trasmitir a otro encargado que designe el responsable los datos personales, y suprimir cualquier copia que esté en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

4. Obligaciones del encargado del tratamiento

El encargado del tratamiento y todo su personal se obliga a:

- ✓ Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- ✓ Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.
- ✓ Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:
  1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado.
  2. Las categorías de tratamientos efectuados por cuenta de cada responsable.
  3. Una descripción general de las medidas técnicas y organizativas de seguridad apropiadas que esté aplicando.
- ✓ No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. Si el encargado quiere subcontratar tiene que informar al responsable y solicitar su autorización previa.
- ✓ Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.
- ✓ Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las me-

didas de seguridad correspondientes, de las que hay que informarles convenientemente.

- ✓ Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
- ✓ Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- ✓ Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento y portabilidad de datos ante la gestoría, ésta debe comunicarlo por correo electrónico a la dirección que indique el responsable. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.
- ✓ Notificación de violaciones de la seguridad de los datos

  El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida y a través de la dirección de correo electrónico que le indique el responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

  Se facilitará, como mínimo, la información siguiente:

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

  b) Datos de la persona de contacto para obtener más información.

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

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

  CARLOS VIÑADO PÉREZ, a petición del responsable, comunicará en el menor tiempo posible esas violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

  La comunicación debe realizarse en un lenguaje claro y sencillo y deberá incluir los elementos que en cada caso señale el responsable, como mínimo:

  a) La naturaleza de la violación de datos.

  b) Datos del punto de contacto del responsable o del encargado donde se pueda obtener 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.

- ✓ Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
- ✓ Implantar las medidas de seguridad técnicas y organizativas necesarias para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- ✓ Destino de los datos

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

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

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

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a) Entregar al encargado los datos necesarios para que pueda prestar el servicio.

b) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

c) Supervisar el tratamiento.

Responsable del fichero Encargado del tratamiento

En a de de

CONTRATO DE PRESTACIÓN DE SERVICIOS ASESORÍA LABORAL

1. Objeto del encargo del tratamiento
Mediante las presentes cláusulas se habilita a MORENO ABOGADOS MARBELLA, S.L., con dirección en AVDA. RICARDO SORIANO, 46 29601 MARBELLA y CIF B93232700 como encargado del tratamiento para tratar por cuenta de INVERSIONES BARUTA 2002, S.L., en calidad de responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio que en adelante se especifica.

El tratamiento consistirá en ASESORÍA LABORAL

2. Identificación de la información afectada
Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad INVERSIONES BARUTA 2002, S.L. como responsable del tratamiento, pone a disposición de la entidad MORENO ABOGADOS MARBELLA, S.L. los datos de identificación de sus empleados.

3. Duración
El presente acuerdo tiene una duración de , siendo renovado automáticamente salvo decisión en contra por alguna de las partes. Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable o trasmitir a otro encargado que designe el responsable los datos personales, y suprimir cualquier copia que esté en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

4. Obligaciones del encargado del tratamiento
El encargado del tratamiento y todo su personal se obliga a:

- ✓ Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- ✓ Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.
- ✓ Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:
  1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.
  2. Las categorías de tratamientos efectuados por cuenta del responsable.
  3. Una descripción general de las medidas técnicas y organizativas de seguridad apropiadas que esté aplicando.
- ✓ No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. Si el encargado quiere subcontratar tiene que informar al responsable y solicitar su autorización previa.
- ✓ Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.
- ✓ Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las me-

didas de seguridad correspondientes, de las que hay que informarles convenientemente.

- ✓ Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
- ✓ Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- ✓ Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento y portabilidad de datos ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección que indique el responsable. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.
- ✓ Notificación de violaciones de la seguridad de los datos

  El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida y a través de la dirección de correo electrónico que le indique el responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

  Se facilitará, como mínimo, la información siguiente:

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

  b) Datos de la persona de contacto para obtener más información.

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

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

  MORENO ABOGADOS MARBELLA, S.L., a petición del responsable, comunicará en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

  La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, incluir los elementos que en cada caso señale el responsable, como mínimo:

  a) La naturaleza de la violación de datos.

  b) Datos del punto de contacto del responsable o del encargado donde se pueda obtener más información.

  c) Describir las posibles consecuencias de la violación de la seguridad de los datos personales. Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

- ✓ Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
- ✓ Implantar las medidas de seguridad técnicas y organizativas necesarias para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- ✓ Destino de los datos

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

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

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

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a) Entregar al encargado los datos necesarios para que pueda prestar el servicio.

b) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

c) Supervisar el tratamiento.

Responsable del fichero Encargado del tratamiento

En a de de

CONTRATO DE PRESTACIÓN DE SERVICIOS MANTENIMIENTO WEB

1. Objeto del encargo del tratamiento
Mediante las presentes cláusulas se habilita a JOSÉ CARLOS MOLINA CERVÁN con dirección en FRANCISCA CARRILLO CASAUX URB. LA CONCHA F2 6 29602 MARBELLA y CIF 78971913X, como encargado del tratamiento, para tratar por cuenta de INVERSIONES BARUTA 2002, S.L., en calidad de responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio que en adelante se especifican**.**

El tratamiento consistirá en MANTENIMIENTO WEB.

2. Identificación de la información afectada
Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad INVERSIONES BARUTA 2002, S.L. como responsable del tratamiento, pone a disposición de la entidad JOSÉ CARLOS MOLINA CERVÁN la información disponible en los equipos informáticos que dan soporte a los tratamientos de datos realizados por el responsable.

3. Duración
El presente acuerdo tiene una duración de , renovable. Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable los datos personales, y suprimir cualquier copia que mantenga en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

4. Obligaciones del encargado del tratamiento
El encargado del tratamiento y todo su personal se obliga a:

- ✓ Utilizar los datos personales a los que tenga acceso sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- ✓ Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

  Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos, el encargado informará inmediatamente al responsable.
- ✓ No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.
- ✓ Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.
- ✓ Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.
- ✓ Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
- ✓ Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- ✓ Notificación de violaciones de la seguridad de los datos

  El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida y a través de la dirección de correo electrónico que le indique el responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

  Se facilitará, como mínimo, la información siguiente:

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

b) Datos de la persona de contacto para obtener más información.

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

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

- ✓ Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
- ✓ Auxiliar al responsable de tratamiento a implantar las medidas de seguridad necesarias para:

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

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

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

- ✓ Destino de los datos

El responsable del tratamiento no conservará datos de carácter personal relativos a los tratamientos del encargado salvo que sea estrictamente necesario para la prestación del servicio, y solo durante el tiempo estrictamente necesario para su prestación.

5. Obligaciones del responsable del tratamiento
Corresponde al responsable del tratamiento:

a) Facilitar al encargado el acceso a los equipos a fin de prestar el servicio contratado.

b) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

c) Supervisar el tratamiento.

Responsable del fichero Encargado del tratamiento

En a de de

CONTRATO DE PRESTACIÓN DE SERVICIOS PREVENCIÓN RIESGOS LABORALES

1. Objeto del encargo del tratamiento
Mediante las presentes cláusulas se habilita a SERVICIO DE PREVENCIÓN ANTEA, S.A. con dirección en CASTELAO, 4 ,29004 MALAGA Y CIF A91125559 como encargado del tratamiento, para tratar por cuenta de INVERSIONES BARUTA 2002, S.L., en calidad de responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio que en adelante se especifican**.**

El tratamiento consistirá en PREVENCIÓN DE RIESGOS LABORALES.

2. Identificación de la información afectada
Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad INVERSIONES BARUTA 2002, S.L. como responsable del tratamiento, pone a disposición de la entidad SERVICIO DE PREVENCIÓN ANTEA, S.A. la información disponible en los equipos informáticos que dan soporte a los tratamientos de datos realizados por el responsable.

3. Duración
El presente acuerdo tiene una duración de , renovable.

Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable los datos personales, y suprimir cualquier copia que mantenga en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

4. Obligaciones del encargado del tratamiento
El encargado del tratamiento y todo su personal se obliga a:

- ✓ Utilizar los datos personales a los que tenga acceso sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- ✓ Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

  Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos, el encargado informará inmediatamente al responsable.
- ✓ No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.
- ✓ Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.
- ✓ Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.
- ✓ Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
- ✓ Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- ✓ Notificación de violaciones de la seguridad de los datos

  El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida y a través de la dirección de correo electrónico que le indique el responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

  Se facilitará, como mínimo, la información siguiente:

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

b) Datos de la persona de contacto para obtener más información.

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

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

- ✓ Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
- ✓ Auxiliar al responsable de tratamiento a implantar las medidas de seguridad necesarias para:

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

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

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

- ✓ Destino de los datos

El responsable del tratamiento no conservará datos de carácter personal relativos a los tratamientos del encargado salvo que sea estrictamente necesario para la prestación del servicio, y solo durante el tiempo estrictamente necesario para su prestación.

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a) Facilitar al encargado el acceso a los equipos a fin de prestar el servicio contratado.

b) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

c) Supervisar el tratamiento.

Responsable del fichero Encargado del tratamiento

En a de de

CONTRATO DE PRESTACIÓN DE SERVICIOS DE VIDEOVIGILANCIA

1. Objeto del encargo del tratamiento
Mediante las presentes cláusulas se habilita a SERVITEL MARBELLA, S.L. con dirección en CALVARIO LOCAL 35 MARBELLA 29600 y CIF B92289446 como encargado del tratamiento, para tratar por cuenta de INVERSIONES BARUTA 2002, S.L., en calidad de responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio que en adelante se especifican**.**

El tratamiento consistirá en SERVICIOS VIDEOVIGILANCIA.

2. Identificación de la información afectada
Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad INVERSIONES BARUTA 2002, S.L. como responsable del tratamiento, pone a disposición de la entidad SERVITEL MARBELLA, S.L. la información disponible en los equipos informáticos que dan soporte a los tratamientos de datos realizados por el responsable.

3. Duración
El presente acuerdo tiene una duración de , renovable. Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable los datos personales, y suprimir cualquier copia que mantenga en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

4. Obligaciones del encargado del tratamiento
El encargado del tratamiento y todo su personal se obliga a:

- ✓ Utilizar los datos personales a los que tenga acceso sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- ✓ Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

  Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos, el encargado informará inmediatamente al responsable.
- ✓ No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.
- ✓ Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.
- ✓ Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.
- ✓ Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
- ✓ Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- ✓ Notificación de violaciones de la seguridad de los datos

  El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida y a través de la dirección de correo electrónico que le indique el responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

  Se facilitará, como mínimo, la información siguiente:

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

b) Datos de la persona de contacto para obtener más información.

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

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

- ✓ Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
- ✓ Auxiliar al responsable de tratamiento a implantar las medidas de seguridad necesarias para:

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

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

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

- ✓ Destino de los datos

El responsable del tratamiento no conservará datos de carácter personal relativos a los tratamientos del encargado salvo que sea estrictamente necesario para la prestación del servicio, y solo durante el tiempo estrictamente necesario para su prestación.

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a) Facilitar al encargado el acceso a los equipos a fin de prestar el servicio contratado.

b) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

c) Supervisar el tratamiento.

Responsable del fichero Encargado del tratamiento

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Tratamiento: **Clientes**

Finalidad del tratamiento

Gestión de la relación con los clientes

Descripción de las categorías de clientes y de las categorías de datos personales:

Clientes:

Personas con las que se mantiene una relación comercial como clientes

Categorías de datos personales:

Los necesarios para el mantenimiento de la relación comercial. Facturar

De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail

Datos bancarios: para la domiciliación de pagos

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:

Administración tributaria

Bancos y entidades financieras

Gestoría

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos:

Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades

Tratamiento: **Potenciales Clientes**

Finalidad del tratamiento

Gestión de la relación con los potenciales clientes

Descripción de las categorías de potenciales clientes y de las categorías de datos personales:

Potenciales clientes:

Personas con las que se busca mantener una relación comercial como clientes

Categorías de datos personales:

Los necesarios para la promoción comercial de la empresa

De identificación: nombre y apellidos y dirección postal, teléfonos, e-mail

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:

No se contempla

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos:

Un año desde el primer contacto

Tratamiento: **Empleados**

Finalidad del tratamiento

Gestión de la relación laboral con los empleados

Descripción de las categorías de empleados y de las categorías de datos personales:

Empleados:

Personas que trabajan para el responsable del tratamiento

Categorías de datos personales:

Los necesarios para el mantenimiento de la relación comercial.

De identificación: nombre, apellidos, número de Seguridad Social, dirección postal, teléfonos, e-mail

Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad y porcentaje de minusvalía

Datos bancarios, para la domiciliación del pago de las nóminas

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:

Gestoría laboral

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos:

Los previstos por la legislación fiscal y laboral respecto a la prescripción de responsabilidades

Tratamiento: **Candidatos**

Finalidad del tratamiento

Gestión de la relación con los candidatos a un empleo en la empresa

Descripción de las categorías de candidatos y de las categorías de datos personales:

Candidatos:

Personas que desean trabajar para el responsable del tratamiento

Categorías de datos personales:

Los necesarios para gestionar los curriculum de posibles futuros empleados

De identificación: nombre, apellidos, dirección postal, teléfonos, e-mail

Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad y otros excluyendo datos de raza, salud o afiliación sindical

Datos académicos

Datos profesionales

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:

No se contempla

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos:

Un año desde la presentación de la candidatura

Tratamiento: **Proveedores**

Finalidad del tratamiento

Gestión de la relación con los proveedores

Descripción de las categorías de proveedores y de las categorías de datos personales:

Proveedores:

Personas con las que se mantiene una relación comercial como proveedores de productos y/o servicios

Categorías de datos personales:

Los necesarios para el mantenimiento de la relación laboral

De identificación: nombre, NIF, dirección postal, teléfonos, e-mail

Datos bancarios: para la domiciliación de pagos

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos:

Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades

Tratamiento: **VideoVigilancia**

Finalidad del tratamiento

Seguridad de las personas y bienes

Descripción de las categorías de interesados y de las categorías de datos personales:

Interesados:

Personas que accedan o intenten acceder a las instalaciones

Categorías de datos personales:

Imágenes

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:

Administración tributaria

Cuerpos y fuerzas de seguridad del estado

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos:

Un mes desde su grabación

ANEXO MEDIDAS DE SEGURIDAD

INFORMACIÓN DE INTERÉS GENERAL

El artículo 5.1.f del Reglamento General de Protección de Datos (RGPD) determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, la destrucción o el daño accidental. Esto implica el establecimiento de medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales y la posibilidad (artículo 5.2) de demostrar que estas medidas se han llevado a la práctica (responsabilidad proactiva).

A tenor del tipo de tratamiento que ha puesto de manifiesto cuando ha cumplimentado este formulario, las medidas mínimas de seguridad mínimas que debería tener en cuenta son las siguientes:

MEDIDAS ORGANIZATIVAS

INFORMACIÓN QUE DEBERÁ SER CONOCIDA POR TODO EL PERSONAL CON ACCESO A DATOS PERSONALES

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de datos personales y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

- DEBER DE CONFIDENCIALIDAD Y SECRETO
    - Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
    - Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.
    - No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.
    - No se comunicarán datos personales o cualquier información personal a terceros, se prestará atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
    - El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

- DERECHOS DE LOS TITULARES DE LOS DATOS

  Se informará a todos los trabajadores acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) teniendo en cuenta lo siguiente:

  - Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión y oposición. El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida.

    Para el **derecho de acceso** se facilitará a los interesados la lista de los datos personales de que disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación, y la identidad del responsable ante el que pueden solicitar la rectificación supresión y oposición al tratamiento de los datos.

    Para el **derecho de rectificación** se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.

    Para el **derecho de supresión** se suprimirán los datos de los interesados cuando los interesados manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.

  El responsable del tratamiento deberá informar a todas las personas con acceso a los datos personales acerca de los términos de cumplimiento para atender los derechos de los interesados, la forma y el procedimiento en que se atenderán dichos derechos.

- VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL
  - Cuando se produzcan violaciones de seguridad DE DATOS DE CARÁCTER PERSONAL, como por ejemplo, el robo o acceso indebido a los datos personales se notificará a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es

- CAPTACIÓN DE IMÁGENES CON CÁMARAS Y FINALIDAD DE SEGURIDAD (VIDEOVIGILANCIA)
  - **UBICACIÓN DE LAS CÁMARAS**: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores.
  - **UBICACIÓN DE MONITORES**: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros.

- **CONSERVACIÓN DE IMÁGENES**: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.
- **DEBER DE INFORMACIÓN**: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto informativo. En la página web de la Agencia disponen de modelos, tanto del pictograma como del texto.
- **CONTROL LABORAL**: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representantes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.
- **DERECHO DE ACCESO A LAS IMÁGENES**: Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso.
  No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

Para más información puede consultar las guías de videovigilancia de la Agencia Española de Protección de Datos que se encuentran a su disposición en la sección de publicaciones de la web www.agpd.es.

MEDIDAS TÉCNICAS

IDENTIFICACIÓN

- Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.
- Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
- Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.
- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
- Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. Para la gestión de las contraseñas puede consultar la guía de privacidad y seguridad en internet de la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

DEBER DE SALVAGUARDA

A continuación se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

- **ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS**: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.
- **MALWARE**: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
- **CORTAFUEGOS O FIREWALL**: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.
- **CIFRADO DE DATOS**: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

- **COPIA DE SEGURIDAD**: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual. Considere que cualquier incidente de seguridad informática que le haya ocurrido a cualquier conocido le puede ocurrir a usted, y prevéngase contra el mismo.

En la Oficina de Seguridad del Internauta (https://www.osi.es) el Instituto Nacional de Ciberseguridad pone a su disposición información y herramientas informáticas gratuitas que pueden ser útiles para garantizar la seguridad de los datos personales en ordenadores y dispositivos electrónicos.

Si desea más información u orientaciones técnicas para garantizar la seguridad de los datos personales puede consultar la web www.incibe.es donde, entre otros documentos, podrá consultar el decálogo de ciberseguridad o el decálogo de buenas prácticas de seguridad en un departamento de informática donde encontrará los aspectos técnicos generales a tener en cuenta para la seguridad de la información de su empresa.