RIOS CONSULTORES S.L.

CLÁUSULAS DE PROTECCIÓN DE DATOS
Instrucciones de uso de la documentación

PERSONAL

POLÍTICA DE SEGURIDAD del personal

Protocolo de seguridad en relación a la protección de datos de carácter personal, para el conocimiento y cumplimiento de todo el personal de la misma.
Este documento debe estar al alcance de todo el personal, tanto si tiene permiso de acceso a datos personales como si no, ya que establece los mecanismos de seguridad implantados en la empresa con el fin de proteger los datos personales.

Acuerdo de TELETRABAJO

Acuerdo de teletrabajo. Incluye los deberes del teletrabajador en materia de protección de datos y la política de seguridad del personal para el tratamiento de datos personales.

POLÍTICA de protección de datos en situaciones de TELETRABAJO

Protocolo de protección de datos para situaciones de movilidad y teletrabajo, que incluye las medidas adoptadas por la organización y las que deberá adoptar el personal en situaciones de teletrabajo.
Las situaciones de teletrabajo que pueden darse como parte de la estrategia de gestión para determinadas áreas o actividades (por ejemplo, personal que viaja con frecuencia) o pueden ser motivadas por situaciones excepcionales e incluso de fuerza mayor.
Estas medidas irán encaminadas a conseguir la resiliencia permanente de los sistemas y servicios de tratamiento, la continuidad de los procesos de negocio y los derechos y libertades de los interesados cuyos datos se están tratando.

Consentimiento para utilizar dispositivos personales para TELETRABAJO

Consentimiento para utilizar los dispositivos personales del interesado (ADSL, teléfono móvil, tablet, ordenador, impresora, etc.) para tener acceso a los recursos de la empresa tales como correos electrónicos, bases de datos y archivos en servidores así como datos y aplicaciones personales, mediante teletrabajo.

Anexo de acta ENTREGA DE EQUIPOS INFORMÁTICOS Y/O DIGITALES

Documento de registro de entrega y devolución de equipos informáticos y/o digitales asignados al personal de la organización.

TRATAMIENTO

Consentimiento explícito (COMERCIAL)

Esta cláusula se deberá presentar ANTES de la RECOGIDA de cualquier DATO PERSONAL de nuestros nuevos clientes, ya que se trata de pedir su consentimiento expreso y autorización para el tratamiento de sus datos personales.

Circular informativa del tratamiento (COMERCIAL)

En el caso de recoger datos personales de FORMA VERBAL, la presente circular deberá SITUARSE en un LUGAR VISIBLE de las instalaciones de la empresa (GARITA, RECEPCIÓN, TABLÓN DE ANUNCIOS, OFICINAS, ATENCIÓN AL PÚBLICO, MOSTRADORES, etc.).

Deber de información en DOCUMENTOS CON DATOS PERSONALES

INCLUIR dicha cláusula en la documentación utilizada para RECOGER DATOS PERSONALES de los interesados, como p. ej., CUESTIONARIOS, ENTREVISTAS o FORMULARIOS, y en documentos de comunicación periódica, como pueden ser, PRESUPUESTOS, FACTURAS, RECIBOS, FAX, etc.
La finalidad es orientativa, la empresa deberá adaptarla.

Circular informativa del tratamiento (CURRÍCULUM) a la recepción IN SITU o por E-MAIL

El presente acuse deberá entregarse, manualmente o por e-mail, en el MOMENTO de la RECEPCIÓN de un CV.

IMÁGENES

Logo informativo VIDEOVIGILANCIA

La presente documentación es obligatoria conforme a lo dispuesto por la Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. También se deberá disponer de la circular informativa a petición de los interesados que la soliciten.
El logo de zona videovigilada deberá ubicarse en un lugar previo a la cámara y suficientemente visible de las instalaciones de la empresa.
Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores.

Circular informativa de VIDEOVIGILANCIA

Esta circular debe estar a disposición de los interesados que la soliciten.
La presente documentación es obligatoria conforme a lo dispuesto por la Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. También se deberá disponer del logo informativo en un lugar previo a la cámara y suficientemente visible de las instalaciones de la empresa.

OTROS FINES

CERTIFICADO de cumplimiento GDPR y LOPDGDD (empresas)

Declaración de cumplimiento de la normativa vigente de Protección de Datos, indicando el cumplimiento de las medidas de seguridad

CERTIFICADO de cumplimiento GDPR y LOPDGDD (profesionales)

Declaración de cumplimiento de la normativa vigente de Protección de Datos, indicando el cumplimiento de las medidas de seguridad

RIOS CONSULTORES S.L.
JUAN PORRAS, 7 - 29003 MALAGA (Málaga)

PERSONAL

RIOS CONSULTORES S.L.
JUAN PORRAS, 7 - 29003 MALAGA (Málaga)

POLÍTICA DE SEGURIDAD del personal

POLÍTICA DE SEGURIDAD DEL PERSONAL PARA EL TRATAMIENTO DE DATOS PERSONALES

1.- ÁMBITO DE APLICACIÓN

El Responsable del tratamiento está comprometido en implantar una cultura de privacidad en la organización, por lo que necesita que las personas autorizadas a tratar datos personales estén informadas del tratamiento de datos y se responsabilicen del mismo.

A toda persona autorizada para tratar datos personales se le exige que lea, comprenda, cumpla y haga cumplir esta Política de seguridad para proteger los datos que forman parte del tratamiento que se le ha encomendado.

Esta Política de seguridad establece las obligaciones y procedimientos que tiene que seguir el personal de la organización, tanto propio como externo, que trata datos personales en el desarrollo de su actividad, y se basa en lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril de 2016 (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD).

En este sentido, para velar y hacer cumplir esta Política, la organización ha designado un Responsable de seguridad que estará a disposición de todo el personal y se encargará de coordinar, controlar, desarrollar y verificar el cumplimiento de las citadas normativas.

2.- CONCEPTOS BÁSICOS

Para proporcionar una mejor comprensión de la protección de datos, definimos los principales conceptos básicos:

Estructura del tratamiento:

- **Datos personales**: Información relativa a una persona física por la cual pueda determinarse su identidad.
- **Tratamiento**: Cualquier operación realizada sobre datos personales: obtención, acceso, intervención, transmisión, conservación y supresión.
- **Interesado**: Persona física sometida al tratamiento de sus datos personales.
- **Fichero**: Conjunto estructurado de datos personales susceptibles de tratamiento para un fin determinado.
- **Responsable del tratamiento**: Organización que determina los fines y los medios del tratamiento.
- **Personal autorizado**: Persona autorizada por el Responsable para realizar un tratamiento de datos mediante un compromiso de confidencialidad.

Categorías de datos:

- **Básicos**: Datos que no correspondan a categorías Penales o Especiales, por ejemplo: nombre, dirección, e-mail, teléfono, edad, sexo, firma, imagen, aficiones, patrimonio, datos bancarios, información académica, profesional, social, comercial, financiera, etc.
- **Penales**: Datos relativos a la comisión de infracciones administrativas o penales, o datos que puedan ofrecer una definición de características de personalidad, etc.
- **Especiales**: Datos relativos al origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos que permitan la identificación unívoca de una persona, datos relativos a la salud o a la vida y orientación sexuales.

3.- PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Los principios fundamentales para realizar un tratamiento de datos son:

- **Licitud**: lealtad y transparencia con el interesado.
- **Limitación de los fines**: tratados para fines determinados.
- **Minimización de los datos**: solo se deben obtener los datos necesarios para alcanzar los fines.
- **Exactitud**: actualizados.
- **Limitación del plazo de conservación**: guardados durante no más tiempo del necesario para conseguir los fines.
- **Integridad y confidencialidad**: aplicación de medidas de seguridad para la protección de los datos en todas las fases del tratamiento.
- **Responsabilidad proactiva**: se debe poder demostrar el cumplimiento de todos los principios de protección de datos.

Consentimiento para realizar un tratamiento de datos

- Para tratar datos deberemos obtener el consentimiento explícito del interesado y guardar el documento probatorio que lo acredite.
- Cuando obtengamos los datos de terceros, deberemos asegurarnos de que la comunicación sea lícita y guardar el documento probatorio que lo acredite.
- No es necesario obtener el consentimiento del interesado cuando el tratamiento se base en una obligación legal (por ejemplo, para emitir una factura).

Información del tratamiento al interesado

Deberemos facilitar la siguiente información al interesado:

- La identidad y los datos de contacto del Responsable del tratamiento
- Los fines del tratamiento.
- La base jurídica del tratamiento.
- El plazo de conservación de los datos o los criterios que lo determinen.
- Los derechos que asisten al interesado.
- Y si existen:

- Los destinatarios o categorías de destinatarios de los datos.
- La transmisión de datos a países u organizaciones establecidas fuera de la UE.

Responsabilidad del tratamiento

El tratamiento de datos se podrá realizar por organizaciones externas siempre y cuando exista una autorización expresa del Responsable y se haya suscrito un contrato para realizar dicho tratamiento conforme a la legislación vigente. Para conocer qué empresas o terceros están autorizados a la cesión de datos, deben dirigirse al Responsable de seguridad.

Las organizaciones externas pueden ser:

- **Encargados del tratamiento**: Organización que trata datos personales por cuenta del Responsable.
- **Destinatarios de datos**: Organización distinta del Encargado, que recibe una comunicación de datos personales del Responsable.

Medidas de seguridad

La organización ha implementado medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado a los riesgos que pueda tener el tratamiento a consecuencia de la destrucción accidental o ilícita de datos, la pérdida, alteración o comunicación no autorizada y el acceso a los datos cuando son transmitidos, conservados u objeto de algún otro tipo de tratamiento.

El personal deberá velar por la seguridad de los datos tratados por la organización y comunicará al Responsable cualquier operación de tratamiento que pueda suponer un riesgo que afecte la protección de datos o los intereses y libertades de los interesados.

Cualquier diseño de una nueva operación de tratamiento o actualización de una operación existente deberá garantizar antes de su implantación, la protección de datos personales y el ejercicio de los derechos de los interesados en todas las fases del tratamiento: obtención, acceso, intervención, transmisión, conservación y supresión.

4 - FUNCIONES Y OBLIGACIONES DEL PERSONAL

El personal deberá actuar en todo momento conforme a las instrucciones detalladas en el acuerdo de confidencialidad suscrito con la organización y las establecidas en esta Política de seguridad. Para ello se establecen las siguientes medidas de protección de datos que el personal está obligado a cumplir expresamente:

Organización de la información

Se deberán clasificar los datos de manera que se puedan ejercer los derechos de los interesados: acceso, rectificación, supresión y portabilidad de los datos y limitación u oposición al tratamiento.

Conservación de los datos

Se deberán conservar los datos en el mobiliario y departamento destinados a tal fin. Para tratamientos automatizados se guardarán los archivos en los soportes, carpetas o directorio de red indicados por el Responsable de seguridad.

No está permitido conservar datos en el escritorio físico o digital. Solo se permite su tratamiento temporal en dicho escritorio para realizar las operaciones que lo precisen debiendo conservarse en el lugar apropiado al término de la jornada laboral.

Acceso a la información

Se deberán aplicar los mecanismos de acceso restringido a la información que haya implementado la organización, y salvaguardar las claves de acceso de toda divulgación o comunicación a otras personas.

Cada persona solo está autorizada a acceder a los recursos que sean necesarios para el desarrollo y cumplimiento de sus funciones.

Se restringirá el acceso a los equipos informáticos mediante procedimientos que puedan identificar y autenticar la persona que accede a los mismos. Los nombres de usuario y contraseña tendrán la consideración de datos personales intransferibles.

Procesamiento de datos

Los soportes documentales e informáticos deberán estar dispuestos de tal forma que no sean accesibles a personas no autorizadas.

Si una persona abandona su puesto de trabajo temporalmente, deberá ocultar los documentos y bloquear el ordenador, de modo que se impida la visualización de la información con la que estaba trabajando.

Cuando se utilicen impresoras o fotocopiadoras, después de la impresión de trabajos con información de carácter personal, se debe recoger de manera inmediata, o imprimir de forma bloqueada, asegurándose de no dejar documentos impresos en la bandeja de salida.

Transporte de soportes

El transporte de soportes que contengan datos personales deberá realizarse únicamente por personal autorizado o empresas externas contratadas para tal fin por el Responsable del tratamiento.

Eliminación de documentos

Cualquier documento físico o soporte digital que quiera ser eliminado y que incluya datos personales, debe ser destruido con la destructora o retirado por una empresa homologada de destrucción de documentos.

Copia de seguridad y recuperación de datos

El personal deberá almacenar toda la información tratada en el directorio de red correspondiente indicado por el Responsable de seguridad, lo que permitirá que a esta información se le apliquen las medidas de seguridad existentes y que se someta a los procedimientos de copias de seguridad aplicados por la organización.

Protección de datos

Se deberán aplicar las medidas de protección de datos establecidas por la organización relativas a la seguridad del tratamiento como pueden ser la seudonimización o cifrado de datos o advertencias de intrusión como antivirus, *antispam*, etc.

Gestión de incidencias

Se considera una incidencia cualquier violación de la seguridad que ocasione la destrucción accidental o ilícita, pérdida, alteración, o el acceso o comunicación no autorizados de datos personales.

El personal tiene la obligación de notificar sin demora injustificada, cualquier incidencia de la que tenga conocimiento al Responsable de seguridad para su conocimiento y para la aplicación de medidas correctivas para remediar y mitigar los efectos que hubiera podido ocasionar. La persona que notifica la incidencia deberá documentarla con una descripción detallada de la misma y la fecha y hora en que se ha producido o se ha tenido conocimiento de ella.

El conocimiento y no notificación de una incidencia por parte del personal se considerará una falta contra la seguridad de los datos y podrá suponer el inicio de acciones legales, así como la reclamación de las indemnizaciones, sanciones y daños o perjuicios que el Responsable se vea obligado a atender a consecuencia de dicho incumplimiento.

ACUERDO DE TELETRABAJO

DEBERES DEL TELETRABAJADOR EN MATERIA DE PROTECCIÓN DE DATOS

MALAGA, ...

Reunidos de una parte D./Dña. JOSE MARIA PLATA ZAFRA, con NIF 25715073S, en nombre y representación de RIOS CONSULTORES S.L., con NIF B92918788 y domicilio social situado en JUAN PORRAS, 7 - 29003 MALAGA (Málaga), en adelante, **EMPLEADOR**.

Y de otra parte D./Dña. ....., con NIF ....., mayor de edad y, en su propio nombre y representación, en adelante **TELETRABAJADOR**.

Ambas partes se reconocen recíprocamente la capacidad legal necesaria para suscribir el presente acuerdo de teletrabajo y

EXPONEN

I. El teletrabajo es una forma de organización y/o de realización del trabajo a distancia, que se lleva a cabo mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación, entendiendo «trabajo a distancia» como una forma de organización del trabajo o de realización de la actividad laboral conforme a la cual esta se presta en el domicilio de la persona trabajadora o en el lugar elegido por esta, durante toda su jornada o parte de ella, con carácter regular.

II. El presente acuerdo no significa un contrato de teletrabajo regulado por el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia, de manera que solo pretende establecer las instrucciones para llevar a cabo temporalmente las funciones laborales a distancia.

No debe confundirse el «teletrabajo» con otras actividades diferentes como pueden ser, p. ej., tele-marketing, tele-venta o prestación de tele-servicios, en los que coincide por el uso de las nuevas tecnologías pero con la diferencia de que dicha prestación se realiza siempre en la sede empresarial.

III. El teletrabajador goza de los mismos derechos que los trabajadores que prestan sus servicios en el centro de trabajo de la empresa, salvo aquellos que sean inherentes a la realización de la prestación laboral en el mismo de manera presencial, por tanto, también debe dar cumplimiento a las mismas obligaciones y, por tal motivo, empleado y empleador deben dar cumplimiento a la vigente normativa de protección de datos de carácter personal, con las particularidades que dicha prestación conlleva y, en este sentido

ACUERDAN

1º.- El empleador es el responsable de adoptar las medidas adecuadas, especialmente respecto al software, para garantizar el cumplimiento de la normativa de protección de los datos de carácter personal usados y procesados por el teletrabajador con fines profesionales.

2º.- El empleador procede a informar al teletrabajador de la política de seguridad del personal, mediante ANEXO al presente acuerdo, de toda legislación o normativa de la empresa referente a la protección de datos de carácter personal y de las limitaciones que se imponen durante la jornada laboral en la utilización del equipo informático o de herramientas informáticas tales como internet y también de las posibles sanciones que derivarán del incumplimiento de las mismas, siendo el teletrabajador el responsable del cumplimiento de estas normas.

3º.- El teletrabajador se compromete al estricto cumplimiento de todas las medidas de carácter necesario que han sido dispuestas por el empleador al objeto de no difundir, perjudicar o usar indebidamente los datos personales y los documentos relacionados con el trabajo. Dichos datos y documentos serán conservados por el teletrabajador con el máximo celo profesional y en el supuesto de ficheros no automáticos en perfecto estado de conservación.

4º.- El teletrabajador se ratifica en su deber de respeto a la obligación profesional de guardar secreto y de tratar

confidencialmente toda la información a la que pueda tener acceso como consecuencia del teletrabajo realizado desde su domicilio.

5º.- El teletrabajador, mediante la suscripción del presente acuerdo específico de teletrabajo, declara conocer sus derechos y deberes en la referida prestación profesional, haber recibido una copia del presente acuerdo y sus documentos anexos, así como poner en conocimiento del empleador cualquier duda, consulta o sugerencia que sobre la materia se pueda plantear, en especial, con carácter previo a la realización del cualquier acto que pueda comprometer la confidencialidad y seguridad de los datos de carácter personal objeto de tratamiento a consecuencia de la realización del teletrabajo.

Y para que conste a los efectos oportunos, en prueba de conformidad de las partes, firman el presente acuerdo, por duplicado, en el lugar y la fecha indicados en el encabezamiento.

Por RIOS CONSULTORES S.L., JOSE MARIA PLATA ZAFRA	El teletrabajador,

ANEXO

POLÍTICA DE SEGURIDAD DEL PERSONAL PARA EL TRATAMIENTO DE DATOS PERSONALES

1.- ÁMBITO DE APLICACIÓN

El Responsable del tratamiento está comprometido en implantar una cultura de privacidad en la organización, por lo que necesita que las personas autorizadas a tratar datos personales estén informadas del tratamiento de datos y se responsabilicen del mismo.

A toda persona autorizada para tratar datos personales se le exige que lea, comprenda, cumpla y haga cumplir esta Política de seguridad para proteger los datos que forman parte del tratamiento que se le ha encomendado.

Esta Política de seguridad establece las obligaciones y procedimientos que tiene que seguir el personal de la organización, tanto propio como externo, que trata datos personales en el desarrollo de su actividad, y se basa en lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril de 2016 (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD).

En este sentido, para velar y hacer cumplir esta Política, la organización ha designado un Responsable de seguridad que estará a disposición de todo el personal y se encargará de coordinar, controlar, desarrollar y verificar el cumplimiento de las citadas normativas.

2.- CONCEPTOS BÁSICOS

Para proporcionar una mejor comprensión de la protección de datos, definimos los principales conceptos básicos:

Estructura del tratamiento:

- **Datos personales**: Información relativa a una persona física por la cual pueda determinarse su identidad.
- **Tratamiento**: Cualquier operación realizada sobre datos personales: obtención, acceso, intervención, transmisión, conservación y supresión.
- **Interesado**: Persona física sometida al tratamiento de sus datos personales.
- **Fichero**: Conjunto estructurado de datos personales susceptibles de tratamiento para un fin determinado.
- **Responsable del tratamiento**: Organización que determina los fines y los medios del tratamiento.
- **Personal autorizado**: Persona autorizada por el Responsable para realizar un tratamiento de datos mediante un compromiso de confidencialidad.

Categorías de datos:

- **Básicos**: Datos que no correspondan a categorías Penales o Especiales, por ejemplo: nombre, dirección, e-mail, teléfono, edad, sexo, firma, imagen, aficiones, patrimonio, datos bancarios, información académica, profesional, social, comercial, financiera, etc.
- **Penales**: Datos relativos a la comisión de infracciones administrativas o penales, o datos que puedan ofrecer una definición de características de personalidad, etc.
- **Especiales**: Datos relativos al origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos que permitan la identificación unívoca de una persona, datos relativos a la salud o a la vida y orientación sexuales.

3.- PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Los principios fundamentales para realizar un tratamiento de datos son:

- **Licitud**: lealtad y transparencia con el interesado.
- **Limitación de los fines**: tratados para fines determinados.
- **Minimización de los datos**: solo se deben obtener los datos necesarios para alcanzar los fines.

- **Exactitud**: actualizados.
- **Limitación del plazo de conservación**: guardados durante no más tiempo del necesario para conseguir los fines.
- **Integridad y confidencialidad**: aplicación de medidas de seguridad para la protección de los datos en todas las fases del tratamiento.
- **Responsabilidad proactiva**: se debe poder demostrar el cumplimiento de todos los principios de protección de datos.

Consentimiento para realizar un tratamiento de datos

- Para tratar datos deberemos obtener el consentimiento explícito del interesado y guardar el documento probatorio que lo acredite.
- Cuando obtengamos los datos de terceros, deberemos asegurarnos de que la comunicación sea lícita y guardar el documento probatorio que lo acredite.
- No es necesario obtener el consentimiento del interesado cuando el tratamiento se base en una obligación legal (por ejemplo, para emitir una factura).

Información del tratamiento al interesado

Deberemos facilitar la siguiente información al interesado:

- La identidad y los datos de contacto del Responsable del tratamiento
- Los fines del tratamiento.
- La base jurídica del tratamiento.
- El plazo de conservación de los datos o los criterios que lo determinen.
- Los derechos que asisten al interesado.
- Y si existen:
    - Los destinatarios o categorías de destinatarios de los datos.
    - La transmisión de datos a países u organizaciones establecidas fuera de la UE.

Responsabilidad del tratamiento

El tratamiento de datos se podrá realizar por organizaciones externas siempre y cuando exista una autorización expresa del Responsable y se haya suscrito un contrato para realizar dicho tratamiento conforme a la legislación vigente. Para conocer qué empresas o terceros están autorizados a la cesión de datos, deben dirigirse al Responsable de seguridad.

Las organizaciones externas pueden ser:

- **Encargados del tratamiento**: Organización que trata datos personales por cuenta del Responsable.
- **Destinatarios de datos**: Organización distinta del Encargado, que recibe una comunicación de datos personales del Responsable.

Medidas de seguridad

La organización ha implementado medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado a los riesgos que pueda tener el tratamiento a consecuencia de la destrucción accidental o ilícita de datos, la pérdida, alteración o comunicación no autorizada y el acceso a los datos cuando son transmitidos, conservados u objeto de algún otro tipo de tratamiento.

El personal deberá velar por la seguridad de los datos tratados por la organización y comunicará al Responsable cualquier operación de tratamiento que pueda suponer un riesgo que afecte la protección de datos o los intereses y libertades de los interesados.

Cualquier diseño de una nueva operación de tratamiento o actualización de una operación existente deberá garantizar antes de su implantación, la protección de datos personales y el ejercicio de los derechos de los interesados en todas las fases del tratamiento: obtención, acceso, intervención, transmisión, conservación y supresión.

4 - FUNCIONES Y OBLIGACIONES DEL PERSONAL

El personal deberá actuar en todo momento conforme a las instrucciones detalladas en el acuerdo de confidencialidad suscrito con la organización y las establecidas en esta Política de seguridad. Para ello, se establecen las siguientes medidas de protección de datos que el personal está obligado a cumplir expresamente:

Organización de la información

Se deberán clasificar los datos de manera que se puedan ejercer los derechos de los interesados: acceso, rectificación, supresión y portabilidad de los datos y limitación u oposición al tratamiento.

Conservación de los datos

Se deberán conservar los datos en el mobiliario y departamento destinados a tal fin. Para tratamientos automatizados se guardarán los archivos en los soportes, carpetas o directorio de red indicados por el Responsable de seguridad.

No está permitido conservar datos en el escritorio físico o digital. Solo se permite su tratamiento temporal en dicho escritorio para realizar las operaciones que lo precisen debiendo conservarse en el lugar apropiado al término de la jornada laboral.

Acceso a la información

Se deberán aplicar los mecanismos de acceso restringido a la información que haya implementado la organización, y salvaguardar las claves de acceso de toda divulgación o comunicación a otras personas.

Cada persona solo está autorizada a acceder a los recursos que sean necesarios para el desarrollo y cumplimiento de sus funciones.

Se restringirá el acceso a los equipos informáticos mediante procedimientos que puedan identificar y autenticar la persona que accede a los mismos. Los nombres de usuario y contraseña tendrán la consideración de datos personales intransferibles.

Procesamiento de datos

Los soportes documentales e informáticos deberán estar dispuestos de tal forma que no sean accesibles a personas no autorizadas.

Si una persona abandona su puesto de trabajo temporalmente, deberá ocultar los documentos y bloquear el ordenador, de modo que se impida la visualización de la información con la que estaba trabajando.

Cuando se utilicen impresoras o fotocopiadoras, después de la impresión de trabajos con información de carácter personal, se debe recoger de manera inmediata, o imprimir de forma bloqueada, asegurándose de no dejar documentos impresos en la bandeja de salida.

Transporte de soportes

El transporte de soportes que contengan datos personales deberá realizarse únicamente por personal autorizado o empresas externas contratadas para tal fin por el Responsable del tratamiento.

Eliminación de documentos

Cualquier documento físico o soporte digital que quiera ser eliminado y que incluya datos personales, debe ser destruido con la destructora o retirado por una empresa homologada de destrucción de documentos.

Copia de seguridad y recuperación de datos

El personal deberá almacenar toda la información tratada en el directorio de red correspondiente indicado por el Responsable de seguridad, lo que permitirá que a esta información se le apliquen las medidas de seguridad existentes y que se someta a los procedimientos de copias de seguridad aplicados por la organización.

Protección de datos

Se deberán aplicar las medidas de protección de datos establecidas por la organización relativas a la seguridad del tratamiento como pueden ser la seudonimización o cifrado de datos o advertencias de intrusión como antivirus, antispam, etc.

Gestión de incidencias

Se considera una incidencia cualquier violación de la seguridad que ocasione la destrucción accidental o ilícita, pérdida, alteración, o el acceso o comunicación no autorizados de datos personales.

El personal tiene la obligación de notificar sin demora injustificada, cualquier incidencia de la que tenga conocimiento al Responsable de seguridad para su conocimiento y para la aplicación de medidas correctivas para remediar y mitigar los efectos que hubiera podido ocasionar. La persona que notifica la incidencia deberá documentarla con una descripción detallada de la misma y la fecha y hora en que se ha producido o se ha tenido conocimiento de ella.

El conocimiento y no notificación de una incidencia por parte del personal se considerará una falta contra la seguridad de los datos y podrá suponer el inicio de acciones legales, así como la reclamación de las indemnizaciones, sanciones y daños o perjuicios que el Responsable se vea obligado a atender a consecuencia de dicho incumplimiento.

POLÍTICA DE PROTECCIÓN DE DATOS EN SITUACIONES DE MOVILIDAD Y TELETRABAJO

RIOS CONSULTORES S.L., como responsable del tratamiento, ha elaborado e implantado esta política de protección de datos para situaciones de movilidad y teletrabajo, que incluye una serie de medidas para cuando se den situaciones que impliquen que algunas de sus actividades se lleven a cabo en situaciones de movilidad y teletrabajo, y que tendrán que ser tenidas en cuenta por el personal que participa en estas acciones de teletrabajo. Situaciones que pueden darse como parte de la estrategia de gestión, general o parcial, para determinadas áreas o actividades (por ejemplo, personal que viaja con frecuencia) o pueden ser motivadas por situaciones excepcionales e incluso de fuerza mayor. Estas medidas irán encaminadas a conseguir que incluso en estas situaciones se consiga la resiliencia permanente de los sistemas y servicios de tratamiento, la continuidad de los procesos de negocio y los derechos y libertades de los interesados cuyos datos se están tratando.

Para la redacción y elaboración de la presente política se han tenido en cuenta las necesidades y los riesgos debidos al acceso a los recursos corporativos desde lugares fuera del control de la organización. Se han determinado las formas de acceso remoto permitidas, los tipos de dispositivos válidos para cada forma de acceso y el nivel de acceso en función de los perfiles de movilidad definidos.

Este protocolo está compuesto por las medidas adoptadas por la organización y las que deberá adoptar el personal en situaciones de teletrabajo, informando de:

- Las principales amenazas por las que pueden verse afectados al trabajar desde fuera de las instalaciones de la organización.
- Las posibles consecuencias que pueden materializarse si se quebrantan las directrices expuestas en esta política.
- El procedimiento para comunicar cualquier incidencia de seguridad que afecte a la información tratada, incluida la información personal (datos personales).
- La existencia y el alcance de actividades de monitorización para el control y la supervisión del teletrabajo.
- La obligación de firmar un acuerdo de teletrabajo que incluya los compromisos adquiridos al desempeñar sus tareas en situación de movilidad.

MEDIDAS ADOPTADAS POR LA ORGANIZACIÓN

A continuación, se enumera el conjunto de medidas adoptadas por RIOS CONSULTORES S.L. para cuando se den las situaciones antes mencionadas y que son adecuadas a la situación concreta de su objeto de negocio:

1. Aplicaciones y prestadores de servicio

Solo se utilizan las soluciones que garantizan un nivel de seguridad adecuado al riesgo del tratamiento y que son conformes a los requisitos exigidos por el GDPR, y en todos los casos se han suscrito los pertinentes contratos de encargados del tratamiento conforme a lo establecido en el artículo 28.3 del GDPR.

2. Acceso a la información

Se han definido los perfiles de movilidad, las responsabilidades y las obligaciones que asumirá el personal de la organización en situaciones de movilidad en función de los roles que tienen asignados, y se aplican restricciones de acceso adicionales en función de la ubicación y del tipo de dispositivo utilizado (equipos portátiles corporativos segurizados, equipos personales externos y dispositivos móviles como smartphones o tablets).

3. Equipos y dispositivos utilizados

Se configuran periódicamente, se revisan y actualizan los servidores de acceso remoto y los equipos corporativos utilizados en estas situaciones:

- Están actualizados a nivel de aplicación, sistema operativo y software antivirus.
- Tienen una configuración por defecto de mínimos privilegios fijada por los servicios TIC que no puede ser desactivada ni modificada por el empleado.
- Instalan únicamente las aplicaciones autorizadas por la organización.
- Activan solo las comunicaciones (Wifi, Bluetooth, NFC, …) y puertos (USB, etc.) necesarios para llevar a cabo las tareas encomendadas.
- Deshabilitan los servicios que no sean necesarios.
- Activan un cortafuegos local.
- Incorporan mecanismos de cifrado de la información.

Cuando se permite el uso de dispositivos particulares del empleado, si es posible, se restringe la conexión a una red segregada que únicamente proporciona un acceso limitado a aquellos recursos que se han identificado como menos críticos y sometidos a menor nivel de riesgo.

4. Accesos realizados a la red corporativa desde el exterior

Se monitorizan con el fin de identificar patrones anormales de comportamiento atribuibles al sistema de movilidad para evitar la propagación de malware y el acceso y uso no autorizado de recursos.

Para ello, se ha informado al personal, con carácter previo y de forma clara, expresa y concisa, de la existencia y el alcance de estas actividades de monitorización, que también se utilizan para verificar el cumplimiento de las obligaciones laborales, teniendo en cuenta y respetando siempre los derechos digitales establecidos en la LOPDGDD, en particular, el derecho a la intimidad y uso de dispositivos digitales y el derecho a la desconexión digital en el ámbito laboral.

Se han diseñado protocolos para gestionar las brechas de seguridad que afecten a datos personales con el propósito de crear un entorno de teletrabajo resiliente.

5. Gestión de la protección de datos y la seguridad

Esta política para situaciones de movilidad se basa en un análisis de riesgos previo en el que se ha evaluado la proporcionalidad entre los beneficios a obtener mediante el acceso a distancia y el impacto potencial de ver comprometido el acceso a datos personales. Se han contemplado en esta política:

- Los procedimientos internos para provisionar y auditar los dispositivos clientes de acceso remoto.
- Los procedimientos de administración y monitorización de la infraestructura.
- Los servicios proporcionados por encargados del tratamiento.
- La forma en la que es revisada y actualizada a los riesgos existentes.

Se han limitado los recursos en función del riesgo que represente una pérdida del dispositivo cliente y la exposición o acceso no autorizado a la información manejada.

Se han planificado y evaluado las aplicaciones y soluciones de teletrabajo teniendo en cuenta los principios de privacidad desde el diseño y por defecto en todas las etapas de despliegue de la solución: desde la definición de los requisitos y necesidades hasta la retirada de la misma o de alguno de sus componentes.

MEDIDAS QUE DEBERÁ ADOPTAR EL PERSONAL EN SITUACIONES DE TELETRABAJO

El personal autorizado para teletrabajar deberá respetar la «Política de protección de datos en situaciones de movilidad y teletrabajo» definida por RIOS CONSULTORES S.L., cumpliendo las medidas y recomendaciones detalladas a continuación, así como el resto de las normas y procedimientos que la desarrollen y, especialmente, lo que concierne al deber de confidencialidad de la persona teletrabajadora con relación a los datos personales a los que tuviera acceso en el desempeño de sus funciones laborales.

1. Proteger el dispositivo utilizado y el acceso al mismo

Medidas dirigidas a la actitud del personal:

- Definir y utilizar contraseñas de acceso robustas y diferentes a las utilizadas en el ámbito de su vida particular.
- No descargar ni instalar ningún software que no haya sido previamente autorizado por la organización.
- Verificar la legitimidad de los correos electrónicos recibidos, comprobando que el dominio electrónico de procedencia es válido y conocido, y desconfiando de la descarga de ficheros adjuntos con extensiones inusuales o el establecimiento de conexiones a través de enlaces incluidos en el cuerpo del correo que presenten cualquier patrón fuera de lo normal.
- Si se utilizan dispositivos corporativos, no utilizarlos con fines particulares evitando el acceso a redes sociales, correo electrónico personal, páginas web con reclamos y publicidad impactante, así como otros sitios susceptibles de contener virus o favorecer la ejecución de código dañino.
- Si se utilizan dispositivos particulares, evitar simultanear la actividad particular con la profesional y definir perfiles independientes para desarrollar cada tipo de tarea.

Medidas dirigidas a la seguridad del dispositivo:

- El sistema antivirus instalado en el equipo debe estar operativo y actualizado.
- Mantener protegidos los mecanismos de autenticación (certificados, contraseñas, tokens, sistemas de doble factor, …) para validarse ante los sistemas de control de acceso remoto de la organización.
- Evitar la conexión de los dispositivos desde lugares públicos mediante redes WIFI abiertas no seguras.
- Desactivar las conexiones WIFI, Bluetooth y similares que no estén siendo utilizadas.
- Cuando no se realice teletrabajo, desconectar la sesión de acceso remoto y apagar o bloquear el acceso al dispositivo.

2. Garantizar la protección de la información que se está manejando

Medidas en tratamientos automatizados (digitales o electrónicos)

- Evitar exponer la pantalla a la mirada de terceros. Si se trabaja habitualmente desde lugares públicos, se debe utilizar un filtro de privacidad para la pantalla.
- Evitar que los dispositivos utilizados estén a la vista de terceros y bloquear las sesiones cuando estos estén desatendidos.

Medidas en tratamientos no automatizados (manuales o en papel)

- Minimizar la documentación en soporte papel y extremar las precauciones para evitar accesos no autorizados.
- Garantizar la destrucción adecuada de la documentación inservible en soporte papel. Evitar arrojar papeles enteros o en trozos en papeleras de hoteles, lugares públicos o en la basura doméstica a los que alguien podría acceder y recuperar información de carácter personal.
- Prevenir que terceros puedan escuchar conversaciones. Utilizar auriculares o retirarse a un espacio aislado.

3. Guardar la información en los espacios de red habilitados

- Utilizar los recursos de almacenamiento proporcionados por la organización. Evitar almacenar información de forma local en el dispositivo utilizado.
- Revisar y eliminar periódicamente la información residual almacenada en el dispositivo, como archivos temporales del navegador o descargas de documentos.
- No utilizar aplicaciones no autorizadas por la organización para compartir información (servicios en nube de alojamiento de archivos, correos personales, mensajería rápida, etc.)
- No bloquear o deshabilitar la copia de seguridad corporativa definida para cada dispositivo.

4. Brechas de seguridad

Cualquier sospecha de anomalía o incidencia que pueda afectar a la seguridad de la información o a la protección de datos personales debe notificarse al responsable encargado, sin dilación y en la mayor brevedad posible, a través de los canales previstos para tal efecto, para que se tomen las medidas de seguridad oportunas destinadas a mitigar los riesgos.

CONSENTIMIENTO PARA UTILIZAR DISPOSITIVOS PERSONALES PARA TELETRABAJO

MALAGA, ...

Conforme con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), solicitamos su consentimiento para utilizar los dispositivos personales del interesado (ADSL, teléfono móvil, tablet, ordenador, impresora, etc.) para tener acceso a los recursos de la empresa tales como correos electrónicos, bases de datos y archivos en servidores así como datos y aplicaciones personales mediante teletrabajo, por lo que se le facilita la siguiente información del tratamiento:

Teletrabajo: forma de organización y/o de realización del trabajo regulado en el artículo 13 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores -ET. El teletrabajo se puede realizar con los dispositivos facilitados por la empresa o con los dispositivos del teletrabajador (entorno BYOD).

Finalidad: llevar a cabo la prestación de la actividad laboral mediante teletrabajo, de manera preponderante en el domicilio del trabajador o en el lugar libremente elegido por este, de modo alternativo a su desarrollo presencial en el centro de trabajo de la empresa.

Legitimación: consentimiento del interesado (art. 6.1.a GDPR).

Medidas de seguridad para teletrabajo con los dispositivos del teletrabajador (entorno BYOD):

- Se utilizarán únicamente los dispositivos personales puestos a disposición por el teletrabajador y autorizados por el responsable.
- Se accederá a los sistemas de información del responsable mediante las aplicaciones web que este ponga a disposición del teletrabajador, sin permitir guardar información en el equipo del usuario.
- Se deberá tener configurado un protocolo de seguridad inalámbrica para evitar accesos no deseados que permita el cifrado punto a punto y la autenticación del usuario y de la red.
- Se deberán seguir las pautas establecidas por el responsable, que podrán ser la actualización de sistemas operativos, apertura de nueva sesión de usuario, *antivirus*, firewall, acceso a escritorio remoto, *cloud* para custodia de documentos, etc.
- Se derivarán las llamadas entrantes a los teléfonos móviles de los propios empleados. En caso de que se realicen llamadas desde el móvil del teletrabajador, se deberá, de forma excepcional, ocultar el número saliente, ya que este es considerado un dato personal y no debe ser comunicado a terceros.

Uso de los datos: queda terminantemente prohibido el uso de la información para otros fines distintos del teletrabajo.

Derechos que asisten al teletrabajador:

- Derecho a retirar el consentimiento en cualquier momento.
- Derecho de acceso, rectificación, portabilidad y supresión de sus datos, y de limitación u oposición a su tratamiento.
- Derecho a presentar una reclamación ante la Autoridad de control (www.aepd.es) si considera que el tratamiento no se ajusta a la normativa vigente.

Datos de contacto para ejercer sus derechos:

RIOS CONSULTORES S.L.. JUAN PORRAS, 7 - 29003 MALAGA (Málaga). E-mail: info@appsia.es

El **teletrabajador** consiente utilizar sus dispositivos personales en los términos expuestos:

Nombre ....., con NIF .....

Firma:

Anexo de acta ENTREGA DE EQUIPOS

MALAGA, ...

En fecha de hoy y en las oficinas del Responsable del Tratamiento RIOS CONSULTORES S.L., mediante el presente documento se realiza la entrega formal de los equipos que se indican en el punto 2.- EQUIPOS INFORMÁTICOS Y/O DIGITALES ASIGNADOS para el cumplimiento de las actividades laborales del USUARIO RESPONSABLE, quien declara la recepción de los mismos en buen estado y se compromete a cuidar de los recursos y hacer uso de ellos para los fines establecidos según el contrato de confidencialidad.

1.- USUARIO RESPONSABLE

Nombre: .....
NIF: .....
Cargo: .....

2.- EQUIPOS INFORMÁTICOS Y/O DIGITALES ASIGNADOS

Descripción/Modelo	Marca	Referencia	Serial
PORTÁTIL			
TELÉFONO MÓVIL			
TABLET			
OTROS			

3.- TIEMPO ESTIMADO DE USO

Se establece que el USUARIO RESPONSABLE dispondrá del equipamiento durante el tiempo definido en su contrato laboral, por lo que se le informa de que deberá entregar dichos equipos, cómo máximo, el último día de alta en la empresa, o por causa incidente, el día que estime oportuno el Responsable del Tratamiento.

4.- ENTREGA

Autorizado por:	Entregado por:	Recibido por:

5.- DEVOLUCIÓN

FECHA DEVOLUCIÓN: ……

Entregado por:	Recibido por:

TRATAMIENTO

RIOS CONSULTORES S.L.
JUAN PORRAS, 7 - 29003 MALAGA (Málaga)

Consentimiento explícito (COMERCIAL)

MALAGA, en fecha .....

RIOS CONSULTORES S.L. es el **Responsable del tratamiento** de los datos personales del **Interesado** y le informa de que estos datos se tratarán de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), por lo que se le facilita la siguiente información del tratamiento:

Fines y legitimación del tratamiento: mantener una relación comercial (por interés legítimo del responsable, art. 6.1.f GDPR) y envío de comunicaciones de productos o servicios (con el consentimiento del interesado, art. 6.1.a GDPR).

Criterios de conservación de los datos: se conservarán durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia y cuando ya no sea necesario para ello, se suprimirán con medidas de seguridad adecuadas para garantizar la anonimización de los datos o la destrucción total de los mismos.

Comunicación de los datos: no se comunicarán los datos a terceros, salvo obligación legal.

Derechos que asisten al Interesado:

- Derecho a retirar el consentimiento en cualquier momento.
- Derecho de acceso, rectificación, portabilidad y supresión de sus datos y de limitación u oposición a su tratamiento.
- Derecho a presentar una reclamación ante la Autoridad de control (www.aepd.es) si considera que el tratamiento no se ajusta a la normativa vigente.

Datos de contacto para ejercer sus derechos:

RIOS CONSULTORES S.L.. JUAN PORRAS, 7 - 29003 MALAGA (Málaga). E-mail: info@appsia.es

El **Interesado** o su representante legal consiente el tratamiento de sus datos en los términos expuestos:

Nombre ....., con NIF .....

Representante legal de ....., con NIF .....

Firma:

Circular informativa del tratamiento (COMERCIAL)

INFORMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

CON FINALIDAD COMERCIAL

RIOS CONSULTORES S.L. es el **Responsable del tratamiento** de los datos personales del **Interesado** y le informa de que estos datos se tratarán de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), por lo que se le facilita la siguiente información del tratamiento:

Fines y legitimación del tratamiento: mantener una relación comercial (por interés legítimo del responsable, art. 6.1.f GDPR) y envío de comunicaciones de productos o servicios (con el consentimiento del interesado, art. 6.1.a GDPR).

Criterios de conservación de los datos: se conservarán durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia y cuando ya no sea necesario para ello, se suprimirán con medidas de seguridad adecuadas para garantizar la anonimización de los datos o la destrucción total de los mismos.

Comunicación de los datos: no se comunicarán los datos a terceros, salvo obligación legal.

Derechos que asisten al Interesado:

- Derecho a retirar el consentimiento en cualquier momento.
- Derecho de acceso, rectificación, portabilidad y supresión de sus datos y de limitación u oposición a su tratamiento.
- Derecho a presentar una reclamación ante la Autoridad de control (www.aepd.es) si considera que el tratamiento no se ajusta a la normativa vigente.

Datos de contacto para ejercer sus derechos:

RIOS CONSULTORES S.L.. JUAN PORRAS, 7 - 29003 MALAGA (Málaga). E-mail: info@appsia.es

Deber de información en DOCUMENTOS CON DATOS PERSONALES

EN CARTAS, PRESUPUESTOS, ALBARANES, FACTURAS, FAX Y DOCUMENTOS CON SUFICIENTE ESPACIO DE IMPRESIÓN

RIOS CONSULTORES S.L. es el Responsable del tratamiento de los datos personales proporcionados bajo su consentimiento y le informa de que estos datos serán tratados de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), con la finalidad de mantener una relación comercial (por interés legítimo del responsable, art. 6.1.f GDPR) y conservarlos durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia. No se comunicarán los datos a terceros, salvo obligación legal. Asimismo, se le informa de que puede ejercer los derechos de acceso, rectificación, portabilidad y supresión de sus datos y los de limitación y oposición a su tratamiento dirigiéndose a RIOS CONSULTORES S.L. en JUAN PORRAS, 7 - 29003 MALAGA (Málaga). E-mail: info@appsia.es y el de reclamación a www.aepd.es.

EN TICKETS DE VENTA Y DOCUMENTOS CON POCO ESPACIO DE IMPRESIÓN

RIOS CONSULTORES S.L. es Responsable del tratamiento de conformidad con el GDPR y la LOPDGDD, con la finalidad de mantener una relación comercial y conservar los datos durante no más tiempo del necesario para ello. No se comunicarán los datos a terceros. Puede ejercer los derechos de acceso, rectificación, portabilidad, supresión, limitación y oposición en JUAN PORRAS, 7 - 29003 MALAGA (Málaga). E-mail: info@appsia.es y el de reclamación a www.aepd.es.

EN TICKETS TPV CON MUY POCO ESPACIO DE IMPRESIÓN

RIOS CONSULTORES S.L. es Responsable del tratamiento de conformidad con el GDPR y la LOPDGDD. Puede ver la política de privacidad en appsia.es y ejercer sus derechos en info@appsia.es.

Circular informativa del tratamiento (CURRÍCULUM) a la recepción IN SITU o por E-MAIL

INFORMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

CON FINALIDAD DE CANDIDATO A EMPLEADO

RIOS CONSULTORES S.L. es el **Responsable del tratamiento** de los datos personales del **Interesado** y le informa de que estos datos se tratarán de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), por interés legítimo del Responsable, facilitándole la siguiente información del tratamiento:

Fin del tratamiento: hacer partícipe al Interesado en los procesos de selección de personal, llevando a cabo un análisis del perfil del solicitante con el objetivo de seleccionar al mejor candidato para el puesto vacante del Responsable.

Legitimación del tratamiento: consentimiento inequívoco mediante una clara acción del interesado (GDPR, art. 6.1.a).

Criterios de conservación de los datos: se conservarán durante un plazo máximo de **un año**, transcurrido el cual se procederá a la supresión de los datos garantizándole un total respeto a la confidencialidad tanto en el tratamiento como en su posterior destrucción. En este sentido, transcurrido el citado plazo, y si desea continuar participando en los procesos de selección del Responsable, le rogamos nos remita nuevamente su currículum.

Actualización de los datos: en caso de producirse alguna modificación en sus datos, le rogamos nos lo comunique por escrito lo antes posible, con objeto de mantener sus datos debidamente actualizados.

Comunicación de los datos: no se comunicarán los datos a terceros, salvo obligación legal.

Derechos que asisten al Interesado:

- Derecho a retirar el consentimiento en cualquier momento.
- Derecho de acceso, rectificación, portabilidad y supresión de sus datos y de limitación u oposición a su tratamiento.
- Derecho a presentar una reclamación ante la Autoridad de control (www.aepd.es) si considera que el tratamiento no se ajusta a la normativa vigente.

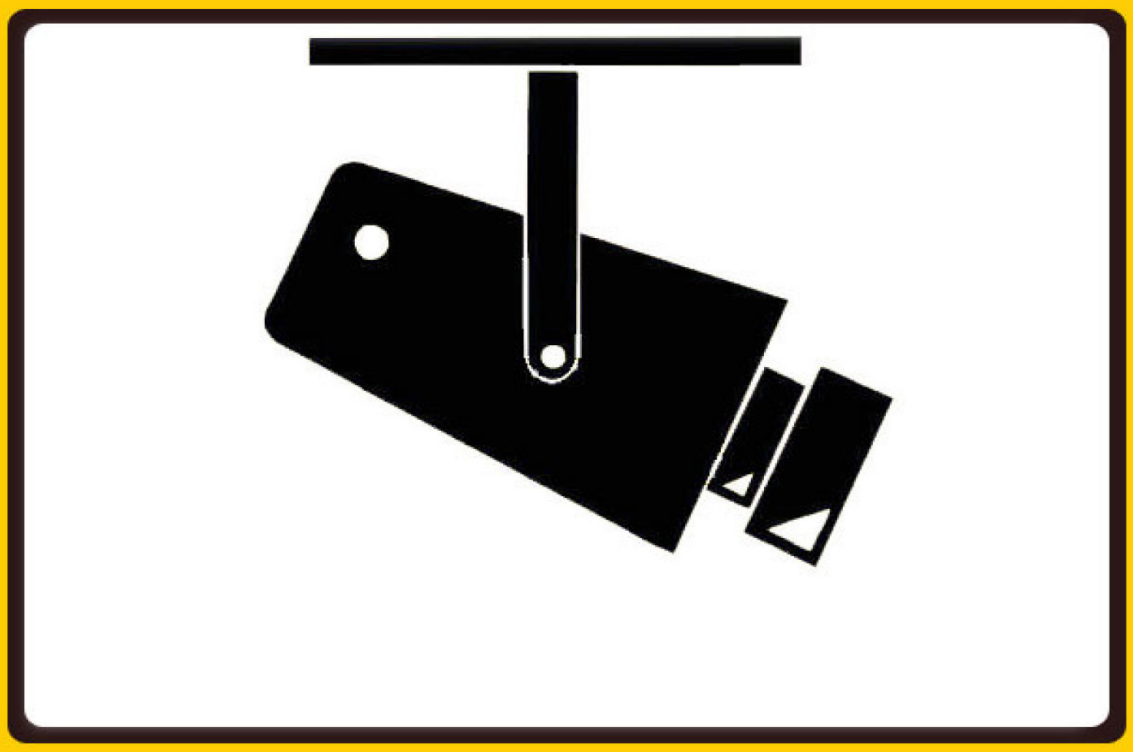
Datos de contacto para ejercer sus derechos:

RIOS CONSULTORES S.L.. JUAN PORRAS, 7 - 29003 MALAGA (Málaga). E-mail: info@appsia.es

IMÁGENES

RIOS CONSULTORES S.L.
JUAN PORRAS, 7 - 29003 MALAGA (Málaga)

ZONA VIDEOVIGILADA



Protección de datos

Reglamento (UE) 2016/679, de 27 de abril (GDPR), y Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD)

Responsable	RIOS CONSULTORES S.L.
Finalidad	Garantizar la seguridad de personas, bienes e instalaciones
Legitimación	Interés público
Conservación	Un máximo de 30 días
Destinatarios	Fuerzas y cuerpos de seguridad
Derechos	Acceso, rectificación, portabilidad y supresión de datos Limitación y oposición al tratamiento
Ejercicio derechos	JUAN PORRAS, 7 - 29003 MALAGA (Málaga). E-mail: info@appsia.es
Reclamación	Ante la autoridad de control en www.aepd.es
Más información	Diríjase al encargado del local.

Circular informativa de VIDEOVIGILANCIA

INFORMACIÓN PARA EL TRATAMIENTO DE DATOS

VIDEOVIGILANCIA

RIOS CONSULTORES S.L. es el **Responsable del tratamiento** de los datos personales del **Interesado** y le informa de que estos datos serán tratados de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), por lo que se le facilita la siguiente información del tratamiento:

Fin del tratamiento: garantizar la seguridad de personas, bienes e instalaciones a través de un sistema de videovigilancia.

Legitimación: interés público (art. 6.1.e del GDPR) basado en la seguridad ciudadana.

Criterios de conservación de los datos: se conservarán un máximo de 30 días naturales.

Comunicación de los datos: no se comunicarán los datos a terceros, excepto a las fuerzas y cuerpos de seguridad o por obligación legal.

Derechos que asisten al Interesado:

- Derecho de acceso, rectificación, portabilidad y supresión de sus datos, y de limitación u oposición a su tratamiento.
- Derecho a presentar una reclamación ante la Autoridad de control (www.aepd.es) si considera que el tratamiento no se ajusta a la normativa vigente.

Datos de contacto para ejercer sus derechos:

RIOS CONSULTORES S.L.. JUAN PORRAS, 7 - 29003 MALAGA (Málaga). E-mail: info@appsia.es

OTROS FINES

CERTIFICADO DE GARANTÍA DE CUMPLIMIENTO DEL GDPR Y LOPDGDD

JOSE MARIA PLATA ZAFRA, con NIF 25715073S, en representación de RIOS CONSULTORES S.L., con NIF B92918788 y domicilio social situado en JUAN PORRAS, 7 - 29003 MALAGA (Málaga),

CERTIFICA

Que de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), RIOS CONSULTORES S.L. está cumpliendo con todas las disposiciones del GDPR para el tratamiento de los datos personales de su responsabilidad, y manifiestamente con los principios descritos en el artículo 5 del GDPR, por los cuales son tratados de manera lícita, leal y transparente en relación con el interesado y adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Que RIOS CONSULTORES S.L. garantiza que ha implementado políticas técnicas y organizativas apropiadas para aplicar las medidas de seguridad que establece el artículo 32 del GDPR con el fin de proteger los derechos y libertades de los interesados, y les ha comunicado la información adecuada para que puedan ejercerlos.

MALAGA, 22/10/2020

Por RIOS CONSULTORES S.L.,

JOSE MARIA PLATA ZAFRA

CERTIFICADO DE GARANTÍA DE CUMPLIMIENTO DEL GDPR Y LOPDGDD

JOSE MARIA PLATA ZAFRA, con NIF 25715073S, en nombre propio y domicilio social situado en JUAN PORRAS, 7 - 29003 MALAGA (Málaga),

CERTIFICA

Que de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), RIOS CONSULTORES S.L. está cumpliendo con todas las disposiciones de las normativas GDPR para el tratamiento de los datos personales de su responsabilidad, y manifiestamente con los principios descritos en el artículo 5 del GDPR, por los cuales son tratados de manera lícita, leal y transparente en relación con el interesado y adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Que RIOS CONSULTORES S.L. garantiza que ha implementado políticas técnicas y organizativas apropiadas para aplicar las medidas de seguridad que establece el GDPR con el fin de proteger los derechos y libertades de los interesados, y les ha comunicado la información adecuada para que puedan ejercerlos.

MALAGA, 22/10/2020

JOSE MARIA PLATA ZAFRA