

Condiciones de Reserva y Anulación y Política de Privacidad

Reserva de animación infantil para comuniones y bodas 2020

Contratación y normas.

Pago y anulación de reserva.

En el momento de la reserva tendrá que hacer un pago del 100€ sobre el total de la actividad contratada, pudiéndose realizar por transferencia bancaria. El importe restante puede abonarlo igualmente por transferencia bancaria durante la semana del evento o en metálico el mismo día del evento a los animadores.

Condiciones de Anulación y/o Modificación:

Devolución del 100 % de la paga y señal, menos 3,00€ en concepto de gastos de gestión y cancelación, cuando la anulación de la reserva se haga con más de 45 días de antelación de la fecha prevista del evento.

Pérdida del 100 % de la paga y señal cuando la anulación se efectúe con menos de 45 días de antelación. La devolución de anticipo en caso de anulación se realizará en un plazo máximo de 30 días desde la solicitud de cancelación.

Modificaciones de los servicios contratados:

Las reservas podrán ser modificadas en número de animadores contratados, hasta 48 horas antes de la celebración del evento, ya que las listas de confirmación de invitados pueden variar con respecto a la previsión inicial de la familia.

La modificación de la reserva de los siguientes servicios: Atracción hinchable, Show de magia, Científico Loco, DJ y catering infantil, deben ser notificadas con más de 45 días ya que son elementos que se contratan con mucha antelación, la anulación o modificación de estos servicios supone la pérdida de la señal entregada previamente.

En caso de lluvia

Tenemos las siguientes opciones:

- Anulación del servicio y devolución de la señal (si así se decide 24 horas antes de la celebración del evento.
- Mantenemos el servicio contratado y se realiza la actividad aprovechando los intervalos en los que no llueva (atendiendo a la previsión de lluvias de AEMET)
- Cambiar el servicio por otro de nuestro catálogo que esté disponible.

POLITICA DE PRIVACIDAD.

1.- INFORMACIÓN BASICA SOBRE PROTECCION DE DATOS:

En Europa y en España existen normas de protección de datos pensadas para proteger su información personal de obligado cumplimiento para nuestra entidad.

Por ello, es muy importante para nosotros que entienda perfectamente qué vamos a hacer con los datos personales que le pedimos.

Así, seremos transparentes y le daremos el control de sus datos, con un lenguaje sencillo y opciones claras que le permitirán decidir qué haremos con su información personal.

Por favor, si una vez leída la presente información le queda alguna duda, no dude en preguntarnos.

¿Para qué vamos a usar sus datos?

Con carácter general, sus datos personales serán usados para poder relacionarnos con usted, poder prestarle nuestros servicios y atender las solicitudes que nos ha realizado por medio de los formularios de nuestra web, redes sociales o por teléfono.

Asimismo, también pueden ser usados para otras actividades, como enviarle publicidad o promocionar nuestras actividades, en estas situaciones necesitaremos su permiso previo. Para ello, pondremos a su disposición una serie de casillas que le permitirán decidir de manera clara y sencilla sobre el uso de su información personal.

TRATAMIENTO DE DATOS DE CLIENTES

Clausula informativa:

Responsable: Identidad: JESÚS MORILLO MORALES (PUCHI ANIMACIÓN) - NIF: 28758578E Dir. postal: Calle Andrés Segovia 10 4ªA, 41008, Sevilla Teléfono: 666326058 Correo elect: puchi.animacion@gmail.com

“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 JESÚS MORILLO MORALES (PUCHI ANIMACIÓN) 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 solicitamos su autorización para ofrecerle productos y servicios relacionados con los solicitados y fidelizarle como cliente.” En caso contrario podrá notificarlo tanto por teléfono al 666326058, como al correo electrónico puchi.animación@gmail.com

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: JESÚS MORILLO MORALES (PUCHI ANIMACIÓN) - NIF: 28758578E Dir. postal: Calle Andrés Segovia 10, 41008, Sevilla Teléfono: 666326058 Correo elect: puchi.animacion@gmail.com

“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.

EMPRESAS DE SERVICIOS

Contratos:

AVISO: En su contrato con la empresa que le presta el servicio deberá incluir las si-guientes cláusulas contractuales:

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a Espacio Web ISP Services S.L., como encargado del tratamiento, para tratar por cuenta de JESÚS MORILLO MORALES (PUCHI ANIMACIÓN), 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 Hosting y proveedor de correo electrónico.

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad JESÚS MORILLO MORALES (PUCHI ANIMACIÓN) como responsable del tratamiento, pone a disposición de la entidad Espacio Web ISP Services 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 1 año , 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.

AVISO: No olvide firmar la última hoja de cada uno de los contratos que se han obtenido.

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

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: 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. Formación

De identificación: nombre, apellidos, número de Seguridad Social, 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:

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

Datos académicos

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

ANEXO MEDIDAS DE SEGURIDAD

INFORMACIÓN DE INTERÉS GENERAL

Este documento ha sido diseñado para tratamientos de datos personales de bajo riesgo de donde se deduce que el mismo no podrá ser utilizado para tratamientos de datos personales

que incluyan datos personales relativos al origen étnico o racial, ideología política religiosa o filosófica, filiación sindical, datos genéticos y biométricos, datos de salud, y datos de orientación sexual de las personas así como cualquier otro tratamiento de datos que entrañe alto riesgo para los derechos y libertades de las personas.

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 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

o Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los datos personales expuestos a 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.

o Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.

o No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.

o 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.

o 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:

o 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, oposición y portabilidad. 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.

Para el derecho de portabilidad los interesados deberán comunicar su decisión e informar al responsable, en su caso, sobre la identidad del nuevo responsable al que facilitar sus datos personales.

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

o 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)

- o **UBICACIÓN DE LAS CÁMARAS:** Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores.
- o **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.
- o **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.
- o **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.
- o **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.
- o **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.aepd.es.

MEDIDAS TÉCNICAS

IDENTIFICACIÓN

- o 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.
- o 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.

- o 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.
- o 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).
- o 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:

- o **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 medida posible.
- o **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.
- o **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.
- o **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.
- o **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.

Si desea más información u orientaciones técnicas para garantizar la seguridad de los datos personales y la información que trata su empresa, el Instituto Nacional de Ciberseguridad (INCIBE) en su página web www.incibe.es, pone a su disposición herramientas con enfoque empresarial en su sección «Protege tu empresa» donde, entre otros servicios, dispone de:

- un apartado de formación con un videojuego, retos para respuesta a incidentes y videos interactivos de formación sectorial,
- un Kit de concienciación para empleados,
- diversas herramientas para ayudar a la empresa a mejorar su ciberseguridad, entre ellas políticas para el empresario, el personal técnico y el empleado, un catálogo de empresas y soluciones de seguridad y una herramienta de análisis de riesgos.
- dossieres temáticos complementados con videos e infografías y otros recursos,
- guías para el empresario,

Además INCIBE, a través de la Oficina de Seguridad del Internauta, pone también a su disposición herramientas informáticas gratuitas e información adicional pueden ser de utilidad para su empresa o su actividad profesional.